

Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Dirección General de Estudios de Posgrado

Facultad de Ingeniería de Sistemas e Informática

Unidad de Posgrado

Modelo de auditoría de seguridad VoIP

TESIS

Para optar el Grado Académico de Doctor en Ingeniería de

Sistemas e Informática

AUTOR

Oscar Danilo GAVILANEZ ALVAREZ

ASESOR

Dr. Glen Dario RODRIGUEZ RAFAEL

Lima, Perú

2025



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

https://creativecommons.org/licenses/by-nc-sa/4.0/

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Gavilanez, O. (2025). *Modelo de auditoría de seguridad VoIP*. [Tesis de doctorado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Unidad de Posgrado]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Oscar Danilo Gavilanez Alvarez
Tipo de documento de identidad	Cédula de identidad
Número de documento de identidad	EC / 0602764748
URL de ORCID	https://orcid.org/0000-0002-7245-5640
Datos de asesor	
Nombres y apellidos	Glen Dario Rodriguez Rafael
Tipo de documento de identidad	DNI
Número de documento de identidad	10062042
URL de ORCID	https://orcid.org/0000-0002-4471-3198
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Luz Sussy Bayona Oré
Tipo de documento	DNI
Número de documento de identidad	08602165
Miembro del jurado 1	
Nombres y apellidos	Ivan Carlo Petrlik Azabache
Tipo de documento	DNI
Número de documento de identidad	10140461
Miembro del jurado 2	
Nombres y apellidos	Igor Jovino Aguilar Alonso
Tipo de documento	DNI
Número de documento de identidad	32931485
Datos de investigación	
Línea de investigación	Tecnologías de la Información

Grupo de investigación	No aplica
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Ecuador Provincia: Chimborazo Ciudad: Riobamba Latitud: -1.67435 Longitud: -78.6483
Año o rango de años en que se realizó la investigación	2018 - 2025
URL de disciplinas OCDE	Informática y Ciencias de la Información https://purl.org/pe-repo/ocde/ford#1.02.00 Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04 Ciencias de la Computación https://purl.org/pe-repo/ocde/ford#1.02.01

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Vicedecanato de Investigación y Posgrado
Unidad de Posgrado

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL GRADO ACADÉMICO DE DOCTOR EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

A los un (01) días del mes de octubre de 2025, siendo las 10:00 a.m., se reunieron en el Auditorio Alfredo Celso Alva Bravo, el Jurado de Tesis conformado por los siguientes docentes:

Dra. Luz Sussy Bayona Oré (Presidente)
Dr. Ivan Carlo Petrlik Azabache (Miembro)
Dr. Igor Jovino Aguilar Alonso (Miembro)
Dr. Glen Dario Rodriguez Rafael (Miembro Asesor)

Se inició la Sustentación invitando al candidato a Doctor ***OSCAR DANILO GAVILANEZ ALVAREZ,*** *para que realice la exposición oral de la tesis para optar el Grado Académico de Doctor en Ingeniería de Sistemas e Informática, siendo la Tesis intitulada:*

"Modelo de auditoría de seguridad VoIP".

Concluida la exposición, los miembros del Jurado de Tesis procedieron a formular sus preguntas que fueron absueltas por el graduando; acto seguido se procedió a la evaluación correspondiente, habiendo obtenido la siguiente calificación:

…… Dieciséis …… (16) …… Bueno ……

Por tanto, el presidente del Jurado, de acuerdo con el Reglamento General de Estudios de Posgrado, otorga al Magíster ***OSCAR DANILO GAVILANEZ ALVAREZ*** *el Grado Académico de Doctor en Ingeniería de Sistemas e Informática.*

Siendo las 12:19 *horas, el presidente del Jurado de Tesis, da por concluido el acto académico de Sustentación de Tesis.*

Dra. Luz Sussy Bayona Oré
(Presidente)

Dr. Ivan Carlo Petrlik Azabache
(Miembro)

Dr. Igor Jovino Aguilar Alonso
(Miembro)

Dr. Glen Dario Rodriguez Rafael
(Miembro Asesor)

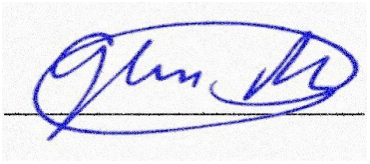
UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

CERTIFICADO DE SIMILITUD

Yo, Glen Darío Rodríguez Rafael en mi condición de asesor acreditado con Dictamen N° 185-UPG-FISI-2018 de la tesis, cuyo título es Modelo de auditoría de seguridad VOIP, presentado por el magíster Oscar Danilo Gavilanez Alvarez para optar el grado Académico de Doctor en Ingeniería de Sistemas e Informática, CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 7% de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional.**

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del grado Académico de Doctor en Ingeniería de Sistemas e Informática.

Lima, 7 de enero de 2025



Firma del Asesor

Nombres y Apellidos del asesor: Glen Darío Rodríguez Rafael

DNI: 10062042

DEDICATORIA

A mis padres, Angel Gustavo (+) y Luz Margarita
El Angel y la Luz de mi vida

Oscar Danilo Gavilanez Alvarez

AGRADECIMIENTO

A la Universidad Nacional Mayor de San Marcos por brindarme la oportunidad y el apoyo necesario para llevar a cabo mis estudios de doctorado. A lo largo de este proceso, la institución ha sido un pilar fundamental, proporcionando los recursos y el entorno académico idóneo para desarrollar mi investigación.

A mi tutor, Dr. Glen Dario Rodriguez Rafael, por su valiosa guía, dedicación y paciencia. Su experiencia, consejos y constante acompañamiento han sido determinantes en cada etapa de la tesis. Su compromiso con mi formación y su disposición para orientarme y motivarme han sido esenciales para lograr este objetivo.

Oscar Danilo Gavilanez Alvarez

ÍNDICE GENERAL

CAPÍTULO 1: INTRODUCCIÓN 1
1.1. Situación Problemática 1
1.2. Formulación del Problema 6
1.2.1. Problema general 7
1.2.2. Problemas específicos 7
1.3. Motivación 8
1.4. Justificación de la investigación 9
1.4.1. Justificación teórica 9
1.4.2. Justificación práctica 14
1.5. Preguntas de investigación 15
1.6. Objetivos de la investigación 16
1.6.1. Objetivo general 16
1.6.2. Objetivos específicos 17
1.7. Organización de la tesis 17
CAPÍTULO 2: MARCO TEÓRICO 20
2.1. Marco epistemológico de la investigación 20
2.2. Bases teóricas 25
2.2.1. Introducción a VoIP 25
2.2.2. Protocolos técnicos de comunicación VoIP 27
2.2.3. Problemas de seguridad en sistemas VoIP 31
2.2.4. Auditoría TI 46
2.2.5. Auditorías de seguridad TI 48
2.2.6. Marcos de trabajo 49
2.2.7. COBIT 4.1 como modelo de madurez y evaluación 60
2.2.8. Requerimientos de Seguridad VoIP 63
2.3. Estado del arte 65
2.3.1. Protocolo de revisión del estado del arte 65
2.3.2. Antecedentes de investigación 67
2.3.3. Investigaciones sobre requerimientos específicos de seguridad en sistemas VoIP 71
2.3.4. Evaluación de frameworks de seguridad y su alineación con requerimientos VoIP 80

2.3.5. Estudios sobre cultura de seguridad y tratamiento de la ingeniería social en VoIP 91
2.3.6. Estudios sobre procedimientos de auditoría en entornos VoIP 94
2.4. Variables de Investigación 96
2.4.1. Variables pregunta general de investigación 96
2.4.2. Variables pregunta secundaria de investigación 1 98
2.4.3. Variables pregunta secundaria de investigación 2 99
2.4.4. Variables pregunta secundaria de investigación 3 101
2.4.5. Variables pregunta secundaria de investigación 4 103
CAPÍTULO 3: METODOLOGÍA 105
3.1. Enfoque metodológico general 105
3.2. Diseño metodológico 105
3.3. Población y muestra 106
3.4. Hipótesis 108
3.4.1. Hipótesis Principal 108
3.4.2. Hipótesis Secundarias 109
3.5. Métodos de Investigación 111
3.6. Técnicas e instrumentos de recolección y análisis de datos 112
3.7. Matriz de consistencia 113
3.8. Operacionalización de variables 113
CAPÍTULO 4: MODELO DE AUDITORÍA DE SEGURIDAD VoIP PROPUESTO 114
4.1. Fundamentación del modelo propuesto 114
4.1.1. Antecedentes 115
4.1.2. Fundamentación de la selección de COBIT 4.1 frente a versiones posteriores 117
4.2. Descripción general del modelo VoIPSAM 118
4.3. Validación del modelo propuesto VoIPSAM 121
4.4. Componentes del modelo VoIPSAM 130
4.4.1. Dominio A. Planear y Organizar 133
4.4.2. Dominio B. Adquirir e Implementar 140
4.4.3. Dominio C. Entrega y Soporte 145
4.4.4. Dominio D. Monitorear y Evaluar 152
4.5. Plan de cultura de seguridad para VoIP 158
4.5.1. Concienciación y formación (PA41) 159

4.5.2. Políticas y procedimientos (PA42) 161
4.5.3. Fomento de una cultura de seguridad (PA43) 162
4.5.4. Actualización y evaluación continua (PD51) 165
4.5.5. Implementación de herramientas de seguridad (PD52) 166
4.5.6. Responsabilidad y reporte (PD53) 168
4.6. Guía de auditoría de seguridad VoIPSAM 170
4.6.1. Referencia 170
4.6.2. Documentos guías de auditoría 175
4.6.3. PT. Papeles de trabajo 187
4.7. Relación integral de los componentes del modelo VoIPSAM 190
4.8. Aplicación práctica del modelo. Estudio de caso 192
4.8.1. Introducción 192
4.8.2. Metodología 193
4.8.3. Perfiles de expertos 194
4.8.4. Resultados 197
CAPÍTULO 5: RESULTADOS Y DISCUSIÓN 198
5.1. Presentación de resultados 199
5.1.1. Resultados de la aplicación del modelo tradicional COBIT 4.1 199
5.1.2. Resultados de la aplicación del modelo propuesto VoIPSAM 200
5.1.3. Resultados de encuestas a expertos sobre los modelos de auditoría 202
5.2. Validación del estudio de caso 203
5.2.1. Fiabilidad de la encuesta 204
5.2.2. Análisis de diferencias de Medias 206
5.2.3. Prueba t para comparación entre modelos 206
5.2.4. Validación externa de los resultados del estudio de caso 207
5.3. Validación de las hipótesis secundarias 215
5.3.1. Validación de la hipótesis secundaria HS1 215
5.3.2. Validación de la hipótesis secundaria HS2 219
5.3.3. Validación de la hipótesis secundaria HS3 221
5.3.4. Validación de la hipótesis secundaria HS4 223
5.4. Validación de la Hipótesis Principal HP 225
5.5. Comparación de resultados y evaluación de madurez 229

5.6. Discusión general de resultados 232
CONCLUSIONES 234
RECOMENDACIONES 236
BIBLIOGRAFÍA 238
ANEXOS 253

LISTA DE TABLAS

Tabla 1. **Marco epistemológico de la investigación.** 22
Tabla 2. **Registro de búsqueda de información para el marco epistemológico.** 23
Tabla 3. **Tipos de problemas de seguridad.** 31
Tabla 4. **Análisis comparativo de los marcos de gobernanza de TI.** 60
Tabla 5. **Evidencia en la literatura que considera a COBIT 4.1 como modelo.** 62
Tabla 6. **Requerimientos básicos de seguridad para sistemas VoIP.** 75
Tabla 7. **Seguridad de la red.** 76
Tabla 8. **Interfaces.** 76
Tabla 9. **Seguridad de datos.** 77
Tabla 10. **Virtualización.** 77
Tabla 11. **Gobernanza.** 78
Tabla 12. **Cumplimiento.** 78
Tabla 13. **Asuntos legales.** 79
Tabla 14. **Ingeniería social.** 80
Tabla 15. **Limitaciones de frameworks y estándares.** 83
Tabla 16. **Requerimientos y necesidades de gestión en VoIP vs USGCB.** 84
Tabla 17. **Requerimientos y necesidades de gestión en VoIP vs NIST 800-53.** 85
Tabla 18. **Requerimientos y necesidades de gestión en VoIP vs GLBA.** 85
Tabla 19. **Requerimientos y necesidades de gestión en VOIP vs ISO 27000.** 86
Tabla 20. **Requerimientos y necesidades de gestión en VOIP vs NERC CIP.** 86
Tabla 21. **Requerimientos y necesidades de gestión en VoIP vs COBIT.** 87
Tabla 22. **Criterios de Gestión VoIP frente a COBIT.** 87
Tabla 23. **Frameworks de seguridad aplicables a la auditoría de sistemas VoIP.** 89
Tabla 24. **Comparación estratégica de frameworks de seguridad y auditoría.** 90
Tabla 25. **Escala de Rensis Likert.** 123
Tabla 26. **Grupos Encuesta A1. Ingeniería Social - VoIPSAM.** 123
Tabla 27. **Grupos Encuesta B1. Modelo de auditoría de seguridad VoIPSAM.** 124
Tabla 28. **Fiabilidad de George y Mallery.** 126
Tabla 29. **Estadísticas de fiabilidad Alfa de Cronbach.** 126
Tabla 30. **Media Estadística de elemento.** 127
Tabla 31. **PGA-1 Plan General de Auditoría VoIPSAM.** 176
Tabla 32. **GA-1. Planificación y alcance de la auditoría.** 177
Tabla 33. **GA-2. Pasos preparatorios.** 178
Tabla 34. **GA-3. Gobernanza.** 179
Tabla 35. **GA-4. Configuración de servidores.** 180
Tabla 36. **GA-5. Red.** 180
Tabla 37. **GA-6. Planificación de contingencias.** 181
Tabla 38. **GA-7. Cultura de seguridad.** 182
Tabla 39. **Nivel de madurez – Estado.** 183
Tabla 40. **Ponderación por área clave.** 184

Tabla 41. **Porcentaje de cumplimiento por nivel de madurez.** 185
Tabla 42**. GA-8. Evaluación de madurez.**..... 187
Tabla 43. **Papel de trabajo de la guía de auditoría.** 188
Tabla 44**. Resultados de los procedimientos evaluados – cumplimiento. COBIT 4.1.** 200
Tabla 45. **Resultados de los procedimientos evaluados – cumplimiento. VoIPSAM.**..... 201
Tabla 46. **Resultados de la aplicación de la encuesta B2CE.**..... 202
Tabla 47. **Resultados de la aplicación de la encuesta B2CE.**..... 204
Tabla 48. **Resultados del alfa de Cronbach por sección.** 205
Tabla 49. **Media por sección.**..... 206
Tabla 50. **Comparación entre modelos. Resultados del valor t y del valor p.**..... 207
Tabla 51. **Perfil expertos. Validación externa de los resultados del estudio de caso** 209
Tabla 52. **Resultados de la validación externa del estudio de caso** 212
Tabla 53. **Resultados de los procedimientos evaluados COBIT 4.1 y VoIPSAM.** 217
Tabla 54. **Validación de la hipótesis general.** 228

LISTA DE FIGURAS

Figura 1. **Tipos de ataques de engaño social en línea.** 10
Figura 2. **Protocolos de VoIP con sesión y medios de tráfico**. 29
Figura 3. **Enumeración de nombres de usuario SIP mediante Wireshark.** 34
Figura 4. **Esquema del ataque Hombre en el medio.** 35
Figura 5. **Ataque de suplantación ARP**. 37
Figura 6. **Ataque de descifrado de contraseñas SIP utilizando el sniffer Cain & Abel.** 38
Figura 7. **Ataque DoS generado por inundación de mensajes.** 39
Figura 8. **Metodología de auditoría basada en minería de procesos.** 48
Figura 9. **Framework Calder-Moir para Gobernanza de TI.** 51
Figura 10. **Dominios del framework COBIT 4.1.** 56
Figura 11. **Dominios VoIPSAM.** 120
Figura 12. **Procesos asociados a los dominios VoIPSAM.** 131
Figura 13. **Procesos asociados al Dominio A. Planear y Organizar.** 134
Figura 14. **Procesos asociados al Dominio B. Adquirir e Implementar** 141
Figura 15. **Procesos asociados al Dominio C. Entrega y Soporte.** 145
Figura 16. **Procesos asociados al Dominio D. Monitorear y Evaluar.** 153

LISTA DE ANEXOS

Anexo A. Matriz de Consistencia 253
Anexo B. Operacionalización de Variables 258
Anexo C. Encuesta A1. Aspectos Ingeniería Social (Modelo Auditoría de Seguridad VoIP) 264
Anexo D. Encuesta B1. Modelo de auditoría de seguridad VoIP 272
Anexo E. Guías de auditoría VoIPSAM 289
Anexo F. Solicitud y aprobación de aplicación del modelo VoIPSAM 338
Anexo G. Encuesta B2CE. Auditoría de Seguridad VoIP (estudio de caso) 345
Anexo H. Resultados de auditorías aplicadas 356
Anexo I. Alfa de Cronbach global y por sección obtenidos mediante SPSS 360
Anexo J. Prueba T Estudio de caso 376
Anexo K. Prueba t - HS1 386
Anexo L. Prueba t – HS3 388
Anexo M. Eficiencia Shapiro-Wilk - Prueba t 391
Anexo N. Artículos Publicados 401
Anexo O. Encuesta de validación externa EVE. Estudio de caso 408

ACRÓNIMOS Y ABREVIATURAS

ARP: Address Resolution Protocol (Protocolo de Resolución de Direcciones)

COBIT: Control Objectives for Information and Related Technologies (Objetivos de Control para Información y Tecnologías Relacionadas)

COSO: Committee of Sponsoring Organizations (Comité de Organizaciones Patrocinadoras)

DHCP: Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host)

DNS: Domain Name System (Sistema de Nombres de Dominio)

DoS: Denial of Service (Denegación de Servicio)

GLBA: Gramm-Leach-Bliley Act (Ley de Privacidad Financiera)

HTTP: Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto)

IAX: Inter-Asterisk eXchange (Intercambio entre Asterisk)

IETF: Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet)

IP: Internet Protocol (Protocolo de Internet)

ISO: International Organization for Standardization (Organización Internacional de Normalización)

ISO/IEC: International Organization for Standardization / International Electrotechnical Commission (Organización Internacional de Normalización / Comisión Electrotécnica Internacional)

ITGI: IT Governance Institute (Instituto de Gobernanza de TI)

ITIL: Information Technology Infrastructure Library (Biblioteca de Infraestructura de Tecnologías de la Información)

LAN: Local Area Network (Red de Área Local)

MAC: Media Access Control (Control de Acceso al Medio)

NGN: Next Generation Network (Red de Próxima Generación)

NIST: National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología)

PCI DSS: Payment Card Industry Data Security Standard (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago)

PSTN: Public Switched Telephone Network (Red Telefónica Pública Conmutada)

QoS: Quality of Service (Calidad de Servicio)

RFC: Request for Comments (Solicitud de Comentarios)

RTP: Real-Time Transport Protocol (Protocolo de Transporte en Tiempo Real)

SCTP: Stream Control Transmission Protocol (Protocolo de Control de Transmisión por Secuencias)

SDP: Session Description Protocol (Protocolo de Descripción de Sesión)

SIP: Session Initiation Protocol (Protocolo de Inicio de Sesión)

SPIT: Spam over Internet Telephony (Correo No Deseado sobre Telefonía por Internet)

SPSS: Statistical Package for the Social Sciences (Paquete Estadístico para Ciencias Sociales)

SRTP: Secure Real-Time Transport Protocol (Protocolo de Transporte en Tiempo Real Seguro)

TCP: Transmission Control Protocol (Protocolo de Control de Transmisión)

TLS: Transport Layer Security (Seguridad de la Capa de Transporte)

TI: Tecnologías de la Información

UDP: User Datagram Protocol (Protocolo de Datagrama de Usuario)

UA: User Agent (Agente de Usuario)

VoIP: Voice over Internet Protocol (Voz sobre Protocolo de Internet)

VoIPSAM: Voice over IP Security Audit Model (Modelo de Auditoría de Seguridad para VoIP)

ZRTP: Z Real-Time Transport Protocol (Protocolo Z de Transporte en Tiempo Real)

RESUMEN

La presente investigación se centró en el desarrollo de un modelo de auditoría de seguridad específico para sistemas VoIP, que integra el tratamiento de la ingeniería social mediante un plan de cultura de seguridad. El objetivo general consistió en implementar un modelo de auditoría de seguridad específico para sistemas VoIP que mejore la eficiencia temporal durante la ejecución de auditorías frente a los modelos tradicionales. Durante el estudio se identificaron requerimientos particulares de seguridad para entornos VoIP, se diseñaron componentes orientados a incrementar la relevancia de las evaluaciones, y se incorporó un plan estratégico de cultura de seguridad enfocado en reducir riesgos asociados al factor humano. Asimismo, se elaboró una guía metodológica que formaliza un procedimiento especializado para la auditoría de estos sistemas. La propuesta, denominada VoIPSAM, fue evaluada en un entorno real, permitiendo evidenciar mejoras significativas en eficiencia y cobertura, cumpliendo así con el objetivo planteado. La metodología adoptó un enfoque cuantitativo, con diseño comparativo, descriptivo y estudio de caso. Se contrastó el modelo propuesto con un modelo de auditoría tradicional, mediante cronometraje de auditorías, encuestas estructuradas a expertos y análisis estadístico. Los resultados demostraron una reducción de 1430 minutos en el tiempo total de auditoría, un mayor porcentaje de cumplimiento (34,97 % frente a 16,92 %), y una cobertura superior en procedimientos e ítems evaluados. Las hipótesis planteadas fueron validadas estadísticamente, evidenciando mejoras en eficiencia, relevancia de componentes y disminución de vulnerabilidades humanas. Además, se observó un avance en el nivel de madurez de los procesos evaluados. Como conclusión, se presenta una propuesta integral, técnicamente sólida y contextualizada, que aporta valor tanto académico como práctico al campo de la auditoría de seguridad VoIP, ofreciendo una solución adaptable y eficaz frente a desafíos emergentes en estos entornos tecnológicos.

PALABRAS CLAVE: Auditoría de seguridad, seguridad VoIP, plan de cultura de seguridad, ingeniería social, modelo VoIPSAM, eficiencia temporal.

ABSTRACT

This research focused on the development of a security audit model specifically designed for VoIP systems, integrating the treatment of social engineering through a security culture plan. The general objective was to implement a model that improves time efficiency in the execution of audits compared to traditional approaches. The study identified specific security requirements for VoIP environments, designed components aimed at increasing the relevance of evaluations, and incorporated a strategic culture plan to reduce risks associated with the human factor. In addition, a methodological guide was developed to formalize a specialized auditing procedure for these systems. The proposed model, named VoIPSAM, was evaluated in a real-world setting, demonstrating significant improvements in efficiency and coverage, thereby fulfilling the stated objective. The methodology adopted a quantitative approach, with a comparative, descriptive, and case study design. The proposed model was contrasted with a traditional audit framework through time-tracking of audit processes, expert surveys, and statistical analysis. The results revealed a reduction of 1,430 minutes in total audit time, a higher compliance rate (34.97% compared to 16.92%), and greater coverage in terms of procedures and items evaluated. The hypotheses were statistically validated, showing improvements in efficiency, the relevance of components, and a reduction in human-related vulnerabilities. Additionally, progress was observed in the maturity level of the processes assessed. In conclusion, this study presents an integrated, technically robust, and context-aware proposal that contributes both academically and practically to the field of VoIP security auditing. The solution offers adaptability and effectiveness in addressing emerging challenges in these technological environments.

KEYWORDS: Security audit, VoIP security, security culture plan, social engineering, VoIPSAM model, time efficiency.

CAPÍTULO 1: INTRODUCCIÓN

1.1. Situación Problemática

La tecnología de Voz sobre Protocolo de Internet (VoIP) se basa en el uso del Protocolo de Internet (IP) para ofrecer servicios de telefonía, brindando ventajas como cuotas mensuales reducidas y tarifas más accesibles para llamadas internacionales y de larga distancia. A pesar de estos beneficios, VoIP conlleva ciertas vulnerabilidades de seguridad que pueden ser aprovechadas por delincuentes para llevar a cabo actividades ilegales. Por ello, resulta fundamental implementar políticas de administración y gestión eficaces que faciliten la evaluación del estado actual de un sistema VoIP.

Las redes telefónicas conmutadas siguen siendo una infraestructura fundamental, y los avances tecnológicos recientes han permitido integrar sistemas modernos y de bajo costo que utilizan internet para realizar llamadas a través de VoIP. Sin embargo, esta evolución también ha dado lugar a un incremento en la cantidad y complejidad de los fraudes cometidos por delincuentes. En particular, la llegada de VoIP ha facilitado que los atacantes adapten herramientas propias del cibercrimen, como las botnets, para ejecutar ataques más sofisticados y difíciles de detectar. Por ejemplo, mediante el uso de bots, los delincuentes pueden realizar llamadas automáticas a múltiples números de forma simultánea con el propósito de establecer contacto con usuarios activos y manipularlos para que ejecuten la acción esperada, convirtiéndolos así en víctima de un fraude. El trabajo desarrollado demuestra que los ataques de VoIP constituyen una amenaza que sustenta parte del ecosistema de llamadas maliciosas (Carrillo et al., 2022).

Actualmente, realizar llamadas a través de tecnología VoIP se ha vuelto una práctica común. Sin embargo, la falta de configuraciones seguras en los teléfonos VoIP los hace vulnerables a diversos ataques que pueden ser ejecutados utilizando herramientas gratuitas como Nmap, Ettercap, Wireshark y programación en Python. Entre las amenazas destaca la serie de ataques conocidos como Phonejack, los cuales incluyen denegación de servicio (DoS) y violaciones de datos personales, simplificando y adaptando técnicas tradicionales de ataque a entornos VoIP. Estos ataques se desarrollan dentro de un modelo de amenaza bien definido, donde los ciberdelincuentes buscan el uso ilegítimo de sistemas, recursos o servicios. Dentro de las acciones maliciosas más relevantes se encuentran la interceptación de comunicaciones (eavesdropping), los ataques DoS y las amenazas a la privacidad, enfocadas en acceder, divulgar o destruir información personal. Cabe destacar que estas amenazas pueden originarse tanto desde el interior como desde el exterior de la red, lo que incrementa el riesgo y la complejidad de proteger los entornos VoIP (Bella et al., 2022).

La seguridad en una red VoIP requiere la integración de prácticas y políticas de gestión, enfocadas en una infraestructura protegida mediante VLANs, firewalls y cifrado. La implementación de estándares y mejores prácticas es fundamental para asegurar los teléfonos VoIP desde su instalación. Además, es necesario el tratamiento de vulnerabilidades y amenazas emergentes, adoptando medidas preventivas tanto en el núcleo como en el perímetro de la red.

La tecnología VoIP desempeña un papel fundamental en los sistemas de comunicación en red, donde la seguridad es un aspecto esencial. Estos sistemas enfrentan diversos riesgos, como los ataques DoS, en los cuales un atacante satura la red con tráfico malicioso, interrumpiendo las comunicaciones de los usuarios. Para proteger VoIP, es crucial identificar vulnerabilidades que puedan derivar en amenazas y problemas de seguridad (Khan et al., 2021).

El fraude en VoIP se basa en el acceso no autorizado a una red VoIP para realizar llamadas sin permiso, generalmente internacionales o de larga distancia. Los delincuentes

suelen aprovechar contraseñas débiles, gateways abiertos y otras vulnerabilidades a nivel de aplicación. Este fraude es uno de los ataques más frecuentes contra la tecnología VoIP.

Según Schmitt (2022) las ciberamenazas representan un desafío permanente en el mundo altamente interconectado de hoy. El Foro Económico Mundial las reconoce como uno de los principales riesgos de seguridad a nivel global. Los ataques dirigidos a dispositivos móviles continúan incrementándose cada año, tanto en volumen como en impacto, generando consecuencias significativas. Estas amenazas pueden clasificarse en diversas categorías, como malware, phishing, vulnerabilidades en la comunicación, ataques a la cadena de suministro, intrusiones físicas y fallos en los mecanismos de autenticación.

Laurens et al. (2022) sostienen que mediante la detección de actividad de voz (VAD) en sistemas VoIP, un atacante puede reconocer patrones en las respuestas automatizadas de los servicios de atención al cliente, lo que le permitiría elaborar perfiles y, en consecuencia, poner en riesgo la seguridad de dichas comunicaciones.

Las redes VoIP presentan vulnerabilidades frente a los ataques de suplantación de identidad del identificador de llamadas debido a la estructura abierta de la señalización del Protocolo de Inicio de Sesión (SIP). Este tipo de suplantación supone una grave amenaza para la seguridad de los sistemas de telecomunicaciones actuales, ya que permite a los atacantes fingir ser usuarios legítimos y obtener información confidencial. A pesar de que estos ataques impactan especialmente a los sectores de telecomunicaciones y financiero, las soluciones disponibles son limitadas y solo se aplican en entornos cerrados entre usuarios del mismo proveedor de servicios (Tas & Baktir, 2024).

Desde la expansión de Internet, la tecnología VoIP ha crecido de manera notable, impulsada principalmente por su bajo costo y facilidad de implementación. El aumento en la dependencia de VoIP como medio de comunicación resalta la urgente necesidad de fortalecer los mecanismos de seguridad. Aunque existen protocolos diseñados para proteger estas redes, VoIP sigue enfrentando serios desafíos relacionados con la

integridad, autenticidad y confidencialidad de la información. Las soluciones actuales no siempre resultan efectivas ni robustas, especialmente en lo que respecta a los procesos de autenticación y acuerdos de claves. Además, presentan limitaciones en eficiencia, escalabilidad y resistencia frente a posibles ataques (Sreenivasulu & Ravikumar, 2025).

VoIP permite la comunicación entre usuarios a través de redes públicas, ofreciendo una infraestructura más económica, flexible, confiable y escalable en comparación con los servicios tradicionales como la Red Telefónica Pública Conmutada (PSTN). Actualmente, es uno de los mecanismos más utilizados para realizar llamadas mediante Internet. No obstante, al tratarse de una tecnología en tiempo real, VoIP está expuesta a importantes riesgos de seguridad, ya que los datos se transmiten a través de la red pública (Internet). Esto convierte la seguridad en un aspecto crítico, ya que cada usuario dentro del sistema puede representar un punto vulnerable. Además, amenazas conocidas en redes públicas, como los ataques Man in the Middle (MitM), generan problemas de fiabilidad y confianza entre las partes que se comunican. La autenticación se vuelve esencial para garantizar comunicaciones seguras en aplicaciones en tiempo real, ya que las vulnerabilidades propias de la red pública afectan directamente la seguridad. A esto se suma la necesidad de fortalecer la privacidad y la fiabilidad en las comunicaciones VoIP, ya que, sin una gestión adecuada, estas podrían verse seriamente comprometidas. Dado que VoIP depende de Internet, las comunicaciones por esta vía estarán expuestas a mayores riesgos si no se diseñan e implementan con el debido cuidado, especialmente considerando que VoIP continúa evolucionando sin contar aún con estándares consolidados (Kara et al., 2023).

Goldstein y Frank (2016) manifiestan que las organizaciones están sometidas a una creciente presión para trabajar de acuerdo con estándares de seguridad utilizados, como la familia de normas de seguridad ISO/IEC 27000. ITIL y COBIT aportan pautas organizativas para la gestión de la seguridad, pero no bastan para diseñar y administrar sistemas de seguridad de TI integrales, pues no afrontan desafíos como la protección de activos corporativos, procesos, tareas y sistemas de información. La creciente integración de tecnologías VoIP en las organizaciones pone en evidencia la importancia de garantizar su seguridad. Los modelos de auditoría de seguridad en la actualidad presentan

limitaciones en cuanto se refiere a la inclusión de aspectos críticos como el tratamiento de amenazas sociales, ingeniería social y un plan de cultura de seguridad.

Las amenazas sociales y la ingeniería social son técnicas cada vez más empleadas por atacantes para comprometer la seguridad de los sistemas VoIP, aprovechando vulnerabilidades humanas que no son específicamente abordadas por los controles técnicos convencionales. Pese a su relevancia, los modelos de auditoría de seguridad tradicionales se enfocan particularmente en aspectos técnicos y generales, sin un tratamiento exhaustivo y específico de amenazas sociales e ingeniería social en el contexto de VoIP, lo cual resulta en evaluaciones de seguridad que pueden dejar a las organizaciones expuestas a riesgos significativos en cuanto a su seguridad. Una cultura de seguridad adecuadamente implementada es esencial para concienciar al personal sobre las amenazas a la seguridad de las comunicaciones VoIP, las organizaciones en la actualidad continúan siendo vulnerables a errores humanos y a una implementación insuficiente de buenas prácticas de seguridad.

Los modelos de auditoría de seguridad tradicionales son generalmente diseñados para una amplia gama de aplicaciones, lo que los hace menos eficientes cuando se aplican a contextos específicos como VoIP, la generalidad de los modelos implica que no pueden abordar de manera óptima las particularidades y los desafíos específicos que presenta la seguridad en sistemas VoIP.

Resulta imprescindible el desarrollo de un modelo de auditoría de seguridad diseñado exclusivamente para VoIP que no solo considere los aspectos técnicos tradicionales, sino que además integre de manera explícita el tratamiento de amenazas sociales e ingeniería social a través de un plan de cultura de seguridad. El modelo sería más eficiente y efectivo, ya que se diseñaría concretamente para abordar los desafíos específicos de la seguridad en VoIP.

1.2. Formulación del Problema

La evolución de las comunicaciones digitales ha impulsado el uso de la tecnología VoIP como una solución eficiente y flexible para la transmisión de voz a través de redes IP. No obstante, esta tecnología presenta vulnerabilidades inherentes debido a su operación en entornos abiertos y a su dependencia de internet, lo que la expone a diversas amenazas de seguridad.

Dentro de estas amenazas, la ingeniería social se ha convertido en un factor de riesgo significativo, ya que explota el factor humano para obtener acceso a sistemas o información sensible, sin necesidad de vulnerar directamente los sistemas técnicos. A pesar de ello, los modelos tradicionales de auditoría de seguridad informática se centran principalmente en aspectos técnicos y no contemplan de manera específica este tipo de amenazas en entornos VoIP.

A pesar de la existencia de modelos y frameworks de auditoría de seguridad ampliamente utilizados en entornos tradicionales de Tecnologías de la Información, estos no abordan de manera específica las particularidades y riesgos inherentes a los sistemas VoIP. Esta limitación genera deficiencias en la eficiencia temporal al momento de realizar auditorías, dificultando la identificación y gestión oportuna de los riesgos y vulnerabilidades propios de esta tecnología.

La ausencia de un modelo de auditoría de seguridad diseñado específicamente para sistemas VoIP repercute directamente en la capacidad de las organizaciones para evaluar de manera efectiva y en menor tiempo su nivel de exposición ante amenazas específicas de este entorno. Esta situación incrementa la posibilidad de que se materialicen incidentes de seguridad que afecten la confidencialidad, integridad y disponibilidad de las comunicaciones VoIP, así como la continuidad de las operaciones de las organizaciones.

En este contexto, resulta necesario desarrollar un modelo de auditoría de seguridad específico para sistemas VoIP que permita mejorar la eficiencia temporal en los procesos de identificación y gestión de riesgos y vulnerabilidades, aportando una herramienta metodológica que responda a las particularidades de esta tecnología y contribuya al fortalecimiento de la seguridad de las comunicaciones en las organizaciones.

1.2.1. Problema general

PG: ¿La ausencia de un modelo de auditoría de seguridad específico para sistemas VoIP limita la eficiencia temporal durante la ejecución de auditorías respecto de los modelos tradicionales?

1.2.2. Problemas específicos

PE1: ¿La insuficiente especificación de los requerimientos de seguridad para sistemas VoIP limita la eficiencia temporal en la ejecución de auditorías de seguridad?

PE2: ¿La ausencia de componentes específicos en los modelos de auditoría tradicionales limita la relevancia de las evaluaciones de seguridad en sistemas VoIP?

PE3: ¿La ausencia de un plan de cultura de seguridad que aborde integralmente la ingeniería social en entornos VoIP incrementa la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano?

PE4: ¿La ausencia de un procedimiento especializado para auditar sistemas VoIP limita la eficiencia temporal en la ejecución de auditorías de seguridad?

1.3. Motivación

La creciente adopción de sistemas de VoIP en entornos corporativos y gubernamentales ha transformado los esquemas tradicionales de comunicación, integrando servicios de voz a infraestructuras de red basadas en protocolos IP. Sin embargo, esta evolución tecnológica también ha incrementado la exposición a amenazas de seguridad que comprometen la confidencialidad, integridad y disponibilidad de las comunicaciones. Ataques como la suplantación de identidad (spoofing), DoS, y la ingeniería social, afectan con frecuencia a este tipo de entornos, debido a sus particularidades técnicas y a la carencia de controles específicos.

En este contexto, surge la necesidad de contar con herramientas metodológicas de auditoría que respondan de forma precisa y especializada a los desafíos inherentes a la seguridad VoIP. Los modelos tradicionales de auditoría, como COBIT 4.1, aunque ampliamente difundidos, no contemplan con suficiente profundidad los riesgos particulares de VoIP, ni integran enfoques orientados al tratamiento de vectores como la ingeniería social, lo que limita su eficacia operativa en la evaluación de estos sistemas.

La presente investigación se motiva en esta brecha teórica y práctica, con el objetivo de implementar un modelo de auditoría de seguridad específico para VoIP, que no solo mejore la eficiencia temporal en la ejecución de auditorías, sino que además incorpore componentes especializados, como un plan de cultura de seguridad, que permita reducir la vulnerabilidad organizacional ante amenazas que explotan el factor humano. Esta propuesta busca aportar al campo de la auditoría de TI desde una perspectiva aplicada, robusta y alineada a las necesidades actuales de protección de infraestructuras de comunicación digital.

1.4. Justificación de la investigación

La presente investigación se justifica por su relevancia tanto en el ámbito académico como en el contexto aplicado. Desde una perspectiva teórica, permite abordar un área especializada de la seguridad en tecnologías de la información, aportando al cuerpo de conocimiento existente sobre auditoría en entornos VoIP. En el plano práctico, la propuesta responde a necesidades concretas de mejora en la eficiencia y especificidad de los procesos de auditoría de seguridad en sistemas de comunicación VoIP. A continuación, se detalla la justificación desde ambos enfoques.

1.4.1. Justificación teórica

La justificación teórica de esta investigación se basa en la necesidad de adaptar los modelos de auditoría de seguridad a las particularidades de VoIP. El desarrollo de VoIP ha traído una gran cantidad de beneficios y servicios satisfactorios a sus usuarios, sin embargo, los servicios VoIP están expuestos a diversas amenazas de seguridad derivadas del Protocolo de Internet, amenazas relacionadas con esta nueva tecnología son entre otras la denegación de servicio, exploits de vulnerabilidad de host y protocolo, vigilancia de las llamadas, secuestro de llamadas, robo de identidad de usuarios, escuchas e inserción, supresión y modificación de flujos de audio; la compleja configuración de la infraestructura de servicios VoIP, servidores DHCP, servidor AAA, routers, SIP register, SIP proxy, servidor DNS, dispositivos de red inalámbricas y por cable complican el proceso de evaluación del sistema VoIP, en este sentido los delincuentes cometen ataques maliciosos a VoIP, consecuencia de aquello la necesidad de un patrón para realizar evaluaciones de dichos sistemas.

De acuerdo con Zhai et al. (2024), SIP ha sido ampliamente utilizado en las comunicaciones multimedia, no obstante, su mecanismo de seguridad sigue siendo vulnerable, lo que genera riesgos como una autenticación de identidad deficiente y la exposición a ataques de fuerza bruta.

En las comunicaciones VoIP, SIP se encarga de establecer y finalizar las sesiones en tiempo real. No obstante, su mecanismo de autenticación presenta vulnerabilidades frente a escuchas ilegales, ataques de fuerza bruta como el robo de contraseñas y suplantación de identidad (spoofing) a nivel de servidor, lo que lo expone a diversos tipos de ataques (Kara et al., 2023).

Tsiatsikas et al. (2013) consideran que el análisis de archivos de registro de gran volumen es por lo general un tanto complejo y lento descuidando la privacidad, sobre todo cuando se trata de VoIP; la literatura sobre cómo las pistas de auditoría pueden ser explotadas para identificar ataques sigue siendo escasa.

Guo et al. (2021) sostienen que según la literatura existen diversos tipos de ataques de engaño social en línea los cuales afectan los objetivos de la seguridad (confidencialidad, integridad y disponibilidad), y alertan sobre la gravedad de los ataques de engaño social en línea como un problema social. La Figura 1 muestra los tipos de ataques de engaño social en línea.

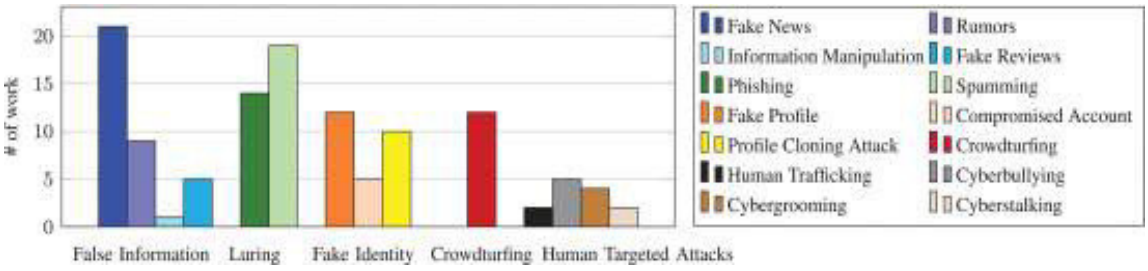


Figura 1. **Tipos de ataques de engaño social en línea.**
Fuente. Guo et al. (2021).

Budiyanto y Gunawan (2023) consideran que actualmente la tecnología VoIP se emplea de forma generalizada en las comunicaciones móviles, pero uno de los mayores desafíos es asegurar que el sistema proteja la confidencialidad de la información y garantice la seguridad de sus usuarios principales.

Hay diversos marcos de trabajo para respaldar la implantación de aspectos del gobierno de TI, cada uno con prioridades específicas que, en gran medida, se complementan. Entre los principales destacan Calder-Moir, ISO 38500 y los propuestos por el IT Governance Institute ITGI, entre ellos COBIT 4.1, Risk IT y ValIT. Los marcos de referencia que brindan herramientas sólidas resultan imprescindibles para alinear los recursos de TI con los objetivos organizativos, garantizando servicios e información que cumplan requisitos de seguridad, finanzas y calidad. Además, existen estándares que sustentan el gobierno de TI y orientan la ejecución de controles específicos, como ISO 20000, ISO 27001, ISO 27002, ITIL, PCI DSS, CMMI, BS 25999 y PMBOK, entre otros. Los marcos Calder-Moir, ISO/IEC 38500 y COBIT comparten la orientación a optimizar inversiones en TI, establecer mejores prácticas de dirección y control, alinear decisiones con objetivos empresariales y priorizar el manejo adecuado de recursos y riesgos. Además, no imponen herramientas específicas, sino que ofrecen un marco de actuación. Los marcos y estándares ITIL, ISO 20000 o ISO 27002 proporcionan lineamientos técnicos para implementar marcos de control como Calder-Moir, ISO/IEC 38500 y COBIT. Asimismo, TOGAF, CMMI y PMBok aportan directrices relevantes en el ámbito del gobierno de TI. Los marcos de referencia ITIL, COBIT, ISO 20000, ISO 27002, TOGAF, CMMI y PMBok pueden combinarse sin excluirse mutuamente, conformando un marco unificado que incluya el tratamiento del control, mejores prácticas y gobierno para la gestión de servicios de TI. El objetivo principal es contar con un modelo integral (Izquierdo, 2009).

Cots et al. (2016) sostienen que el establecimiento de auditorías es un beneficio específico de la gestión de acuerdo con normas y no se puede extender a otros frameworks como ITIL. Vilarinho y da Silva (2011) manifiestan que ITIL se considera un referente de mejores prácticas en la gestión de servicios y goza de amplia adopción en el ámbito empresarial, sin embargo, ITIL presenta lagunas en la especificación de gestión de riesgos.

Los modelos de control de alto nivel tales como COSO, palancas de mando Simons, y los modelos de gobernanza de TI, tales como COBIT, sirven como fuente de inspiración para el diseño de sistemas de control interno. La gestión del riesgo se sugiere a menudo como una técnica para señalar debilidades específicas a la línea de negocio y

decidir sobre las medidas de control apropiadas (por ejemplo, COSO ERM, NIST-800-30). Los métodos de gestión de riesgos apoyan a las empresas en decidir sobre la aplicación de medidas de control, sin embargo, no están diseñados como un medio para explicar y motivar el cumplimiento de decisiones a los auditores externos. Aunque la cuantificación de los riesgos en las categorías alta, media o baja los hace medibles para la empresa, la evaluación de riesgos puede también oscurecer el razonamiento que subyace a las decisiones de aplicación de control, por ejemplo, acerca de las dependencias en la arquitectura del sistema, compensaciones, o prioridades estratégicas. A diferencia de los métodos de gestión de riesgos, la argumentación basada en el valor no hace consideraciones de la compañía expresa. Proporciona la subyacente motivación por la que una empresa ha elegido a cierta ciencia el diseño del sistema de control. Sin embargo, un inconveniente de teoría de la argumentación es que no proporciona conceptos de razonar de forma explícita acerca de los riesgos y las vulnerabilidades en el sistema, por lo tanto más investigación es necesaria para integrar de manera más elaborada estos conceptos en el esquema de la argumentación y preguntas críticas (Burgemeestre et al., 2011).

Según Draxler y Stevens (2011) la disposición y configuración de sistemas de TI es parte de las operaciones de TI habituales que se llevan a cabo ya sea por el departamento interno de TI o mediante la contratación de un socio externo. el estándar ITIL no aborda el usuario único como el cliente de un servicio TI, si la organización en su conjunto, por lo tanto, el tema de adaptación no se aborda en el estándar ITIL (ni por los usuarios finales solos ni en cooperación con el proveedor de servicios).

Con el aumento de los delitos informáticos, difusión de virus, DDoS y robo de identidad, la seguridad ha tomado un rol fundamental en el diseño de los sistemas de información. Se prescriben medidas de seguridad por diversos tipos de leyes y reglamentos, como La ley Sarbanes Oxley, códigos de gobierno corporativo, las regulaciones financieras, las leyes de protección de la privacidad y los estándares de la industria como COBIT 4.1, ISO 27001 y NIST 800-53 (Burgemeestre et al., 2013).

Existen trabajos respecto a ataques, amenazas y vulnerabilidades en sistemas de VoIP, enmarcados dentro del ámbito de seguridad, además modelos de análisis forense, modelos de protección, modelos generales con recomendaciones, políticas de seguridad y evaluaciones de amenazas y vulnerabilidades, a través de un análisis de los casos se evidencian debilidades registradas de tipo técnico en los trabajos revisados, es menester en este sentido trabajar a nivel administrativo de seguridad para lo cual se ha considerado una opción viable el análisis de auditoría de seguridades para VoIP, a través de revisión de la literatura al respecto existen trabajos particulares que hacen referencia a métodos, técnicas y metodologías de gestión de TI con recomendaciones de seguridad.

Varios criterios y requerimientos de gestión propios para sistemas VoIP no son contemplados por COBIT y se deben considerar en la propuesta del Modelo de Auditoría de Seguridad VoIP, entre ellos autenticación, no repudio, integridad, disponibilidad, riesgos de servicio VoIP, gestión de ataques, diseño y gestión de sistema de seguridad TI integral.

Estándares y prácticas como ISO/IEC 27002 y COBIT definen las acciones a implementar, mientras que ITIL proporciona las directrices para la administración de los servicios de TI, aunque en este caso no se cubren todos los aspectos administrativos de gestión de seguridad que contempla VoIP, además los mecanismos actuales de auditoría no contemplan el uso de dispositivos móviles, entre otros.

La ingeniería social es una forma de ataque que busca comprometer la seguridad de la información para obtener acceso a sistemas o redes. Estos ataques ocurren principalmente cuando las víctimas desconocen los métodos, modelos o marcos existentes para prevenirlos. Actualmente, no se cuenta con investigaciones específicas que analicen de manera efectiva y sistemática la prevención de ataques de ingeniería social. Entre las estrategias de prevención utilizadas se encuentran campañas de concientización, marcos de sensores de seguridad enfocados en el factor humano, enfoques centrados en el usuario y modelos que analizan la vulnerabilidad de los usuarios (Syafitri et al., 2022).

1.4.2. Justificación práctica

La presente investigación tiene una relevancia práctica al implementar un modelo de auditoría de seguridad específico para sistemas VoIP, cuyo diseño busca mejorar la eficiencia temporal en la realización de auditorías frente a los modelos tradicionales. Este modelo permitirá a las organizaciones realizar evaluaciones más rápidas y precisas, adaptadas a las particularidades y vulnerabilidades inherentes de los entornos VoIP.

Además, la integración de un plan de cultura de seguridad orientado al tratamiento de la ingeniería social fortalece la sensibilización y preparación del personal, mitigando riesgos asociados al factor humano. La aplicación del modelo facilitará la reducción de tiempos en las auditorías, contribuyendo a mejorar la seguridad de la información corporativa. La justificación práctica se sustenta en varias razones:

- Protección de recursos críticos, las comunicaciones VoIP contienen información confidencial y valiosa por lo que el modelo de auditoría de seguridad VoIP garantizaría la seguridad óptima de los recursos de comunicación por voz, registros de llamadas, datos de clientes y conversaciones sensibles.

- Cumplimiento normativo, el modelo permitiría a las organizaciones cumplir con regulaciones y estándares de seguridad que exigen la protección de la información y la privacidad de los datos.

- Reducción de riesgos financieros, el modelo permitiría reducir dichos riesgos al identificar y abordar proactivamente las vulnerabilidades.

- Continuidad del negocio, el modelo garantizaría que las medidas de seguridad implementadas respalden la permanencia operativa del negocio ante incidentes.

- Fortalecimiento de la cultura de seguridad, el modelo de auditoría de seguridad VoIP promovería una mayor conciencia de seguridad dentro de la organización.

- Evaluación y mejora continua, el modelo facilitaría una evaluación constante y sistemática de la seguridad VoIP en una entidad, permitiendo la detección temprana de problemas y la implementación oportuna de mejoras en seguridad.

Un modelo de auditoría de seguridad VoIP puede establecer consideraciones de gestión, administración, configuración, análisis de ataques, amenazas y vulnerabilidades, entre otras; lo que permitirá a los administradores de red una evaluación del sistema y el conocimiento del estado real del mismo de acuerdo a los requisitos de seguridad VoIP, estableciendo cumplimiento en medidas de gestión, organizativas y técnicas. Un modelo diseñado específicamente para VoIP facilitará la implementación de auditorías, optimizando tiempo en entornos organizacionales donde la seguridad es crítica.

1.5. Preguntas de investigación

Para abordar el problema planteado y guiar el desarrollo de la presente investigación, se enuncia la pregunta de investigación principal.

- ¿La implementación de un modelo de auditoría de seguridad específico para sistemas VoIP mejora la eficiencia temporal durante la ejecución de auditorías respecto de los modelos tradicionales?

Además, con el propósito de desglosar el problema en aspectos específicos que requieren un análisis más detallado, se plantean las siguientes preguntas de investigación secundarias.

- ¿La incorporación funcional de los requerimientos de seguridad específicos para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad?

- ¿La integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP incrementa la relevancia de las evaluaciones de seguridad en dichos sistemas?
- ¿La incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP reduce la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano?
- ¿La integración operativa de un procedimiento especializado en una guía de auditoría específica para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad?

1.6. Objetivos de la investigación

Los objetivos de esta investigación definen la dirección y el alcance del estudio, guiando el desarrollo metodológico y la validación del modelo propuesto. El objetivo general establece la finalidad central de la investigación, orientada a ofrecer una solución innovadora y eficiente en el ámbito de la auditoría de seguridad para sistemas VoIP. A su vez, los objetivos específicos desglosan las metas particulares que deben alcanzarse para cumplir con dicho propósito, abordando aspectos clave como los requerimientos técnicos, la estructuración del modelo, la incorporación de un enfoque cultural para mitigar riesgos humanos, y la elaboración de una guía metodológica especializada. A continuación, se detallan el objetivo general y los objetivos específicos que orientan la presente investigación.

1.6.1. Objetivo general

Implementar un modelo de auditoría de seguridad específico para sistemas VoIP que mejore la eficiencia temporal durante la ejecución de auditorías frente a los modelos tradicionales.

1.6.2. Objetivos específicos

- Determinar los requerimientos de seguridad específicos para sistemas VoIP que mejoren la eficiencia temporal en la ejecución de auditorías de seguridad.
- Implementar componentes específicos en el modelo de auditoría de seguridad propuesto para sistemas VoIP que incrementen la relevancia de las evaluaciones de seguridad.
- Implementar un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP orientado a la reducción de la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano.
- Implementar una guía de auditoría específica para sistemas VoIP que incorpore un procedimiento especializado orientado a la mejora de la eficiencia temporal en la ejecución de auditorías de seguridad.

1.7. Organización de la tesis

La presente tesis se encuentra estructurada en cinco capítulos, organizados de forma lógica y secuencial para facilitar la comprensión del desarrollo investigativo y la propuesta del modelo. Cada capítulo aborda una etapa específica del estudio, desde la contextualización del problema hasta la validación de resultados, integrando los fundamentos teóricos, metodológicos y aplicados que sustentan la investigación. A continuación, se describe brevemente el contenido de cada capítulo.

Capítulo 1. Introducción

Este capítulo presenta la situación problemática, la formulación del problema y la motivación del estudio. Además, se desarrollan las justificaciones teórica y práctica que respaldan la investigación, junto con las preguntas de ivestigación y objetivos planteados, proporcionando así el marco conceptual que orienta el desarrollo del estudio.

Capítulo 2. Marco Teórico

Este capítulo desarrolla el marco epistemológico que sustenta la investigación y presenta las bases teóricas relacionadas con la tecnología VoIP, incluyendo los principales protocolos de comunicación y las problemáticas de seguridad asociadas. Asimismo, se aborda el concepto de auditoría de seguridad en tecnologías de la información, se revisan los marcos de trabajo existentes y se detallan los requerimientos específicos de seguridad para entornos VoIP. Finalmente, se incorpora el estado del arte, con énfasis en investigaciones recientes y enfoques relevantes al objeto de estudio.

Capítulo 3. Metodología

En este capítulo se expone el enfoque metodológico que orienta la investigación, así como el diseño adoptado para su desarrollo. Se describen la población y muestra, las hipótesis planteadas, los métodos utilizados, y las técnicas e instrumentos empleados para la recolección y análisis de datos. Además, se presenta la matriz de consistencia que articula los elementos fundamentales del estudio, junto con la operacionalización de las variables, garantizando la coherencia entre los objetivos de la investigación y los procedimientos aplicados.

Capítulo 4. Modelo de Auditoría de Seguridad VoIP Propuesto

Este capítulo presenta el modelo VoIPSAM, incluyendo su fundamentación conceptual, la descripción general de su estructura y los resultados de su validación. Se expone de forma detallada cada uno de sus componentes funcionales, agrupados en dominios operativos, así como el plan de cultura de seguridad diseñado específicamente para entornos VoIP. Asimismo, se introduce la guía de auditoría VoIPSAM, elaborada para facilitar su aplicación en escenarios reales. Finalmente, se analiza la integración de todos los componentes del modelo y se demuestra su aplicabilidad mediante un estudio de caso.

Capítulo 5. Resultados y Discusión

En este capítulo se presentan los resultados obtenidos a partir de la aplicación del modelo VoIPSAM en el estudio de caso, así como su validación. Se expone el análisis

correspondiente a la validación de las hipótesis, tanto secundarias como principal, y se incluye una comparación de los resultados obtenidos frente a modelos tradicionales. Además, se incorpora una evaluación del nivel de madurez alcanzado con el modelo VoIPSAM y, finalmente, se desarrolla una discusión integral de los hallazgos, considerando su relevancia teórica, metodológica y práctica.

CAPÍTULO 2: MARCO TEÓRICO

2.1. Marco epistemológico de la investigación

Según Freire (2020), la búsqueda de información representa la base fundamental que sostiene todo el proceso de investigación; la calidad de la información obtenida es clave para construir un marco teórico sólido y actualizado, validar las hipótesis con fundamentos precisos, minimizar sesgos y asegurar la fiabilidad de los resultados, entre otros aspectos.

Las bases de datos representan una recopilación organizada y estructurada de información y datos, con el propósito de facilitar su posterior utilización. En este contexto, las bases de datos de carácter académico o científico constituyen plataformas de información creadas para almacenar documentos junto con sus características. Estos documentos son el producto de actividades académicas y científicas, como actas de congresos, artículos y capítulos de libros. Su finalidad radica en respaldar la generación de nuevo conocimiento, al mismo tiempo que proporciona métricas y datos relacionados con la producción científica. Esto a su vez permite a los responsables de la gestión científica tomar decisiones informadas de manera fundamentada.

Dentro del marco epistemológico es necesaria la revisión de literatura de los modelos, marcos de trabajo (frameworks) y estándares de auditoría existentes para gestionar la seguridad de VoIP y determinar su relevancia. El marco epistemológico se

desarrolla en la intersección de los campos de investigación en seguridad de TI y el dominio específico de VoIP, para determinar un sólido fundamento a nivel teórico y conceptual el marco se basa en tres aspectos de relevancia interrelacionados: seguridad de TI, VoIP y auditoría de seguridad.

La seguridad de TI tiene como base el cuerpo de conocimiento que está relacionado con la seguridad de las TI, incluye conceptos fundamentales sobre ciberseguridad, amenazas cibernéticas, protocolos de seguridad, gestión de riesgos y cumplimiento normativo; en este sentido las teorías y prácticas de seguridad de TI proveerán el marco general para comprender los desafíos y las soluciones en el entorno de VoIP.

El dominio específico de VoIP incluye conceptos de protocolos de comunicación VoIP como SIP, Protocolo de Transporte en Tiempo Real (RTP), además considera la calidad de servicio (QoS), la arquitectura de redes VoIP y las amenazas específicas de seguridad en entornos VoIP.

La auditoría se seguridad abarca las metodologías y prácticas de auditoría de seguridad, las cuales permiten en forma esencial evaluar y asegurar la confidencialidad, integridad y disponibilidad de los sistemas y la información en un entorno VoIP, conjuntamente incluye técnicas de análisis de riesgos, procesos de auditoría, normativas y estándares de seguridad, junto con métodos para la detección y mitigación de vulnerabilidades.

El cruce de seguridad de TI, VoIP y auditoría de seguridad brinda una perspectiva integral sobre cómo abordar los desafíos de seguridad en el contexto de la implementación y operación de sistemas de comunicación VoIP, mediante la comprensión de la seguridad de TI, la tecnología VoIP y los métodos de auditoría se establece la base específica para desarrollar la propuesta del Modelo de Auditoría de Seguridad VoIP, el cual busca integrar y aplicar las mejores prácticas y enfoques de seguridad en VoIP, adaptándolas a las necesidades específicas de seguridad de recursos, actividades, procedimientos y sistemas

de información empresariales. La Tabla 1 muestra el marco epistemológico de la investigación aplicable al Modelo de Auditoría de Seguridad VoIP.

Tabla 1. **Marco epistemológico de la investigación.**

Área	**Componentes**	**Enfoque y contribuciones**
Seguridad de TI	- Principios de seguridad cibernética - Gestión de riesgos - Cumplimiento normativo	- Contextualización de la importancia de la seguridad en VoIP - Identificación de vulnerabilidades comunes en sistemas de TI - Establecimiento de bases teóricas para la seguridad de VoIP
VoIP	- Protocolos de comunicación VoIP - Amenazas específicas de seguridad en VoIP	- Comprensión de la tecnología y la arquitectura de VoIP - Identificación de riesgos únicos en sistemas de comunicación VoIP - Evaluación de medidas de seguridad específicas para VoIP
Auditoría de Seguridad	- Metodologías de evaluación de riesgos - Procedimientos de auditoría - Estándares de seguridad y cumplimiento	- Adaptación de enfoques de auditoría de seguridad a entornos VoIP - Desarrollo de un marco de valoración de riesgos específico - Incorporación de normativas de seguridad

Fuente. Elaborada por el autor.

La Tabla 2 presenta el registro organizado de las fuentes de información, los términos de búsqueda, los resúmenes relevantes y otros detalles que permiten construir la base teórica y conceptual del estudio.

Tabla 2. **Registro de búsqueda de información para el marco epistemológico.**

Fuente de información	**Términos de búsqueda**	**Resumen de la información relevante**	**Conceptos clave identificados**	**Teorías o modelos relevantes**
Bases de Datos Académicas (IEEE Xplore, Scopus, Web of Science, ScienceDirect, SpringerLink, Google Scholar, ProQuest, EBSCO)	“VoIP security”, “Security audit VoIP”, “VoIP vulnerabilities”	Se identifican múltiples estudios que evidencian vulnerabilidades específicas en redes VoIP como ataques DoS, secuestro de llamadas y debilidades en protocolos. Se revisan enfoques de auditoría aplicados para abordar estas problemáticas.	Vulnerabilidades de seguridad, auditoría de seguridad, ataques de denegación de servicio, secuestro de llamadas	Mitigación de riesgos
Revistas Técnicas	“VoIP security challenges”, “VoIP encryption protocols”	Abordan los desafíos contemporáneos en VoIP, incluyendo la falta de cifrado robusto. Se discuten protocolos y su rol en la protección de la privacidad.	Encriptación, privacidad, desafíos técnicos, protocolos VoIP	Protocolos de seguridad en VoIP
Conferencias en línea	"VoIP security best practices", "VoIP case studies"	Se presentan buenas prácticas para la seguridad VoIP como autenticación de usuarios, segmentación de red, y monitoreo. Casos de estudio evidencian incidentes resueltos mediante prácticas efectivas.	Buenas prácticas, autenticación, monitoreo, estudios de caso	Gestión de incidentes, enfoques prácticos
Libros especializados en VoIP y Seguridad	“VoIP hacking techniques”, “VoIP threats and countermeasures”	Analizan técnicas de ataque específicas a VoIP y presentan contramedidas técnicas y organizacionales para prevenir compromisos de seguridad.	Ataques VoIP, técnicas de intrusión, contramedidas	Contramedidas técnicas, gestión de amenazas
Investigación en Línea – Whitepapers	“VoIP security case studies”, “VoIP audit methodologies”	Documentos técnicos de instituciones y proveedores presentan incidentes y metodologías aplicadas para auditar y corregir	Casos de seguridad VoIP, metodologías de auditoría	Auditoría de seguridad en VoIP

Fuente de información	Términos de búsqueda	Resumen de la información relevante	Conceptos clave identificados	Teorías o modelos relevantes
		brechas de seguridad.		
Portales de Noticias y Normativa	"VoIP security breaches", "VoIP compliance"	Informes sobre brechas de seguridad, privacidad y desafíos legales. Se analiza el impacto del cumplimiento regulatorio en la adopción de soluciones seguras.	Regulaciones, cumplimiento, brechas de seguridad	Marco legal en telecomunicaciones
Libros sobre Auditoría de Seguridad Informática	"Security audit methodology", "Audit process steps", "Frameworks for security audit"	Enfoques para llevar a cabo auditorías de seguridad en diversas áreas, incluida la tecnología. Se discuten metodologías de auditoría, pasos del proceso de auditoría y cómo adaptarlos a entornos tecnológicos específicos como las comunicaciones VoIP.	Metodologías, procesos, marcos de referencia	COBIT, ISO/IEC 27001
Artículos sobre Requerimientos de Seguridad en VoIP	"VoIP security requirements", "technical security standards for VoIP"	Se detallan requerimientos técnicos mínimos de seguridad VoIP en la autenticación, integridad de datos y disponibilidad	Requerimientos técnicos, autenticación, disponibilidad	NIST SP 800-58
Publicaciones sobre Cultura de Seguridad	"Security awareness programs", "security culture in organizations"	Se exploran elementos que constituyen una cultura de seguridad sólida: políticas, concientización, entrenamiento, y liderazgo organizacional.	Cultura organizacional, concientización, liderazgo en seguridad	Frameworks de concienciación (ENISA, ISO 27002)
Artículos sobre Ingeniería Social en VoIP	"Social engineering VoIP threats", "human factor in VoIP security"	Se discuten técnicas comunes de ingeniería social aplicadas a entornos VoIP (vishing, spoofing), y la necesidad de mecanismos preventivos.	Ingeniería social, vulnerabilidad humana, vishing	Modelos de ataque de ingeniería social, enfoques de defensa proactiva

Fuente. Elaborada por el autor.

2.2. Bases teóricas

2.2.1. Introducción a VoIP

Stanescu et al. (2023) sostienen que VoIP es una tecnología que posibilita la realización de llamadas telefónicas mediante Internet, eliminando la dependencia de los sistemas telefónicos analógicos tradicionales. VoIP se refiere a tecnologías y protocolos que permiten transmitir voz y multimedia a través de internet, en lugar de la PSTN, la comunicación de voz utiliza el Protocolo de Internet IP, el costo es un factor importante que ha impulsado las implementaciones de VoIP, de esta forma las organizaciones pueden ahorrar miles de dólares al año al optar por esta tecnología, sin embargo, se deben considerar problemas relacionados con su seguridad.

VoIP es una tecnología que proporciona comunicaciones de voz en redes informáticas como internet y otras redes basadas en IP. VoIP permite disminuir los gastos en telefonía utilizando paquetes de conmutación de internet. En la ingeniería de VoIP, la señal de audio principal se muestrea y codifica al final del proceso de envío en un flujo digital de tasa de bits constante. Este flujo de datos digitales comprimidos se divide en paquetes iguales para facilitar su reproducción. Cada paquete contiene datos de audio, información de la dirección de salida y predicción del destino. El flujo de paquetes se recrea mediante una etiqueta de tiempo. Luego, estos paquetes se colocan en un conmutador de paquetes de digital a analógico para que el oído humano los pueda entender (Brahmbhatt et al., 2017).

El servicio de VoIP ha sido ampliamente adoptado en los últimos años, sin embargo, muchas organizaciones que lo han implementado desconocen o subestiman los riesgos de seguridad y las vulnerabilidades asociadas. Además, las redes VoIP pueden ser fácilmente explotadas y utilizadas de manera indebida, lo que las hace vulnerables a diversos ataques (Suthar & Rughani, 2020).

El uso de protocolos sin cifrar, la falta de una apropiada autenticación y la complejidad de implementar una adecuada seguridad de extremo a extremo son ejemplos del por qué las redes de VoIP son susceptibles a ataques. Las redes de conmutación de circuitos, usadas para transmitir voz, requieren un circuito exclusivo durante la llamada, incluso en los silencios, lo que genera un uso ineficiente de los recursos. Las redes de conmutación de paquetes dividen la información en paquetes que siguen rutas distintas, permitiendo compartir recursos entre conexiones simultáneas. Los paquetes se reensamblan en el destino para entregar el mensaje completo.

Los servicios de VoIP están expuestos a diversas amenazas de seguridad derivadas del Protocolo de Internet IP, como por ejemplo la denegación de servicios, exploits de vulnerabilidad de host y protocolo, vigilancia y secuestro de llamadas, robo de identidad de los usuarios, escuchas e inserción, supresión y modificación de los flujos de audio, entre otros; los atacantes aprovechan estas brechas de seguridad para realizar acciones ilegales, incluidos ataques maliciosos a VoIP, además la compleja configuración de la infraestructura de servicios como los servidores DHCP, servidor AAA (Authentication, Authorization and Accounting), routers, registro SIP, proxy SIP, servidor DNS y dispositivos de red inalámbricas y por cable complican el proceso de análisis de evidencia digital, en este sentido la reconstrucción de la causa raíz del incidente o escenario del delito se concibe como una tarea difícil sin un modelo específico para guiar el proceso.

Geneiatakis et al. (2008) manifiestan que una infraestructura de VoIP hereda y utiliza diversos protocolos de la arquitectura de pila de internet. Específicamente los niveles de red y de transporte emplean el Protocolo de Internet IP y TCP, UDP o SCTP, respectivamente. Además, a nivel de aplicación no sólo explotan protocolos bien conocidos como DNS, DHCP, etc., también se utilizan los dedicados a manejar sesiones y transporte.

2.2.2. Protocolos técnicos de comunicación VoIP

Los principales protocolos utilizados con VoIP son SIP y H.323 en la capa de sesión, se utilizan para establecer una llamada telefónica, y RTP en la capa de medios, que se ocupa del transporte de la llamada. SIP y H.323 establecen una conexión de la llamada y lo manejan fuera de RTP, el cual envía a los medios para la llamada. IAX (Inter-Asterisk eXchange protocol) es el protocolo que realiza la configuración de la sesión y transferencia de multimedia (por ejemplo, voz).

Los sistemas de comunicación VoIP se sustentan en un conjunto de protocolos técnicos especializados que permiten establecer, gestionar y transportar sesiones de voz sobre redes IP. SIP es el protocolo encargado de la señalización necesaria para iniciar, modificar y finalizar llamadas, mediante el intercambio estructurado de mensajes que definen parámetros esenciales como direcciones, códecs y disponibilidad de los participantes. Para el transporte del flujo de audio, VoIP emplea RTP, diseñado para transmitir paquetes de voz con baja latencia y sincronización adecuada, lo que garantiza la continuidad de la comunicación en tiempo real. Además, cuando se requieren medidas adicionales de protección, estos protocolos pueden operar con extensiones seguras como TLS para la señalización SIP y SRTP para el cifrado de los medios, fortaleciendo la autenticidad, confidencialidad e integridad de las transmisiones. La correcta configuración de estos mecanismos es fundamental porque la seguridad de VoIP depende directamente de la robustez con la que se implementan y combinan sus protocolos de señalización y transporte dentro de la infraestructura de red (Alvanos et al., 2018).

Geneiatakis et al. (2008) realizan una taxonomía de los protocolos de nivel de aplicación:

- Señalización: Protocolos que se emplean para manejar una sesión de voz o multimedia entre dos o más entidades de la red de VoIP. Los protocolos de señalización más conocidos son: SIP, H.323, MGCP y SKINY.

- Servicios: Protocolos como DNS y DHCP se utilizan para ofrecer servicios adicionales, tales como la resolución de nombres de direcciones y configuración dinámica.
- Medios: Protocolos como RTP, SRTP y ZRTP se utilizan para transmitir información de medios (voz, video) entre las entidades que han establecido previamente una sesión.

Los componentes operacionales de SIP incluyen los agentes de usuario (UA) y los servidores SIP (Servidores Proxy and Register). Los UAs son los puntos finales de las comunicaciones SIP y pueden incluir una variedad de dispositivos y aplicaciones de software. Además, pueden servir como vías de acceso a otras redes (por ejemplo, PSTN). Por otro lado, los servidores SIP establecen y apoyan las sesiones SIP de UAs, y están a cargo del proceso de señalización (Rosenberg et al., 2002).

En el RFC 3261 que describe el Protocolo de inicio de sesión SIP, Rosenberg et al. (2002) definen varios mensajes que UAs y servidores pueden utilizar para las comunicaciones SIP eficientes. Estos mensajes se pueden dividir en dos categorías principales, mensajes de solicitud (o métodos), y mensajes de respuesta. Los mensajes de solicitud podrán contribuir a registrar a los servidores del Register, enviar la invitación a participar en las sesiones existentes, reconociendo el establecimiento de sesión, modificar los parámetros de la sesión y la cancelación de las sesiones en curso. Los mensajes de respuesta se utilizan para proporcionar la reacción adecuada para el uso de los mensajes de petición, dependiendo de la situación correspondiente.

Dwivedi (2009) sostiene que la configuración para una llamada de VoIP por lo general se lleva a cabo con unos pocos servidores de apoyo, tales como SIP Proxy/Register y/o gatekeeper H.323/gateway. Una vez que la sesión se establece usando SIP o H.323, la llamada se envía al protocolo de medios, que es RTP. La Figura 2 muestra los protocolos de VoIP con sesión y medios de tráfico.

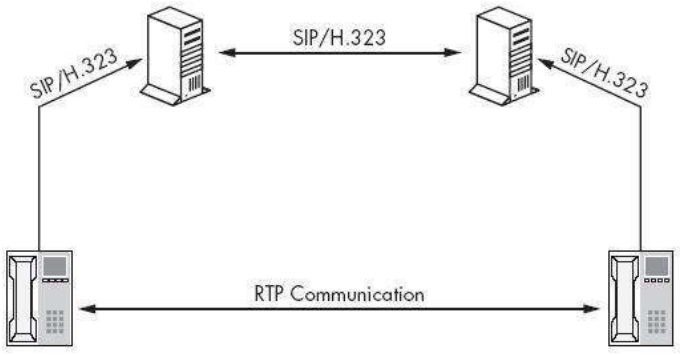


Figura 2. **Protocolos de VoIP con sesión y medios de tráfico**.
Fuente. Dwivedi (2009).

Cualquiera de los protocolos SIP o H.323 se utilizan para la configuración de la sesión, ambos utilizan RTP como medio de comunicación. SIP y H.323 pueden coexistir en un entorno, por ejemplo en una oficina X usando SIP y una oficina Y utilizando H.323, pero el mismo teléfono utiliza SIP y H.323 al mismo tiempo; ambos protocolos prestan servicios similares de configuración, pero lo realizan de forma muy distinta, SIP está diseñado en forma similar a HTTP, donde los métodos como REGISTER, INVITE, FORWARD, LOOKUP, and BYE se utilizan para establecer una llamada, por otro lado H.323 utiliza una colección de subprotocolos, tales como H.225, H.245, H.450, H.239 y H.460 para realizar la configuración de la sesión; ambos protocolos utilizan servidores de apoyo tales como servidores SIP Proxies, SIP Register, H.323 gatekeeper, and H.323 gateway, entre los dos extremos para establecer una llamada, SIP y H.323 utilizan el protocolo RTP para la capa de medios, el cual transfiere audio entre dos o más dispositivos terminales.

IAX, un protocolo no tan popular, se utiliza entre 2 servidores Asterisk, a diferencia de SIP y H.323, IAX se puede utilizar para establecer una llamada entre dos extremos (dispositivos terminales) así como para el canal de medio de comunicación. IAX no utiliza RTP para la transferencia como medio de comunicación debido a que el soporte está integrado en el propio protocolo, lo que lo hace atractivo para organizaciones que desean la simplicidad en sus implementaciones de VoIP. Los protocolos de transporte

garantizan la entrega íntegra de los datos desde el origen hasta el destino, asegurando el cumplimiento de los requisitos de calidad de servicio y ancho de banda.

Los paquetes VoIP utilizan RTP encapsulado en UDP (User Datagram Protocol), ya que este protocolo es más liviano que TCP (Transmission Control Protocol) para aplicaciones en tiempo real. RTP organiza los paquetes y gestiona retrasos o pérdidas durante la transmisión. H.323 usa el estándar para la seguridad H.235 para proporcionar seguridad, incluyendo la autenticación, integridad y privacidad; SIP usa 2 mecanismos: end to end y hop to hop, en el primero HTTP (Hypertext Transfer Protocol) proporciona la autenticación.

Según Basicevic et al. (2008) SIP es más flexible en el sentido de que cubre sólo intencionadamente un subconjunto de la funcionalidad necesaria para la telefonía VoIP y se caracteriza con la capacidad para ser utilizado con diferentes protocolos de transporte y otros, mientras que los diseñadores de H.323 trataron de cubrir todos los aspectos de la funcionalidad de VoIP y han dejado menos espacio para la combinación con otros protocolos. SIP tiene una sintaxis de texto basado en HTTP, y sus extensiones son en la mayoría de los casos basados en XML, mientras que H.323 utiliza la sintaxis binaria basada en ASN.1. La razón más importante para la dominación real del protocolo SIP es la arquitectura SIP y las características de la forma de protocolo de forma natural en el entorno de internet - que es hoy el entorno de telefonía de paquetes más importante, mientras que H.323 hereda algunas características de los protocolos de la telefonía fija.

SIP por sí solo no garantiza un proceso de validación sólido en las redes VoIP, uno de los elementos más importantes para proteger su seguridad es precisamente la autenticación. La confidencialidad, autenticidad e integridad de los mensajes SIP se suelen reforzar mediante protocolo de Seguridad de la Capa de Transporte (TLS) o alternativas como S/MIME (Extensiones Seguras/Multipropósito para Correo de Internet), las cuales operan bajo un modelo de arquitectura centralizada. Estos mecanismos permiten asegurar la comunicación de extremo a extremo a través de la Infraestructura de Clave Pública (PKI) (Kara et al., 2023).

2.2.3. Problemas de seguridad en sistemas VoIP

La protección de un sistema VoIP está estrechamente vinculada a la seguridad tanto de sus elementos físicos como lógicos. Esto implica salvaguardas sobre componentes de hardware como el acceso físico controlado al equipo, la infraestructura de red, y los servidores; así como mecanismos de defensa frente a amenazas que puedan comprometer el correcto desempeño del software utilizado en la plataforma. La integridad del sistema requiere considerar no solo ataques físicos, sino también vulnerabilidades asociadas a fallos o alteraciones en las aplicaciones y servicios que soportan VoIP (Kumar & Roy, 2021). Los tipos de problemas de seguridad se muestran en la Tabla 3.

Tabla 3. **Tipos de problemas de seguridad.**

Tipo de Problema de Seguridad	**Problemas**	**Posibles Soluciones**
Vulnerabilidades para atacantes	Conexión física y acceso a la red	Implementación adecuada de autorización de usuarios
Intercepción (Eavesdropping)	Pérdida de privacidad	Cifrado de los datos
Equipos no autorizados (Rogue Sets)	Amenaza a la confidencialidad	Mecanismo de bloqueo de red
Ataque de suplantación (Spoofing)	Acceso no autorizado	Configuración adecuada del firewall
Ataques de Denegación de Servicio (DoS)	Mensajes falsos SIP INVITE y agotamiento de memoria	Verificación de la dirección IP de origen de los paquetes al enviar respuestas
Ataques DoS basados en inundación (Flooding)	Consumo de recursos de memoria y procesamiento	Diseño de un esquema de mitigación
Ataque DoS a medios de VoIP	Indisponibilidad de la transmisión	Implementación de firewall a nivel de hardware y software

Fuente: Kumar y Roy (2021).

Un intento para superar las normas sobre seguridad de una red de ordenadores se considera como un ataque, basado en una amenaza por la explotación de vulnerabilidades, su efectividad depende de la combinación de 3 factores: contramedidas y mecanismos de

seguridad empleados, existencia de vulnerabilidades específicas en la infraestructura y habilidades particulares del atacante, y herramientas utilizadas para realizar el ataque. VoIP se ha consolidado como una tecnología de comunicación predominante debido a su costo accesible y capacidad de expansión; no obstante, los sistemas VoIP enfrentan graves desafíos de seguridad, entre ellos la intercepción de llamadas, ataques DoS, secuestro de sesiones y suplantación de identidad. Estas vulnerabilidades surgen de la propia naturaleza de las comunicaciones basadas en internet, las cuales son propensas a diversas ciberamenazas. Las tecnologías de vishing automatizado podrían vulnerar la confidencialidad de las comunicaciones VoIP al extraer credenciales mediante llamadas engañosas, poner en riesgo la integridad del flujo de datos de voz al alterar la interacción esperada, y socavar la disponibilidad del servicio si los ataques masivos conducen a la saturación o interrupción del sistema de llamadas (Figueiredo et al., 2024).

En los sistemas VoIP persiste una vulnerabilidad crítica asociada al Spam over Internet Telephony (SPIT), un tipo de ataque que automatiza el envío masivo de llamadas o mensajes de voz con fines fraudulentos. Este problema surge porque los protocolos subyacentes como SIP no fueron diseñados con mecanismos nativos para autenticar la legitimidad de una llamada entrante, lo que facilita que agentes maliciosos generen volúmenes elevados de tráfico no deseado. Nazih et al. (2023) señalan que estos ataques no solo saturan los recursos de red y degradan la calidad del servicio, sino que además constituyen una vía para ejecutar fraudes, campañas de ingeniería social y otras actividades ilícitas que se ocultan tras la infraestructura VoIP. Debido al crecimiento del tráfico automatizado y las técnicas de evasión utilizadas por los atacantes, los métodos tradicionales de filtrado resultan insuficientes, por lo que se requieren enfoques avanzados de detección y mitigación basados en aprendizaje profundo para identificar patrones anómalos en el comportamiento de las llamadas.

VoIP presenta nuevos riesgos de seguridad que los atacantes aprovechan para cometer ilícitos, lo que exige expertos forenses y modelos específicos para el análisis y suministro de evidencia digital. SIP cuenta con varias vulnerabilidades de seguridad, algunas están documentadas en el RFC 3261 del IETF (Rosenberg et al., 2002). Por lo

tanto existen varios ataques de seguridad a SIP, entre los cuales se pueden citar: enumeración de nombres de usuario, hombre en el medio, escucha no autorizada, descifrado de contraseñas SIP, denegación de servicio, suplantación de identidad (phishing) en VoIP, fraude por llamadas de peaje y spam por telefonía en Internet, entre otros. A continuación, se documentan los principales ataques que comprometen la seguridad en entornos VoIP.

a. Enumeración de nombres de usuario

Dwivedi (2009) respecto al ataque denominado enumeración de nombres de usuarios manifiesta que consiste en obtener información de cuentas válidas registradas en una red de VoIP, esto se puede conseguir por sniffing, cuando la autenticación es requerida entre un agente de usuario y un servidor SIP, el URI (Uniform Resource Identifier) estándar de SIP se envía y recorre la red en texto plano (a menos que algún tipo de cifrado de transporte se haya utilizado como TLS (Transport Layer Security) y puede ser esnifeado por un atacante en la red, pues una red de conmutación ofrece poca protección, es posible ejecutar un ataque de envenenamiento ARP tipo hombre en el medio y capturar todos los URI de SIP dentro de la subred local.

El uso de nombres de usuario sin cifrar ejerce más presión sobre la seguridad de la contraseña del cliente, un usuario malintencionado puede intentar varios ataques una vez que se captura el nombre de usuario, por ejemplo, como un ataque de fuerza bruta, además, las empresas suelen utilizar nombres de usuario o extensiones de teléfono como contraseñas, si un atacante puede obtener fácilmente un nombre de usuario o la extensión telefónica, el agente de usuario puede ser fácilmente comprometido.

En la Figura 3 se presenta un ejemplo de un nombre de usuario capturado en la red utilizando Wireshark.

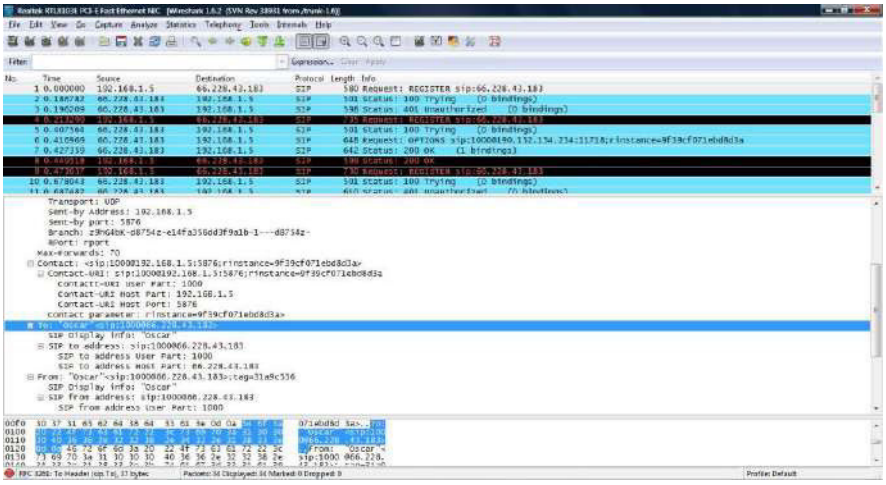


Figura 3. **Enumeración de nombres de usuario SIP mediante Wireshark.**
Fuente. Dwivedi (2009).

b. Hombre en el medio

Hombre en el medio (Man in the middle o MitM) es un tipo de ciberataque donde un tercero intercepta la comunicación o el flujo de datos entre dos partes (como el servidor legítimo y la víctima) con distintos objetivos, como espiar el tráfico, bloquear la comunicación o desviar la conexión hacia un sitio malicioso (Santoso & Finn, 2024).

Los ataques de suplantación del Protocolo de Resolución de Direcciones (ARP) representan una amenaza crítica para los entornos que integran comunicaciones VoIP, debido a que comprometen directamente el flujo de paquetes de voz en redes de acceso inalámbrico o cableado. Cuando un atacante manipula las tablas ARP mediante respuestas falsificadas, logra desviar el tráfico RTP o SIP hacia un dispositivo no autorizado, generando escenarios de intercepción, degradación deliberada de la calidad de voz o incluso interrupciones completas del servicio. Este tipo de ataque altera la correspondencia legítima entre direcciones IP y MAC, permitiendo al adversario posicionarse como intermediario y obtener acceso al contenido de la comunicación sin ser detectado.

Los sistemas VoIP que operan sobre infraestructuras VoWi-Fi son especialmente susceptibles a estas técnicas, ya que la naturaleza abierta de los medios inalámbricos facilita la inserción de tramas ARP manipuladas. La manipulación maliciosa de ARP afecta la disponibilidad y la integridad de las llamadas, al provocar latencia adicional, pérdida de paquetes, fluctuaciones en el jitter e interrupción del canal de señalización. Además, la suplantación ARP puede actuar como fase inicial para ataques más avanzados, como la inyección de tráfico fraudulento, la modificación de parámetros de sesión o el desvío de llamadas hacia destinos manipulados (Lu et al., 2024).

Este conjunto de riesgos confirma que la protección de VoIP no puede limitarse a mecanismos de cifrado y autenticación en los protocolos superiores, sino que debe incluir controles robustos a nivel de red, tales como inspección dinámica de ARP, listas de control de acceso basadas en direcciones MAC, segmentación del tráfico de voz y detección temprana de anomalías. La mitigación adecuada de la suplantación ARP se convierte así en un elemento indispensable dentro de cualquier modelo de auditoría o arquitectura de seguridad para comunicaciones VoIP. La Figura 4 muestra el esquema del ataque Hombre en el medio.

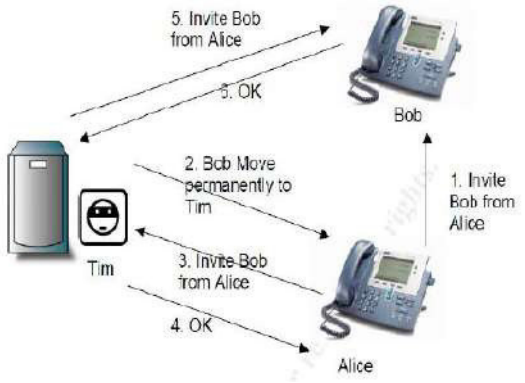


Figura 4. **Esquema del ataque Hombre en el medio.**
Fuente. Dwivedi (2009).

Se interceptan los mensajes de señalización de SIP por parte del atacante y se hace pasar por la parte llamante, una vez en este estado se pueden secuestrar llamadas.

- Alice envía un mensaje de invitación a bob y este mensaje se detecta mediante un atacante.
- El atacante envía un mensaje de respuesta a Alice suplantando a Bob. En respuesta el Atacante establece la nueva dirección de Alice a su ordenador.
- Alice envía un nuevo mensaje INVITE al atacante. Según Alice se está conectando a Bob.
- El atacante envía un acuse de recibo para establecer la conexión entre él y Alice.
- Al mismo tiempo, el atacante envía un mensaje de invitación a Bob y puede falsificar la identificación de Alice.
- El atacante responde ok y se establecen las conexiones entre Bob y el atacante.

Ahora el atacante puede hacer lo que sea y puede grabar el contenido de la conversación.

c. Escucha no autorizada

La escucha no autorizada (eavesdropping) consiste en interceptar comunicaciones sin participar en ellas, como streams de audio y mensajes de señalización. Esto ocurre cuando VoIP comparte el mismo medio físico para datos y voz, sin redes independientes o separaciones lógicas (VLANs). Mediante el ataque de suplantación ARP, se puede ejecutar un ataque man in the middle para la captura y análisis de conversaciones VoIP transmitidas en RTP, que transfiere datos en tiempo real como video y audio, comprimidos en códecs para su conversión en ambos extremos (Dwivedi, 2009).

Eavesdropping es un tipo de ataque en el que un atacante intercepta el canal de comunicación con el fin de acceder a información confidencial, el adversario puede optar por permanecer pasivo o utilizar los datos obtenidos para realizar un ataque activo, como interferencias, inserción de información falsa o suplantación de identidad. En cualquiera de los casos, el atacante debe mantenerse oculto, ya que ser detectado haría que el ataque fracase (Yasar & Yazicigil, 2023).

d. Suplantación de identidad

Según Kondoth et al. (2023) un atacante malicioso puede capturar el tráfico de la red y acceder a toda la información transmitida con el fin de obtener datos sensibles, esto se vuelve aún más sencillo en redes inalámbricas, ya que su carácter de transmisión abierta las hace vulnerables y accesibles para quienes buscan interceptar las comunicaciones. El spoofing o ataque de suplantación de identidad consiste en que un atacante malicioso intenta obtener acceso no autorizado a un sistema con el objetivo de modificar su configuración, lo que puede generar fallos en el funcionamiento o provocar un comportamiento incorrecto del sistema. La Figura 5 muestra el esquema de un ataque de suplantación ARP.

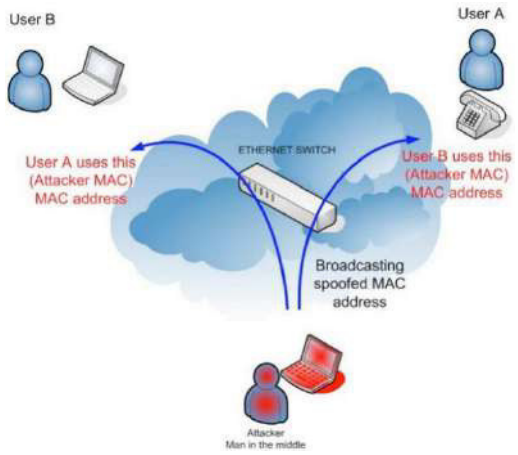


Figura 5. **Ataque de suplantación ARP**.
Fuente: Dwivedi (2009).

e. Descifrado de contraseñas SIP

Según Dwivedi (2009) el descifrado de contraseñas SIP consiste en averiguar la contraseña SIP de un determinado usuario, suele realizarse a través de la técnica de fuerza bruta y con el uso de un diccionario, especialmente efectivo con contraseñas débiles, se disponen de métodos y herramientas para vulnerar la autenticación y descifrar hashes

digest, permitiendo obtener contraseñas y suplantar la identidad de la víctima con fines maliciosos. En la Figura 6 se puede apreciar el ataque de descifrado de contraseñas SIP usando el sniffer Cain & Abel.

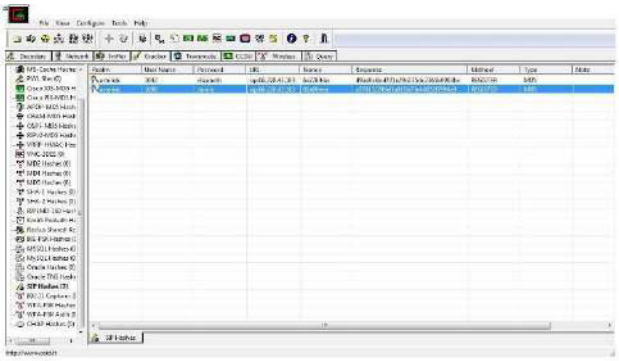


Figura 6. **Ataque de descifrado de contraseñas SIP utilizando el sniffer Cain & Abel.**
Fuente: Dwivedi (2009).

f. Denegación de servicio

Huseinović et al. (2020) considera que los ataques de denegación de servicio DoS ocurren cuando un atacante o un grupo de atacantes buscan inutilizar un servicio, sistema informático o recurso de red, impidiendo su acceso a los usuarios legítimos. En un ataque DoS convencional, el atacante, ubicado en un extremo de la red, genera tráfico malicioso que se transmite a través de controladores y una red de dispositivos comprometidos (zombis o bots) con el objetivo de saturar y bloquear los servidores seleccionados. Actualmente, las empresas especializadas en seguridad informática consideran los ataques DoS como una de las principales amenazas para los proveedores de servicios.

Según Dwivedi (2009) un ataque DoS afecta una red al hacer que un servicio o recurso se vuelva inaccesible para usuarios legítimos, generalmente mediante el consumo del ancho de banda o la saturación de los recursos computacionales de la víctima.

El ataque se produce al saturar los puertos con flujo excesivo de información, provocando que el servidor se sobrecargue e incapaz de atender solicitudes. En VoIP, los ataques DoS específicos incluyen inundación de paquetes RTP, malformación de mensajes INVITE y cierre de sesiones con mensajes BYE y CANCEL. La Figura 7 muestra un ataque DoS generado por inundación de mensajes.

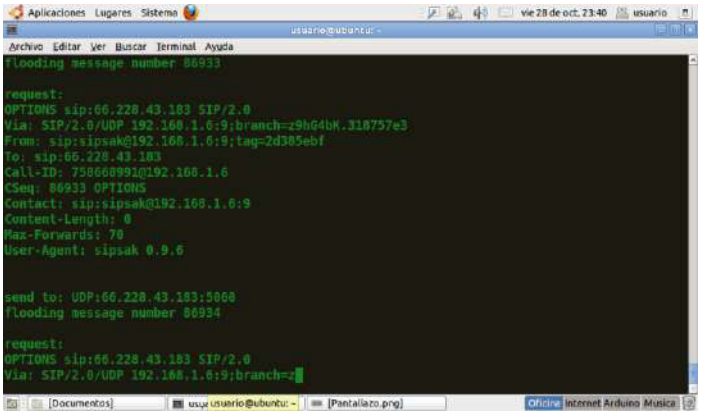


Figura 7. **Ataque DoS generado por inundación de mensajes.**
Fuente. Dwivedi (2009).

g. Spam y suplantación de identidad (phishing) en VoIP

Dwivedi (2009) considera que este tipo de ataque implica que una persona que llama finja ser de una organización digna de confianza y solicite información confidencial y crítica, es un ataque contra la privacidad de los datos, en este caso la propia víctima da a sus datos personales. La suplantación de identidad (phishing) funciona de la siguiente manera: un ladrón de datos envía un mensaje de correo electrónico o un mensaje de voz para hacer parecer que se trata de un mensaje oficial de una compañía que tiene intereses financieros o de otro tipo como su banco, en el mensaje, se le informa acerca de un problema que pone en alarma al usuario y se pide ir a un sitio web o llamar a un número de teléfono donde el usuario tiene que dar sus datos personales como número de tarjeta de crédito, contraseñas, etc.

h. Fraude por llamadas de peaje

Implica acceder de forma no autorizada a los servicios de VoIP, se puede realizar mediante la manipulación de los mensajes y la configuración de los componentes de señalización de VoIP, lo que permite que los hackers sean capaces de secuestrar los sistemas, entrar directamente en los teléfonos y copiar las credenciales y colocarlas en su propio equipo (Dwivedi, 2009).

i. Spam a través de telefonía por internet

El spam por telefonía en Internet (SPIT) consiste en el envío de llamadas masivas no deseadas a través de redes VoIP; está emergiendo como un problema crítico que puede afectar la experiencia de uso de VoIP. A diferencia del spam en correos electrónicos, cuya detección y filtrado son más efectivos, las estrategias de mitigación del SPIT enfrentan dificultades significativas para su identificación y bloqueo en tiempo real. El SPIT consiste en el envío de mensajes de voz a un destinatario, haciéndose pasar por una fuente confiable, como una entidad bancaria o un servicio en línea. Generalmente, estos intentos buscan obtener información confidencial, como contraseñas o números de tarjetas de crédito, mediante engaños. El SPIT es un tipo de ataque que perjudica significativamente la experiencia del usuario. Se han desarrollado diversas técnicas para detectar llamadas SPIT (Behan et al., 2022)

Este tipo de fraude abarca todas aquellas llamadas no solicitadas o de carácter abusivo, como las llamadas spam o las estafas telefónicas. Estas pueden ejecutarse de distintas formas, desde phishing telefónico suplantando a una empresa, hasta telemarketing agresivo o llamadas automáticas con mensajes pregrabados. Entre los principales objetivos de este fraude está obtener información sobre los usuarios (por ejemplo, confirmar si el número pertenece a una persona real) y manipular a los destinatarios para que realicen alguna acción que pueda generar beneficios económicos para el estafador. Gran parte de estas llamadas se enmarcan en este tipo de fraude, donde

los atacantes podrían utilizar sistemas VoIP comprometidos para ejecutar campañas fraudulentas o identificar nuevas víctimas potenciales (Carrillo et al., 2022).

j. Ingeniería social

Según Washo (2021) la ingeniería social consiste en emplear tácticas de manipulación y engaño con el propósito de acceder a información sensible, actualmente, se reconoce como una de las amenazas más significativas para la seguridad de la información. Su impacto es cada vez mayor, afectando tanto a personas como a organizaciones de manera creciente.

La ingeniería social es una forma de ataque capaz de burlar las defensas de hardware y software diseñadas para prevenir amenazas, su detección y prevención se complica si se confía únicamente en la tecnología, ya que estas acciones se enfocan en manipular a los propios usuarios de los sistemas y dispositivos; por lo tanto la participación activa del usuario es fundamental en la prevención de este tipo de ataques, además, las técnicas de ingeniería social son diversas y constantemente evolucionan según el método que se utilice (Syafitri et al., 2022).

La ingeniería social consiste en obtener información sobre sistemas informáticos mediante métodos que incluyen profundamente medios no técnicos. Mientras que la seguridad técnica de la mayoría de los sistemas críticos es alta, los sistemas siguen siendo vulnerables a los ataques de los ingenieros sociales. La ingeniería social es una técnica en la que no se requiere ninguna herramienta técnica (avanzada), puede ser utilizada por cualquier persona, y es barata (Vilarinho & da Silva, 2011).

VoIP se ha consolidado como una tecnología ampliamente utilizada, ya que permite a los usuarios hacer llamadas telefónicas a través de la internet pública. Algunas de sus características predominantes tales como la eficiencia, la rentabilidad y la larga distancia de la comunicación permiten a VoIP estar al margen de las tradicionales redes telefónicas públicas conmutadas (PSTN). SIP corresponde al protocolo de señalización

contemporáneo utilizado en las redes VoIP, el protocolo en sí es vulnerable a la mayoría de las amenazas que se producen en las redes VoIP. Independientemente de registrar incidentes altamente escalables, es considerado por los expertos como el futurista objetivo para los atacantes. Son pocos los estudios que han abordado la prevención de los ataques de ingeniería social, a pesar de que estas técnicas representan un alto riesgo y pueden generar graves pérdidas para las organizaciones (Syafitri et al., 2022).

Salahdine y Kaabouch (2019) definen la ingeniería social como una de las mayores amenazas a la seguridad en redes, pues no se dirige a vulnerabilidades técnicas sino al eslabón humano, aprovechando la tendencia natural de las personas a confiar. Un patrón típico en la ejecución de este tipo de ataques está estructurado en cuatro fases: recolección de información sobre la víctima; establecimiento de una relación de confianza; explotación de la información para ejecutar el ataque; y salida sin dejar rastros. Respecto a las estrategias de mitigación, destacan dos líneas principales: políticas, auditoría y definición de procedimientos internos; educación, capacitación y concienciación continua del personal, ya que las defensas puramente técnicas suelen ser insuficientes cuando el atacante apela al factor humano.

Los ataques de vishing, o suplantación de identidad por voz, aprovechan las debilidades humanas para manipular a las víctimas a través de llamadas telefónicas y hacer que proporcionen datos confidenciales (Bin Adam et al., 2023).

El vishing se ha consolidado como una de las amenazas más relevantes en los entornos VoIP, debido a que los atacantes aprovechan la flexibilidad y bajo costo de las plataformas de voz sobre IP para automatizar llamadas fraudulentas, ocultar su identidad y manipular a los usuarios mediante técnicas de ingeniería social. Las campañas de vishing modernas ya no se limitan a simples llamadas engañosas, sino que involucran múltiples señales digitales propias de ecosistemas VoIP, tales como patrones de tráfico, características acústicas y contenido textual asociado a la comunicación. Vishing constituye un riesgo inherente a las infraestructuras VoIP actuales, existe la necesidad de incorporar técnicas de detección inteligentes y controles específicos para el tráfico de voz

sobre IP, ya que los métodos tradicionales basados en filtros estáticos o listas de bloqueo resultan insuficientes frente a ataques que evolucionan rápidamente y explotan vulnerabilidades propias de la telefonía basada en IP (Mishra et al., 2024).

La ingeniería social consiste en la manipulación psicológica de las personas para obtener acceso no autorizado a redes, sistemas y datos confidenciales. Un ataque de este tipo ocurre cuando la víctima desconoce las tácticas utilizadas y cómo protegerse contra ellas. Aunque los avances en tecnologías de comunicación han mejorado la conectividad, también han aumentado la exposición de información personal en línea, muchas veces sin medidas de seguridad adecuadas. Los hackers pueden explotar la ingeniería social sin importar las tecnologías de seguridad implementadas. Aunque los métodos varían, el objetivo es el mismo: engañar y manipular a individuos, empresas u organizaciones para obtener información confidencial, que luego puede ser utilizada para robo de datos, fraude financiero o venta en la red oscura (Abubaker et al., 2023).

En los últimos años, la cantidad y la sofisticación de los ataques cibernéticos se han incrementado significativamente. Esto crea una gran cantidad de desafíos desde una perspectiva de seguridad. En primer lugar, para el seguimiento de una red, las alertas generadas necesitan ser presentadas y que se resuman de manera significativa. En segundo lugar, se necesitan análisis adicionales para identificar ataques sofisticados y correlacionados (Vasilomanolakis et al., 2015).

Un sistema de gestión de riesgos (RMS) asegura que una empresa gestione las amenazas de manera proactiva, coordinada, rentable y priorizada. La gestión del riesgo se puede adaptar para satisfacer las necesidades de cada negocio. Se puede utilizar para educar al personal, y darles una comprensión más profunda de los riesgos corporativos. Esto convierte a los gerentes en la gente de negocios, y hace que el negocio sea más eficaz. La Auditoría de la seguridad puede formar parte de un sistema de gestión de riesgos (Sadgrove, 2016).

La ingeniería social continúa siendo uno de los vectores más críticos dentro del panorama de amenazas contemporáneo, debido a que explota vulnerabilidades humanas más que fallos tecnológicos. Un análisis reciente propone una ontología específica del dominio de la ingeniería social y demuestra cómo su representación estructurada en grafos de conocimiento permite identificar relaciones entre técnicas de ataque, canales de interacción y patrones de persuasión utilizados por los atacantes (Wang et al., 2021). Este enfoque evidencia que la ingeniería social opera como un sistema complejo donde intervienen factores cognitivos, contextuales y organizacionales, lo que exige modelos de seguridad capaces de mapear y comprender estas interacciones para anticipar escenarios de riesgo. En consecuencia, la integración de marcos formales que describan taxonomías de ataque, tácticas empleadas y flujos de explotación constituye un recurso valioso para diseñar estrategias de mitigación más precisas, especialmente en entornos sensibles como VoIP, donde la manipulación del usuario puede comprometer procesos de comunicación críticos.

La ingeniería social se consolida como un factor decisivo dentro del ámbito de la seguridad de la información, especialmente por su capacidad para explotar vulnerabilidades humanas a través de técnicas como el phishing, el vishing, el pretexting o la manipulación psicológica. Su impacto no solo revela debilidades operativas, sino también brechas formativas que requieren ser abordadas desde una perspectiva profesional. La evidencia reciente muestra que la comprensión profunda de los métodos de persuasión, la identificación de patrones de manipulación y el fortalecimiento de competencias conductuales son elementos esenciales para prevenir intrusiones exitosas. En consecuencia, las organizaciones necesitan desarrollar perfiles profesionales capaces de reconocer señales de engaño, responder con criterio técnico y aplicar protocolos de verificación que dificulten la explotación del factor humano, consolidando así un enfoque de seguridad integral más allá de las medidas puramente tecnológicas (Oliinyk & Oleksiuk, 2024).

Las amenazas de VoIP han sido ya estudiadas durante mucho tiempo. Básicamente, una taxonomía de tales amenazas las divide en varias categorías macro, que incluyen los siguientes representantes principales (Chiappetta et al., 2013).

- Amenazas sociales: este tipo de ataques tienen los usuarios finales como objetivos finales; vishing (es decir, la voz phishing), el robo de servicio y SPIT (spam sobre telefonía por internet) pertenecen a esta categoría.

- Espionaje: estos ataques suelen tener lugar cuando un usuario malicioso no autorizado llega a ser capaz de interceptar una llamada VoIP y, por ejemplo, la reconstrucción de toda una conversación entre dos usuarios.

- La interrupción intencionada: se refiere principalmente a la denegación de servicio, cuyo objetivo es impedir que un servicio esté disponible para los usuarios finales, incluyendo tanto ataques tradicionales a la infraestructura de la red IP como todo un conjunto de nuevas amenazas dirigidas específicamente a sistemas y aplicaciones VoIP.

- Abuso de servicio: este tipo particular de amenazas se refiere principalmente a todas aquellas situaciones en las que se presta un servicio de VoIP en un contexto comercial, fraudes de facturación normalmente entran en esta categoría.

Entre estas amenazas, SPIT y vishing sin duda juegan un papel importante, ya que representan una combinación fatal de bajo costo de implementación y alta efectividad. SPIT se refiere a la aplicación de correo no deseado para las comunicaciones VoIP. Básicamente consiste en la entrega de información no deseada a los usuarios de VoIP sin protección. El primer lugar en el ranking SPIT es indiscutiblemente propiedad de los llamados televendedores, es decir, la gente tratando de vender algo por teléfono (Chiappetta et al., 2013).

Figueiredo et al. (2024) sostienen que vishing es un tipo de ingeniería social en el que los atacantes emplean llamadas telefónicas para engañar a las personas y obtener información confidencial, como datos personales, credenciales de seguridad o detalles financieros. Para manipular a sus víctimas, se aprovechan de la apariencia de autenticidad y la sensación de urgencia en la comunicación de voz, haciéndose pasar por entidades legítimas como bancos o servicios de soporte técnico. Esta amenaza es especialmente peligrosa, ya que evade los controles de seguridad diseñados para proteger la información. Según Syafitri et al. (2022) para lograr hacer efectivo este tipo de ataque, los atacantes recurren a estrategias psicológicas como intimidaciones, provocar ansiedad o dar noticias positivas, con el fin de que la víctima no sospeche que está siendo manipulada.

El vishing se ha consolidado como una de las modalidades más sofisticadas de ingeniería social, al combinar técnicas de manipulación psicológica con el uso de sistemas de voz sobre IP. En este contexto, Nyassi et al. (2024) señalan que los atacantes emplean tácticas de persuasión emocional para inducir a las víctimas a revelar información sensible o realizar acciones no autorizadas durante una llamada telefónica. Este tipo de ataque genera patrones detectables en la dinámica emocional de la conversación, los cuales pueden ser identificados mediante modelos de Markov ocultos. Las fluctuaciones emocionales constituyen indicadores relevantes para diferenciar entre llamadas legítimas y llamadas maliciosas. Estos hallazgos evidencian que el vishing no solo compromete la confidencialidad de las comunicaciones VoIP, sino que también representa una amenaza difícil de mitigar con mecanismos exclusivamente técnicos, reforzando la necesidad de políticas de concienciación, monitoreo activo y análisis conductual en los procesos de auditoría de seguridad. Es probable que el phishing y otras tácticas de ingeniería social continúen en los próximos años con mayor complejidad y sofisticación (Thomas et al., 2020).

2.2.4. Auditoría TI

Según Esparza et al. (2020) la auditoría informática se ha vuelto un componente esencial para asegurar la eficiencia y correcta utilización de los sistemas informáticos

dentro de las organizaciones; el resultado de una auditoría está influenciado por diversos factores, entre ellos, el papel del auditor de TI.

La adopción de auditorías estructuradas orientadas a la gestión de servicios de TI contribuye a fortalecer la gobernanza tecnológica y a reducir los riesgos derivados de fallos en la infraestructura y en las operaciones de TI; optimizando la eficiencia, calidad y seguridad en los procesos vinculados con la administración de las tecnologías de la información dentro de las organizaciones (Zumba et al., 2018).

Los controles de sistema que integran TI en sus operaciones combinan tanto procesos manuales como automatizados, lo que puede restringir la supervisión de las actividades de TI y complicar la administración de las verificaciones automáticas. Debido a esto, muchas organizaciones han incrementado su inversión en auditorías de TI, dado que la mayoría de los procesos empresariales dependen de herramientas tecnológicas (Salihu & Hoti, 2022).

Las TI desempeñan un papel fundamental en las operaciones diarias de las organizaciones modernas, y una gestión inadecuada de los cambios puede representar riesgos significativos para la continuidad del negocio. Para abordar esta problemática, marcos como COBIT proporcionan guías y mejores prácticas para una correcta administración de los cambios en TI. Además, los accionistas suelen recurrir a auditorías para asegurar que la implementación se realice conforme a los procedimientos establecidos (Fraga et al., 2024).

Según Imran et al. (2023) las auditorías de procesos tradicionales, al realizarse de forma manual y mediante muestreo, se apoyan principalmente en la experiencia y juicio de los auditores. La minería de procesos (PM) ofrece una alternativa para optimizar y modernizar estas auditorías, mejorando su precisión y eficiencia. La Figura 8 muestra una metodología de auditoría basada en minería de procesos.

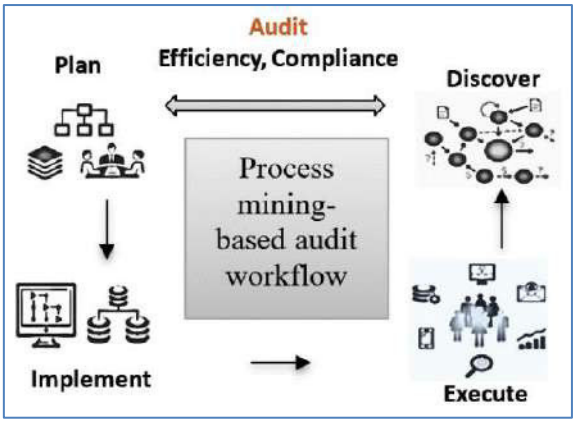


Figura 8. **Metodología de auditoría basada en minería de procesos.**
Fuente. Imran et al. (2023).

La necesidad de realizar auditorías de TI ha crecido, así como las expectativas sobre la calidad de estos procesos, estándares internacionales pueden aplicarse para fortalecer las recomendaciones dentro de las auditorías de TI. La adopción de tecnologías emergentes ofrece a las empresas ventajas y riesgos. Para enfrentar estos retos y asegurar el cumplimiento normativo, las organizaciones recurren a marcos de buenas prácticas que respaldan una gestión efectiva de TI, siendo COBIT uno de los principales modelos de gobernanza en este ámbito (Salihu & Hoti, 2022).

2.2.5. Auditorías de seguridad TI

Las auditorías de seguridad de TI determinan si un sistema de información y sus administradores cumplen con las expectativas legales de protección de datos de los clientes, así como con los estándares necesarios para asegurar el éxito frente a diversas amenazas a la seguridad de la compañía. Las auditorías de TI tradicionales normalmente se dividen en dos categorías principales: interna y externa. Las auditorías internas se refieren al trabajo de los propios empleados de una organización, preocupación por procesos organizativos muy específicos y se centran principalmente en la optimización y gestión de riesgos. Las auditorías externas dan una perspectiva externa sobre la habilidad de una organización para adherirse a las leyes y regulaciones vigentes. Las organizaciones han utilizado las auditorías de TI tradicionales para evaluar cuestiones tales como la

disponibilidad de los usuarios autorizados, la integridad y la confidencialidad en el almacenamiento y transmisión de datos (Ryoo et al., 2014).

Una empresa requiere medidas de seguridad específicas alineadas con objetivos pertinentes, diseñadas para abordar riesgos asociados a los procesos de negocio y los activos a proteger. El auditor debe determinar si dichas medidas son apropiadas para las circunstancias y cumplen con los requisitos reglamentarios. El establecimiento de una norma en una auditoría, es decir, concretar y determinar si las medidas de seguridad son apropiadas para una situación particular, puede considerarse como una tarea de ingeniería de requerimientos importantes. Las metodologías de ingeniería de seguridad buscan facilitar la planificación y aplicación de controles de seguridad de manera sistemática. Sin embargo, no toman en cuenta los objetivos de negocio y los valores que desempeñan un papel para decidir sobre las medidas de seguridad. La ingeniería de seguridad requiere una perspectiva más amplia. Se sugiere integrar las exigencias de seguridad con los requisitos funcionales y las limitaciones derivadas de otras fuentes. Lo ideal es que el resultado de las medidas de seguridad sea mejorar la vinculación entre los procesos de negocio y los sistemas de información existentes. Por otra parte, hay poca investigación sobre la resolución de conflictos entre los objetivos, requisitos y valores (Burgemeestre et al., 2013).

2.2.6. Marcos de trabajo

Existen muchos marcos de trabajo (frameworks) relacionados con la gestión de TI, además de estándares y metodologías en uso actualmente. Ninguno de ellos, por sí mismos, son frameworks de gobernanza de TI independientes, pero todos tienen un papel útil en la gestión eficiente de las operaciones de TI. En el ámbito de la auditoría de seguridad informática, los marcos de trabajo constituyen referentes fundamentales que proporcionan estructuras sistemáticas, buenas prácticas y lineamientos metodológicos para evaluar, controlar y mejorar la seguridad de los sistemas de información. Su adopción permite establecer procesos coherentes y estandarizados, facilitando la identificación de

riesgos, la implementación de controles y la medición del cumplimiento en función de objetivos definidos.

Para el contexto específico de esta investigación, resulta necesario considerar frameworks ampliamente reconocidos como COBIT, ISO/IEC 27001 y NIST SP 800-53, entre otros. Estos marcos ofrecen enfoques variados, desde la gobernanza estratégica hasta la implementación operativa de controles técnicos, cada uno con distintos niveles de abstracción, aplicabilidad y orientación hacia entornos tecnológicos concretos.

La selección y análisis de dichos frameworks permite identificar sus fortalezas y limitaciones al ser aplicados en contextos VoIP, evidenciando la necesidad de modelos más específicos que respondan a las particularidades de estos entornos. A continuación, se presentan los principales marcos de trabajo aplicables a la gestión y evaluación de la seguridad en entornos VoIP.

a. Framework Calder-Moir

El framework para Gobernanza de TI está diseñado para ayudar a utilizar todos estos marcos y normas superpuestas e implementar la mejor orientación práctica que figura en la norma internacional ISO/IEC 38500. El framework integra diversos estándares y marcos mediante una representación gráfica que conecta tópicos clave como estrategia empresarial, planificación de TI, riesgos, recursos, operaciones y gestión del cambio (IT Governance, 2025). El Framework Calder-Moir para Gobernanza de TI se muestra en la Figura 9.

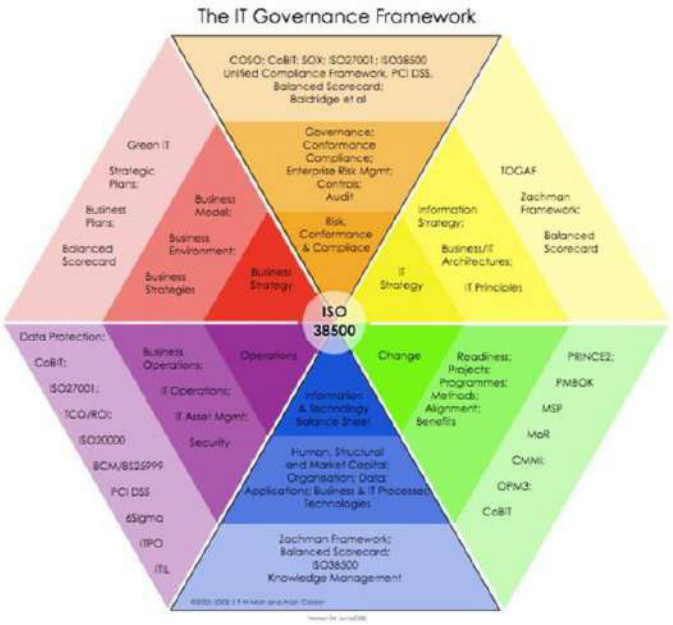


Figura 9. **Framework Calder-Moir para Gobernanza de TI.**
Fuente. IT Governance (2025).

b. ISO 27000

Las normas ISO 27000 son estándares enfocados en la seguridad de la información, proporcionando beneficios como eficiencia operativa, reducción de costos y mayor protección. Su aplicación es válida para organizaciones de cualquier tamaño o sector, siendo fundamentales para garantizar la integridad, confidencialidad y disponibilidad de los datos (Babilonia, 2023).

La seguridad informática, la ciberseguridad y la protección de la privacidad son aspectos fundamentales para las empresas y organizaciones en la actualidad. La familia ISO/IEC 27000 incluye más de una docena de normas que incorporan buenas prácticas en la protección de datos y en el fortalecimiento de la capacidad de recuperación ante incidentes cibernéticos. En conjunto, estas normas permiten a organizaciones de cualquier sector y tamaño administrar la seguridad de activos críticos, como información financiera, propiedad intelectual, datos de empleados y la información confidencial proporcionada por terceros (ISO, 2022).

La norma ISO/IEC 27001 es el estándar más reconocido a nivel global para la gestión de la seguridad de la información (SGSI) y sus requisitos, la norma establece un marco para los sistemas de gestión de la seguridad de la información (SGSI), ofreciendo a organizaciones de cualquier tamaño y sector directrices para la planificación, implementación, mantenimiento y mejora continua de la seguridad de la información. La norma ISO 27002 se utiliza normalmente en la práctica (*ISO/IEC 27001*, 2022).

c. NERC CIP

Con el fin de garantizar la fiabilidad de los sistemas de generación y transmisión de energía, North American Electric Reliability Corporation (NERC) Protección de Infraestructuras Críticas (CIP) obliga a un amplio rango de ambos controles técnicos y de procedimiento que se deben implementar y documentar. El cumplimiento de NERC CIP implica controles específicos de seguridad técnicas, así como controles de procedimiento alrededor de la formación, aplicación de políticas, el acceso (tanto físico como cibernético), y más. El cumplimiento de NERC CIP también exige una amplia documentación (Cole, 2016).

d. SAS 70 Tipo II

SAS 70, la declaración sobre Normas de Auditoría No. 70 es una norma de auditoría desarrollada por el Instituto Americano de Contadores Públicos Certificados (AICPA) que proporciona orientación sobre organizaciones de servicios de auditoría. La norma enumera una serie de factores de riesgo ilustrativos para ayudar a los auditores a detectar el fraude (Salas & Reyes, 2015). La norma proporciona a las organizaciones y sus auditores información sobre el control interno, verificando su existencia, documentación, implementación y efectividad operativa, además de analizar su diseño y desempeño.

e. GLBA

La Ley Gramm-Leach-Bliley (GLB o GLBA), regula cómo las instituciones financieras gestionan la información privada de los individuos. Incluye tres reglas clave: Privacidad Financiera, que controla la recopilación y divulgación de datos financieros; Salvaguardas, que exige programas de seguridad para proteger la información; y las disposiciones contra pretextos, que prohíben acceder a datos privados mediante engaños. Además, obliga a las instituciones a notificar por escrito a los clientes sobre sus políticas de privacidad y prácticas de intercambio de información (Cuaresma, 2002).

f. PCI DSS

El Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago es una norma global destinada a proteger los datos en transacciones con tarjetas (crédito, débito, cajero automático) para todas las entidades que procesan, almacenan, o transmiten datos del titular de la tarjeta y/o autenticación confidencial de datos transmitidos en línea (Dupuis et al., 2019).

PCI DSS consta de requisitos técnicos y operativos que procesan transacciones de pago, desarrolladores de software, fabricantes de aplicaciones y dispositivos utilizados en estas transacciones para reforzar la protección de los datos de las cuentas vinculadas a tarjetas de pago (Elluri et al., 2018). Las empresas que manejan datos de tarjetas deben cumplir con el estándar para evitar la pérdida de permisos para procesar tarjetas de débito y crédito. Proveedores y comerciantes de servicios están obligados a validar su cumplimiento regularmente.

g. COBIT

COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas) es un marco conceptual creado por ISACA con el propósito de orientar la gobernanza y la gestión efectiva de las Tecnologías de la Información en las organizaciones. Su finalidad

es asegurar la alineación estratégica entre las TI y los objetivos del negocio, promoviendo el uso eficiente de los recursos y un control adecuado de los riesgos. Este framework ofrece un conjunto estructurado de buenas prácticas, herramientas de análisis y modelos de madurez que fortalecen los procesos de toma de decisiones y favorecen el cumplimiento de las normativas en el entorno tecnológico. COBIT es un marco de gobernanza y gestión de la información, la tecnología se gestiona como una empresa en su conjunto, contiene los componentes y factores de diseño para construir y mantener el sistema de gobierno que la organización necesita (Awaludin Rizal et al., 2020).

La literatura confirma la vigencia de COBIT 4.1 como un marco sólido para la evaluación de procesos y objetivos de control en la gobernanza de tecnologías de la información. Kartika y Aprilinda (2019) desarrollaron una aplicación de gobernanza fundamentada en los dominios de planificación, organización, adquisición e implementación, empleando el modelo de madurez de COBIT 4.1 para identificar tanto el nivel actual como el nivel objetivo de procesos institucionales. Se evidencia que los objetivos de control definidos por COBIT 4.1 permiten valorar de manera precisa el grado de madurez de la gestión de TI y, al mismo tiempo, orientar recomendaciones de mejora plenamente alineadas con las metas estratégicas de la organización.

Dentro del campo de la seguridad de la información, COBIT 4.1 constituye un marco de trabajo que apoya la identificación, evaluación y control de los riesgos asociados a los sistemas de tecnologías de la información. Mediante la aplicación de prácticas estructuradas de gestión y control, permite establecer medidas que protegen los activos digitales y aseguran la continuidad de las operaciones organizacionales. Este framework se ha consolidado como un estándar ampliamente reconocido para la gobernanza y gestión de TI, al ofrecer un conjunto coherente de herramientas, principios y directrices que facilitan la consecución de los objetivos estratégicos, la gestión efectiva de riesgos y el cumplimiento de las exigencias regulatorias. COBIT 4.1 estructura la gestión de TI en diversos procesos, cada uno compuesto por un conjunto de actividades específicas. Cada proceso se encuentra regulado por múltiples objetivos de control, y todos ellos se evalúan

utilizando un conjunto común de atributos de madurez (Ariyadi & Dirgahayu, 2015). La Figura 10 muestra los dominios del framework COBIT 4.1.

La evolución de COBIT ha sido significativa desde su creación. COBIT 5 publicada en 2012 consolidó marcos anteriores como Val IT y Risk IT, ofreciendo una perspectiva integral orientada a la gobernanza de las tecnologías de la información. Posteriormente, COBIT 2019 incorporó actualizaciones significativas destinadas a responder a la evolución tecnológica y a los nuevos requerimientos organizacionales. Esta última versión destaca por su enfoque adaptable y flexible, permitiendo a las organizaciones ajustar la implementación del marco según sus características y necesidades particulares.

Diversos estudios han analizado la aplicación y efectividad de COBIT en diferentes contextos. Wolden et al. (2015) evaluaron la efectividad de la implementación del marco de seguridad de la información de COBIT 5 en la reducción de riesgos de ciberataques en sistemas de gestión de cadena de suministro, los resultados indicaron que COBIT 5 proporciona una estructura sólida para identificar y mitigar riesgos asociados a ciberataques, mejorando la postura de seguridad de las organizaciones.

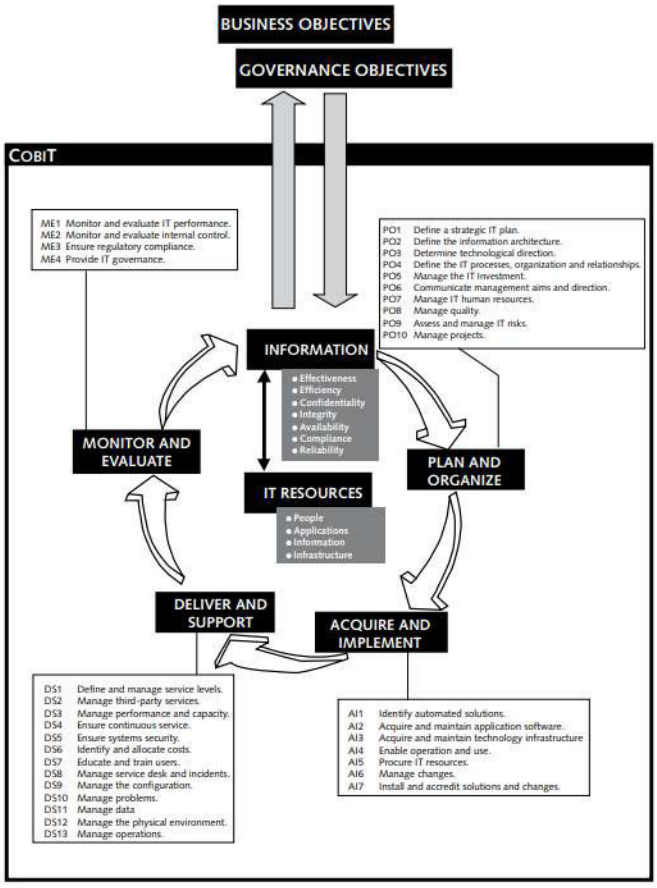


Figura 10. **Dominios del framework COBIT 4.1.**
Fuente. ISACA (2007)

COBIT 5 constituye un marco de referencia orientado a apoyar a las organizaciones en la definición de metas de gobernanza y en la planificación estratégica para maximizar el valor del negocio, permite la identificación y gestión de riesgos, así como la mejora en la prestación de servicios de tecnologías de la información (Tsai et al., 2015).

Kerr y Murthy (2013) consideran la importancia de los procesos de TI definidos por COBIT para la gestión efectiva de la seguridad de la información. El estudio subrayó que la implementación de los procesos de COBIT contribuye significativamente a la mejora de la seguridad de la información dentro de las organizaciones.

Amorim et al. (2021) sostienen que la flexibilidad de COBIT es objeto de análisis al explorar el uso de metodologías ágiles para la adopción de COBIT, proponiendo un enfoque que combina la estructura de COBIT con la adaptabilidad de las metodologías ágiles, facilitando una implementación más eficiente y adaptable a las necesidades cambiantes de las organizaciones.

COBIT se ha consolidado como un estándar internacionalmente reconocido para la gobernanza y gestión de TI, ofreciendo herramientas y prácticas que ayudan a las organizaciones a alcanzar sus objetivos estratégicos mientras gestionan eficazmente los riesgos y aseguran el cumplimiento normativo. Su aplicación en diversos sectores y contextos ha demostrado ser efectiva, y su evolución continua refleja su adaptabilidad a los desafíos emergentes en el ámbito de las tecnologías de la información.

h. USGCB y SCAP

Los ajustes de la Línea de base de Configuración del Gobierno de Estados Unidos USGCB (anteriormente FDCC) reemplazan la configuración del Federal Desktop Core Configuration (FDCC) y proporcionan líneas base de seguridad sugeridas para productos de tecnología de la información ampliamente implementados en agencias. El FDCC surgió de un esfuerzo por la Oficina de Administración y Presupuesto (OMB) para definir una configuración de escritorio estándar para PCs con Windows en el Gobierno Federal. El Protocolo de Automatización de Contenido Seguridad SCAP, fue desarrollado para promover la interoperabilidad entre los productos de seguridad dispares (Sun et al., 2022).

i. FISMA/NIST 800-53

La Ley Federal de Gestión de Seguridad de la Información sostiene la racionalización de los procesos de negocio para asegurar su continuidad, mejorar la eficiencia operativa y maximizar la seguridad de las infraestructuras de TI de las organizaciones (Joint Task Force, 2022).

j. ITIL Biblioteca de Infraestructura de Tecnología de la Información

El framework ITIL es una recopilación de prácticas diseñadas para gestionar servicios de TI, con un enfoque en su alineación con las necesidades empresariales, a pesar de afirmar que el riesgo debe ser identificado, medido y mitigado, no aclara cuál es el método concreto para ser utilizado en la gestión de riesgos. En cualquier marco de Gobierno de TI, se espera encontrar un conjunto de directrices de gestión de riesgos para hacer frente a las oportunidades y amenazas de la organización. En el marco COBIT, por ejemplo, hay un fuerte componente de manejo de riesgos basado en el control de todos los procesos de la organización. El marco de gobernanza de TI ITIL es menos amplio, el componente de gestión de riesgo está implícito en el proceso, pero en una forma muy abstracta, no evidente y no especifica cómo se desea el escenario de negocios real, todas las organizaciones requieren de estándares que alerten a sus clientes a la organización de procesos de calidad. En el ámbito de la gestión de riesgos y la gobernanza de TI existe la ISO 31000 y 20000. Para implementar la norma ISO 20000, ITIL suele ser la opción. Sin embargo, la gestión del riesgo no se muestra con claridad porque no hay una manera obvia para poner en práctica el manejo de riesgos en ITIL. Pese a la gestión de riesgos que se hace referencia en algunos de los libros de ITIL, está enfocado principalmente en optimizar la operación y garantizar la continuidad del servicio (Vilarinho & da Silva, 2011).

ITIL constituye un compendio de buenas prácticas orientadas a la gestión de las tecnologías de la información, así como al fortalecimiento de los niveles de soporte y calidad en los servicios de TI. Este marco es el más adoptado a nivel global para asegurar que los servicios tecnológicos se mantengan alineados con los objetivos estratégicos de la organización, incluso en contextos de cambio (Al-Ashmoery et al., 2021).

La seguridad de TI ha atraído considerable atención en los últimos años. En primer lugar, una industria centrada en la protección tiene evolucionado no sólo a través de software especializado, sino también a través de servicios de consultoría. En segundo lugar, las empresas deben cumplir con un volumen cada vez mayor de las legislaciones

vigentes. La Tercera, Las organizaciones están sometidas a una creciente presión para trabajar de acuerdo con estándares de seguridad ampliamente utilizados, como la familia de normas de seguridad ISO / IEC 27000 y Common Criteria. Los marcos de gestión COBIT e ITIL proporcionan pautas organizativas para la gestión de la seguridad y prometen legitimación. Si bien estos enfoques son importantes, no son suficientes para la planificación y administración de sistemas integrales de seguridad TI, ya que no abordan todos los retos. Hay una necesidad de un método para guiar el diseño de los sistemas de seguridad de TI que equilibre los objetivos y limitaciones de diversas perspectivas (Goldstein & Frank, 2016).

Con respecto al diseño de los lugares de trabajo informatizados existe permeabilidad en las normas comunes para la gestión de TI como ITIL y COBIT. Estas normas describen un conjunto de "mejores prácticas", incluyendo el aprovisionamiento de servicios de TI y el mantenimiento y operación de infraestructuras TI. La disposición y configuración de sistemas de TI es por lo tanto una parte de los servicios TI comunes, realizados por proveedores de servicios que puede ser el departamento de TI interno o subcontratado a un socio externo. El estándar ITIL no aborda el usuario único como el cliente de un servicio TI, si la organización en su conjunto. Por lo tanto, el tema de adaptación no se aborda en el estándar ITIL (ni por los usuarios finales solos ni en cooperación con el proveedor de servicios) (Draxler & Stevens, 2011).

Las organizaciones enfrentan diversos retos al implementar un marco de gobernanza de TI (ITG) que sea coherente e integrado, por lo que recurren a marcos de mejores prácticas en este ámbito. Estos marcos proporcionan definiciones y principios aplicables a empresas de distintos sectores y tamaños, permitiendo una mejor alineación entre la TI y los objetivos estratégicos de la organización. Entre los marcos de gobernanza de TI más reconocidos se encuentran COBIT, ITIL, ISO 27001 y el marco de gobernanza de TI Calder-Moir. La Tabla 4 presenta una comparación estructurada de los marcos COBIT, ITIL, ISO 27001.

Tabla 4. **Análisis comparativo de los marcos de gobernanza de TI.**

Área	**COBIT**	**ITIL**	**ISO 27001**
Función	Mapeo de procesos de TI	Gestión de niveles de servicio de TI	Marco de seguridad de la información
Área	4 procesos y 34 dominios	9 procesos	10 dominios
Entidad emisora	ISACA	OGC	ISO
Implementación	Auditoría de sistemas de información	Gestión del nivel de servicio	Cumplimiento con estándares de seguridad
Consultores	Firma de contabilidad, Firma de consultoría de TI	Firma de consultoría de TI	Firma de consultoría de TI, Firma de seguridad, Consultor de redes

Fuente: Alratrout et al. (2022).

2.2.7. COBIT 4.1 como modelo de madurez y evaluación

COBIT 4.1 ha sido tradicionalmente reconocido como un marco de gobernanza de tecnologías de la información enfocado en controles, procesos y mejores prácticas. No obstante, la literatura científica contemporánea demuestra que su utilidad trasciende el nivel de framework, ya que incorpora un modelo formal de madurez, derivado del Capability Maturity Model (CMM), que permite evaluar el grado de capacidad y desempeño de los procesos de TI. Este modelo de madurez es ampliamente utilizado para valorar niveles de desarrollo organizacional, identificar brechas de control y establecer planes de mejora continua en múltiples sectores.

Diversos estudios académicos demuestran que COBIT 4.1 no solo se utiliza como marco de trabajo o framework, sino que es tratado explícitamente como un modelo de madurez, un modelo de evaluación e incluso como un modelo formal de gobernanza. Fasihuddin et al. (2022) se refieren directamente al "COBIT model" y al "COBIT 4.1 maturity model" al aplicarlo para medir la madurez de la gobernanza de TI en organizaciones saudíes. Neto y Ferreira (2013) describen el modelo de madurez de COBIT 4.1 como un componente esencial para representar ontológicamente los procesos de gobernanza de TI, enfatizando que COBIT 4.1 incorpora un modelo de madurez derivado del CMM. Ariyadi y Dirgahayu (2015) utilizan explícitamente el "COBIT 4.1 maturity model", proponiendo un método de evaluación basado en los atributos de proceso de dicho modelo.

En estudios aplicados, Kartika y Aprilinda (2019) adoptan COBIT 4.1 como modelo para calificar la madurez de la gobernanza TI en empresas públicas, mientras que Tjhin (2014) aplica el modelo de madurez de COBIT 4.1 para auditar el proceso "Acquire and Implement" de una empresa de telecomunicaciones. En sectores no tradicionales, Žvanut et al. (2020) confirman la aplicabilidad del modelo de procesos y madurez de COBIT 4.1 en la mejora de calidad del sector salud, resaltando su uso directo como maturity model.

Finalmente, Debreceny y Gray (2013) realizan un estudio multinacional utilizando el COBIT 4.1 maturity model como modelo estándar para evaluar la madurez de procesos de TI en diversas organizaciones. La existencia de esta evidencia acumulada demuestra que COBIT 4.1 es reconocido en la literatura no solo como un marco general, sino como un modelo formal de madurez, gobernanza y evaluación, lo que valida plenamente su comparación con un modelo especializado dentro de un mismo nivel funcional de auditoría y evaluación de seguridad.

La síntesis de los principales estudios que consideran explícitamente a COBIT 4.1 como modelo, lo cual sustenta la validez del enfoque utilizado en esta investigación se aprecian en la Tabla 5.

Tabla 5. **Evidencia en la literatura que considera a COBIT 4.1 como modelo.**

Autor	Título del estudio	Referencia a COBIT 4.1	Relevancia en investigación
Fasihuddin et al. (2022)	Measuring the maturity of Information Technology Governance based on COBIT	Emplean los términos "COBIT model" y "COBIT 4.1 maturity model" para medir la madurez de la gobernanza TI	Evidencia directa de COBIT 4.1 como modelo formal de madurez
Neto y Ferreira (2013)	Metamodel of the IT governance framework COBIT	Describen el maturity model of COBIT 4.1 como parte estructural del marco	Refuerza que COBIT 4.1 incorpora un modelo de madurez reconocido académicamente
Ariyadi y Dirgahayu (2015)	Assessment to COBIT 4.1 maturity model based on process attributes and control objectives	El estudio se basa explícitamente en el "COBIT 4.1 maturity model"	Muestra que COBIT 4.1 funciona como modelo de evaluación de procesos TI
Kartika y Aprilinda (2019)	Maturity rating of information technology governance for SOE	Aplican COBIT 4.1 como modelo para determinar niveles de madurez en gobernanza TI	Evidencia COBIT 4.1 como modelo utilizado en el sector público
Tjhin (2014)	Audit Domain Acquire and Implement with COBIT 4.1	Utiliza COBIT 4.1 como modelo de madurez para evaluar auditoría TI	Confirma uso de COBIT 4.1 como modelo de auditoría aplicable
Žvanut et al. (2020)	Applicability of COBIT processes representation structure for quality improvement in healthcare: A Delphi study	Adoptan el COBIT 4.1 maturity model como referencia evaluativa	Demuestra aplicabilidad del modelo COBIT 4.1 fuera del sector TI tradicional
Debreceny y Gray (2013)	IT Governance and Process Maturity: A Multinational Field Study	Utilizan COBIT 4.1 como modelo estándar de madurez en organizaciones multinacionales	Prueba reconocimiento internacional de COBIT 4.1 como modelo maduro y consolidado

Fuente: Elaborada por el autor.

2.2.8. Requerimientos de Seguridad VoIP

Sin seguridad, los sistemas de gestión no pueden adaptarse a entornos no confiables a nivel mundial, tales como internet; sin interoperabilidad, no pueden interactuar con las herramientas existentes y los sistemas heredados. La creciente complejidad de los sistemas distribuidos a nivel mundial, a partir de un conjunto de recursos conectados por las infraestructuras de red a un conjunto de servicios coordinados centrados en la red, ha motivado la evolución de los modelos tradicionales de gestión (Bellavista et al., 1999).

La Telefonía sobre IP ha sido ampliamente desplegada, con el apoyo de la estandarización de protocolos de señalización y de transferencia de medios de comunicación de VoIP. Este despliegue también ha dado lugar a la aparición de varias amenazas de seguridad, incluidos los ataques heredados de la capa IP y ataques específicos a la capa de aplicación. Una gran variedad de mecanismos de seguridad se ha propuesto para hacer frente a ellos, pero estos mecanismos pueden degradar seriamente un servicio tan crítico.

La arquitectura en comunicaciones basadas en VoIP hace vulnerables los sistemas a múltiples vectores de ataque que pueden comprometer la confidencialidad, integridad y disponibilidad de las comunicaciones de voz. Estas amenazas se originan tanto en protocolos inseguros y configuraciones deficientes, como en la ausencia de mecanismos robustos de autenticación y monitoreo continuo. En consecuencia, las organizaciones que adoptan VoIP como medio principal de comunicación enfrentan riesgos significativos, ya que una intrusión o manipulación no solo puede afectar el flujo de datos en tiempo real, sino también derivar en pérdidas operativas y exposición de información sensible (Ramly et al., 2024).

Dado que el esquema de autenticación SIP original no proporciona autenticación mutua y no puede apoyar la integridad y la protección de la confidencialidad, adolece de

varios ataques. Por otra parte, el coste computacional del esquema de autenticación original es muy alta en los servidores proxy SIP. Por lo tanto, el esquema de autenticación original debe ser mejorado para satisfacer los requisitos de seguridad y eficiencia de SIP. Un protocolo eficiente y seguro de acuerdo de claves autenticado es crucial para proteger la información confidencial en las comunicaciones de audio de los servicios basados en SIP. Sin embargo, el protocolo de autenticación original de SIP sólo ofrece autenticación de un solo sentido y no puede apoyar la integridad y la protección de la confidencialidad en un nivel aceptable en la práctica. Por otro lado, dado que la autenticación original del protocolo SIP se basa en el mecanismo digest del Protocolo de Transferencia de Hipertexto (HTTP), el coste computacional resulta elevado en los servidores proxy SIP ampliamente utilizados. En este contexto, el trabajo de Zhang et al. (2016) presenta contribuciones relevantes, al proponer requisitos de seguridad especiales orientados a la protección de la privacidad, los cuales no habían sido considerados en la mayoría de estudios previos. Estas contribuciones incluyen: autenticación fuerte, mecanismos de protección de la privacidad y mayor eficiencia; además manifiesta que las medidas de seguridad suelen ser inversamente proporcionales al rendimiento, por lo cual se han propuesto varios protocolos de acuerdo de claves autenticadas para equilibrar la seguridad y la eficiencia, en este contexto el rendimiento es un aspecto relevante a tomar en cuenta dentro de la gestión de seguridad como un factor crítico que afecta directamente a las aplicaciones de voz, así como la eficiencia.

El esquema de autenticación para VoIP debe satisfacer varios requisitos de seguridad y eficiencia, con el fin de cumplir con varios objetivos, entre ellos proveer seguridad contra diversos ataques, proporcionar elementos de seguridad y generar protección de la privacidad.

La transmisión de los flujos VoIP es sensible para la calidad de servicio (QoS), tres cuestiones se toman con frecuencia como criterios de evaluación: retardo de extremo a extremo, retraso jitter y pérdida de paquetes (Zhang & Fischer, 2019).

2.3. Estado del arte

El análisis del estado del arte permitió situar el problema de investigación dentro del panorama actual de avances científicos y tecnológicos. En el ámbito de VoIP, la literatura refleja una evolución constante en su implementación, acompañada por un aumento proporcional en los riesgos asociados a su seguridad. Esta situación ha impulsado una notable producción académica enfocada en la identificación de vulnerabilidades, el diseño de marcos regulatorios y la formulación de estrategias de protección. No obstante, muchas de estas contribuciones evidencian limitaciones al ser aplicadas en contextos operativos reales, principalmente por su escasa orientación hacia auditorías especializadas, la insuficiente atención a amenazas derivadas de la ingeniería social y la falta de modelos operativos ajustados a las particularidades de las comunicaciones VoIP. A partir de este análisis y acorde a las preguntas de investigación, se identificaron cinco líneas temáticas prioritarias: los antecedentes relevantes sobre seguridad en entornos VoIP, los requerimientos técnicos específicos para su protección, la evaluación crítica de frameworks existentes y su correspondencia con dichos requerimientos, los enfoques sobre cultura organizacional y riesgos humanos, y los estudios centrados en procedimientos especializados de auditoría en este tipo de entornos.

2.3.1. Protocolo de revisión del estado del arte

La revisión del estado del arte se realizó siguiendo un enfoque sistemático y riguroso, con el objetivo de identificar, analizar y sintetizar la literatura científica y técnica más relevante relacionada con la seguridad y auditoría en sistemas VoIP. Este proceso metodológico se estructuró en cinco etapas principales:

- *Definición de los objetivos de la revisión*

Se estableció como propósito de la revisión examinar las investigaciones previas, marcos de trabajo (frameworks), normativas, metodologías de auditoría, requerimientos de seguridad, amenazas emergentes (como la ingeniería social) y las carencias existentes en el ámbito de la seguridad VoIP.

- *Estrategia de búsqueda*

Se diseñó una estrategia de búsqueda mediante la combinación de palabras clave y operadores booleanos. Las búsquedas se ejecutaron en las siguientes bases de datos académicas de alto impacto: IEEE Xplore, ScienceDirect (Elsevier), SpringerLink, Scopus, Web of Science. Se incluyeron whitepapers técnicos de instituciones reconocidas como ISACA, NIST, entre otros organismos internacionales de ciberseguridad.

- *Palabras clave utilizadas:*

"VoIP security", "VoIP audit", "VoIP vulnerabilities", "security audit frameworks", "social engineering VoIP", "VoIP risk management", "auditing methodologies", "security culture VoIP", "VoIP threat modeling", entre otras.

- *Criterios de inclusión y exclusión*

Se definieron los siguientes criterios para garantizar la relevancia y actualidad de la información:

Criterios de inclusión:

- Publicaciones científicas revisadas por pares.
- Documentos técnicos y guías de organismos especializados.
- Estudios empíricos, revisiones sistemáticas, y casos de uso aplicados a VoIP.

Criterios de exclusión:

- Documentos sin respaldo institucional ni científico.
- Publicaciones duplicadas.
- Artículos centrados únicamente en aspectos generales de TI sin aplicación específica a VoIP.

- *Evaluación y síntesis de resultados*

Se organizó la información recopilada identificando patrones, vacíos de investigación y convergencias teóricas. La información se clasificó en torno a cuatro ejes temáticos alineados con las preguntas de investigación:

- Requerimientos específicos de seguridad en VoIP.
- Evaluación de frameworks y su alineación con VoIP.
- Cultura de seguridad y ataques de ingeniería social.
- Procedimientos de auditoría específicos para VoIP.

- *Validación y trazabilidad*

Para garantizar la trazabilidad de los datos y la transparencia del proceso, se mantuvo un registro de búsqueda documentado que incluye: bases de datos consultadas, términos de búsqueda, artículos revisados y seleccionados, y síntesis de la información clave. Este registro se presenta en el apartado correspondiente al Marco Epistemológico (sección 2.1).

2.3.2. Antecedentes de investigación

La implementación de VoIP ha transformado las comunicaciones permitiendo la transmisión de voz mediante redes IP y con ello los consecuentes desafíos significativos en términos de seguridad de la información. Garantizar integridad, disponibilidad y confidencialidad en las comunicaciones y los datos en sistemas VoIP se ha convertido actualmente en una prioridad crítica para las organizaciones.

La tecnología VoIP ha emergido como una solución ampliamente adoptada en el ámbito de las telecomunicaciones debido a su eficiencia económica y adaptabilidad operativa. No obstante, su uso generalizado ha intensificado la exposición a diversas amenazas y riesgos de seguridad que deben ser gestionados de manera rigurosa (Ramly et al., 2024). A diferencia de los sistemas telefónicos convencionales, VoIP se basa en infraestructuras de red de datos basadas en el protocolo IP, lo que implica que hereda las vulnerabilidades inherentes a dichas redes. Además, incorpora riesgos específicos asociados al tráfico de voz digitalizado. Desde mediados de la década del 2000, diversos estudios ya anticipaban que la convergencia entre servicios de voz y datos introduciría desafíos adicionales para garantizar la seguridad de las comunicaciones en entornos corporativos (Kumar & Roy, 2021).

Actualmente, dichas inquietudes se mantienen plenamente vigentes, ya que la arquitectura abierta de las infraestructuras VoIP continúa representando una superficie de exposición crítica frente a diversas amenazas, tales como la interceptación de comunicaciones, suplantación de identidad, ataques DoS, entre otros vectores que explotan vulnerabilidades específicas de sus protocolos subyacentes (Ramly et al., 2024).

Estudios de casos y ejemplos de incidentes en la industria como vulnerabilidades explotadas, filtración de conversaciones y abuso de servicios de VoIP, demuestran la importancia y necesidad de una auditoría de seguridad efectiva en plataformas VoIP para identificar y mitigar riesgos. Según Suthar y Rughani (2020) gran parte de las organizaciones que han adoptado servicios de VoIP desconocen o ignoran los problemas de seguridad y vulnerabilidades de VoIP, una red susceptible de abuso y fácil de explotar mediante ataques como DoS, manipulación de registros y secuestro, ataques de autenticación, identificador de llamadas, suplantación de identidad, ataques de intermediario, escuchas pasivas y activas entre otros.

Diversas investigaciones realizadas en la última década han clasificado las amenazas asociadas a los entornos VoIP. Ramly et al. (2024) exponen una clasificación de ataques organizada en distintas categorías, que incluyen DoS y ataques de intermediario MitM, suplantación de identidad (spoofing), secuestro de llamadas, spam telefónico (SPIT), fraudes por voz (vishing), software malicioso y fraude relacionado con tarifas de llamadas. Esta diversidad de vectores de ataque evidencia que los sistemas VoIP están expuestos tanto a amenazas compartidas con otros servicios basados en red como a riesgos específicos inherentes a las comunicaciones de voz. Las vulnerabilidades en infraestructuras VoIP no sólo permiten el acceso no autorizado, sino que alimentan ecosistemas completos de llamadas maliciosas. Carrillo et al. (2022) desplegaron un honeypot VoIP basado en Asterisk expuesto a Internet y registraron alrededor de 300 000 intentos de llamada dirigidos a cuentas con credenciales débiles, provenientes de más de 2 200 direcciones IP únicas y asociados a más de 200 000 números telefónicos distintos; se evidencia que los sistemas VoIP comprometidos se utilizan de forma sistemática para diferentes esquemas de fraude telefónico, lo que pone de manifiesto la necesidad de

abordar los riesgos específicos de seguridad VoIP mediante mecanismos de protección y modelos de gestión de amenazas especializados.

Estudios contemporáneos han aportado revisiones integrales sobre el estado actual de la seguridad en VoIP. En este sentido, Kumar y Roy (2021) presentan una visión detallada de los principales desafíos que enfrenta esta tecnología, así como de los requisitos necesarios en términos de protección, destacando que el crecimiento acelerado en su adopción por parte de las organizaciones amplía considerablemente la superficie de exposición frente a amenazas potenciales. De manera similar, Ramly et al. (2024) sostienen que, si bien se han desarrollado soluciones orientadas a mitigar ciertos riesgos, estas aún resultan insuficientes para garantizar una protección sólida e integral de los sistemas VoIP, evidenciando brechas persistentes en su infraestructura de seguridad. En síntesis, los estudios revisados coinciden en que la incorporación de VoIP ha transformado significativamente el panorama de amenazas, lo cual demanda enfoques especializados que permitan equiparar sus niveles de protección con los exigidos en otras infraestructuras tecnológicas críticas.

La literatura existente en cuanto a seguridad de VoIP y auditoría de seguridad ofrece una base sólida para la investigación, en este sentido estudios anteriores han identificado vulnerabilidades específicas en entornos VoIP que pueden comprometer tanto la confidencialidad como disponibilidad en las comunicaciones. Varias investigaciones sobre métodos de encriptación y autenticación en VoIP resaltan la importancia de aplicar medidas de seguridad efectivas para proteger la autenticidad de los usuarios y la integridad de las conversaciones.

Respecto a auditoría de seguridad existen enfoques generales que abordan el análisis de sistemas de TI, sin embargo, VoIP requiere una adaptación particular de dichos enfoques. Investigaciones sobre auditoría de sistemas y redes han proporcionado marcos de trabajo para evaluar la conformidad con estándares de seguridad y mejores prácticas, no obstante, la aplicación de estas metodologías en sistemas VoIP aún no se ha explorado a fondo.

Durante las últimas décadas, las estrategias de fraude han estado en constante evolución en la industria de las telecomunicaciones, desde enfoques simples para realizar llamadas gratuitas en los primeros días hasta esquemas complejos basados en múltiples partes interesadas, redes y tecnologías. La identificación oportuna de conductas fraudulentas es sumamente importante en esta industria. Según la Encuesta Global de Pérdidas por Fraude de 2015 realizada a proveedores de servicios de telecomunicaciones, la pérdida monetaria que el fraude causó ese año se estimó en 38.100 millones de dólares estadounidenses, lo que representa el 1,69% de los ingresos globales. Sin embargo, la pérdida monetaria no es el único problema causado por los intentos de fraude exitosos. Los casos fraudulentos pueden dañar gravemente la reputación de una empresa, especialmente si provocan la interrupción del servicio (Irarrázaval et al., 2021).

La seguridad en VoIP es un aspecto crítico dentro del ecosistema de comunicaciones modernas, especialmente considerando su integración con el Internet de las Cosas (IoT). A pesar de su creciente adopción, muchos sistemas VoIP aún operan en configuraciones tradicionales sin medidas de seguridad adecuadas, lo que los expone a múltiples amenazas. Biondi et al. (2020) han identificado la familia de ataques Phonejack, los cuales evidencian diversas vulnerabilidades en los teléfonos VoIP: Phonejack 1 explota fallos en los dispositivos, Phonejack 2 permite ejecutar ataques DoS en redes telefónicas y Phonejack 3 posibilita el rastreo de llamadas. Esta situación resalta la necesidad de implementar medidas de seguridad adicionales, ya que confiar únicamente en las protecciones de la red subyacente puede ser una estrategia insuficiente.

Laurens et al. (2022) consideran que, aunque el tráfico VoIP se encuentre completamente cifrado y protegido, la implementación de la supresión de silencio en estos sistemas podría ser aprovechada por un atacante para analizar y reconocer mensajes de voz automatizados en servicios de atención al cliente. Este ataque de canal lateral permitiría no solo identificar con precisión el número de servicio al cliente al que se realiza la llamada, sino también determinar las opciones seleccionadas por el usuario durante la interacción.

Los antecedentes de investigación indican la existencia de desafíos de seguridad específicos en la implementación de VoIP y la consecuente importancia de la auditoría de seguridad como una herramienta para abordar dichos desafíos. En este sentido existe la necesidad de un modelo específico que integre los conocimientos y las mejores prácticas de seguridad en VoIP con enfoques de auditoría. La presente investigación busca cerrar esta brecha al implementar un modelo de auditoría de seguridad VoIP como una estrategia adecuada para proteger las infraestructuras de TI y asegurar la protección de las comunicaciones empresariales en sistemas VoIP.

2.3.3. Investigaciones sobre requerimientos específicos de seguridad en sistemas VoIP

La protección de las comunicaciones VoIP exige la implementación de mecanismos de autenticación y control de acceso más robustos que los utilizados en redes tradicionales. En plataformas basadas en el Protocolo de Internet, la ausencia de verificaciones fuertes de identidad permite que actores maliciosos suplanten terminales, manipulen la señalización SIP o intercepten flujos RTP en tránsito. Los esquemas de autenticación convencionales resultan insuficientes frente a ataques contemporáneos, como el secuestro de sesiones, la manipulación de invitaciones SIP y el acceso no autorizado a recursos internos. La autenticación mutua, junto con la gestión segura de claves y la validación estricta de credenciales, reduce de manera significativa la superficie de ataque en VoIP. Los modelos de seguridad que integran autenticación reforzada y políticas de control de acceso granular permiten mitigar amenazas críticas, garantizando que solo usuarios, dispositivos y servicios legítimos puedan participar en la comunicación (Youness, 2023).

La suplantación de identidad en llamadas, conocida como Caller ID spoofing, ha sido identificada como una de las amenazas más significativas en contextos de comunicación VoIP, en consecuencia, se vuelve imprescindible implementar mecanismos de autenticación robustos durante las fases de registro y señalización (por ejemplo, el uso de SIP con autenticación mutua), con el fin de garantizar que únicamente usuarios y

dispositivos autorizados puedan iniciar o recibir comunicaciones VoIP (Tas & Baktir, 2024).

Estudios recientes han explorado el empleo de técnicas criptográficas avanzadas como alternativa para reforzar los mecanismos de autenticación en entornos VoIP, Jaber (2022) analiza la aplicación de criptografía de clave simétrica y asimétrica en entornos VoIP, subrayando la importancia de fortalecer los mecanismos basados en clave pública ante el creciente nivel de sofisticación de los atacantes. Los sistemas VoIP actuales deben implementar protocolos de seguridad como SIP sobre TLS y SRTP, con el fin de proteger la confidencialidad y mantener la integridad de las comunicaciones en tiempo real.

La arquitectura VoIP exige mecanismos de protección robustos para garantizar comunicaciones seguras, debido a que su funcionamiento depende de protocolos abiertos y de la transmisión de paquetes en redes potencialmente expuestas. La ausencia de configuraciones adecuadas permite que las comunicaciones sean vulnerables a interceptación, espionaje, ataques de denegación de servicio y manipulación de tráfico. La aplicación sistemática de cifrado en la señalización y en los flujos de medios, junto con procesos de autenticación y control de acceso, constituye un requisito esencial para mitigar riesgos inherentes a la transmisión de voz sobre redes IP. La seguridad no debe considerarse como un componente aislado, sino como un elemento transversal que condiciona la confiabilidad, disponibilidad y calidad global del servicio VoIP, por lo que su diseño y operación requieren políticas específicas y un modelo de gestión alineado con estas amenazas emergentes (Kishore et al., 2024).

En el contexto de redes corporativas basadas en VoIP, resulta esencial limitar la exposición del tráfico de voz y señalización a segmentos no confiables de la infraestructura. Estudios recientes sobre el despliegue seguro de IP-PBX demuestran que el análisis del tráfico y la identificación de vulnerabilidades permiten detectar escenarios en los que es factible la intercepción de llamadas y el acceso no autorizado a los servidores de telefonía. La incorporación de mecanismos de cifrado como TLS en la señalización SIP, junto con un diseño de red que enfatice el control de acceso y la correcta

segmentación, contribuye a proteger la confidencialidad e integridad de las comunicaciones, reduciendo de forma significativa el riesgo de que el tráfico VoIP pueda ser capturado o manipulado en tránsito (Yakubova et al., 2023). En síntesis, asegurar la confidencialidad de las comunicaciones mediante técnicas de cifrado, ya sea a través de protocolos como SRTP a nivel de aplicación, o mediante mecanismos como VPN o IPsec a nivel de red, constituye un requisito imprescindible para garantizar la seguridad en entornos VoIP.

La integridad de los flujos de señalización en entornos VoIP es un requisito clave para garantizar que los mensajes de control (por ejemplo, INVITE, BYE) no sean modificados o falsificados durante la transmisión. El protocolo S-SIP aborda precisamente esta necesidad al incorporar mecanismos de protección de integridad en la señalización SIP, mediante distribución de claves, autenticación mutua y algoritmos criptográficos (Younes & Albalawi, 2022).

De igual forma, resulta imprescindible garantizar la disponibilidad y la calidad del servicio (QoS), debido a que las comunicaciones VoIP presentan una alta susceptibilidad a la latencia y a la pérdida de paquetes. En este sentido, los sistemas deben diseñarse con mecanismos de resiliencia que les permitan resistir ataques DoS, los cuales buscan colapsar los servidores SIP o saturar el ancho de banda, comprometiendo así la continuidad y fiabilidad de la comunicación (Ramly et al., 2024).

En los entornos VoIP, la disponibilidad se configura como un componente esencial de la seguridad, ya que cualquier interrupción en el servicio de voz compromete directamente la continuidad operativa de la organización y puede ser utilizada como una táctica de distracción para facilitar intrusiones adicionales. Diversos estudios han evidenciado que la adopción de mecanismos como la limitación de la tasa de solicitudes (rate limiting), la implementación de controladores de borde de sesión (Session Border Controllers, SBCs) y el despliegue de arquitecturas redundantes contribuyen significativamente a mantener una alta disponibilidad, incluso frente a escenarios de ataque deliberado (Khan et al., 2021).

Un requerimiento adicional, vinculado al surgimiento de nuevas problemáticas, es la implementación de mecanismos para el filtrado de comunicaciones no deseadas y la mitigación de amenazas de ingeniería social. La proliferación de spam en entornos de telefonía IP (SPIT) y las llamadas con fines fraudulentos evidencian la necesidad de incorporar herramientas capaces de identificar y bloquear llamadas automatizadas con comportamiento malicioso. En este sentido, Ramly et al. (2024) destacan tanto el SPIT como el vishing entre los vectores de ataque prioritarios en VoIP, lo que implica que las soluciones de seguridad deben contemplar funcionalidades como listas de bloqueo dinámicas, mecanismos de verificación interactiva (por ejemplo, CAPTCHA de voz) y estrategias complementarias que permitan diferenciar comunicaciones legítimas de intentos de intrusión.

Finalmente, los aspectos relacionados con la seguridad física y la correcta configuración de los dispositivos VoIP constituyen una dimensión que no puede ser ignorada. Es fundamental proteger los terminales (como teléfonos IP y adaptadores) frente a manipulaciones no autorizadas, establecer contraseñas robustas para el acceso a buzones de voz y desactivar funciones innecesarias que puedan ampliar la superficie de ataque.

En síntesis, la literatura especializada reciente coincide en que los entornos VoIP deben adherirse a un conjunto riguroso de requisitos de seguridad, entre los que se incluyen: mecanismos de autenticación robustos, cifrado e integridad de extremo a extremo, resiliencia frente a ataques DoS, así como controles específicos contra comunicaciones no deseadas y fraudes. Todo ello debe enmarcarse dentro de un enfoque integral de ciberseguridad, basado en buenas prácticas como la aplicación de actualizaciones periódicas, la segmentación de redes y el monitoreo constante del entorno (Ramly et al., 2024).

Varios requerimientos básicos de seguridad para sistemas VoIP según Zhang et al. (2016) y Zhang & Fischer (2019) se consolidan en la Tabla 6.

Tabla 6. **Requerimientos básicos de seguridad para sistemas VoIP.**

Requerimiento	**Autor**	**Trabajo**	**Justificación**
Autenticación	(Zhang et al., 2016)	Un protocolo ligero de acuerdo de claves autenticado con preservación de la privacidad para VoIP basado en SIP	Las medidas de seguridad suelen ser inversamente proporcionales al rendimiento. El esquema de autenticación SIP original no proporciona autenticación mutua y no puede apoyar la integridad y la protección de la confidencialidad Los requisitos de seguridad especiales para protección de privacidad, que no han sido considerados en la mayoría de los trabajos previos son: autenticación fuerte, la protección de privacidad y eficiencia. El esquema de autenticación para VoIP debe satisfacer varios requisitos de seguridad y eficiencia, con el fin de cumplir con varios objetivos, entre ellos: proveer seguridad contra diversos ataques, proporcionar elementos de seguridad y generar protección de la privacidad
Integridad			
Confidencialidad			
Privacidad			
Eficiencia			
Rendimiento			
Seguridad contra diversos ataques			
Elementos de seguridad			
Calidad de servicio QoS	(Zhang & Fischer, 2019)	Un estudio sobre comunicación anónima de voz sobre IP: ataques y defensas	La transmisión de los flujos VoIP es sensible para la calidad de servicio (QoS), tres cuestiones se toman con frecuencia como criterios de evaluación: retardo de extremo a extremo, retraso jitter y pérdida de paquetes

Fuente: Elaborada por el autor.

Gonzalez et al. (2012) realizaron una clasificación de varios problemas de seguridad potenciales determinando las siguientes categorías: seguridad de la red, interfaces, seguridad de datos, virtualización, gobernanza, cumplimiento, asuntos legales e ingeniería social. Su adaptabilidad a sistemas VoIP se muestra consolidada en las Tablas 7 - 14.

Tabla 7. **Seguridad de la red.**

Categoría	Descripción	Subcategorías	Justificación
Seguridad de la red	Problemas asociados con las comunicaciones de red y configuraciones	seguridad en la transferencia	Arquitecturas, intercambio de recursos (mecanismos de protección contra ataques: sniffing, spoofing, man-in-the-middle)
		cortafuegos	Los cortafuegos protegen la infraestructura de red contra propios y extraños, prevención de denegación de servicio (DoS) y los procedimientos de evaluación y detección de la seguridad (necesidad de adaptar soluciones existentes)
		configuración de seguridad	Configuración de protocolos, sistemas y tecnologías para proporcionar los niveles requeridos de seguridad y privacidad sin comprometer el rendimiento o eficiencia

Fuente: Elaborada por el autor.

Tabla 8. **Interfaces.**

Categoría	Descripción	Subcategorías	Justificación
Interfaces	Concentra todas las cuestiones relacionadas con las interfaces de usuario, administración y programación para el uso y control	API	Interfaces de programación para acceder a los recursos y sistemas virtualizados (protección con el fin de prevenir el uso malicioso)
		Interfaz administrativa	Permite el control remoto de los recursos, el desarrollo (codificación, despliegue, pruebas) y herramientas de aplicación (gestión de acceso de usuarios, configuraciones)
		Interfaz del usuario	Interfaz del usuario final para explorar proporcionados recursos y herramientas (el servicio en sí), lo que implica la necesidad de adoptar medidas para proteger el entorno
		Autenticación	Mecanismos necesarios para permitir el acceso al sistema. La mayoría de los servicios se basan en cuentas regulares en consecuencia son susceptibles a ataques

Fuente: Elaborada por el autor.

Tabla 9. **Seguridad de datos.**

Categoría	Descripción	Subcategorías	Justificación
Seguridad de datos	Protección de datos en términos de confidencialidad, disponibilidad e integridad	Criptografía	Para asegurar los datos sensibles, requeridos por la industria, el estado y las regulaciones federales.
		Redundancia	Fundamental para prevenir la pérdida de datos, asegurando la disponibilidad e integridad.
		Eliminación	Técnicas de eliminación de datos elementales son insuficientes, la destrucción completa de los datos, incluidas las referencias de registro y los registros de copias de seguridad ocultas, es un requisito importante.

Fuente: Elaborada por el autor.

Tabla 10. **Virtualización.**

Categoría	Descripción	Subcategorías	Justificación
Virtualización	Aislamiento entre máquinas virtuales, las vulnerabilidades de hipervisor y otros problemas asociados a la utilización de las tecnologías de virtualización.	Aislamiento	Aunque lógicamente aislado, todas las máquinas virtuales comparten el mismo hardware y en consecuencia los mismos recursos, permitiendo a las entidades maliciosas explotar las fugas de datos y ataques cross-VM
		Hypervisor de vulnerabilidades	El hipervisor es el componente principal del software de virtualización. A pesar de que se conocen las vulnerabilidades de seguridad para hipervisores, las soluciones son todavía escasas y muchas veces de propiedad, exigiendo más estudios para estos aspectos de seguridad.
		Fuga de datos	El hipervisor para Exploit de vulnerabilidades y la falta de controles de aislamiento para filtrar datos de infraestructuras virtualizadas, generan datos sensibles, afectando su confidencialidad e integridad.
		Identificación VM	Falta de controles para la identificación de las máquinas virtuales que se están utilizado para la ejecución de un proceso específico o para el almacenamiento de archivos.

Categoría	Descripción	Subcategorías	Justificación
		Ataques Cross-VM	Incluye los intentos para estimar las tasas de tráfico del proveedor con el fin de robar claves criptográficas y aumentar las posibilidades de ataques Cross-VM.

Fuente: Elaborada por el autor.

Tabla 11. **Gobernanza.**

Categoría	Descripción	Subcategorías	Descripción
Gobernanza	Temas relacionados con controles administrativos y de seguridad.	Control de datos	Control de redundancia, ubicación, sistemas de archivos y otras configuraciones pertinentes.
		Control de seguridad	Pérdida de la gobernabilidad sobre mecanismos y políticas de seguridad, prohibición de evaluación de condiciones de uso del lado del cliente respecto a pruebas de vulnerabilidad y penetración y Acuerdos de Nivel de Servicio insuficientes (SLA) conducen a brechas de seguridad.
		Bloqueo	Dependencia de usuario potencial de un proveedor de servicio en particular debido a la falta de normas bien establecidas, pueden generar vulnerabilidades de migración y terminación del servicio.

Fuente: Elaborada por el autor.

Tabla 12. **Cumplimiento.**

Categoría	Descripción	Subcategorías	Justificación
Cumplimiento	Requisitos relativos a las capacidades de la disponibilidad del servicio y de auditoría.	Acuerdos de Nivel de Servicio (SLA)	Mecanismos que permitan garantizar la continuidad del servicio y procedimientos básicos de seguridad que deben adoptarse.
		Pérdida de servicio	Cortes de servicio, necesidad de fuertes políticas de recuperación de desastres y recomendaciones del proveedor para implementar la redundancia del lado del cliente si procede.

Categoría	Descripción	Subcategorías	Justificación
		Auditoría	Permite evaluaciones de seguridad y disponibilidad, metodologías eficientes son necesarias para el análisis de forma continua de las condiciones de servicio y por lo general obligaciones por contratos legales o reglamentarios.
		Conformidad de servicio	Las obligaciones y los requisitos generales de servicios contractuales deben ser respetados, ofrecer SLAs predefinidos, necesidades de servicio y atención al cliente básicas.

Fuente: Elaborada por el autor.

Tabla 13. **Asuntos legales.**

Categoría	Descripción	Subcategorías	Justificación
Asuntos legales	Aspectos relacionados con los requisitos de ley y judiciales, como ubicaciones de datos y gestión de privilegios.	Ubicación de datos	Los datos del cliente, en múltiples jurisdicciones en función de la ubicación geográfica se ven afectados, directa o indirectamente, por las medidas de aplicación legales
		E-descubrimiento	Como resultado de medidas de aplicación de la ley, el hardware podría ser confiscado para las investigaciones relacionadas con un cliente en particular, que afecta a todos los clientes cuyos datos se almacenan en el mismo hardware. La divulgación de datos es fundamental en este caso.
		Privilegio de los proveedores	Maliciosas actividades generadas en el entorno de los proveedores son amenazas potenciales a la integridad, disponibilidad y confidencialidad de la información de los clientes y procesos.
		Legislación	Preocupaciones jurídicas relacionadas con los nuevos conceptos introducidos por VoIP

Fuente: Elaborada por el autor.

Tabla 14. **Ingeniería social.**

Categoría	Descripción	Subcategorías	Justificación
Ingeniería Social	La ingeniería social es la adquisición de información sobre los sistemas informáticos mediante métodos que incluyen profundamente medios no técnicos	Vulnerabilidad	La ingeniería social es la adquisición de información sobre los sistemas informáticos mediante métodos que incluyen profundamente medios no técnicos. Mientras que la seguridad técnica de la mayoría de los sistemas críticos es alta, los sistemas siguen siendo vulnerables a los ataques de los ingenieros sociales (Beckers et al., 2015). Las amenazas sociales representan una combinación fatal de bajo costo de implementación y alta efectividad (Chiappetta et al., 2013).
		Innovación	Existe falta de preocupación por la ingeniería social, en la literatura profesional de la informática, los escritores e investigadores dedican su tiempo exclusivamente a los "problemas de seguridad técnica".
		Confidencialidad	Seguridad de que la información no sea revelada a personas no autorizadas.
		Disponibilidad	Disponibilidad confiable y puntual de datos y servicios de información para usuarios autorizados.
		Integridad	Los datos deben estar protegidos contra la modificación o destrucción no autorizada.
		Administración de riesgos empresariales	La administración de riesgos se puede adaptar para satisfacer las necesidades de cada negocio. Se puede utilizar para educar al personal, y darles una comprensión más profunda de los riesgos corporativos (Sadgrove, 2016).

Fuente: Elaborada por el autor.

2.3.4. Evaluación de frameworks de seguridad y su alineación con requerimientos VoIP

Para garantizar una gestión integral de la seguridad en entornos VoIP, es fundamental apoyarse en marcos de referencia consolidados en ciberseguridad, evaluando su capacidad para abordar los riesgos específicos que presentan estas tecnologías. Un marco de referencia ampliamente utilizado es el NIST Cybersecurity Framework (CSF),

cuyo enfoque basado en cinco funciones fundamentales (Identificar, Proteger, Detectar, Responder y Recuperar) puede ser aplicado al contexto de VoIP. En este sentido, su implementación implica inicialmente reconocer los activos críticos asociados a VoIP, tales como servidores SIP, gateways y terminales, junto con sus respectivas vulnerabilidades.

Posteriormente, se requiere establecer controles de protección específicos, como el cifrado mediante SRTP, firewalls adaptados a VoIP y segmentación de red mediante VLAN para tráfico de voz. Asimismo, es necesario implementar mecanismos de detección de incidentes mediante sistemas de monitoreo de tráfico y sistemas de detección de intrusiones (IDS) adaptados a protocolos de voz. La función de respuesta contempla la ejecución de procedimientos ante incidentes de seguridad, como la notificación inmediata de accesos no autorizados al servidor Call Manager.

Finalmente, la capacidad de recuperación debe incluir copias de respaldo de configuraciones críticas y planes de contingencia que garanticen la continuidad de las comunicaciones. Aunque el CSF no prescribe controles técnicos específicos, su aplicabilidad al entorno VoIP puede verse fortalecida cuando se complementa con normas técnicas detalladas, como los controles definidos por la ISO/IEC 27001, particularmente en lo que respecta a la gestión segura de infraestructuras VoIP. Diversos investigadores coinciden en que los marcos de seguridad de carácter general requieren adaptaciones específicas para su aplicación efectiva en entornos VoIP. Un aspecto particularmente delicado es el equilibrio entre los requisitos de seguridad y el desempeño del servicio. Estrategias convencionales como la inspección profunda de paquetes o el uso de cifrado de alta intensidad pueden afectar negativamente la calidad de las llamadas, generando latencia, fluctuaciones (jitter) y pérdida de paquetes. Kuhn et al. (2005) advertían sobre la necesidad de adaptar los mecanismos de seguridad de red para responder a la naturaleza altamente sensible al tiempo de las aplicaciones VoIP.

En consecuencia, la evaluación de los frameworks de seguridad debe considerar en qué medida sus controles se articulan con los requerimientos de calidad de servicio

(QoS) propios de los entornos VoIP. Un caso ilustrativo es la aplicación del enfoque Zero Trust, el cual demanda la autenticación y autorización explícita de cada flujo de comunicación, eliminando cualquier suposición de confianza implícita en la red. La implementación de este modelo en VoIP requiere soluciones técnicas que garanticen seguridad sin comprometer el rendimiento. En esta línea, Fox et al. (2023) desarrollaron y validaron experimentalmente un prototipo de arquitectura Zero Trust aplicado a comunicaciones VoIP, evidenciando su viabilidad para lograr una protección efectiva sin deterioro significativo en la calidad del servicio. Las conclusiones extraídas del estudio evidencian que es factible alcanzar elevados estándares de seguridad como la microsegmentación del tráfico de voz y la autenticación continua de dispositivos terminales, sin comprometer de manera relevante la calidad de la experiencia del usuario en las llamadas. Esta integración exitosa refleja una adecuada correspondencia entre los principios de un framework moderno como Zero Trust y los requerimientos particulares de los entornos VoIP, permitiendo enfrentar amenazas actuales mediante una perspectiva integral y adaptativa.

También resulta pertinente tener en cuenta los marcos normativos y guías específicas por sector. Un ejemplo es la guía NIST SP 800-58, enfocada en la seguridad de VoIP, que, a pesar de haber sido publicada en 2005, continúa siendo un documento de referencia. Esta guía resalta la importancia de medidas como la segmentación de las redes de voz y datos, así como la utilización de protocolos seguros. De hecho, muchas de las buenas prácticas promovidas por marcos de ciberseguridad actuales se fundamentan en estos principios iniciales. Por otro lado, frameworks orientados a la gobernanza y auditoría, como COBIT desarrollado por ISACA, contemplan dentro de sus controles la gestión de los servicios de comunicación. ISACA incluso ha desarrollado un programa específico de aseguramiento para entornos VoIP, centrado particularmente en aspectos clave como el control de acceso, la autenticación y el cifrado. Esto pone de manifiesto que los marcos de auditoría ampliamente reconocidos integran puntos de control alineados con las necesidades críticas de seguridad en VoIP, tales como verificar la existencia de mecanismos robustos de autenticación y cifrado en las comunicaciones de voz (Malhotra, 2018).

A partir del análisis del estado del arte, se evidencia que, si bien existe una creciente convergencia entre los marcos generales de ciberseguridad y las necesidades específicas de los entornos VoIP, aún subsisten vacíos. Investigaciones recientes recomiendan la expansión de las guías actuales para contemplar contextos emergentes, como la telefonía IP en la nube y las soluciones de comunicaciones unificadas en dispositivos móviles. Existe la necesidad de incorporar enfoques como cultura de seguridad en el ámbito de las comunicaciones de voz.

En definitiva, al adaptar y alinear los frameworks existentes con las particularidades de VoIP, se persigue no solo cumplir con las normativas, sino también asegurar que los controles implementados resulten efectivos ante las amenazas reales que enfrentan los sistemas de telefonía IP contemporáneos.

Según la literatura existen limitaciones de los frameworks y estándares de auditoría y seguridad aplicables a VoIP, los cuales se muestran en la Tabla 15.

Tabla 15. **Limitaciones de frameworks y estándares.**

Autor	**Trabajo**	**Limitaciones de frameworks y estándares**
(Cots et al., 2016)	Benefits of ISO 20000 IT service management certification	El establecimiento de auditorías es un beneficio específico de la gestión de acuerdo con normas y no se puede extender a otros frameworks como ITIL
(Vilarinho & da Silva, 2011)	Risk management model in ITIL	ITIL presenta lagunas en la especificación de Gestión de Riesgos
(Goldstein & Frank, 2016)	Componentes de un método de modelado multiperspectiva para el diseño y gestión de sistemas de seguridad TI	COBIT e ITIL no son suficientes para el diseño y gestión de los sistemas de seguridad TI integrales, no abordan los retos en cuanto a protección de recursos TI (activos de la compañía, tareas, procesos y sistemas de información corporativa)
(Burgemeestre et al., 2011)	Value-based argumentation for justifying compliance	Los métodos de gestión de riesgos apoyan a las empresas en decidir sobre la aplicación de medidas de control, sin embargo, no están diseñados como un medio para explicar y motivar el cumplimiento de decisiones a los auditores externos
(Draxler & Stevens, 2011)	Supporting the collaborative appropriation of an	El estándar ITIL no aborda el usuario único como el cliente de un servicio TI, el tema de adaptación no se aborda en el

Autor	Trabajo	Limitaciones de frameworks y estándares
	open software ecosystem	estándar ITIL (ni por los usuarios finales solos ni en cooperación con el proveedor de servicios)
(Burgemeestre et al., 2013)	Argumentación basada en valores para el diseño y auditoría de medidas de seguridad	Las normas de seguridad de la información como COBIT o NIST 800-53 se organizan en torno a un conjunto de objetivos de control genéricos, las normas abiertas deben ser traducidas en normas específicas para su aplicación. Las metodologías de ingeniería de seguridad permiten la planificación y aplicación de medidas de seguridad de manera sistemática, no toman en cuenta los objetivos de negocio y los valores que desempeñan para decidir sobre los controles de seguridad. Se debe integrar las exigencias de seguridad con requisitos funcionales y limitaciones derivadas de otras fuentes. El resultado de las medidas de seguridad mejora la vinculación entre procesos de negocio y sistemas de información, hay poca investigación sobre la resolución de conflictos entre los objetivos, requisitos y valores.

Fuente: Elaborada por el autor.

Las Tablas 16-21 presentan el análisis de frameworks en relación con los requerimientos y necesidades de gestión en sistemas VoIP.

Tabla 16. **Requerimientos y necesidades de gestión en VoIP vs USGCB.**

USGCB y SCAP	Requerimiento de sistemas VoIP
USGCB es una norma diseñada para proporcionar una única configuración, consistente a través de toda la empresa, tanto para computadoras personales de escritorio y portátiles, y por lo tanto reducir los costos asociados con el apoyo, la compatibilidad de aplicaciones y al mismo tiempo para mejorar la seguridad. SCAP se basa en un conjunto de estándares abiertos que enumeran los problemas de seguridad de configuración, fallas de software y nombres de productos. Se utiliza para medir los sistemas para determinar la presencia de vulnerabilidades conocidas y proporcionar un mecanismo para clasificar los resultados con el fin de evaluar el potencial impacto. (Sun et al., 2022).	- Se requiere la evaluación automatizada de sistemas VoIP - Generar la capacidad de administrar de forma segura la configuración de políticas de grupo para VoIP - Gestión de seguridad integradas para el cumplimiento de normativas y políticas, para asegurar los activos de TI y gestionar el riesgo. - Gestión de configuración efectiva de todos los sistemas conectados a la red VoIP e identificación de aquellos donde el sistema deriva de sus configuraciones esperadas. - Minimizar riesgos y evitar interrupciones del servicio.

Fuente: Elaborada por el autor.

Tabla 17. **Requerimientos y necesidades de gestión en VoIP vs NIST 800-53.**

FISMA/NIST 800-53	Requerimiento de sistemas VoIP
Se deben implementar estrategias y procesos para: - Asegurar los niveles de servicio, cumplimiento de políticas y la gestión adecuada del riesgo. - Asegurar todos los bienes y servicios. - Reducir el costo y la complejidad de la gestión de heterogéneas infraestructuras de TI. (Joint Task Force, 2022).	- Gestionar la configuración efectiva desde el descubrimiento de todos los sistemas conectados a la red a través de la creación y la gestión de las líneas de base a través de dichos sistemas, y la identificación de aquellos donde el sistema deriva de sus configuraciones esperadas. - Supervisar los controles de seguridad heterogéneos en toda la organización, permitir la identificación rápida del potencial y las amenazas existentes y proporcionar un conocimiento detallado y preciso de seguridad para el personal que permita la recuperación rápida y reducción de los tiempos de exposición. - Políticas de monitoreo en tiempo real y auditoría de cambios (informes). - Generar evaluaciones precisas y oportunas de riesgos de seguridad - Gestión de los derechos de identidad de usuario y de acceso.

Fuente: Elaborada por el autor.

Tabla 18. **Requerimientos y necesidades de gestión en VoIP vs GLBA.**

Ley Gramm-Leach-Bliley (GLBA)	Requerimiento de sistemas VoIP
- Los proveedores de servicios financieros deben proteger la información del cliente contra amenazas a la seguridad, confidencialidad e integridad. Sin embargo, GLBA no es un estándar de seguridad técnica. (Cuaresma, 2002).	- Establecimiento de un programa de seguridad para proteger la información del usuario - La evaluación de la capacidad de las políticas de seguridad para identificar y controlar amenazas internas y externas - La gestión y el control de los riesgos que pongan en peligro la información del cliente - Establecimiento de política de seguridad. Políticas necesarias para hacer frente a los controles de acceso, el uso de cifrado, controles de cambio, la vigilancia y respuesta a incidentes. - Evaluación de riesgos de seguridad de información y gestión de la configuración. - Controles de acceso para sistemas. Monitoreo en tiempo real y auditoría - Reportes de fallos de seguridad, auditoría para aplicaciones de seguridad y dispositivos (cortafuegos, antivirus, sistemas de detección de intrusos), así como para los dispositivos de red.

Fuente: Elaborada por el autor.

Tabla 19. **Requerimientos y necesidades de gestión en VOIP vs ISO 27000.**

ISO 27000	Requerimiento de sistemas VoIP
- El reto de hacer frente a la exigencia general de los controles de cumplimiento, incluso para un reglamento puede ser intimidante y el costo prohibitivo. Multiplicado eso por dos o incluso tres reglamentos, la complejidad crece de manera exponencial. ¿Cómo se gestionan las organizaciones maduras el reto de demostrar el cumplimiento de múltiples regulaciones? - La clave del éxito radica en la identificación de un marco común para la implementación y el mapeo de los requisitos normativos a ese marco. Los requerimientos de ISO 27002 son muy amplios en su impacto, afectando normalmente todos los aspectos de una organización de TI. (ISO, 2022)	- Desarrollar un conjunto de políticas, estándares y directrices internas de seguridad. - Control de acceso. Se requiere por parte del Administrador de recursos la capacidad de controlar privilegios administrativos en un nivel granular, reduciendo significativamente la cantidad de usuarios con acceso privilegiado a información empresarial confidencial - Administración de los derechos de identidad y acceso de los usuarios, racionalizar la administración de contraseñas, control de acceso a la información sensible dentro o fuera del firewall con VPN SSL, inicio de sesión único - Gestión de niveles de servicio, asegurando el cumplimiento de SLA, reduciendo tiempos de recuperación y abordando de manera efectiva las causas raíz de los problemas del sistema y las aplicaciones que podrían provocar interrupciones. - Protección contra intrusiones, gestión de eventos de seguridad - Generación de informes sobre deficiencias de seguridad, incluyendo software malicioso, múltiples identificadores de usuario y cuentas, contraseñas débiles, derechos de acceso de usuario apropiado

Fuente: Elaborada por el autor.

Tabla 20. **Requerimientos y necesidades de gestión en VOIP vs NERC CIP.**

NERC	Requerimiento de sistemas VoIP
NERC CIP implica controles específicos de seguridad técnicas, así como controles de procedimiento alrededor de la formación, aplicación de políticas, el acceso (tanto físico como cibernético) (Cole, 2016).	- Administración segura de registros, análisis de eventos y detección de amenazas a la información y la seguridad. - Evaluación de los ajustes de seguridad - Administración de usuarios - Integración de herramientas de seguridad y cumplimiento

Fuente: Elaborada por el autor.

Tabla 21. **Requerimientos y necesidades de gestión en VoIP vs COBIT.**

COBIT	Requerimiento de sistemas VoIP
COBIT establece las mejores prácticas para los controles de TI, pero las empresas deben determinar qué controles realizar para su organización específica. Eso hace de COBIT un framework muy general. El usuario que implemente COBIT debe: - Asegurar que la aplicación se adapte a sus requisitos reglamentarios - Selección de los controles adecuados para su organización - Seguimiento y presentación de informes sobre el programa (Awaludin Rizal et al., 2020)	– Se requiere gestión de seguridad integrada. – Se deben identificar, implementar y automatizar los controles más críticos. – Definir, gestionar e informar sobre un conjunto coherente de controles internos sobre datos y sistemas corporativos.

Fuente: Elaborada por el autor.

Es necesario citar diversos aspectos en la gestión para VoIP, en este contexto se presenta un análisis por área de los criterios de gestión VoIP en base al framework COBIT los cuales se pueden apreciar en la Tabla 22. Criterios de Gestión VoIP frente a COBIT.

Tabla 22. **Criterios de Gestión VoIP frente a COBIT.**

Área / COBIT	Criterios de Gestión VoIP
Control de Acceso	En VoIP el control de acceso es de diferente naturaleza, VoIP realmente no tiene un valor de autorización, pero el Uniform Resource Identifier (URI) es un valor que cada agente de usuario VoIP contiene. El valor puede ser utilizado para autorizar a los endpoints. COBIT no es adecuado para VoIP
Desarrollo de Aplicaciones	Existe de otra forma, pero no hay necesidad de hacerlo. Se usan aplicaciones del mercado (PBX, softphones, servidores proxy, clientes de mensajería instantánea, clientes peer-to-peer)
Gestión de Activos	Los activos de VoIP son de naturaleza particular (uso de centralitas, hardphones y softphones), COBIT trata sobre activos de información protegidos en general
Operaciones de Negocios	VoIP se centra en gestión de transmisión de voz mediante protocolos de comunicación, COBIT trata sobre procesos de negocios globales

Área / COBIT	**Criterios de Gestión VoIP**
Comunicaciones	Protocolos de comunicación específicos de VoIP (señalización, cifrado, transporte, gestión de clave)
Cumplimiento	VoIP contempla el cumplimiento de principios de estándares de privacidad y seguridad generales y aplica principios puntuales y específicos en cuanto a riesgos de servicio VoIP
Gobierno Corporativo	El alineamiento de TI con el negocio en VoIP es de personalización flexible para para satisfacer las necesidades de los proveedores de servicios, es capaz de eliminar los problemas de interoperabilidad con eficacia y reducir los costes de mantenimiento para proveedores de servicios. COBIT es un framework para el control y el gobierno de TI, pero es general y global
Clientes	VoIP maneja en forma exclusiva la gestión de clientes como agentes de usuarios mediante un servidor de registro. COBIT considera los clientes en forma general como usuarios en base a necesidades del mercado
Gestión de Incidentes	Gestión de incidentes de seguridad de la información en COBIT. VoIP aplica análisis de vulnerabilidades y medidas de protección
Operaciones de TI	COBIT contempla en forma global las Operaciones de TI
Outsourcing	No es necesaria una integración en VoIP, el uso de servidores externos se puede considerar dentro de la infraestructura de VoIP
Entorno Físico	Contemplado en COBIT dentro de los objetivos de control. En VoIP se particulariza la infraestructura física
Políticas y Procedimientos	Gestión global de políticas y procedimientos en COBIT, aplica la particularidad en VoIP
Privacidad/Confidencialidad	Privacidad y protección de datos personales. En VoIP se maneja en forma específica a través de la escucha no autorizada de llamadas
Seguridad	COBIT no contempla aspectos específicos de autenticación, no repudio, integridad y disponibilidad para sistemas VoIP

Fuente: Tsai et al. (2015).

Con el objetivo de identificar las restricciones que presentan los marcos vigentes en el ámbito de las auditorías VoIP, se lleva a cabo un análisis comparativo de frameworks, tomando en cuenta criterios relevantes como la cobertura en materia de seguridad, el nivel de especificidad técnica y su aplicabilidad práctica. La Tabla 23 muestra un resumen comparativo de frameworks de seguridad aplicables a la auditoría de sistemas VoIP.

Tabla 23. **Frameworks de seguridad aplicables a la auditoría de sistemas VoIP.**

Framework	Enfoque	Cobertura de seguridad	Nivel de especificidad para VoIP	Fortalezas	Limitaciones
COBIT 4.1 (Ariyadi & Dirgahayu, 2015)	Gobierno y gestión de TI orientado a procesos	Seguridad como uno de los dominios clave	Baja–Media	Claridad en procesos de control, madurez en el entorno empresarial	Limitada especificidad técnica para VoIP; enfoque generalista
COBIT 5 / COBIT 2019 (Tsai et al., 2015).	Gobernanza integral y holística de la empresa y TI	Seguridad incluida como habilitador	Baja	Visión estratégica, alineación con metas corporativas	Demasiado abstracto para auditorías técnicas específicas; difícil operativización para VoIP
ISO/IEC 27001 (ISO, 2022)	Gestión de la seguridad de la información	Establece controles de seguridad (ISO 27002)	Media	Reconocido internacionalmente, adaptable, centrado en el riesgo	Requiere contextualización y personalización; no ofrece guías específicas para VoIP
NIST SP 800-53 (Joint Task Force, 2022).	Controles de seguridad y privacidad en sistemas federales	Amplio conjunto de controles técnicos, operativos y de gestión	Media	Altamente detallado, categorización por impacto y riesgo	Complejo de aplicar sin guía metodológica; requiere alto nivel técnico
ITIL (Al-Ashmoery et al., 2021)	Gestión de servicios de TI	Considera seguridad como parte de la gestión operativa	Baja	Orientación al servicio, integración con procesos de soporte	No está orientado a auditoría ni a evaluaciones técnicas específicas

Fuente: Elaborada por el autor.

A partir del análisis realizado, se evidencia que, aunque marcos como COBIT, ISO/IEC 27001 y NIST constituyen fundamentos robustos para la gestión y auditoría de la seguridad de la información, presentan limitaciones sustanciales en su aplicación directa a entornos VoIP. Estas limitaciones se derivan principalmente de su carácter generalista, elevado nivel de abstracción o enfoque restringido hacia evaluaciones técnicas puntuales. La tabla 24 muestra la comparación estratégica de frameworks de seguridad y auditoría.

Tabla 24. **Comparación estratégica de frameworks de seguridad y auditoría.**

Framework	Alcance principal	Enfoque metodológico	Nivel de detalle técnico	Aplicabilidad en VoIP	Ventajas clave	Limitaciones relevantes
COBIT 4.1 (Ariyadi & Dirgahayu, 2015)	Gobernanza y gestión de TI	Procesos estructurados con objetivos de control	Alto (34 procesos, 210 objetivos)	Medio-alto (requiere adaptación)	Estabilidad, madurez, claridad en procesos	Orientado a la gestión y control de procesos TI, con alcance limitado en aspectos específicos de seguridad, especialmente en entornos como VoIP
COBIT 5 / COBIT 2019 (Tsai et al., 2015).	Gobernanza integral de TI y alineación con negocio	Holístico, basado en metas y principios	Medio (más genérico que 4.1)	Bajo (nivel de abstracción alto)	Personalizable, centrado en valor empresarial	Menor detalle técnico operativo para auditorías
NIST SP 800-53 (Joint Task Force, 2022).	Seguridad de la información y gestión de riesgos	Basado en controles y familias de seguridad	Alto (más de 1000 controles)	Alto (adaptable a múltiples sistemas, incluyendo VoIP)	Exhaustividad, enfoque federal, alineación con FISMA	Complejidad y carga administrativa
ISO/IEC 27001 (ISO, 2022)	Sistema de gestión de seguridad de la información (SGSI)	Gestión de riesgos, mejora continua	Medio (recomendaciones generales)	Medio (necesita complementarse con controles técnicos)	Reconocimiento global, enfoque normativo	Enfoque más organizacional que técnico

Fuente: Elaborada por el autor.

Si bien marcos como COBIT, ISO/IEC 27001 y NIST representan solidez en la gestión y auditoría de la seguridad de la información, presentan ciertas restricciones cuando se intenta su aplicación directa a entornos VoIP. Estas restricciones se deben, en gran medida, a su enfoque generalista, alto nivel de abstracción o a que se centran principalmente en evaluaciones técnicas aisladas.

2.3.5. Estudios sobre cultura de seguridad y tratamiento de la ingeniería social en VoIP

La ingeniería social se ha consolidado como uno de los vectores de amenaza más sutiles y peligrosos en el contexto de los sistemas VoIP, al centrarse en la manipulación del comportamiento humano más que en la explotación directa de fallos técnicos. Investigaciones recientes evidencian un incremento sostenido en la incidencia de ataques basados en ingeniería social, tales como el phishing, el vishing (phishing por voz) y diversos tipos de fraude telefónico, los cuales constituyen una preocupación creciente para las organizaciones debido a su potencial para comprometer la seguridad mediante el engaño a usuarios legítimos. En efecto, un informe global publicado en 2024 revela que aproximadamente dos tercios de los especialistas en ciberseguridad consideran que las técnicas basadas en ingeniería social representan las amenazas con mayor crecimiento, atribuyéndose esta tendencia a la persistente influencia del error humano como causa determinante en numerosos incidentes relacionados con la seguridad de la información (ISACA, 2024).

En el ámbito de las comunicaciones VoIP, los ataques de ingeniería social suelen manifestarse mediante llamadas o mensajes de voz diseñados para manipular a los usuarios, con el objetivo de obtener credenciales, acceder a información confidencial o perpetrar fraudes financieros a través del engaño. Un caso recurrente es la suplantación del personal de soporte técnico, en la cual el atacante se presenta como miembro del equipo de TI para solicitar contraseñas o inducir modificaciones en la configuración del sistema telefónico. Asimismo, en escenarios de fraude financiero por voz (vishing), el

atacante simula ser un representante bancario con el fin de que la víctima proporcione información sensible relacionada con sus cuentas.

Investigaciones recientes han centrado su atención en la creciente incidencia de ataques de ingeniería social y en las posibles estrategias para su mitigación. Datos estadísticos correspondientes a 2023 evidencian que aproximadamente el 70% de las organizaciones informaron haber sido objeto de intentos de vishing durante ese período, mientras que las pérdidas económicas asociadas a fraudes telefónicos continúan en ascenso. De acuerdo con un informe de CrowdStrike, Alger (2025) sostiene que los incidentes de vishing experimentaron un incremento del 442% en la segunda mitad de 2024, lo que refleja una preocupante intensificación de este tipo de amenaza. Una cifra preocupante que evidencia el creciente nivel de sofisticación y organización de los atacantes en este ámbito. Las técnicas utilizadas abarcan desde llamadas automatizadas a gran escala (robocalls) diseñadas para engañar a los receptores, hasta campañas dirigidas específicamente a empleados clave (como administradores) con el objetivo de obtener credenciales sensibles, como las de acceso a la central telefónica (PBX). Incluso se han documentado ataques combinados que utilizan correo electrónico y llamadas telefónicas secuenciales, en los que el atacante envía primero un mensaje por email y luego realiza una llamada para reforzar la credibilidad del engaño.

Carrillo et al. (2022) evidenciaron, a través del despliegue de un honeypot orientado a VoIP, cómo los ciberdelincuentes aprovechan las vulnerabilidades en sistemas PBX para ejecutar no solo fraudes relacionados con el uso indebido de servicios de llamadas (fraude de peaje), sino también para llevar a cabo campañas de spam por voz y distintas modalidades de estafa, utilizando como plataforma las infraestructuras que han sido previamente comprometidas donde numerosos atacantes logran acceder a sistemas VoIP explotando credenciales débiles o reutilizadas, lo que pone de manifiesto una carencia significativa de conciencia en materia de seguridad por parte de los administradores responsables de la gestión de estos entornos. Este hallazgo subraya la importancia de la cultura de seguridad: si los operadores configuran sistemas con

contraseñas por defecto o débiles, los controles técnicos implementados pueden quedar anulados por un descuido humano.

La cultura de seguridad hace referencia al conjunto de actitudes, creencias y prácticas compartidas dentro de una organización en relación con la protección de la información. Una cultura robusta en este ámbito implica que todos los actores (empleados, administradores y usuarios) mantengan una conciencia activa sobre los riesgos y demuestren compromiso con las normativas y procedimientos de seguridad. Diversos estudios destacan que el fortalecimiento de dicha cultura resulta clave para mitigar los riesgos asociados a la ingeniería social en entornos VoIP. Una de las estrategias más eficaces para proteger a una organización consiste en fomentar una cultura donde los colaboradores comprendan tanto las consecuencias de posibles filtraciones como la necesidad de adherirse a las políticas de seguridad establecidas (Batchelor et al., 2023).

Fortalecer la protección frente a ataques de ingeniería social en entornos VoIP requiere capacitar al personal para reconocer señales de vishing y SPIT, fomentar la verificación proactiva de identidad ante comunicaciones inusuales y establecer procedimientos formales para reportar actividades sospechosas sin temor a repercusiones. La evidencia empírica muestra que la formación enfocada en identificar técnicas de persuasión utilizadas en llamadas fraudulentas incrementa notablemente la capacidad de los usuarios para resistir este tipo de engaños. Hashmi et al. (2023) demostraron que los participantes expuestos a entrenamientos específicos sobre vishing desarrollan una mayor habilidad para detectar y rechazar intentos de fraude telefónico, lo que respalda la inclusión de ejercicios simulados y campañas de concienciación continua en las estrategias de seguridad organizacional.

Además, se han impulsado iniciativas orientadas a incorporar soluciones tecnológicas que fortalezcan la mitigación de ataques de ingeniería social en entornos VoIP. Por ejemplo, algunos sistemas incluyen filtros automáticos capaces de identificar llamadas inusuales (como aquellas con identificadores irregulares) y activar mecanismos de verificación antes de permitir su recepción. Asimismo, se ha planteado la utilización

de marcos como SOAR (Security Orchestration, Automation and Response) para automatizar las respuestas ante intentos de manipulación detectados, permitiendo una reacción más ágil y coordinada frente a este tipo de amenazas (Waelchli & Walter, 2025).

No obstante, la primera línea de defensa continúa siendo el usuario final y la cultura organizacional. Un enfoque integral (respaldado por ISACA y otras entidades especializadas) recomienda la combinación de mecanismos técnicos (como listas negras, validación estricta del identificador de llamadas, y filtros automatizados), con medidas administrativas sólidas (incluyendo políticas institucionales claras, programas de capacitación continua y simulacros de ingeniería social), con el fin de reducir significativamente el impacto y la eficacia de estos ataques en entornos VoIP.

En resumen, la concienciación, capacitación y el compromiso activo de los usuarios resultan fundamentales para complementar los controles técnicos, permitiendo la conformación de un entorno VoIP robusto y preparado frente a las amenazas basadas en ingeniería social.

2.3.6. Estudios sobre procedimientos de auditoría en entornos VoIP

Asegurar un entorno VoIP no constituye una acción puntual centrada únicamente en la configuración inicial, sino que demanda un enfoque sostenido de auditoría y mejora continua. Los procedimientos de auditoría en estos entornos comprenden desde la verificación del cumplimiento de políticas de seguridad y configuraciones críticas, hasta la realización de pruebas de penetración altamente especializadas. En general, una auditoría de seguridad en VoIP inicia revisando la implementación efectiva de controles esenciales previamente establecidos: por ejemplo, si se han activado protocolos de cifrado como SRTP y TLS, si los servidores SIP y buzones de voz utilizan mecanismos robustos de autenticación y contraseñas seguras, y si la red está segmentada correctamente y protegida mediante firewalls adaptados a VoIP. Las guías de auditoría desarrolladas por organismos especializados, como las plantillas de ISACA ponen énfasis en estos aspectos, priorizando el control de acceso, la autenticación y el cifrado como elementos

fundamentales a examinar (ISACA, 2025). Dichos lineamientos permiten asegurar que la auditoría verifique no solo la existencia, sino también la eficacia de las salvaguardas que garantizan la autenticidad de los usuarios y la confidencialidad de las comunicaciones en la infraestructura VoIP. Más allá de las evaluaciones estáticas de configuración, un elemento esencial dentro del proceso de auditoría es la verificación activa de seguridad, mediante pruebas de penetración (pentesting) que simulan ataques reales sobre la infraestructura VoIP, lo cual permite la detección de debilidades como autenticación deficiente, configuraciones incorrectas en los servidores o uso de protocolos inseguros.

En escenarios operativos, una auditoría integral de sistemas VoIP debe incluir actividades de validación activa mediante herramientas especializadas. Esto implica la ejecución de escaneos para detectar puertos abiertos y vulnerabilidades inherentes a protocolos como SIP, pruebas controladas de suplantación de identidad o interceptación de llamadas, así como la simulación de ataques de denegación de servicio. Estos procedimientos permiten evaluar la capacidad del sistema para resistir eventos de riesgo en condiciones reales. Dichas pruebas complementan la revisión documental de controles establecidos y ofrecen evidencia empírica sobre el nivel de seguridad alcanzado en la plataforma auditada.

La falta de procedimientos específicos para auditar sistemas VoIP afecta la estandarización, trazabilidad y eficiencia temporal de los procesos de evaluación. Si bien existen guías generales para auditorías de TI, estas no contemplan aspectos críticos como la calidad del servicio en tiempo real, los protocolos VoIP o las amenazas específicas al canal de voz.

Por tanto, se concluye que un procedimiento específico y documentado representa una contribución sustantiva al fortalecimiento de los mecanismos de control y evaluación en entornos VoIP.

En base a la revisión de literatura se determinó que no existe un marco de seguridad que considere ataques de ingeniería social a pesar de ser un aspecto importante en la

gestión de seguridad VoIP; además, no existe un marco específico que cubra todas las categorías de requisitos de seguridad para sistemas VoIP, por lo que se requiere un modelo más extenso (Gavilanez et al., 2017).

2.4. Variables de Investigación

Se definen a continuación las variables en base a las preguntas de investigación, junto con sus respectivas dimensiones.

2.4.1. Variables pregunta general de investigación

¿La implementación de un modelo de auditoría de seguridad específico para sistemas VoIP mejora la eficiencia temporal durante la ejecución de auditorías respecto de los modelos tradicionales?

Variable Independiente: Implementación de un modelo de auditoría de seguridad específico para sistemas VoIP.

Definición conceptual

Marco metodológico orientado a atender las necesidades y amenazas específicas de los sistemas VoIP, considerando tanto vulnerabilidades técnicas como amenazas de origen humano (Gavilanez et al., 2017).

La implementación de un modelo de auditoría de seguridad específico para sistemas VoIP se concibe como un enfoque integral que evalúa, de manera sistemática, los componentes técnicos, operativos y humanos que intervienen en la seguridad de las comunicaciones VoIP. Este enfoque considera tanto las vulnerabilidades inherentes a la arquitectura, protocolos y componentes del sistema, como los riesgos asociados a amenazas de origen humano, tales como la ingeniería social, el fraude y el abuso de

servicios, con el propósito de fortalecer la protección del sistema y optimizar los procesos de evaluación de seguridad (Ramly et al., 2024).

Definición operacional

Implementación del modelo de auditoría de seguridad específico para sistemas VoIP derivado de la revisión bibliográfica y aplicado de forma práctica en auditorías reales.

Dimensiones

De acuerdo con el enfoque integral de seguridad para sistemas VoIP propuesto por Ramly et al., (2024), la seguridad efectiva de estos sistemas debe abordarse de manera holística, considerando simultáneamente aspectos técnicos, operativos y humanos. En coherencia con dicho planteamiento, la variable independiente se estructura en las siguientes dimensiones, todas derivadas del marco conceptual y analítico:

- Incorporación funcional de requerimientos de seguridad específicos para sistemas VoIP.
- Integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP.
- Incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP.
- Integración operativa de un procedimiento especializado en una guía de auditoría específica para sistemas VoIP.

Las cuatro dimensiones definidas para la variable independiente se encuentran respaldadas de manera coherente y unificada en el estudio de Ramly et al. (2024), quienes proponen un enfoque integral de seguridad para sistemas VoIP que abarca requerimientos técnicos, integración de componentes, mitigación del factor humano y procedimientos especializados de evaluación. En consecuencia, dichas dimensiones no constituyen elementos aislados, sino componentes interrelacionados de un mismo marco conceptual de seguridad VoIP, plenamente reconocido en la literatura científica reciente.

Variable Dependiente: Eficiencia temporal durante la ejecución de auditorías

Definición conceptual

Capacidad de completar un proceso de auditoría de forma efectiva utilizando la menor cantidad de tiempo posible sin sacrificar la calidad del trabajo (Tan et al., 2025).

Definición operacional

Tiempo efectivo registrado en minutos para la ejecución de cada auditoría, permitiendo comparar la duración entre el modelo tradicional y el modelo propuesto bajo condiciones similares

Dimensión

Tiempo efectivo total de ejecución de auditorías.

2.4.2. Variables pregunta secundaria de investigación 1

¿La incorporación funcional de los requerimientos de seguridad específicos para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad?

Variable Independiente: Incorporación funcional de requerimientos de seguridad específicos para VoIP.

Definición conceptual

Aplicación práctica de un conjunto estructurado de requisitos técnicos y organizativos orientados a mitigar amenazas y vulnerabilidades inherentes a los entornos VoIP (Gavilanez et al., 2017). Define las necesidades técnicas y organizacionales específicas que deben cubrirse en la auditoría de sistemas VoIP, considerando sus vulnerabilidades únicas.

Esta dimensión se fundamenta en la necesidad de identificar y evaluar los requerimientos de seguridad asociados a la arquitectura, protocolos y componentes

propios de los sistemas VoIP, tales como SIP, RTP, IP-PBX, gateways y dispositivos finales. El estudio de Ramly et al. (2024) establece que la ausencia de requerimientos específicos orientados a VoIP limita la efectividad de las evaluaciones de seguridad, por lo que su incorporación funcional resulta esencial para una auditoría especializada y eficiente.

Definición operacional

Inclusión efectiva de los requerimientos de seguridad específicos dentro del modelo propuesto y su aplicación en auditorías reales.

Dimensión

Cobertura de requerimientos (áreas)

Variable Dependiente: Eficiencia temporal en la ejecución de auditorías de seguridad

Definición conceptual

Habilidad para ejecutar un proceso de auditoría de manera eficiente, optimizando el tiempo empleado sin comprometer la calidad de los resultados obtenidos (Tan et al., 2025).

Definición operacional

Tiempo total requerido (en minutos) para ejecutar auditorías completas con cada modelo.

Dimensión

Tiempo efectivo total de ejecución de auditorías por etapa.

2.4.3. Variables pregunta secundaria de investigación 2

¿La integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP incrementa la relevancia de las evaluaciones de seguridad en dichos sistemas?

Variable Independiente: Integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP

Definición conceptual

Inclusión funcional de componentes diseñados exclusivamente para abordar amenazas y características propias de sistemas VoIP dentro del modelo de auditoría (Gavilanez et al., 2017). Conjunto de elementos técnicos y procedimentales diseñados para evaluar aspectos propios de la arquitectura y funcionamiento de los sistemas VoIP.

Esta dimensión considera la evaluación integrada de los componentes técnicos y operativos que conforman el ecosistema VoIP, incluyendo servidores SIP, firewalls, VPN, mecanismos de control de acceso y herramientas de monitoreo. Según Ramly et al. (2024), la seguridad de VoIP no puede analizarse de forma aislada por componente, sino mediante un enfoque integrado que permita identificar vulnerabilidades cruzadas y optimizar los procesos de evaluación de seguridad.

Definición operacional

Incorporación efectiva de componentes VoIP en el modelo de auditoría de seguridad específico para sistemas VoIP.

Dimensión

Integración de componentes específicos.

Variable Dependiente: Relevancia de las evaluaciones de seguridad en sistemas VoIP

Definición conceptual

Nivel de utilidad y especificidad de la auditoría para abordar aspectos clave de seguridad VoIP (Gavilanez et al., 2017). Existe una relación directa entre la relevancia de las evaluaciones de seguridad en sistemas VoIP y la eficiencia temporal en las auditorías, ya que la focalización de la auditoría en componentes relevantes y críticos del sistema

mejora la eficiencia temporal al reducir tareas redundantes y direccionar el análisis hacia aspectos de mayor impacto (Jaafar & Al-Daamy, 2024). Además, cuando las auditorías son diseñadas con criterios específicos del entorno tecnológico, permiten reducir significativamente el tiempo de ejecución sin comprometer la calidad del control interno (Sun et al., 2024).

Definición operacional

Valoración de expertos sobre aspectos evaluados

Dimensión

Relevancia de los resultados de auditoría.

2.4.4. Variables pregunta secundaria de investigación 3

¿La incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP reduce la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano?

Variable Independiente: Incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP.

Definición conceptual

Integración práctica y sistemática de un conjunto de políticas, acciones y capacitaciones orientadas a concienciar sobre los riesgos de ingeniería social en entornos VoIP (Gavilanez et al., 2017).

Ramly et al. (2024) reconocen que, además de las amenazas técnicas, los sistemas VoIP son altamente vulnerables a ataques que explotan el factor humano, tales como vishing, SPIT y fraude telefónico. En este contexto se destaca la necesidad de incorporar estrategias orientadas a la concienciación, prevención y mitigación de amenazas humanas como parte integral de la seguridad VoIP.

Definición operacional

Diseño e inclusión del plan de cultura de seguridad en el modelo de auditoría de seguridad VoIP propuesto cuya percepción de relevancia se compara con un modelo tradicional.

Dimensión

Presencia funcional del plan de cultura de seguridad en los procesos de auditoría.

Variable Dependiente: Percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano

Definición conceptual

Nivel de exposición que los evaluadores perciben que posee una organización frente a amenazas de ingeniería social que comprometen la seguridad de los sistemas VoIP. Según Vrhovec (2021), variables como la percepción de vulnerabilidad y la severidad del peligro están directamente relacionadas con la intención del usuario de adherirse a campañas de concienciación sobre ingeniería social, lo que refleja que una mayor conciencia de riesgo estimula respuestas organizacionales frente a amenazas humanas.

La incorporación de un plan de cultura de seguridad que disminuya la percepción de vulnerabilidad frente a amenazas de ingeniería social no solo fortalece el entorno organizacional, sino que también contribuye significativamente a la eficiencia temporal de los procesos de auditoría. Esto se debe a que un entorno con usuarios más conscientes y capacitados reduce la cantidad de hallazgos inesperados y minimiza la necesidad de revisiones extensas sobre prácticas inseguras del personal, acortando así los ciclos de verificación. Siddiqi et al. (2022) destacan que las organizaciones que implementan medidas proactivas frente a la ingeniería social, como la capacitación continua y simulaciones periódicas, logran mejorar su postura de seguridad y simplificar los procesos

de auditoría al reducir puntos críticos de riesgo humano. Una percepción organizacional de menor vulnerabilidad se traduce en una ejecución de auditoría más eficiente.

Definición operacional

Valoración experta sobre el nivel de percepción de vulnerabilidad organizacional ante ataques de ingeniería social.

Dimensión

Nivel percibido de exposición organizacional frente a ataques de ingeniería social.

2.4.5. Variables pregunta secundaria de investigación 4

¿La integración operativa de un procedimiento especializado en una guía de auditoría específica para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad?

Variable Independiente: Integración operativa de un procedimiento especializado en una guía de auditoría específica para sistemas VoIP.

Definición conceptual

Aplicación estructurada de un conjunto de pasos específicos dentro de una guía de auditoría orientada a mejorar el desempeño temporal del proceso de auditoría. La implementación estructurada de procedimientos específicos dentro de una guía de auditoría ha demostrado ser una estrategia eficaz para optimizar el tiempo de ejecución en procesos de evaluación. Esta estructuración permite reducir redundancias, mejorar la secuenciación de tareas y focalizar los esfuerzos en aspectos críticos del sistema evaluado, lo cual incide directamente en el desempeño temporal del proceso de auditoría (Motl & Kordík, 2021).

La dimensión se sustenta en la propuesta metodológica de Ramly et al. (2024), quienes plantean la necesidad de aplicar procedimientos específicos para la evaluación de ataques VoIP, tales como escaneo SIP, eavesdropping, ataques de denegación de servicio

y fuerza bruta. La adopción de procedimientos especializados permite una evaluación más precisa y eficiente del nivel de seguridad del sistema, optimizando el tiempo de ejecución de la auditoría en comparación con enfoques genéricos.

Definición operacional

Implementación del procedimiento detallado incluido en la guía de auditoría, aplicado en auditorías reales comparadas con procesos tradicionales.

Dimensión

Aplicación del procedimiento especializado integrado en la guía de auditoría.

Variable Dependiente: Eficiencia temporal en la ejecución de auditorías de seguridad

Definición conceptual

Capacidad para llevar a cabo una auditoría maximizando la eficiencia en el tiempo, asegurando integridad y calidad de los hallazgos obtenidos (Tan et al., 2025).

Definición operacional

Tiempo total requerido (en minutos) para ejecutar auditorías completas con cada modelo.

Dimensión:

Tiempo efectivo de ejecución de auditoría.

CAPÍTULO 3: METODOLOGÍA

3.1. Enfoque metodológico general

La presente investigación se sustenta en un enfoque cuantitativo, el cual permite la medición objetiva, el análisis estadístico y la validación empírica de los resultados obtenidos a partir de la aplicación del modelo propuesto. Este enfoque posibilita examinar de manera precisa y sistemática la relación entre variables clave como la eficiencia temporal, la relevancia de los componentes de seguridad y la reducción de la vulnerabilidad ante ataques que explotan el factor humano.

El enfoque cuantitativo se articula con un diseño metodológico de carácter comparativo y descriptivo, lo que permite contrastar el modelo propuesto (VoIPSAM) con un modelo de auditoría tradicional (COBIT 4.1) en contextos reales, sustentando las conclusiones a partir de datos medibles y replicables. La validación se realiza mediante pruebas estadísticas, recolección estructurada de datos y el análisis de percepción de expertos, garantizando rigor científico en todas las etapas del proceso investigativo.

3.2. Diseño metodológico

El diseño adoptado se estructura en torno a tres enfoques metodológicos complementarios:

- Diseño comparativo: Se empleó para contrastar cuantitativamente los resultados de auditorías realizadas con VoIPSAM y COBIT 4.1, particularmente en términos de eficiencia temporal y valoración de componentes.
- Diseño descriptivo: Orientado a caracterizar los requerimientos específicos de seguridad VoIP, así como los elementos diferenciales incorporados en el modelo propuesto.
- Estudio de caso: Se aplicó en una institución pública de educación superior que cuenta con sistemas VoIP implementados, lo cual permitió evaluar la aplicabilidad y eficacia del modelo en un entorno real de auditoría.

3.3. Población y muestra

La población del estudio estuvo conformada por cuatro expertos en seguridad informática de la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la ESPOCH, con experiencia comprobada en la implementación y auditoría de sistemas VoIP. Los expertos especializados en tecnologías de la información y comunicaciones han participado activamente en procesos de auditoría aplicando modelos tradicionales como COBIT 4.1, lo cual los posiciona como referentes técnicos idóneos para evaluar propuestas orientadas a mejorar la seguridad en entornos VoIP.

Dado el tamaño reducido de la población y el carácter especializado de la evaluación requerida, se adoptó un muestreo censal, considerando a la totalidad de expertos como muestra. Esta decisión metodológica está respaldada por criterios de suficiencia teórica, ya que los participantes cuentan con un alto nivel de experiencia, certificaciones profesionales y dominio de modelos de auditoría. Su participación permitió obtener una valoración cualitativa y cuantitativa altamente confiable del modelo propuesto.

En estudios de evaluación y validación de modelos o sistemas, especialmente aquellos de carácter cualitativo o de validación experta, es aceptado trabajar con muestras reducidas debido a la profundidad y calidad del análisis proporcionado por cada experto participante. Según Nielsen y Landauer (1993), la mayor parte de los hallazgos y problemas en pruebas de sistemas se identifican con los primeros usuarios, y una muestra de tres a cinco personas resulta suficiente para obtener información representativa y relevante. Esto se sustenta en el principio de que cada nuevo evaluador aporta menor cantidad de hallazgos únicos respecto al anterior, debido a la convergencia de observaciones.

En investigaciones orientadas a la evaluación de modelos y detección de problemas, la literatura científica respalda la utilización de muestras reducidas de expertos o usuarios, debido a la alta capacidad de identificación de hallazgos relevantes desde las primeras interacciones. Según Faulkner (2003), a partir de pruebas con un número reducido de evaluadores (entre tres y cinco) es posible detectar un porcentaje significativo de los problemas críticos de un sistema o modelo. En particular, sus resultados demuestran que con cinco evaluadores se puede identificar en promedio el 85% de los problemas de usabilidad y con cuatro evaluadores se alcanza una cobertura superior al 75%.

Por lo tanto, la participación de cuatro expertos en la validación del estudio de caso en esta investigación se justifica teórica, estadística y metodológicamente, dado que asegura un equilibrio entre la eficiencia de recursos y la obtención de resultados representativos y sólidos para la identificación de aspectos críticos, garantizando así la pertinencia y confiabilidad del proceso de validación.

Adicionalmente, con el fin de fortalecer la validez externa del estudio, se incorporó una fase complementaria de validación de los resultados del estudio de caso mediante expertos externos a la institución donde se ejecutaron las auditorías, la fase estuvo conformada por cinco expertos de perfil académico-investigador, con formación doctoral en universidades de distintos países y experiencia en seguridad de la información y entornos VoIP. Los expertos fueron seleccionados por criterios de idoneidad académica,

experiencia profesional y participación independiente respecto al proceso de auditoría desarrollado en la institución objeto del estudio.

Dado el carácter especializado de esta validación, se utilizó un muestreo intencional por criterio experto, considerando la totalidad de los expertos seleccionados. Su participación permitió evaluar la coherencia metodológica, consistencia interna y transferibilidad de los resultados del estudio de caso, fortaleciendo así la validez externa de la investigación.

3.4. Hipótesis

La formulación de hipótesis constituye un componente esencial dentro del enfoque cuantitativo de la presente investigación, al permitir establecer relaciones comprobables entre las variables involucradas. En este estudio, las hipótesis han sido planteadas con base en los problemas específicos identificados y orientan el análisis empírico sobre la efectividad del modelo propuesto para la auditoría de seguridad en sistemas VoIP, en comparación con enfoques tradicionales.

3.4.1. Hipótesis Principal

Hipótesis Principal HP. La implementación de un modelo de auditoría de seguridad específico para sistemas VoIP mejora la eficiencia temporal durante la ejecución de auditorías respecto de los modelos tradicionales.

Variable Independiente (VI): Implementación de un modelo de auditoría de seguridad específico para sistemas VoIP.

Variable Dependiente (VD): Eficiencia temporal durante la ejecución de auditorías.

Validación: Se aplicaron auditorías reales utilizando ambos modelos (VoIPSAM y COBIT 4.1). Se registraron los tiempos de ejecución y se contrastaron mediante la prueba t de Student para muestras relacionadas, previa verificación de normalidad con Shapiro-Wilk. El análisis evidenció una reducción significativa del tiempo de auditoría al aplicar el modelo propuesto.

3.4.2. Hipótesis Secundarias

a) ***Hipótesis Secundaria HS1:*** La incorporación funcional de los requerimientos de seguridad específicos para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad.

- **Variable Independiente (VI):** Incorporación funcional de los requerimientos de seguridad específicos para sistemas VoIP.

- **Variable Dependiente (VD):** Eficiencia temporal en la ejecución de auditorías de seguridad.

- **Validación:** Se determinaron y aplicaron requerimientos específicos de seguridad VoIP en auditorías reales. Se compararon los tiempos obtenidos en auditorías. El análisis descriptivo y la prueba t de Student para muestras relacionadas evidenciaron mejoras en eficiencia temporal.

b) ***Hipótesis Secundaria HS2:*** La integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP incrementa la relevancia de las evaluaciones de seguridad en dichos sistemas.

- **Variable Independiente (VI):** Integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP.

- **Variable Dependiente (VD):** Relevancia de las evaluaciones de seguridad en sistemas VoIP.

- **Validación:** Se aplicó una encuesta estructurada a expertos para valorar la relevancia de los componentes del modelo VoIPSAM frente a COBIT 4.1. Se usó una escala tipo Likert y se analizó la diferencia de medias con prueba t para muestras independientes. Los resultados demostraron una mayor valoración del modelo propuesto.

c) ***Hipótesis Secundaria HS3:*** La incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP reduce la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano.

- **Variable Independiente (VI):** Incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP.

- **Variable Dependiente (VD):** Percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano.

- **Validación:** Se incluyó el plan de cultura en el modelo VoIPSAM y se aplicó una encuesta a expertos para comparar su valoración respecto al modelo tradicional. La prueba t de Student para muestras independientes evidenció una mejor percepción sobre la reducción de vulnerabilidad asociada a este componente.

d) ***Hipótesis Secundaria HS4:*** La integración operativa de un procedimiento especializado en una guía de auditoría específica para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad.

- **Variable Independiente (VI):** Integración operativa de un procedimiento especializado en una guía de auditoría específica para sistemas VoIP.

- **Variable Dependiente (VD):** Eficiencia temporal en la ejecución de auditorías de seguridad.

- **Validación:** Se diseñó e implementó una guía con procedimiento especializado. Se aplicaron auditorías reales y se midieron los tiempos. La comparación de resultados mediante análisis descriptivo y prueba t de Student para muestras relacionadas confirmó la mejora en eficiencia temporal.

3.5. Métodos de Investigación

La presente investigación adopta un enfoque cuantitativo con técnicas complementarias documentales y de validación empírica, lo cual permite tanto la evaluación objetiva de resultados medibles como la fundamentación conceptual de los componentes propuestos. Dado el carácter aplicado de la tesis, orientado al diseño, implementación y validación de un modelo de auditoría específico para sistemas VoIP, se recurre a diversos métodos según el propósito de cada hipótesis.

En términos generales, se empleó el método comparativo para contrastar la eficiencia temporal entre el modelo VoIPSAM propuesto y un modelo tradicional (COBIT 4.1), así como el método descriptivo para identificar y estructurar los requerimientos de seguridad y los componentes específicos requeridos en entornos VoIP. Además, se adoptó un método de validación empírica basada en encuestas a expertos para valorar la relevancia de los elementos introducidos en el modelo, tales como el plan de cultura de seguridad y los procedimientos especializados.

Para el estudio de la eficiencia temporal, se aplicó el diseño cuasiexperimental de grupos no equivalentes con mediciones de tiempos reales de ejecución de auditorías, lo que permitió comparar objetivamente los efectos del modelo propuesto frente al modelo

de referencia. Las mediciones fueron sometidas a pruebas estadísticas de normalidad y contrastes paramétricos (t de Student) según correspondía, garantizando la validez de los resultados.

Finalmente, para aquellos componentes cuya evaluación no podía realizarse exclusivamente por medios cuantitativos, se integraron técnicas cualitativas de análisis documental y revisión normativa, bajo un diseño mixto de alcance explicativo y analítico.

Esta combinación metodológica permitió sustentar empíricamente cada una de las hipótesis de investigación y validar, desde múltiples dimensiones, la implementación de un modelo de auditoría de seguridad integral y específico para sistemas VoIP.

3.6. Técnicas e instrumentos de recolección y análisis de datos

Con el objetivo de garantizar la rigurosidad metodológica y la validez de los resultados obtenidos, en este apartado se describen las técnicas y los instrumentos utilizados para la recolección y el análisis de datos en función de cada una de las hipótesis formuladas.

Se contemplaron métodos de observación directa, revisión documental, aplicación de encuestas estructuradas y cronometraje de auditorías, así como pruebas estadísticas que permitieron comparar la eficiencia y la relevancia de los modelos de auditoría evaluados. La triangulación de datos y la aplicación de pruebas de hipótesis estadísticas contribuyeron a la validación empírica de los hallazgos, asegurando la coherencia entre los objetivos planteados y los resultados alcanzados. Las técnicas e instrumentos utilizados se muestran en el **Anexo A Matriz de consistencia**.

3.7. Matriz de consistencia

La matriz de consistencia se encuentra en el **Anexo A Matriz de Consistencia**, la matriz organiza y relaciona los componentes clave de la investigación, asegurando que todos estén alineados de manera lógica y coherente para garantizar la validez del estudio

3.8. Operacionalización de variables

La operacionalización de variables se muestra en el **Anexo B Operacionalización de Variables** y detalla cómo se midieron y analizaron las variables de la investigación.

CAPÍTULO 4: MODELO DE AUDITORÍA DE SEGURIDAD VoIP PROPUESTO

4.1. Fundamentación del modelo propuesto

El capítulo describe el modelo de auditoría de seguridad propuesto, diseñado específicamente para sistemas VoIP. Su desarrollo responde directamente a la problemática identificada en la investigación: la ausencia de un modelo de auditoría de seguridad específico para sistemas VoIP limita la eficiencia temporal durante la ejecución de auditorías respecto de los modelos tradicionales.

En este contexto, el modelo propuesto, denominado VoIPSAM (VoIP Security Audit Model), se plantea como una solución metodológica que atiende las particularidades técnicas y de seguridad propias de los entornos VoIP. A diferencia de marcos de trabajo genéricos, VoIPSAM incorpora controles específicos para protocolos, así como mecanismos de prevención frente a amenazas frecuentes.

El modelo ha sido diseñado con un enfoque orientado a la eficiencia operativa, estructurado en fases secuenciales que integran actividades, instrumentos y criterios de evaluación concretos. Esta estructura permite reducir los tiempos asociados a la ejecución de auditorías, optimizando la recopilación de evidencias, el análisis de cumplimiento y la generación de informes, lo cual constituye un aporte diferencial respecto de los modelos tradicionales.

4.1.1. Antecedentes

La importancia de VoIP, la tecnología que permite realizar llamadas telefónicas a través de internet, radica en su funcionalidad, múltiples características, ventajas y ahorro de costos. VoIP está expuesta a diversas amenazas de seguridad que comprometen la confidencialidad, disponibilidad e integridad de los datos. La auditoría de sistemas es un proceso de revisión de Sistemas de Información (SI) y Tecnología de la Información (TI) que permite a las organizaciones identificar hallazgos, mitigar riesgos e implementar controles adecuados para proteger información crítica y valiosa.

Numerosos riesgos están vinculados a comunicaciones, sistemas de información y equipos que carecen de controles de seguridad actualizados, además de la cantidad de amenazas internas, aumentando por tanto el factor de riesgo. Cada día se desarrollan nuevos sistemas que afectan a la seguridad de la información de las organizaciones, siendo necesario contar con una estrategia de seguridad completa para evitar fugas y fallos en los sistemas. Las empresas deben evitar numerosos riesgos de seguridad, incluido el fraude, la divulgación no autorizada de información y el robo de identidad, entre otros. Se toman como referencia las buenas prácticas de marcos de trabajo aplicables a entornos VoIP, entre ellos COBIT 4.1, el cual proporciona una gestión integral de los procesos de gobernanza, control, aseguramiento y auditoría de las tecnologías de la información a un nivel amplio y estructurado.

VoIP es un sistema único, en consecuencia, se requiere de un modelo personalizado que gestione adecuadamente los riesgos específicos de seguridad de las comunicaciones al utilizar el Protocolo de Internet IP. En VoIP uno de los riesgos específicos que requieren una gestión diferenciada es el SPIT, un tipo de ataque que explota la arquitectura de voz sobre IP para realizar llamadas masivas o maliciosas que pueden afectar la disponibilidad del servicio y comprometer la calidad de las comunicaciones. (Nazih et al., 2023) demuestran que estas amenazas no solo representan una molestia operativa, sino que pueden ser utilizadas como vectores iniciales para

campañas más complejas, incluyendo ingeniería social y perturbación del servicio, se considera un enfoque basado en autoencoders convolucionales, capaz de distinguir patrones anómalos en el tráfico SIP y detectar intentos de SPIT con alta precisión, lo que evidencia que los entornos VoIP requieren mecanismos de defensa especializados que respondan a sus vulnerabilidades inherentes. Estos resultados refuerzan la necesidad de modelos de seguridad adaptados a VoIP, con capacidades de identificación temprana de anomalías y técnicas avanzadas de protección frente a ataques orientados a la manipulación de las comunicaciones de voz.

La ingeniería social se refiere a aprovechar el elemento humano de la seguridad para comprometer información vital; cuando se compara la facilidad de uso y el costo de ejecución de la ingeniería social con ataques más técnicos a las empresas, se vuelve evidente por qué la ingeniería social es una herramienta tan común. Se debe prestar especial atención tanto a las violaciones técnicas de seguridad como a las formas no técnicas de piratería informática, como la ingeniería social. La seguridad es un problema de personas y de gestión; por lo tanto, los controles físicos y técnicos no son suficientes para proteger la seguridad de la información (Gavilanez et al., 2017). Como método de ataque considerablemente popular en la comunidad de hackers, la ingeniería social ha dado lugar a amenazas graves a la seguridad, generalizadas y persistentes (Wang et al., 2020).

La ingeniería social continúa consolidándose como una de las tácticas más efectivas utilizadas por los atacantes para comprometer sistemas organizacionales. Almutairi y Alghamdi (2022) en su estudio reportaron que más del 63 % de los participantes desconocía por completo el concepto de ingeniería social, mientras que un 67 % no tenía información sobre los diferentes tipos de ataques asociados. Estos datos evidencian que, pese a su alta prevalencia, la ingeniería social sigue dependiendo principalmente de brechas humanas de percepción y formación, lo que incrementa la vulnerabilidad de las organizaciones ante campañas de fraude, phishing o manipulación psicológica. La limitada conciencia del personal refuerza la necesidad de implementar

programas sistemáticos de capacitación que permitan reducir el impacto de estos ataques y fortalecer la postura de seguridad institucional.

4.1.2. Fundamentación de la selección de COBIT 4.1 frente a versiones posteriores

A pesar de la evolución del marco COBIT 4.1 hacia versiones más recientes como COBIT 5 y COBIT 2019, la elección de COBIT 4.1 como modelo de referencia responde a criterios técnicos, metodológicos y prácticos, se fundamenta en cuatro ejes argumentativos clave: amplia adopción en contextos organizacionales, enfoque operativo y técnico frente al enfoque estratégico de versiones posteriores, compatibilidad con modelos específicos y la coherencia metodológica que ofrece para la evaluación empírica de la eficiencia temporal en auditorías de seguridad VoIP. A continuación, se muestran los ejes argumentativos:

- Eje 1. Enfoque operativo y técnico frente al enfoque estratégico de COBIT 5/2019.
  COBIT 4.1 presenta un enfoque centrado en el control y la auditoría técnica de TI, con procesos detallados, metas de control, prácticas recomendadas y métricas. COBIT 5 y COBIT 2019, por su parte, priorizan un enfoque de gobernanza estratégica y empresarial, útil para alinear TI con los objetivos organizacionales, pero menos detallado para auditorías técnicas como las de seguridad VoIP.

- Eje 2. Orientación a objetivos de control específicos, útil para auditorías técnicas.
  COBIT 4.1 incluye objetivos de control específicos para cada proceso, algo fundamental para auditorías detalladas de sistemas complejos como VoIP. COBIT 5 y 2019 omiten estos objetivos y se enfocan en principios de alto nivel y metas de gobierno.

- Eje 3. Compatibilidad con fines comparativos de investigación aplicada.
  COBIT 4.1 ofrece una estructura estandarizada que permite comparar su rendimiento con modelos alternativos, de forma práctica y cuantificable en auditorías reales.

- Eje 4. Vigencia en entornos operativos que no han migrado a modelos más recientes. Muchas organizaciones, especialmente en el sector público y educativo (como universidades o gobiernos), continúan usando COBIT 4.1 por su simplicidad, madurez y disponibilidad de documentación.

Aunque COBIT 4.1 es clasificado formalmente como un framework, la literatura científica demuestra claramente su tratamiento como modelo evaluativo, en particular mediante el Modelo de madurez COBIT 4.1. Este modelo permite valorar el nivel de madurez y desempeño de procesos organizacionales, funcionando como un modelo formal de evaluación, lo que lo sitúa metodológicamente en el mismo nivel que VoIPSAM, cuyo propósito es servir como modelo específico de auditoría para sistemas VoIP. Por tanto, la comparación no se realiza entre categorías incompatibles (framework vs. modelo), sino entre dos modelos de evaluación aplicados a un mismo proceso de auditoría.

4.2. Descripción general del modelo VoIPSAM

En el contexto de la seguridad VoIP, se propone un modelo de auditoría de seguridad específico para sistemas VoIP, orientado a mitigar los riesgos inherentes a este tipo de entornos tecnológicos y a proteger de forma integral la información crítica. VoIPSAM ha sido diseñado considerando principios fundamentales de la seguridad de la información, tales como la confidencialidad, integridad y disponibilidad, garantizando así que los datos y servicios estén protegidos contra accesos no autorizados, modificaciones indebidas o interrupciones en su disponibilidad. La aplicación efectiva y conjunta de estos principios permite alcanzar un estado aceptable de seguridad en los sistemas VoIP.

La construcción del modelo se fundamentó en un proceso metodológico riguroso que integró diversas fuentes de conocimiento y análisis. Se tomaron en cuenta los antecedentes relevantes sobre los riesgos de seguridad en entornos VoIP, los requerimientos técnicos específicos para su protección, así como una evaluación crítica

de frameworks reconocidos lo cual permitió identificar las limitaciones de dichos marcos de trabajo en cuanto a su aplicabilidad específica a escenarios VoIP, evidenciando la necesidad de un modelo más adaptado a este tipo de entornos.

Adicionalmente, el modelo incorpora un enfoque integral que contempla no solo aspectos técnicos, sino también elementos organizacionales y humanos. En particular, se aborda la problemática de la ingeniería social a través de la incorporación de un plan de cultura de seguridad, estructurado sobre procesos personalizados de establecimiento, alineación y monitoreo de políticas internas. Estas políticas deben estar orientadas a las necesidades específicas de cada organización, y ser coherentes con su visión institucional, dado que por sí solas no garantizan la seguridad si no se articulan con el contexto organizacional y el comportamiento humano. De este modo, VoIPSAM provee una estructura técnica de auditoría y fortalece la gestión cultural de la seguridad, promoviendo un entorno más robusto frente a amenazas tanto tecnológicas como sociales.

VoIPSAM presenta un enfoque integral que incluye al usuario como recurso TI, permitiendo proteger las operaciones corporativas y mantener la reputación y la competitividad de una organización; si los sistemas de información están protegidos los activos también, el modelo incluye controles específicos basados en políticas de seguridad.

El modelo se organiza en torno a cuatro dominios principales que estructuran el ciclo de vida del proceso de auditoría: Planear y Organizar (Dominio A), Adquirir e Implementar (Dominio B), Entrega y Soporte (Dominio C), y Monitorear y Evaluar (Dominio D). Estos dominios interactúan de manera cíclica y secuencial, garantizando la cobertura integral de los procesos críticos asociados a la seguridad de los sistemas VoIP. Los dominios del modelo se observan en la Figura 11.

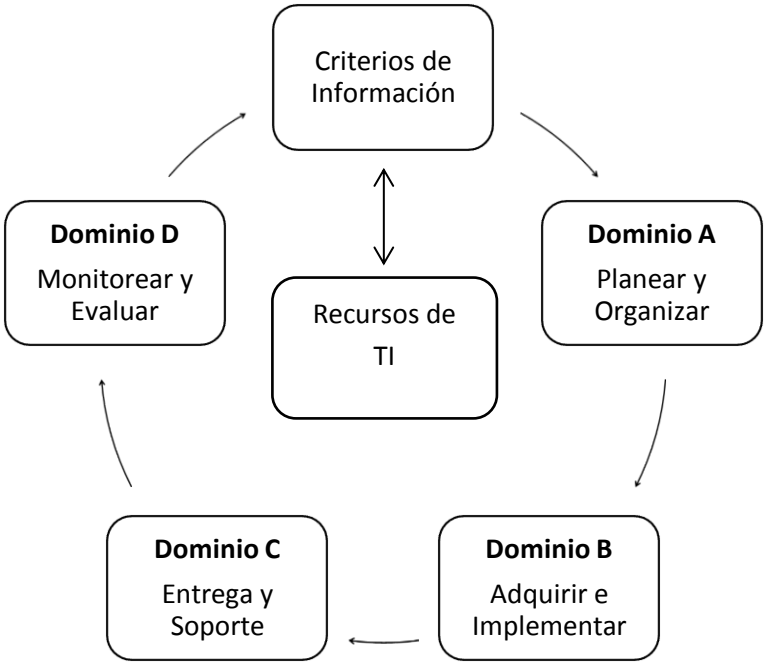


Figura 11. **Dominios VoIPSAM.**
Fuente. Elaborada por el autor.

En el núcleo del modelo se ubican los Recursos de Tecnologías de la Información, los cuales constituyen los medios sobre los que se aplican los procesos de auditoría. Dichos recursos están orientados a cumplir con los Criterios de Información, los cuales representan los atributos esenciales que debe cumplir la información en un entorno seguro: eficacia, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

La interacción entre los dominios, los recursos y los criterios de información permite al modelo VoIPSAM estructurar una auditoría especializada y adaptada al contexto VoIP, asegurando tanto la cobertura técnica como el alineamiento con los objetivos estratégicos de la organización. Esta configuración posibilita una evaluación más precisa, orientada a la mitigación de riesgos específicos del entorno VoIP y al fortalecimiento de la cultura de seguridad institucional.

4.3. Validación del modelo propuesto VoIPSAM

Una vez estructurado el modelo VoIPSAM y definida su configuración general se procedió a realizar su validación orientada a analizar la pertinencia, coherencia interna y aplicabilidad teórica.

Esta fase tuvo como objetivo principal revisar la solidez conceptual y estructural del modelo. Para ello, se sometió a revisión por parte de expertos en auditoría de seguridad y en tecnologías VoIP, quienes evaluaron los componentes del modelo, sus dominios, lineamientos técnicos, así como los mecanismos propuestos para abordar riesgos organizacionales, especialmente aquellos asociados a la ingeniería social. La retroalimentación obtenida permitió realizar ajustes en la formulación del modelo, reforzar su alineación con los criterios de seguridad de la información y garantizar su viabilidad metodológica para auditorías especializadas en entornos VoIP.

La validación del modelo propuesto de auditoría de seguridad VoIPSAM se presenta en las Secciones 5 y 6 del artículo denominado “VoIP security auditing model based on COBIT 4.1” de los autores Oscar Danilo Gavilanez Alvarez y Glen Dario Rodriguez Rafael, publicado en “International Journal of Security and Networks” e indexado en Scopus https://www.scopus.com/pages/publications/85132258795 (Gavilanez & Rodriguez, 2022). El artículo se puede apreciar en el **Anexo N Artículos publicados**.

El artículo publicado en el International Journal of Security and Networks y utilizado en esta investigación fue sometido a un proceso de revisión científica riguroso. La revista es peer-reviewed, lo que significa que todos los manuscritos son evaluados por expertos independientes antes de su aceptación. En particular, el proceso editorial se basa en una evaluación doble ciego (double-blind review), donde se preserva el anonimato de autores y revisores para garantizar objetividad y ausencia de sesgo. Los evaluadores externos examinan la originalidad, relevancia, metodología y contribución científica de

cada artículo, emitiendo recomendaciones que determinan la aceptación, modificación o rechazo.

A continuación se detalla el proceso de validación del modelo. Se plantearon 2 encuestas como instrumentos de validación considerando los principales aspectos de acuerdo a las políticas de seguridad del modelo propuesto:

- ***Encuesta A1. Aspectos Ingeniería Social (Modelo Auditoría de Seguridad VoIP).*** La encuesta determina la relevancia/pertinencia de varios aspectos de Ingeniería Social considerados en el Modelo de Auditoría de Seguridad VoIP propuesto, aspectos que evalúan la seguridad en cuanto a confidencialidad, integridad y disponibilidad. Para la aplicación de la encuesta A1 se consideraron cuatro expertos en ingeniería social y auditoría de seguridades en VoIP, en ambos casos se determinó como perfil mínimo a ingenieros en sistemas informáticos, ingenieros en electrónica y telecomunicaciones, y especialistas en detección y prevención de fraudes informáticos. Los expertos en ingeniería social participantes en el estudio cuentan con una experiencia mínima de dos años en peritaje informático, prevención de fraudes informáticos, psicofisiología forense y auditoría de tecnologías de la información, y pertenecen a instituciones de Argentina, Perú y Ecuador. La encuesta A1 se encuentra en el **Anexo C Encuesta A1. Aspectos Ingeniería Social (Modelo Auditoría de Seguridad VoIP)**.

- ***Encuesta B1. Modelo de auditoría de seguridad VoIP***. La encuesta determina la importancia y aplicabilidad del modelo propuesto que evalúe el impacto de los problemas de seguridad y enfrente los desafíos relacionados con la protección de los recursos de TI. Se tomaron en cuenta cuatro expertos en auditoría de seguridades en VoIP, quienes cumplen con una experiencia mínima de 2 años en seguridad de la información, consultores de seguridad, auditores de seguridad y además poseen certificaciones de seguridad, los expertos pertenecen a instituciones de Perú, Argentina, Ecuador e Italia. La encuesta B1 se encuentra en el **Anexo D Encuesta B1. Modelo de auditoría de seguridad VoIP**.

Para las preguntas incluidas en las encuestas se empleó una escala de valoración numérica de cinco niveles, organizada en orden ascendente y corresponde a la escala de Rensis Likert, como se muestra en la Tabla 25.

Tabla 25. **Escala de Rensis Likert.**

Ítem	**Valor**
Muy en desacuerdo	1
En desacuerdo	2
Ni de acuerdo ni en desacuerdo	3
De acuerdo	4
Muy de acuerdo	5

Fuente: Elaborada por el autor.

Se agruparon las preguntas según su área común respectiva como se aprecia en las Tablas 26 y 27; estos valores corresponden a las respuestas de cuatro expertos según la escala Likert mencionada en la Tabla 25.

Tabla 26. **Grupos Encuesta A1. Ingeniería Social - VoIPSAM.**

Pregunta: ¿Es adecuado incluir en un modelo de auditoría de seguridad para sistemas VoIP…?				
Grupo1. Ingeniería social (pruebas de penetración de seguridad)	**Valor**			
A1. ¿incentivos y motivadores en ingeniería social?	5	1	5	4
A2. ¿Phishing/Vishing?	5	3	4	2
A3. ¿Pretexting?	5	5	5	2
A4. ¿Media Dropping?	5	4	5	2
A5. ¿Tailgating?	5	4	5	2
Grupo 2. Plan de Cultura de seguridad	**Valor**			
A6. ¿revisión de las políticas de seguridad (de la información) vigentes?	5	5	5	4
A7. ¿evaluación del cumplimiento de las políticas de seguridad?	5	5	5	4
A8. ¿evaluación de recursos humanos?	5	4	4	2
A9. ¿la definición de un plan de desarrollo de cultura de seguridad?	5	3	5	3
A10. ¿evaluación de valores clave que afectan a la cultura de seguridad de la organización?	5	3	5	3
A11. ¿evaluación de la división de la responsabilidad y la autoridad, e incorporación de esos valores en las jerarquías y divisiones organizacionales?	5	4	5	3
A12. ¿evaluación de conceptualización de la seguridad de la información por parte de la organización?	5	5	4	3

A13. ¿evaluación de la descripción de la gestión y el control de la información como un recurso compartido?	5	4	5	4
A14. ¿evaluación de la selección y priorización de las actividades funcionales cotidianas de la organización, incluidas tareas, interacciones, decisiones y evaluaciones?	5	4	5	3
A15. ¿evaluación de la gestión de la tecnología como un recurso organizacional?	5	4	5	2
A16. ¿evaluación de…? a) Cómo las personas son tratadas y utilizadas como un recurso dentro de la organización. b) Comprensión y gestión del riesgo dentro de la organización. c) Formas en que la organización entiende y asume la responsabilidad. d) Desempeño y responsabilidad como requisito básico para la organización	5	3	5	3

Fuente: Elaborada por el autor.

Tabla 27. **Grupos Encuesta B1. Modelo de auditoría de seguridad VoIPSAM.**

Pregunta: ¿Es adecuado incluir en un modelo de auditoría de seguridad para sistemas VoIP…?				
Grupo 3. Definir un Plan Estratégico de TI	**Valor**			
B1.1. Gestión de valor	5	5	3	4
B1.2. Negocios – Alineación TI	5	5	4	5
Grupo 4. Definir la Arquitectura de la Información	**Valor**			
B2.1. Información del modelo de arquitectura empresarial	5	4	4	4
B2.2. Esquema de clasificación de datos	5	4	4	5
Grupo 5. Definir los procesos, organización y relaciones	**Valor**			
B3.1. Establecimiento de funciones y responsabilidades	5	5	5	4
B3.2. Responsabilidad sobre el riesgo, seguridad y cumplimiento	5	5	5	4
B3.3. Datos y sistema de propiedad	5	4	4	3
Grupo 6. Definir Plan de Cultura de seguridad	**Valor**			
B4.1. Configuración de seguridad establecida a partir de políticas de auditoría	5	4	5	5
B4.2. Directivas de contraseña	5	4	5	5
B4.3. Controles de acceso de la aplicación	4	5	5	5
B4.4. Controles de seguridad física	5	4	5	5
B4.5. Restricción de los detalles del sistema de VoIP implementado	5	4	5	4
B4.6. Establecimiento de directrices	5	3	4	5
Grupo 7. Administrar la calidad de servicio (QoS)	**Valor**			
B5.1. Generar un plan de gestión para criterios de evaluación	5	4	5	4
B5.2. Equilibrar el rendimiento de la red con el costo del servicio	5	4	5	5
Grupo 8. Monitorear y evaluar el control interno	**Valor**			
B6.1. Seguimiento del marco de control interno	3	4	5	5
B6.2. Revisión de supervisión	4	5	5	4
B6.3. Excepciones de Control	3	4	4	5

Pregunta: ¿Es adecuado incluir en un modelo de auditoría de seguridad para sistemas VoIP…?				
B6.4. Control de autoevaluación	3	4	5	4
B6.5. Acción correctiva	4	5	5	5
Grupo 9. Garantizar el cumplimiento de los requisitos externos	**Valor**			
B7.1. Identificar los requerimientos de las leyes, regulaciones y cumplimientos contractuales	3	5	5	4
B7.2. Optimización de la respuesta a los requerimientos externos	4	4	4	5
B7.3. Evaluación del cumplimiento de los requisitos externos	3	4	4	5
B7.4. Aseguramiento positivo del cumplimiento	3	5	4	4
Grupo 10. Proporcionar gobierno de TI	**Valor**			
B8.1. Establecimiento de un marco de gobierno de TI	3	4	5	5
B8.2. Entrega de valor	2	5	4	5
Grupo 11. Evaluar QoS	**Valor**			
B9.1. Evaluar QoS rentable	4	3	4	4
B9.2. Evaluar QoS en base a la medición de parámetros según estándares de calidad	3	3	4	4
Grupo 12. Monitorear plan de cultura de seguridad	**Valor**			
B10.1. Administración de Supervisión de implementaciones y operaciones del servidor VoIP	5	4	5	5
B10.2. Preparar una muestra de las implementaciones de servidores VoIP recientes	5	3	4	5
B10.3. Seleccionar implementaciones del servidor VoIP de alto riesgo o de alto perfil	5	3	4	5
B10.4. Obtener la documentación del proyecto	5	5	4	5
B10.5. Determinar si el seguimiento del proyecto de servidor VoIP está en alineación con las normas de la empresa	5	4	4	4
B10.6. Determinar si las operaciones del servidor de VoIP son monitoreadas de manera compatible con otros procesos operativos	5	3	4	4
B10.7. Emisión del monitoreo del plan de seguridad	5	4	4	5
B10.8. Evaluar la función de supervisión para la eficacia, integridad y escaladas apropiadas y oportunas	5	3	4	4

Fuente: Elaborada por el autor.

Resultados

George y Mallery (2021) sugieren recomendaciones para evaluar los coeficientes alfa de Cronbach, la Tabla 28 presenta los coeficientes alfa (α) junto con su correspondiente interpretación.

Tabla 28. **Fiabilidad de George y Mallery.**

Resultado estadístico	Significado
$\alpha \geq 0{,}90$	excelente
$0{,}90 > \alpha \geq 0{,}80$	bueno
$0{,}80 > \alpha \geq 0{,}70$	aceptable
$0{,}70 > \alpha \geq 0{,}60$	cuestionable
$0{,}60 > \alpha \geq 0{,}50$	deficiente
$\alpha < 0{,}50$	inaceptable

Fuente: George y Mallery (2021).

La consistencia interna y el grado de confiabilidad de las variables del cuestionario utilizadas en la encuesta se midieron utilizando los valores Alfa de Cronbach. IBM SPSS Statistics permitió medir en términos de estadísticas de confiabilidad, matriz de correlación entre ítems y estadísticas totales de ítems. La Tabla 28 de estadísticas de confiabilidad proporciona los valores actuales del Alfa de Cronbach. Esto oscila entre 0 y 1. El valor alfa de Cronbach preferido debe ser superior a 0,7. Se cree que un valor inferior a 0,6 es deficiente, mientras que un valor inferior a 0,5 es generalmente inaceptable. Sin embargo, un valor superior a 0,8 se considera bueno y un valor superior a 0,9 se considera excelente.

Mediante el análisis de fiabilidad utilizando SPSS, se consideró el Alfa de Cronbach para cada grupo de preguntas por separado, los resultados se detallan en la Tabla 29, los cuales garantizan la consistencia interna del instrumento.

Tabla 29. **Estadísticas de fiabilidad Alfa de Cronbach.**

Grupo	Criterio	Alfa de Cronbach	N elementos	Significado
G1	A1. Ingeniería Social (Pruebas de penetración)	0,868	5	bueno
G2	A2. Plan de Cultura de seguridad	0,967	11	excelente
G3	B1. Definir un Plan Estratégico de TI	0,833	2	bueno
G4	B2. Definir la Arquitectura de la Información	0,727	2	aceptable

G5	B3. Definir los procesos, organización y Relaciones	0,917	3	excelente
G6	B4. Definir Plan de Cultura de seguridad	0,768	6	aceptable
G7	B5. Administrar la calidad de servicio (QoS)	0,727	2	aceptable
G8	B6. Monitorear y Evaluar el Control Interno	0,760	11	aceptable
G9	B7. Garantizar el cumplimiento de los requisitos externos	0,745	4	aceptable
G10	B8. Proporcionar Gobierno de TI	0,814	2	bueno
G11	B9. Evaluar QoS	0,727	2	aceptable
G12	B10. Monitorear Plan de Cultura de Seguridad	0,931	8	excelente

Fuente: Elaborada por el autor.

La confiabilidad se evaluó mediante el coeficiente Alfa de Cronbach, utilizado para medir la consistencia interna de los cuestionarios. Este análisis considera las correlaciones entre las variables o ítems que componen la escala, bajo el supuesto de que todos miden un mismo constructo y están estrechamente relacionados. Un valor del alfa cercano a 1 indica una mayor consistencia interna entre los ítems analizados.

El análisis de fiabilidad mediante el alfa de Cronbach para las encuestas muestra valores mayores a 0,7; resultados que garantizan la consistencia interna de los instrumentos aplicados. Las encuestas se aplicaron a expertos en ingeniería social y auditoría de seguridades en VoIP, los resultados de la media estadística por pregunta ponderada a un valor de 5 se detallan en la Tabla 30.

Tabla 30. **Media Estadística de elemento.**

Pregunta: ¿Es adecuado incluir en un modelo de auditoría de seguridad para sistemas VoIP…?	**Media**
A1. ¿Incentivos y motivadores en Ingeniería Social?	3,75
A2. ¿Phishing/Vishing?	3,50
A3. ¿Pretexting?	4,25
A4. ¿Media Dropping?	4,00

Pregunta: ¿Es adecuado incluir en un modelo de auditoría de seguridad para sistemas VoIP…?	**Media**
A5. ¿Tailgating?	4,00
A6. ¿revisión de las políticas de Seguridad (de la información) vigentes?	4,75
A7. ¿evaluación del cumplimiento de las políticas de seguridad?	4,75
A8. ¿evaluación de Recursos Humanos?	3,75
A9. ¿definición de un Plan de Desarrollo de Cultura de Seguridad?	4,00
A10. ¿evaluación de valores clave que afectan a la cultura de seguridad de la organización?	4,00
A11. ¿evaluación de la división de la responsabilidad y la autoridad, e incorporación de esos valores en las jerarquías y divisiones organizacionales?	4,25
A12. ¿evaluación de conceptualización de la seguridad de la información por parte de la organización?	4,25
A13. ¿evaluación de la descripción de la gestión y el control de la información como un recurso compartido?	4,50
A14. ¿evaluación de la selección y priorización de las actividades funcionales cotidianas de la organización, incluidas tareas, interacciones, decisiones y evaluaciones	4,25
A15. ¿evaluación de la gestión de la tecnología como un recurso organizacional?	4,00
A16. ¿evaluación de…? a) Cómo las personas son tratadas y utilizadas como un recurso dentro de la organización. b) Comprensión y gestión del riesgo c) Formas en que la organización entiende y asume la responsabilidad. d) Desempeño y responsabilidad como requisito básico para la organización	4,00
B1.1. Gestión de Valor	4,25
B1.2. Negocios – Alineación TI	4,75
B2.1. Información de Arquitectura Empresarial Modelo	4,25
B2.2. Esquema de Clasificación de Datos	4,50
B3.1. Establecimiento de funciones y responsabilidades	4,75
B3.2. Responsabilidad sobre el Riesgo, Seguridad y Cumplimiento	4,75
B3.3. Datos y Sistema de Propiedad	4,00
B4.1. Configuración de seguridad establecida a partir de Políticas de Auditoría	4,75

Pregunta: ¿Es adecuado incluir en un modelo de auditoría de seguridad para sistemas VoIP…?	**Media**
B4.2. Directivas de contraseña	4,75
B4.3. Controles de acceso de la aplicación	4,75
B4.4. Controles de seguridad física	4,75
B4.5. Restricción de los detalles del sistema de VoIP implementado	4,50
B4.6. Establecimiento de directrices	4,25
B5.1. Generar un plan de gestión para criterios de evaluación	4,50
B5.2. Equilibrar el rendimiento de la red con el costo del servicio	4,75
B6.1. Seguimiento del Marco de Control Interno	4,25
B6.2. Revisión de Supervisión	4,50
B6.3. Excepciones de Control	4,00
B6.4. Control de Autoevaluación	4,00
B6.5. Acción Correctiva	4,75
B7.1. Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales	4,25
B7.2. Optimización de la respuesta a los requerimientos externos	4,25
B7.3. Evaluación del cumplimiento de los requisitos externos	4,00
B7.4. Aseguramiento Positivo del Cumplimiento	4,00
B8.1. Establecimiento de un Marco de Gobierno de TI	4,25
B8.2. Entrega de valor	4,00
B9.1. Evaluar QoS Rentable	3,75
B9.2. Evaluar QoS en base a la medición de parámetros según estándares de calidad	3,50
B10.1. Administración de Supervisión de implementaciones y operaciones del servidor VoIP	4,75
B10.2. Preparar una muestra de las implementaciones de servidores VoIP recientes	4,25
B10.3. Seleccionar implementaciones del servidor VoIP de alto riesgo o de alto perfil	4,25
B10.4. Obtener la documentación del proyecto	4,75
B10.5. Determinar si el seguimiento del proyecto de servidor VoIP estaba / está en alineación con las normas de la empresa	4,25
B10.6. Determinar si las operaciones del servidor de VoIP son monitoreadas de manera compatible con otros procesos operativos	4,00
B10.7. Emisión del Monitoreo del Plan de seguridad	4,50

Pregunta: ¿Es adecuado incluir en un modelo de auditoría de seguridad para sistemas VoIP…?	**Media**
B10.8. Evaluar la función de supervisión para la eficacia, integridad y escaladas apropiadas y oportunas	4,00

Fuente: Elaborada por el autor.

Mediante la comprobación por medias estadísticas, las encuestas indican que las preguntas A1, A2, A8, B9.1 y B9.2 presentan valores por bajo 4, por lo tanto, se eliminaron los procesos respectivos. Con el resultado de validación se establecieron las políticas de seguridad según los casos e ítems a ser auditados lo cual se evidencia en 5.3 Guía de auditoría de seguridad VoIPSAM. El modelo propuesto fue validado por expertos en ingeniería social y auditoría de seguridades en VoIP, la validación de 52 aspectos considerados muestra como resultado 47 ítems con valores de medias estadísticas iguales o superiores a 4 que garantizan la consistencia de los ítems planteados.

4.4. Componentes del modelo VoIPSAM

En base a la validación del modelo propuesto VoIPSAM, se establecen los procesos definitivos asociados a los dominios, los cuales se muestran en la Figura 12 (Gavilanez & Rodriguez, 2022).

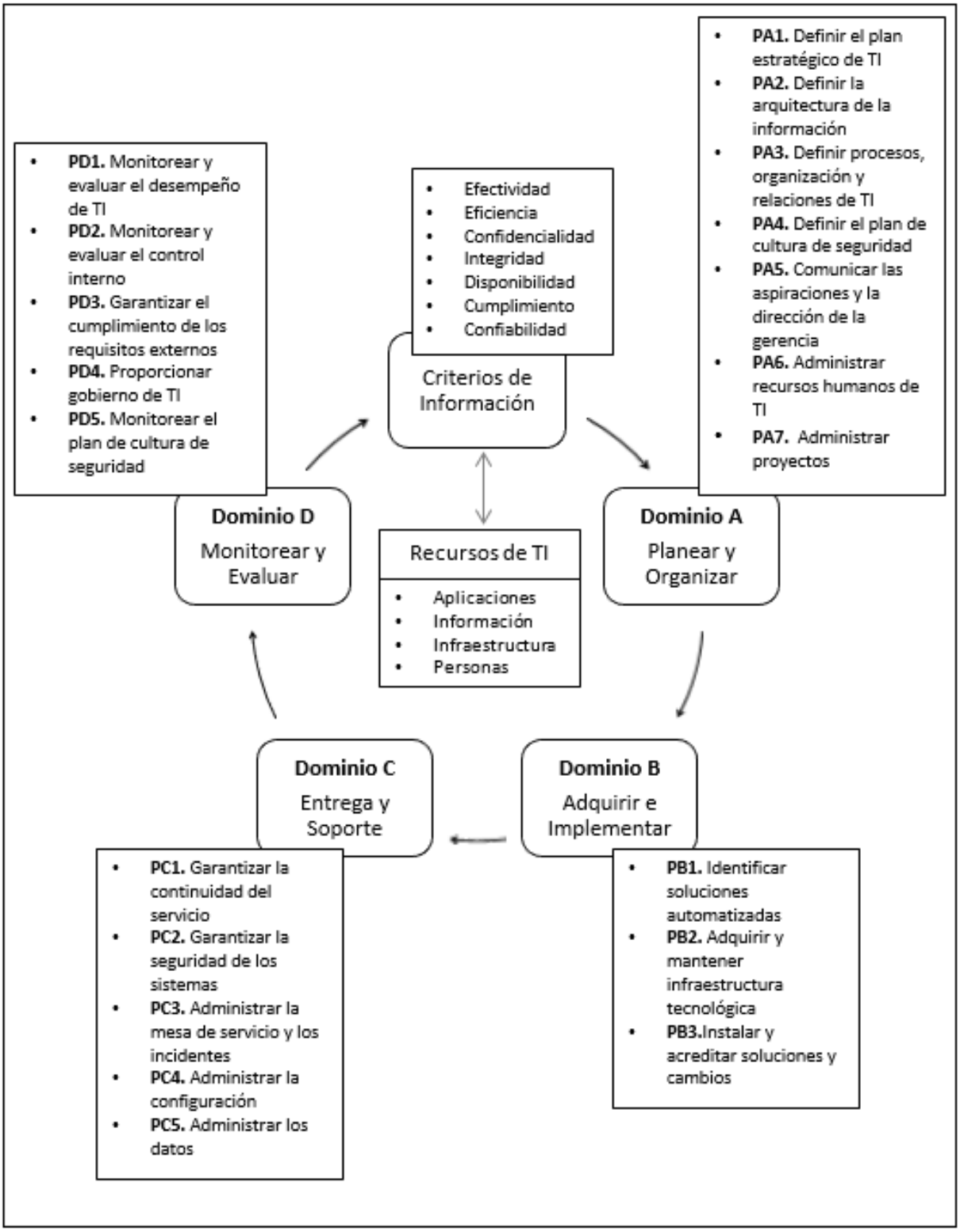


Figura 12. **Procesos asociados a los dominios VoIPSAM.**
Fuente: Gavilanez y Rodriguez (2022).

El dominio A *Planear y Organizar* incluye el plan estratégico de TI en el cual se deben establecer los procesos de auditoría de seguridad, de esta forma el beneficio de los procesos se extiende al modelo. El diseño y gestión del sistema de seguridad integral de TI incluye protección de recursos TI en la definición del plan estratégico y procesos de TI, lo que permite salvaguardar la protección de activos de la compañía. La definición del Plan de Cultura de Seguridad aporta en la aplicación de medidas de control incluyendo la ingeniería social.

El modelo concibe el tratamiento específico de la auditoría desde la perspectiva de la seguridad para sistemas VoIP, el efecto de las auditorías depende en gran medida de la gestión, razón por la cual se incluye un enfoque de directrices de auditoría específico de seguridad para VoIP que permita el respectivo monitoreo y reporte de la eficacia de los controles internos (cumplimiento de políticas, seguridad de la información y controles de cambios) mediante el dominio D *Monitorear y Evaluar*.

El modelo propuesto aborda al usuario como cliente de un servicio TI, al mismo tiempo aplica normas de seguridad específicas para auditoría de seguridad en VoIP lo cual se verifica a través del Monitoreo del Plan de Cultura de Seguridad contenido en el dominio D *Monitorear y Evaluar*; se integran las exigencias de seguridad para auditoría VoIP con los requisitos funcionales en la definición de procesos y plan estratégico de TI.

La información es importante para cualquier persona, compañía u organización, el daño o mal uso de la información puede resultar en un desastre para el usuario o para toda la empresa, además, la aparición de internet introduce oportunidades para que una persona no autorizada tenga acceso a la información; siendo necesaria la aplicación de un modelo de auditoría que permita establecer la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

La adecuada gestión de la seguridad de la información requiere implementar y mantener acciones que garanticen la integridad, disponibilidad y confidencialidad, requerimientos fundamentales para evaluar la seguridad de un sistema:

a) **Confidencialidad** es la protección de la información que sólo puede compartirse entre personas autorizadas para el caso, significa protección de la privacidad de los datos, prevención de acceso no autorizado a recursos, servicios o datos, es decir sólo las personas autorizadas pueden acceder a los datos, servicios o recursos. La confidencialidad está relacionada con la privacidad, que significa información personal individual, es el blanco atacado con mayor frecuencia. Existen algunos mecanismos utilizados para proteger la confidencialidad de los datos cuando éstos se transfieren en la red, como cerraduras de puertas, pantallas de privacidad, guardias de seguridad, contraseñas, tokens seguros y tecnologías de cifrado.

b) **Integridad** significa mantener los datos en su forma original sin ninguna modificación, entre sus objetivos constan: asegurar la información en la forma original, evitar modificaciones no autorizadas y evitar modificaciones incorrectas por accidente.

c) **Disponibilidad** representa que la información, servicio, recurso o dispositivo requerido esté siempre disponible cuando sea necesario por el usuario autorizado, la disponibilidad puede verse afectada por problemas técnicos (mal diseño del sistema, falla de dispositivo), fenómenos naturales (inundaciones, incendios) o humanos (accidental o de propósito).

Las medidas de seguridad deben mejorar la vinculación entre los procesos de negocio y sistemas de información existentes, las políticas consideradas en VoIPSAM se describen a continuación en cada dominio.

4.4.1. Dominio A. Planear y Organizar

Este dominio reúne los procesos que permiten establecer la dirección estratégica de la seguridad en tecnologías VoIP, asegurando su alineación con los objetivos institucionales y las necesidades operativas. Incluye la planificación de recursos, políticas, estructura organizacional y capacidades tecnológicas, con el fin de garantizar que las

soluciones implementadas protejan eficazmente los sistemas de comunicación y respondan de manera anticipada a los desafíos técnicos y de seguridad que presenta el entorno VoIP. La Figura 13 detalla los procesos asociados al Dominio A.

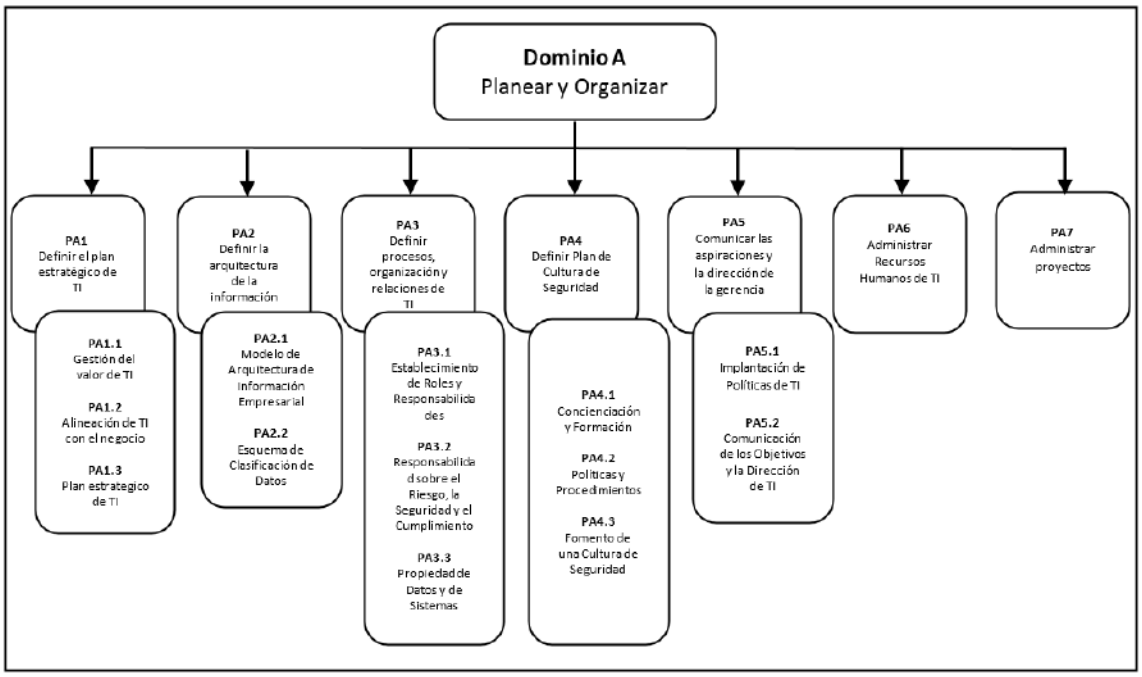


Figura 13. **Procesos asociados al Dominio A. Planear y Organizar.**
Fuente. Elaborada por el autor.

Proceso PA1. Definir el plan estratégico de TI

Establece una visión de largo plazo sobre cómo las tecnologías de la información, en particular los sistemas VoIP, pueden contribuir a los objetivos institucionales bajo un enfoque de seguridad integral. Implica identificar prioridades estratégicas relacionadas con la protección de las comunicaciones, definir recursos clave y establecer acciones concretas que garanticen la confidencialidad, integridad y disponibilidad de los servicios VoIP, todo ello en coherencia con la planificación global de la organización.

- PA1.1 Gestión del valor de TI

  Implica trabajar conjuntamente con las áreas estratégicas de la organización para garantizar que las inversiones destinadas a tecnologías VoIP y su seguridad estén debidamente justificadas. Esto se logra mediante la priorización de iniciativas que presenten beneficios claros, alineadas con los objetivos institucionales, y respaldadas por análisis que demuestren su viabilidad, impacto en la protección de las comunicaciones y valor agregado para el negocio.

- PA1.2 Alineación de TI con el negocio

  Promueve la colaboración activa entre los responsables de tecnología y las áreas estratégicas de la organización, con el fin de asegurar que las decisiones relacionadas con los sistemas VoIP y su seguridad estén integradas en la planificación institucional. Se busca una comprensión compartida de los objetivos, permitiendo que las soluciones de comunicación y sus controles de protección se ajusten a las necesidades del negocio y contribuyan directamente a su desarrollo sostenible.

- PA1.3 Plan estratégico de TI

  Contempla la elaboración de un plan estratégico que defina con claridad los recursos necesarios para implementar y mantener soluciones VoIP seguras. Incluye la proyección de presupuestos, identificación de fuentes de financiamiento, lineamientos para la adquisición de tecnologías y cumplimiento de requisitos legales y normativos. Este plan sirve como base para el desarrollo de acciones tácticas que aseguren la protección y sostenibilidad de los servicios de comunicación de la organización.

Proceso PA2. Definir la arquitectura de la información

Consiste en establecer la estructura lógica y técnica que regula el tratamiento de la información generada y utilizada por los sistemas VoIP. Incluye la definición de cómo deben organizarse, integrarse y protegerse los datos relacionados con las comunicaciones, garantizando su disponibilidad, consistencia e integridad. Asimismo, busca asegurar que el flujo de información entre las áreas de la organización sea eficiente, seguro y alineado con los objetivos operativos y estratégicos.

- PA2.1 Modelo de arquitectura de información empresarial

  Consiste en diseñar y actualizar un modelo estructurado que represente cómo se organiza y gestiona la información relacionada con los sistemas VoIP dentro de la organización. El objetivo es proporcionar una base coherente que facilite el desarrollo de aplicaciones seguras, el intercambio de datos entre plataformas y el soporte a la toma de decisiones estratégicas, en coherencia con los lineamientos del plan tecnológico institucional.

- PA2.2 Esquema de clasificación de datos

  Establece un sistema de categorización de la información gestionada por los servicios VoIP, considerando su nivel de sensibilidad y criticidad para la organización. Clasificaciones como información pública, confidencial o restringida permiten definir responsabilidades de custodia, aplicar niveles de seguridad diferenciados, y establecer controles adecuados para su acceso, cifrado, almacenamiento, conservación y eliminación. Este esquema sirve como base para proteger eficazmente los datos en entornos de comunicación digital y cumplir con políticas internas y normativas legales.

Proceso PA3. Definir procesos, organización y relaciones de TI

Define cómo se distribuyen las funciones, responsabilidades y niveles de autoridad dentro del área de TI, con un enfoque específico en la gestión segura de sistemas VoIP. Establece los mecanismos de coordinación y colaboración entre TI y otras áreas organizacionales, asegurando una integración efectiva de los procesos de comunicación, monitoreo, soporte y seguridad en todo el entorno institucional.

- PA3.1 Establecimiento de roles y responsabilidades

  Se centra en asignar de manera clara las funciones, atribuciones y responsabilidades tanto del personal técnico como de los usuarios que interactúan con los sistemas VoIP. Incluye la definición de límites de autoridad, obligaciones de cumplimiento y mecanismos de coordinación, con el objetivo de garantizar una gestión segura,

eficiente y alineada con los requerimientos organizacionales en materia de comunicaciones y protección de la información.

- PA3.2 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento
  Consiste en asignar la responsabilidad de los riesgos asociados a los sistemas VoIP a niveles ejecutivos con capacidad de decisión, asegurando su adecuada gestión. Incluye la definición de roles estratégicos y operativos encargados de supervisar la seguridad de la información, la protección física de los recursos tecnológicos y el cumplimiento de normativas aplicables, garantizando así un enfoque integral y proactivo frente a los riesgos en el entorno de comunicaciones IP.

- PA3.3 Propiedad de datos y de sistemas
  Establece mecanismos para que las áreas responsables dentro de la organización asuman formalmente la custodia y gestión de los datos y sistemas vinculados a la infraestructura VoIP. A través de procedimientos y herramientas específicas, se facilita la identificación de propietarios, la clasificación de la información según su sensibilidad y la aplicación de medidas de protección acordes con su nivel de criticidad, contribuyendo a una gestión segura y responsable de los activos de información.

Proceso PA4. Definir el plan de cultura de seguridad

Tiene como finalidad desarrollar una estrategia institucional que fomente comportamientos seguros y una conciencia activa frente a los riesgos que afectan la seguridad en sistemas VoIP. Incluye actividades de capacitación, campañas de sensibilización y la adopción de políticas internas que refuercen prácticas responsables entre los usuarios. Su implementación busca minimizar vulnerabilidades relacionadas con el factor humano, especialmente aquellas derivadas de ataques de ingeniería social, fortaleciendo así la postura de seguridad organizacional.

- PA4.1 Concienciación y formación

  Contempla el desarrollo de programas de capacitación específicos para reforzar el conocimiento del personal frente a amenazas relacionadas con la seguridad en entornos VoIP, especialmente aquellas vinculadas a la ingeniería social. Incluye la implementación de sesiones formativas con ejemplos basados en incidentes reales, así como la realización de simulacros (campañas de phishing controladas o pruebas de respuesta ante engaños) que permitan evaluar la capacidad de los usuarios para reconocer y reaccionar adecuadamente ante intentos de manipulación o intrusión.

- PA4.2 Políticas y procedimientos

  Establece directrices claras y procedimientos operativos enfocados en la prevención, detección y respuesta ante amenazas de ingeniería social que comprometan la seguridad de los sistemas VoIP. Comprende la formulación de políticas institucionales que definan prácticas seguras, así como la implementación de mecanismos de control como autenticación robusta, validación de identidad y restricciones de acceso. Estas medidas buscan fortalecer la protección del entorno de comunicaciones, reduciendo los riesgos asociados al comportamiento humano y a la manipulación psicológica de los usuarios.

- PA4.3 Fomento de una cultura de seguridad

  Promueve la creación de un entorno organizacional donde la seguridad de la información en sistemas VoIP, sea parte integral del comportamiento diario. Involucra el compromiso activo de la alta dirección, una comunicación constante sobre buenas prácticas y amenazas emergentes, así como el uso de incentivos que refuercen actitudes responsables. Además, fomenta la participación del personal en la identificación y reporte de intentos de ingeniería social, fortaleciendo así una cultura preventiva y colaborativa.

Proceso PA5. Comunicar las aspiraciones y la dirección de la gerencia

Tiene como objetivo transmitir de forma clara y sistemática la visión institucional, los objetivos estratégicos y las prioridades definidas por la alta dirección en relación con

la seguridad de los sistemas VoIP. Busca asegurar que todos los niveles de la organización comprendan y adopten de manera coherente los lineamientos establecidos, fomentando una cultura de compromiso, responsabilidad compartida y alineación con las políticas que rigen la protección de las comunicaciones digitales.

- PA5.1 Implantación de políticas de TI

  Garantiza que las políticas relacionadas con el uso y la seguridad de los sistemas VoIP sean implementadas de forma efectiva y comunicadas a todo el personal involucrado. Se enfoca en integrar dichas políticas como parte fundamental de las actividades operativas, asegurando que su aplicación sea comprendida, adoptada y respaldada por los distintos niveles organizacionales, con el fin de mantener un entorno de comunicaciones seguro y alineado con los objetivos institucionales.

- PA5.2 Comunicación de los objetivos y la dirección de TI

  Asegura que los lineamientos estratégicos y los objetivos definidos para la gestión y protección de los sistemas VoIP sean comunicados de forma clara y oportuna a todos los actores relevantes dentro de la organización. Su finalidad es lograr que tanto usuarios como responsables técnicos comprendan el rumbo institucional en materia de seguridad tecnológica, fomentando una participación activa y coherente con las metas establecidas para resguardar las comunicaciones digitales.

Proceso PA6. Administrar recursos humanos de TI

Se orienta a gestionar de forma estratégica al personal involucrado en la administración, operación y protección de los sistemas VoIP. Incluye la planificación de perfiles, la asignación de funciones, el desarrollo de competencias técnicas y la evaluación del desempeño, con el fin de asegurar que el equipo cuente con las capacidades necesarias para implementar y mantener medidas de seguridad efectivas, alineadas con los objetivos institucionales.

Proceso PA7. Administrar proyectos

Abarca la planificación, ejecución y control de proyectos orientados al fortalecimiento de la infraestructura VoIP y su seguridad. Implica coordinar recursos, gestionar riesgos técnicos y asegurar una comunicación efectiva entre los equipos involucrados, con el objetivo de cumplir los plazos, presupuestos y requisitos definidos. Su finalidad es asegurar que cada iniciativa tecnológica contribuya de manera efectiva a la protección de las comunicaciones y se mantenga alineada con las prioridades estratégicas de la organización.

4.4.2. Dominio B. Adquirir e Implementar

Comprende las acciones orientadas a identificar, desarrollar, adaptar e incorporar soluciones tecnológicas que fortalezcan la seguridad y eficiencia de los sistemas VoIP. Se enfoca en asegurar que las herramientas y plataformas seleccionadas no solo cumplan con los requerimientos funcionales y de protección de la información, sino también se integren en los procesos organizacionales, contribuyendo al rendimiento estable y seguro del entorno operativo. Los procesos asociados al Dominio B se muestran en la Figura 14.

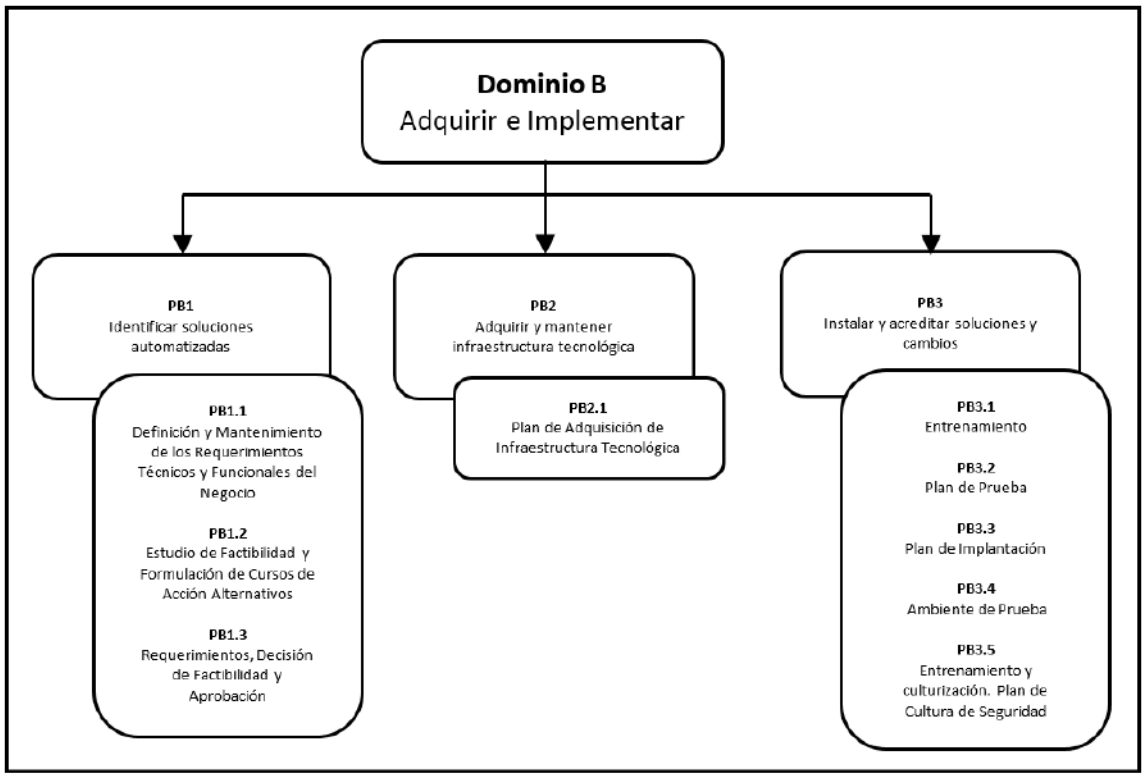


Figura 14. **Procesos asociados al Dominio B. Adquirir e Implementar**.
Fuente. Elaborada por el autor.

Proceso PB1. Identificar soluciones automatizadas

Se enfoca en analizar los requerimientos específicos de la organización en materia de comunicaciones y seguridad VoIP, con el fin de proponer herramientas tecnológicas que permitan automatizar tareas críticas. Incluye la evaluación de opciones técnicas que aporten eficiencia, reduzcan la probabilidad de errores humanos y se integren de manera segura con los procesos existentes, garantizando la continuidad operativa y el control de los servicios de VoIP.

- PB1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio.

  Consiste en identificar, documentar y actualizar los requerimientos funcionales y técnicos que debe cumplir la infraestructura VoIP para responder a las necesidades operativas y de seguridad de la organización. Incluye la priorización de estas especificaciones en coordinación con las partes interesadas, asegurando que las

soluciones seleccionadas estén alineadas con los objetivos institucionales y los criterios de protección de la información.

- PB1.2 Estudio de factibilidad y formulación de cursos de acción alternativos.
  Implica la elaboración de un análisis de viabilidad técnica, operativa y económica para determinar si los requerimientos definidos para soluciones VoIP pueden ser implementados eficazmente. En coordinación con las áreas de gestión y tecnología, se exploran distintas alternativas de acción, se evalúa su factibilidad en términos de compatibilidad, costos y riesgos, y se presentan recomendaciones fundamentadas a los responsables de la toma de decisiones.

- PB1.3 Requerimientos, decisión de factibilidad y aprobación
  Asegura que los requerimientos técnicos y funcionales, así como los resultados del estudio de factibilidad, sean formalmente revisados y aprobados por los responsables del negocio en puntos críticos previamente definidos. La aprobación incluye tanto la validación de las necesidades planteadas como la selección de la alternativa más adecuada para su implementación. La decisión final sobre la solución de seguridad VoIP y el enfoque a seguir debe estar alineada con los objetivos estratégicos institucionales y contar con el respaldo del promotor del proyecto.

Proceso PB2. Adquirir y mantener infraestructura tecnológica

Contempla la gestión integral de la infraestructura tecnológica necesaria para soportar los servicios VoIP, abarcando su adquisición, configuración y mantenimiento. Su propósito es asegurar que los componentes físicos y lógicos seleccionados sean compatibles con los requerimientos de seguridad, disponibilidad y escalabilidad del entorno organizacional, permitiendo un funcionamiento estable, eficiente y protegido frente a posibles vulnerabilidades o fallos operativos.

- PB2.1 Plan de adquisición de infraestructura tecnológica
  Consiste en elaborar un plan estructurado que defina las acciones necesarias para adquirir, implementar y mantener la infraestructura tecnológica requerida para

garantizar la seguridad en los sistemas VoIP. El plan debe estar alineado con la estrategia tecnológica institucional y responder a los requerimientos funcionales y técnicos previamente establecidos, asegurando la compatibilidad, escalabilidad y protección del entorno de comunicaciones.

Proceso PB3. Instalar y acreditar soluciones y cambios

Abarca la implementación estructurada de nuevas soluciones tecnológicas o actualizaciones en los sistemas VoIP, garantizando que se realicen de manera segura y conforme a los requerimientos funcionales definidos. Incluye la verificación técnica y la validación de que los cambios no comprometan la integridad, disponibilidad ni la confidencialidad del servicio, asegurando que el entorno continúe operando bajo condiciones óptimas de seguridad.

- PB3.1 Entrenamiento

  Se enfoca en preparar al personal técnico y a los usuarios finales mediante programas de formación específicos que aborden la operación segura de los sistemas VoIP. La capacitación debe ejecutarse conforme a un plan estructurado y adaptado a cada proyecto de desarrollo, implementación o mejora tecnológica, utilizando contenidos alineados con los riesgos, procedimientos y herramientas propios del entorno de comunicaciones IP.

- PB3.2 Plan de prueba

  Establece la creación de un plan de pruebas estructurado que permita validar la correcta implementación y el nivel de seguridad de las soluciones VoIP. El plan debe basarse en los estándares de la organización e incluir la definición de roles, responsabilidades, criterios de inicio y finalización de pruebas, así como los procedimientos de evaluación. Su aprobación por parte de los actores clave es esencial para asegurar su validez y efectividad antes de la puesta en marcha del sistema o sus componentes.

- PB3.3 Plan de implantación

  Consiste en elaborar un plan detallado para la puesta en marcha de soluciones VoIP, incorporando medidas específicas de seguridad y mecanismos de respaldo que garanticen una transición controlada y libre de riesgos. El plan debe ser revisado y aprobado por los actores clave involucrados, asegurando que las actividades de despliegue se ejecuten conforme a lo establecido y que existan protocolos de recuperación ante posibles fallos.

- PB3.4 Ambiente de prueba

  Consiste en habilitar un entorno controlado que reproduzca las condiciones del sistema VoIP en operación, permitiendo validar su comportamiento antes del despliegue final. El entorno debe contemplar medidas de seguridad, controles internos, procedimientos operativos, integridad de los datos, manejo de cargas de trabajo y protección de la privacidad, asegurando así que las pruebas reflejen con fidelidad el entorno real y permitan anticipar posibles fallos o vulnerabilidades.

- PB3.5 Entrenamiento y culturización. Plan de cultura de seguridad

  Establecer un programa integral de formación y concientización orientado a fortalecer la cultura de seguridad en la organización, con énfasis en la protección de sistemas VoIP. La capacitación abarca tanto aspectos técnicos como el uso seguro de plataformas de comunicación IP, la configuración de dispositivos y la detección de amenazas asociadas a la ingeniería social, como componentes conceptuales más amplios, relacionados con la seguridad informática y su impacto en las operaciones diarias.

  La culturización, por su parte, busca integrar los principios de seguridad en la mentalidad y el comportamiento de todos los empleados. Este enfoque promueve un entorno en el que la seguridad sea percibida como una responsabilidad compartida y prioritaria en todas las decisiones, fomentando la participación activa del personal en la protección de la información y los activos institucionales. A través de la educación continua, la comunicación efectiva y la ejemplaridad desde la alta dirección, se

consolida una cultura organizacional resiliente frente a amenazas, fortaleciendo la postura general de seguridad de la empresa.

4.4.3. Dominio C. Entrega y Soporte

Comprende los procesos destinados a garantizar la entrega eficaz, el funcionamiento continuo y el soporte adecuado de los servicios tecnológicos vinculados a los sistemas VoIP. Su propósito es asegurar que las comunicaciones se desarrollen de manera estable, segura y conforme a los requerimientos de la organización, proporcionando atención oportuna a los usuarios, gestionando incidentes y manteniendo la operatividad del entorno tecnológico bajo estándares de calidad y disponibilidad. Los procesos asociados al Dominio C se muestran en la Figura 15.

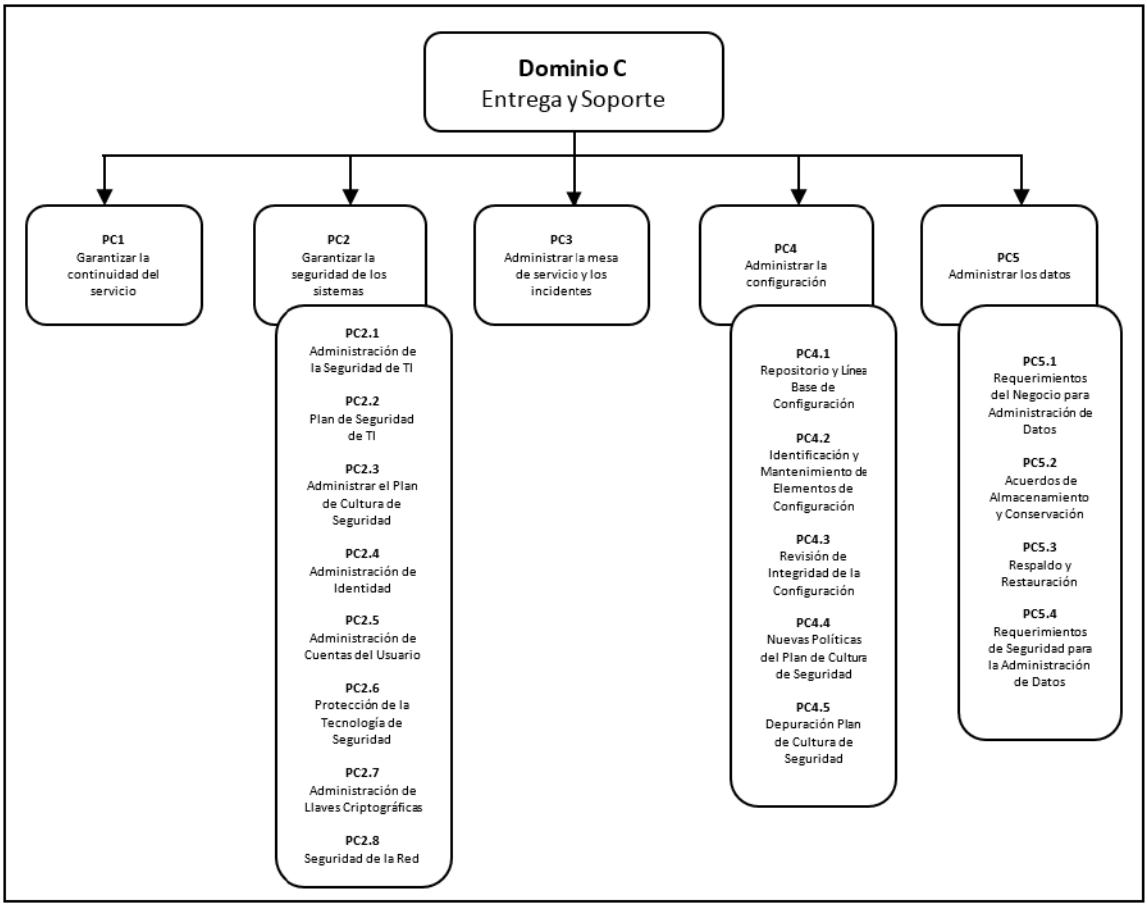


Figura 15. **Procesos asociados al Dominio C. Entrega y Soporte.**
Fuente: Elaborada por el autor.

Proceso PC1. Garantizar la continuidad del servicio

Se enfoca en asegurar la disponibilidad permanente de los servicios de comunicación VoIP, incluso ante incidentes inesperados, fallos técnicos o situaciones de emergencia. Para ello, se diseñan e implementan planes de prevención, recuperación y respuesta que permitan reducir el impacto operativo y garantizar que los sistemas críticos continúen funcionando. Estas estrategias incluyen medidas específicas de respaldo y contingencia para preservar la integridad y estabilidad de las comunicaciones en escenarios adversos.

Proceso PC2. Garantizar la seguridad de los sistemas

Tiene como objetivo salvaguardar la infraestructura VoIP frente a accesos no autorizados, modificaciones indebidas y amenazas tanto internas como externas. Incluye la aplicación de controles técnicos, procedimientos administrativos y mecanismos de supervisión continua que permitan preservar la confidencialidad, integridad y disponibilidad de las comunicaciones. Contempla la detección proactiva de vulnerabilidades y la implementación de medidas correctivas para mantener un entorno seguro y confiable.

- PC2.1 Administración de la seguridad de TI

  Se encarga de coordinar y supervisar las acciones de seguridad implementadas en los sistemas VoIP, asegurando que estén alineadas con las necesidades operativas y los objetivos estratégicos de la organización. Incluye la planificación, ejecución y seguimiento de controles técnicos y administrativos que fortalezcan la protección del entorno de comunicaciones, garantizando que las medidas adoptadas respondan de forma eficaz a los riesgos identificados y a los requerimientos institucionales.

- PC2.2 Plan de seguridad de TI

  Consiste en transformar los requerimientos de negocio, las obligaciones de cumplimiento normativo y los riesgos identificados en un plan integral de seguridad enfocado en la protección de los sistemas VoIP. El plan debe contemplar la infraestructura tecnológica disponible, las características de la cultura organizacional

y los recursos necesarios, incluyendo servicios, personal, equipos y soluciones de software. Además, se debe asegurar su ejecución mediante políticas, procedimientos formales y acciones de comunicación que permitan que los usuarios y las partes interesadas comprendan y adopten los lineamientos establecidos.

- PC2.3 Administrar el plan de cultura de seguridad

  Se encarga de coordinar, monitorear y ajustar continuamente las acciones destinadas a fortalecer la cultura de seguridad organizacional, con énfasis en la protección de los sistemas VoIP. Implica asegurar que las actividades formativas, las prácticas internas y los mensajes estratégicos se implementen de manera coherente, y que el plan evolucione en función de los cambios en el entorno tecnológico, los riesgos emergentes y las necesidades institucionales. Su propósito es fomentar un entorno donde la seguridad sea entendida, valorada y aplicada por todos los miembros de la organización.

- PC2.4 Administración de identidad

  Tiene como objetivo garantizar que cada usuario que interactúe con los sistemas VoIP esté correctamente identificado mediante credenciales únicas y mecanismos de autenticación apropiados. Los permisos de acceso deben ser coherentes con las funciones laborales, los requerimientos operativos y las políticas de seguridad de la organización. La solicitud y aprobación de estos accesos debe involucrar a la gerencia y a los responsables de los sistemas, mientras que su control debe recaer en la unidad encargada de la seguridad VoIP. Todas las identidades y privilegios deben registrarse en un repositorio centralizado y mantenerse actualizados. Además, se deben implementar soluciones de autenticación robustas y procedimientos de acceso eficientes, adaptados a las particularidades de las plataformas VoIP y orientados a garantizar su seguridad, trazabilidad y sostenibilidad operativa.

- PC2.5 Administración de cuentas del usuario

  Establece lineamientos para administrar de manera controlada el ciclo de vida de las cuentas de usuario en los sistemas VoIP, incluyendo su creación, modificación,

suspensión y eliminación. Todas las acciones deben seguir procedimientos formales, contar con aprobaciones verificables por parte de los responsables de los datos o sistemas, y aplicarse tanto a usuarios internos como externos, incluidos administradores, en condiciones normales y de emergencia. Además, los derechos de acceso deben estar claramente definidos en acuerdos o contratos, y sujetarse a revisiones periódicas que permitan verificar la vigencia, pertinencia y adecuación de los privilegios asignados.

- PC2.6 Protección de la tecnología de seguridad

  Tiene como objetivo garantizar que las soluciones tecnológicas implementadas para proteger los sistemas VoIP sean resistentes frente a intentos de sabotaje, manipulación o uso indebido. Asimismo, se debe evitar que estas tecnologías expongan documentación técnica o información sensible de forma innecesaria. Para ello, se aplican controles físicos, lógicos y administrativos que aseguren la integridad de los mecanismos de seguridad, preservando tanto su funcionalidad como la confidencialidad de los elementos que las componen.

- PC2.7 Administración de llaves criptográficas

  Establece directrices para la administración segura de las llaves criptográficas utilizadas en la protección de comunicaciones VoIP. Incluye la definición de políticas y procedimientos que regulen la generación, distribución, almacenamiento, uso, renovación y eliminación de llaves, asegurando su confidencialidad e integridad. Se deben aplicar controles estrictos para evitar accesos no autorizados o alteraciones, garantizando que los mecanismos de cifrado funcionen correctamente y mantengan la seguridad de la información transmitida.

- PC2.8 Seguridad de la red

  Este proceso se enfoca en aplicar mecanismos de control y administración que garanticen la protección de las redes utilizadas para la transmisión de VoIP. Incluye la implementación de técnicas de autenticación, segmentación, monitoreo y filtrado de tráfico para autorizar el acceso solo a usuarios y dispositivos permitidos, así como

para supervisar y controlar los flujos de información. El objetivo es prevenir accesos no autorizados, minimizar riesgos de interceptación o alteración de datos, y mantener la integridad y disponibilidad de las comunicaciones VoIP.

Proceso PC3. Administrar la mesa de servicio y los incidentes

Establece un canal formalizado de atención para responder de manera eficiente a incidentes, fallos o solicitudes relacionados con los sistemas VoIP. Incluye el registro detallado de cada evento, su análisis técnico, clasificación según criticidad, escalamiento a los niveles de soporte correspondientes y el seguimiento hasta su resolución. Además de contribuir a la disponibilidad continua del servicio, este proceso permite detectar patrones recurrentes, analizar causas raíz y generar reportes que faciliten la implementación de medidas preventivas y la mejora continua de la seguridad y operatividad del entorno de comunicaciones.

Proceso PC4. Administrar la configuración

Se encarga de controlar de manera sistemática todos los elementos que conforman la infraestructura VoIP, incluyendo hardware, software, componentes de red y parámetros de seguridad. Su propósito es mantener un inventario actualizado y confiable de las configuraciones vigentes, permitiendo rastrear cambios, prevenir inconsistencias, y asegurar que todas las modificaciones sean autorizadas, documentadas y alineadas con los estándares técnicos y de seguridad establecidos por la organización.

- PC4.1 Repositorio y línea base de configuración

  Establece la creación y mantenimiento de un repositorio centralizado que documente los componentes de configuración y activos relacionados con la infraestructura VoIP, así como los cambios que se realicen sobre ellos. La gestión de esta información permite mantener una línea base de configuración actualizada, que sirve como referencia para validar la integridad del sistema y facilita la restauración de su estado original en caso de errores, incidentes o modificaciones no autorizadas.

- PC4.2 Identificación y mantenimiento de elementos de configuración

Se enfoca en establecer procedimientos claros para identificar, registrar y mantener actualizados los elementos de configuración que componen la infraestructura VoIP. Cada cambio debe documentarse en el repositorio central y vincularse con los procesos de gestión de cambios, incidentes y problemas, permitiendo así un control integral del entorno, una trazabilidad precisa y una respuesta coordinada ante cualquier alteración que pueda afectar la estabilidad o seguridad del sistema.

- PC4.3 Revisión de integridad de la configuración

  Contempla la revisión periódica de los registros de configuración de los sistemas VoIP para garantizar su integridad tanto en el estado actual como en su historial de cambios. Incluye la validación del software instalado frente a las políticas institucionales, con el objetivo de detectar aplicaciones no autorizadas, versiones no licenciadas o implementaciones que excedan los términos contractuales. Las inconsistencias identificadas deben ser reportadas y corregidas oportunamente, contribuyendo al cumplimiento normativo y a la seguridad operativa del entorno.

- PC4.4 Nuevas políticas del plan de cultura de seguridad

  Se enfoca en el diseño, revisión y adopción de nuevas políticas que refuercen la cultura de seguridad dentro de la organización, particularmente en lo relacionado con los sistemas VoIP. Estas directrices permiten establecer normas claras de comportamiento, buenas prácticas y responsabilidades orientadas a la protección de los activos digitales, la integridad de la información y la concientización del personal. Su implementación es clave para fomentar una mentalidad organizacional proactiva frente a los riesgos de seguridad y para consolidar una postura institucional sólida y sostenible.

- PC4.5 Depuración plan de cultura de seguridad

  Tiene como finalidad evaluar de forma continua la estructura y contenido del plan de cultura de seguridad institucional, con el objetivo de identificar y eliminar elementos que resulten ineficaces, redundantes o desalineados con los objetivos de protección de

los sistemas VoIP. A través de esta depuración, se corrigen deficiencias y se optimiza el enfoque del plan, garantizando su pertinencia frente a los cambios en el entorno organizacional, las amenazas emergentes y las necesidades específicas de concientización y comportamiento seguro dentro de la organización.

Proceso PC5. Administrar los datos

Se orienta a garantizar una administración adecuada de los datos generados, transmitidos y almacenados a través de los sistemas VoIP. Implica establecer políticas y controles para asegurar la integridad, disponibilidad, confidencialidad y trazabilidad de la información, considerando todo su ciclo de vida. Además, abarca la clasificación, almacenamiento seguro, respaldo, retención y eliminación de datos, en conformidad con los requerimientos legales, normativos y organizacionales, asegurando así la protección de la información crítica y la continuidad del servicio.

- PC5.1 Requerimientos del negocio para administración de datos

  Garantiza que los datos relacionados con los sistemas VoIP sean gestionados conforme a las necesidades del negocio, asegurando su procesamiento íntegro, exacto y en el momento adecuado. También contempla que los resultados generados estén disponibles según lo establecido por los requerimientos institucionales, incorporando mecanismos que permitan la recuperación de procesos en caso de interrupciones y la reejecución controlada de tareas críticas, sin comprometer la calidad ni la seguridad de la información.

- PC5.2 Acuerdos de almacenamiento y conservación

  Establece e implementa procedimientos formales para el archivado, almacenamiento y retención segura de los datos generados por los sistemas VoIP. Estas prácticas deben estar alineadas con los objetivos estratégicos de la organización, las políticas de seguridad de la información y los marcos regulatorios aplicables. El propósito es garantizar que la información relevante se conserve durante el tiempo requerido, en condiciones que aseguren su integridad, disponibilidad y protección frente a accesos no autorizados o pérdidas accidentales.

- PC5.3 Respaldo y restauración

  Establece las directrices para realizar copias de seguridad y restaurar aplicaciones, sistemas, configuraciones y datos vinculados a los servicios VoIP. Los procedimientos deben garantizar la disponibilidad y recuperación oportuna de la información en caso de fallos, incidentes o desastres, en coherencia con los objetivos del negocio y el plan de continuidad operativa. Se debe asegurar que los respaldos se realicen con la frecuencia adecuada, se almacenen de forma segura y se prueben periódicamente para validar su eficacia.

- PC5.4 Requerimientos de seguridad para la administración de datos

  Define políticas y procedimientos destinados a proteger los datos relacionados con los sistemas VoIP a lo largo de su ciclo de vida. Se enfoca en garantizar la confidencialidad, integridad y disponibilidad de la información mediante controles alineados con los objetivos organizacionales, las políticas internas de seguridad y las normativas legales vigentes. La gestión segura de datos debe incluir medidas para prevenir accesos no autorizados, pérdidas, manipulaciones indebidas y exposiciones accidentales, fortaleciendo así la postura general de seguridad de la organización.

4.4.4. Dominio D. Monitorear y Evaluar

El dominio agrupa los procesos orientados a supervisar, evaluar y asegurar el desempeño de los servicios y controles asociados a los sistemas VoIP. Su propósito es verificar el cumplimiento de políticas, normativas y objetivos institucionales en materia de seguridad y operación, proporcionando información precisa y oportuna para la toma de decisiones y la mejora continua. A través del monitoreo sistemático y la evaluación periódica, se busca mantener altos niveles de eficacia, confiabilidad y alineación con los requerimientos del entorno organizacional. Los procesos asociados al Dominio D se muestran en la Figura 16.

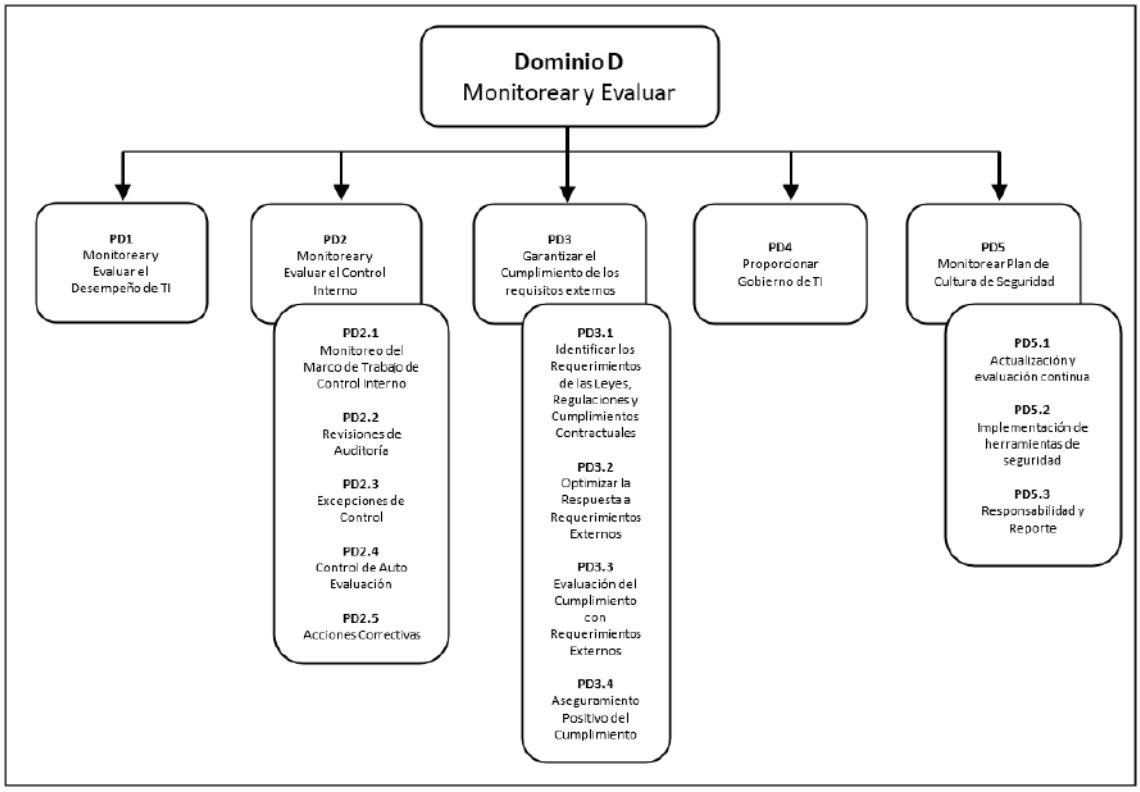


Figura 16. **Procesos asociados al Dominio D. Monitorear y Evaluar.**
Fuente. Elaborada por el autor.

Proceso PD1. Monitorear y evaluar el desempeño de TI

Se centra en establecer mecanismos de monitoreo que permitan evaluar el rendimiento de los servicios y controles aplicados a la infraestructura VoIP. Para ello, se definen indicadores clave de desempeño (KPI), se generan reportes periódicos y se identifican desviaciones respecto a los estándares establecidos. Esta información posibilita la toma de decisiones oportunas y correctivas, asegurando que las operaciones se mantengan alineadas con las políticas institucionales y con los objetivos de seguridad y eficiencia definidos por la organización.

Proceso PD2. Monitorear y evaluar el control interno

Se enfoca en verificar que los mecanismos de control implementados para proteger los sistemas VoIP funcionen de manera eficaz y conforme a los lineamientos definidos por la organización. Implica realizar evaluaciones periódicas sobre la aplicación de políticas, procedimientos y controles técnicos, con el fin de identificar debilidades, inconsistencias o áreas de mejora. La retroalimentación obtenida permite fortalecer la gobernanza de la seguridad y asegurar que las medidas de protección se mantengan efectivas frente a los riesgos operativos y tecnológicos.

- PD2.1 Monitoreo del marco de trabajo de control interno

  Consiste en monitorear, evaluar y ajustar de manera continua la estructura de control interno aplicada a la gestión y protección de los sistemas VoIP. Su propósito es asegurar que el entorno de control se mantenga eficaz, alineado con los objetivos estratégicos de la organización y adaptable frente a cambios tecnológicos o regulatorios. Esta supervisión permite identificar oportunidades de mejora y optimizar los mecanismos existentes para fortalecer la seguridad, el cumplimiento y la eficiencia operativa en el entorno de comunicaciones IP.

- PD2.2 Revisiones de auditoría

  Consiste en revisar y analizar, a través de auditorías formales, la efectividad y eficiencia de los controles internos implementados en la gestión de los sistemas VoIP. Estas evaluaciones permiten identificar debilidades, validar el cumplimiento de políticas y normativas, y verificar que los mecanismos de seguridad contribuyan al logro de los objetivos organizacionales. Los hallazgos obtenidos se utilizan como base para fortalecer la gobernanza y mejorar continuamente los procesos relacionados con la protección de las comunicaciones.

- PD2.3 Excepciones de control

  Se orienta a identificar desviaciones o fallos en la aplicación de los controles internos asociados a la seguridad y operación de los sistemas VoIP. Incluye el análisis de las causas raíz de dichas excepciones, la notificación oportuna a las partes interesadas y

la implementación de medidas correctivas que prevengan su recurrencia. La gestión efectiva de estas excepciones contribuye a mantener la integridad del entorno de control y a reforzar la resiliencia del sistema frente a riesgos operativos o de seguridad.

- PD2.4 Control de auto evaluación

  Establece un mecanismo sistemático para que las propias unidades responsables valoren la eficacia e integridad de los controles aplicados en los procesos, políticas y acuerdos relacionados con la gestión de sistemas VoIP. A través de un programa continuo de autoevaluación, se busca identificar deficiencias, validar el cumplimiento de estándares y fortalecer la capacidad de control interno sin depender exclusivamente de auditorías externas. Esta práctica promueve la mejora proactiva y el compromiso con la seguridad dentro de la organización.

- PD2.5 Acciones correctivas

  Se enfoca en gestionar de forma estructurada las medidas correctivas que surgen de auditorías, evaluaciones o revisiones de control interno vinculadas a los sistemas VoIP. Comprende la identificación de las no conformidades, el inicio y seguimiento de los planes de mejora, y la verificación de su ejecución efectiva. Su objetivo es asegurar que los hallazgos sean resueltos oportunamente, fortaleciendo los controles y reduciendo la exposición a riesgos futuros.

Proceso PD3. Garantizar el cumplimiento de los requisitos externos

Tiene como finalidad verificar que los sistemas VoIP y sus procesos asociados operen conforme a las normativas legales, estándares internacionales, políticas regulatorias y compromisos contractuales aplicables. Implica identificar los requisitos externos relevantes, supervisar su cumplimiento y aplicar medidas correctivas en caso de desviaciones. Su implementación garantiza que la organización minimice riesgos legales, mantenga su reputación institucional y demuestre responsabilidad frente a entornos regulados.

- PD3.1 Identificar los requerimientos de las leyes, regulaciones y cumplimientos contractuales.

  Se enfoca en la detección y actualización continua de leyes, normativas y obligaciones contractuales que impacten la operación y seguridad de los sistemas VoIP, tanto a nivel local como internacional. Estos requerimientos deben ser integrados en los estándares, políticas, metodologías y procedimientos de TI de la organización, asegurando que las prácticas implementadas estén alineadas con el marco legal vigente y con los compromisos adquiridos con terceros.

- PD3.2 Optimizar la respuesta a requerimientos externos.

  Consiste en revisar y adaptar de manera continua los estándares, políticas, metodologías y procedimientos relacionados con la gestión y seguridad de los sistemas VoIP, con el fin de garantizar su conformidad con las exigencias legales, regulatorias y contractuales. Además, se asegura que estas actualizaciones sean comunicadas de forma clara y efectiva a todas las partes involucradas, promoviendo el cumplimiento institucional y reduciendo riesgos asociados a incumplimientos normativos.

- PD3.3 Evaluación del cumplimiento con requerimientos externos.

  Se orienta a evaluar si los estándares, políticas, metodologías y procedimientos adoptados en la gestión y seguridad de los sistemas VoIP cumplen efectivamente con los requisitos legales, regulatorios y contractuales aplicables. Implica realizar revisiones sistemáticas que permitan identificar brechas de cumplimiento, garantizar la alineación con el marco normativo vigente y establecer acciones correctivas en caso de desviaciones.

- PD3.4 Aseguramiento positivo del cumplimiento.

  Tiene como finalidad garantizar y documentar que las políticas internas derivadas de requisitos legales, reglamentarios o contractuales se estén cumpliendo de manera efectiva en el contexto de la seguridad VoIP. Incluye la verificación de que las acciones correctivas recomendadas hayan sido ejecutadas oportunamente por los responsables del proceso, y que los registros de cumplimiento sean comunicados y

respaldados por evidencias que permitan demostrar la conformidad institucional ante auditorías o revisiones externas.

Proceso PD4. Proporcionar gobierno de TI

Busca implementar un marco de gobernanza que defina claramente el liderazgo, las estructuras organizativas, los procesos y las responsabilidades asociadas a la gestión de los sistemas VoIP. Su propósito es asegurar que las decisiones relacionadas con las inversiones, controles y servicios de seguridad VoIP estén alineadas con los objetivos estratégicos de la organización, promoviendo la transparencia, la rendición de cuentas y el uso eficiente de los recursos tecnológicos.

Proceso PD5. Monitorear el plan de cultura de seguridad

Establece estrategias para monitorear de manera continua la implementación del plan de cultura de seguridad, asegurando su alineación con los objetivos institucionales en materia de protección de sistemas VoIP. Implica controlar el cumplimiento de las actividades planificadas, evaluar los beneficios alcanzados, analizar los costos asociados y gestionar los riesgos vinculados. La retroalimentación obtenida permite ajustar el plan de forma dinámica, fortaleciendo su efectividad y sostenibilidad en el tiempo.

- PD5.1 Actualización y evaluación continua

  Promueve la actualización permanente de las políticas de seguridad y la evaluación sistemática de los riesgos asociados al uso de sistemas VoIP. Su finalidad es mantener al día las estrategias de protección frente a amenazas emergentes, como los ataques de ingeniería social. Incluye la implementación de herramientas técnicas, así como la ejecución de revisiones periódicas que permitan ajustar las políticas institucionales y fortalecer la postura de seguridad de forma proactiva.

- PD5.2 Implementación de herramientas de seguridad

  Contempla la incorporación de soluciones tecnológicas que refuercen la protección de los sistemas VoIP frente a amenazas como software malicioso, spam y accesos no autorizados. Incluye la implementación de filtros antispam, herramientas antimalware

y mecanismos de autenticación robusta, adaptados a las particularidades del entorno. Asimismo, se prevé la revisión y actualización periódica de estas herramientas en función de la evolución de los métodos de ataque, garantizando su efectividad y pertinencia operativa.

- PD5.3 Responsabilidad y reporte

  Se orienta a establecer canales seguros y confidenciales para la notificación de incidentes relacionados con la seguridad de los sistemas VoIP, garantizando que los colaboradores puedan reportar eventos sin temor a represalias. Incluye la adopción de una política explícita de no represalias, así como la evaluación periódica de los programas de incentivos utilizados para fomentar comportamientos responsables y participativos en materia de seguridad. Su objetivo es consolidar un entorno organizacional donde la denuncia oportuna y la corresponsabilidad sean pilares clave de la cultura de protección institucional.

4.5. Plan de cultura de seguridad para VoIP

El plan constituye una estrategia integral que tiene como objetivo fortalecer la seguridad de las comunicaciones VoIP mediante la sensibilización y formación de los usuarios frente a amenazas de ataques de ingeniería social. El plan contempla 2 procesos básicos, la definición y monitoreo del plan de cultura de seguridad.

La definición del plan de cultura de seguridad (PA4) incluye subprocesos que permiten generar una conciencia sólida sobre la importancia de la seguridad en VoIP, con un enfoque particular en la identificación y prevención de ataques de ingeniería social. Los subprocesos contemplan concienciación y formación, políticas y procedimientos, y fomento de un entorno orientado a la seguridad.

El monitoreo del plan de cultura de seguridad (PD5) tiene como objetivo asegurar el seguimiento continuo y la evaluación del plan para medir su efectividad, detectar áreas de mejora, y realizar ajustes que mantengan la cultura de seguridad alineada con las amenazas emergentes y las necesidades de la organización. Se incluyen subprocesos para actualización y evaluación continua, implementación de herramientas de seguridad, responsabilidad y reporte.

4.5.1. Concienciación y formación (PA41)

La formación detallada sobre amenazas sociales y técnicas de ingeniería social es fundamental, puede incluir ejemplos basados en casos reales para mayor impacto. La simulación de ataques de ingeniería social permite evaluar la preparación del personal y su capacidad para identificar amenazas.

a) Sesiones de capacitación

Descripción. Programa periódico de capacitación sobre amenazas de seguridad, abarcando amenazas sociales y técnicas específicas de ingeniería social en VoIP.

Tratamiento de ataques

- Sesiones dedicadas a explicar y ejemplificar amenazas sociales.
- Enfoque en cómo identificar y reportar incidentes de Vishing.
- Métodos de prevención y reporte de robo de servicio y SPIT (spam telefónico por internet).

Programa personalizado. Desarrollar entrenamientos específicos por departamento, con ejemplos de ingeniería social relevantes para cada función.

Simulaciones de crisis de ingeniería social. Introducir ejercicios de simulación de crisis centrados en ataques VoIP para que los empleados practiquen respuestas y procedimientos de emergencia.

Procedimientos de control

- **Control de programa de entrenamiento.** Establecer un calendario para sesiones regulares de capacitación sobre amenazas de seguridad en VoIP, documentando la asistencia de los empleados.
- **Evaluación posterior a la sesión.** Realizar pruebas de conocimiento después de cada sesión para medir la comprensión de las amenazas de seguridad y los protocolos de respuesta.
- **Seguimiento de incidentes reportados.** Registrar y analizar los incidentes reportados relacionados con las amenazas tratadas en las sesiones para evaluar la efectividad de la formación.

b) Simulacros de phishing y pruebas de concientización

Descripción. Simulaciones de ataques de ingeniería social para evaluar la capacidad de los empleados para identificar y reportar diversos tipos de ataques.

Tratamiento de ataques

- Escenarios Vishing y SPIT incluidos en los simulacros para sensibilizar sobre estas amenazas específicas.

Escenarios personalizados. Adaptar los escenarios de phishing a las tareas y riesgos diarios de cada departamento.

Educación externa. Ofrecer materiales educativos a los empleados para compartir con sus contactos externos, fortaleciendo la concienciación sobre seguridad VoIP en sus entornos personales.

Procedimientos de control

- **Seguimiento de simulacros de phishing.** Registrar los resultados de los simulacros de ataques de ingeniería social, incluyendo la identificación y respuestas de los empleados.

- **Análisis de desempeño possimulacro.** Revisar las respuestas y tiempos de respuesta durante los simulacros para identificar áreas de mejora y necesidades de refuerzo en la capacitación.

4.5.2. Políticas y procedimientos (PA42)

Las políticas claras y las cláusulas detalladas sobre prevención, detección y respuesta ante ataques de ingeniería social son cruciales. La implementación de controles de acceso estrictos y autenticación robusta puede ser fundamental para prevenir estos ataques.

a) Políticas de seguridad

Descripción. Documentos formales que establecen directrices para el uso seguro de sistemas VoIP, incluyendo medidas específicas contra amenazas de espionaje, interrupción intencionada y abuso de servicio.

Tratamiento de ataques

- Cláusulas detalladas sobre prevención, detección y respuesta ante cada tipo de ataque mencionado.

Procedimientos de control

- **Control de actualización de políticas.** Mantener un registro de revisiones y actualizaciones en las políticas de seguridad VoIP, documentando los cambios y las fechas de implementación.
- **Auditorías de cumplimiento.** Realizar auditorías periódicas para garantizar el cumplimiento de las políticas establecidas y documentar las áreas de no conformidad para su corrección.
- **Pruebas de vulnerabilidad.** Ejecutar pruebas de penetración regulares para verificar la efectividad de las políticas en la prevención de ataques.

Actualizaciones personalizadas. Implementar actualizaciones de políticas basadas en las tendencias actuales de ataques de ingeniería social específicos para VoIP.

Análisis de políticas posimplementación. Evaluar la efectividad de las nuevas políticas tras su implementación y ajustarlas según sea necesario.

b) Procedimientos de verificación de identidad

Descripción. Métodos y procesos para verificar la identidad de los usuarios antes de acceder a sistemas VoIP, con enfoque en prevenir el robo de servicio y el espionaje.

Tratamiento de ataques

- Implementación de controles de acceso estrictos y autenticación robusta para prevenir estos ataques.

Procedimientos de control

- **Verificación de identidad y acceso.** Supervisar la implementación de controles de acceso, incluyendo autenticación multifactor (MFA) y registros de acceso a sistemas VoIP.
- **Evaluación de controles de acceso.** Realizar evaluaciones de rutina para asegurar la efectividad de los controles de acceso e identificar posibles brechas de seguridad.

Exploración de soluciones avanzadas. Investigar e implementar sistemas de autenticación avanzados que puedan mitigar ataques basados en ingeniería social.

4.5.3. Fomento de una cultura de seguridad (PA43)

Una comunicación continua y el involucramiento de la alta dirección y son fundamentales para fortalecer una cultura de seguridad sólida. Los incentivos pueden ser efectivos para fomentar el comportamiento seguro y la denuncia de intentos de ingeniería social.

a) Liderazgo comprometido

Descripción. Compromiso visible de la alta dirección hacia la prevención de todas las categorías de ataques de ingeniería social en VoIP.

Tratamiento de ataques

- Mensajes claros y ejemplos de liderazgo sobre los peligros y la importancia de reportar todos los tipos de ataques.

Procedimientos de control

- **Seguimiento del compromiso de la alta dirección.** Registrar actividades y comunicaciones de liderazgo relacionadas con la seguridad en VoIP para evaluar el nivel de compromiso.
- **Encuestas de satisfacción de empleados.** Llevar a cabo encuestas periódicas para medir la percepción de los empleados sobre el involucramiento de la alta dirección en la seguridad.

Comunicación de escenarios relevantes. Liderazgo que destaque la importancia de identificar y reportar ataques de ingeniería social específicos para VoIP.

b) Comunicación constante

Descripción. Mantenimiento de una comunicación activa sobre la importancia de la seguridad, resaltando casos reales y consejos para evitar cada tipo de ataque.

Tratamiento de ataques

- Enfoque específico en comunicar estrategias de prevención para cada categoría de ataque mencionado.

Procedimientos de control

- **Evaluación de comunicaciones de seguridad.** Revisar registros de comunicaciones internas sobre seguridad para garantizar la divulgación adecuada de medidas preventivas contra ataques de ingeniería social.
- **Retroalimentación de comunicación.** Recopilar comentarios de los empleados sobre la efectividad y relevancia de la comunicación sobre seguridad para realizar ajustes necesarios.

Retroalimentación de comunicación. Implementar un sistema de retroalimentación para ajustar y mejorar las comunicaciones sobre seguridad VoIP.

c) Incentivos y motivadores

Descripción. Establecimiento de programas de incentivos para reforzar comportamientos seguros y la denuncia de intentos de ingeniería social.

Tratamiento de ataques

- Reconocimiento y recompensas para empleados que identifiquen y reporten con éxito intentos de ataques de ingeniería social, independientemente del tipo y naturaleza.

Procedimientos de control

- **Evaluación de Programas de Incentivos**. Realizar análisis periódicos para medir la efectividad de los programas de incentivos en la detección y denuncia de ataques de ingeniería social.

Recompensas personalizadas. Adaptar los programas de incentivos según la efectividad para detectar y reportar ataques de ingeniería social específicos para cada departamento.

4.5.4. Actualización y evaluación continua (PD51)

La actualización continua de políticas y evaluación de riesgos es esencial para mantenerse al día con las últimas amenazas. La implementación de herramientas de seguridad como filtros antispam y sistemas de autenticación robustos puede fortalecer significativamente la defensa contra ataques de ingeniería social.

a) Revisiones periódicas de políticas

Descripción. Actualizaciones regulares de políticas de seguridad VoIP, incluyendo medidas actualizadas contra todas las variantes de ataques de ingeniería social.

Tratamiento de ataques

Revisión constante y actualización de políticas para incluir estrategias contra nuevos métodos de ataques identificados.

Procedimientos de control

- **Registro de actualizaciones de seguridad.** Mantener un registro de las actualizaciones implementadas en las herramientas de seguridad, como filtros antispam y sistemas de autenticación.
- **Programación de revisiones.** Establecer un calendario para revisiones regulares de políticas, con un equipo designado para identificar y abordar las lagunas en las políticas actuales relacionadas con ataques de ingeniería social.
- **Evaluación de cambios.** Realizar análisis posteriores a las revisiones para determinar la efectividad de las actualizaciones en la prevención y detección de nuevos métodos de ataques.

Monitoreo de efectividad. Evaluar el impacto de las actualizaciones de políticas en la prevención y detección de nuevos métodos de ataques VoIP.

b) Evaluación de Riesgos

Descripción. Evaluaciones continuas de los riesgos de ingeniería social en VoIP, identificando y abordando nuevos métodos de ataque.

Tratamiento de ataques

- Análisis de tendencias y patrones de ataques para ajustar estrategias de prevención y seguridad.

Procedimientos de control

- **Análisis de riesgos y tendencias.** Realizar evaluaciones periódicas de riesgos basadas en análisis de tendencias y patrones de ataques de ingeniería social identificados.
- **Análisis de tendencias de ataque.** Mantener un equipo dedicado para el análisis continuo de tendencias y patrones de ataques, permitiendo ajustes inmediatos en las estrategias de seguridad en respuesta a nuevas amenazas identificadas.

Análisis específicos. Realizar evaluaciones basadas en análisis de tendencias y patrones de ataques de ingeniería social específicos para VoIP.

4.5.5. Implementación de herramientas de seguridad (PD52)

Implementar herramientas como filtros antispam y antimalware es esencial. También es importante revisar y ajustar estas herramientas según los cambios en las tendencias de ataques.

a) Filtros antispam y antimalware

Descripción. Uso de software para detectar y bloquear correos y llamadas no deseadas, incluyendo SPIT.

Tratamiento de ataques

- Configuración específica para la detección y bloqueo de llamadas y mensajes de SPIT.

Procedimientos de control

- **Revisión y actualización de configuraciones.** Establecer revisiones periódicas de las configuraciones de los filtros para asegurar que estén alineadas con las últimas técnicas de detección y bloqueo de SPIT.

Configuraciones personalizadas. Ajustar las configuraciones de los filtros según las últimas técnicas de detección y bloqueo de SPIT.

b) Seguridad en la autenticación

Descripción. Implementación de sistemas de autenticación robustos para prevenir suplantaciones y accesos no autorizados.

Tratamiento de ataques

- Configuración de sistemas de autenticación para mitigar ataques basados en suplantación de identidad.

Procedimientos de control

- **Auditorías de autenticación** Realizar auditorías regulares para verificar la integridad y efectividad de los sistemas de autenticación, identificando y corrigiendo posibles vulnerabilidades.

Auditorías frecuentes. Realizar auditorías regulares para garantizar la integridad de los sistemas de autenticación y corregir vulnerabilidades.

4.5.6. Responsabilidad y reporte (PD53)

Establecer un canal seguro para reportar incidentes y la política de no represalias son cruciales para fomentar un entorno de denuncia seguro y confiable. Evaluar regularmente la eficacia de los programas de incentivos es clave para garantizar su continuidad y efectividad.

a) Canal de reporte de incidentes

Descripción. Establecimiento de un canal seguro y confidencial para reportar incidentes de ingeniería social, incluyendo todos los tipos de ataques mencionados.

Tratamiento de ataques

- Capacitación y fomento para reportar cualquier intento de ingeniería social, independientemente de su naturaleza.

Procedimientos de control

- **Seguimiento de incidentes reportados.** Mantener un registro detallado de incidentes de ingeniería social reportados, incluyendo acciones tomadas y resultados de la investigación.
- **Monitoreo del canal de reporte.** Establecer un equipo encargado de supervisar y responder rápidamente a los informes recibidos a través del canal de incidentes, garantizando una respuesta oportuna y adecuada.

Monitoreo proactivo. Establecer un equipo dedicado para responder rápidamente a los informes de incidentes de ingeniería social.

b) Política de no represalias

Descripción. Garantizar que los empleados se sientan seguros al reportar incidentes y se eviten represalias por hacerlo.

Tratamiento de ataques

- Comunicación clara de la política de no represalias para fomentar la denuncia de intentos de ingeniería social de cualquier tipo.

Procedimientos de control

- **Encuestas de satisfacción.** Realizar encuestas periódicas para evaluar la percepción de los empleados sobre la efectividad de la política de no represalias y hacer ajustes según la retroalimentación recibida.

Evaluación de percepción. Realizar encuestas periódicas para evaluar la percepción de los empleados sobre la efectividad de la política de no represalias.

c) Evaluación de incentivos y motivadores

Descripción. Revisión y análisis de la eficacia de los programas de incentivos en la detección y reporte de intentos de ingeniería social.

Tratamiento de ataques

- Ajustes según resultados para fortalecer y adaptar los programas de incentivos que estimulen la detección y denuncia de ataques de ingeniería social.

Procedimientos de control

- **Evaluación de programas de incentivos.** Monitorear la efectividad de los *programas de incentivos en la detección y reporte de intentos de ataques, ajustando según los resultados.
- **Análisis de efectividad de incentivos.** Evaluar regularmente la eficacia de los programas de incentivos en relación con la detección y denuncia de intentos de ingeniería social, ajustando los programas según los resultados obtenidos.

Análisis continuo. Monitorear constantemente la efectividad de los programas de incentivos y ajustarlos según los resultados obtenidos.

4.6. Guía de auditoría de seguridad VoIPSAM

4.6.1. Referencia

El modelo de auditoría de seguridad VoIPSAM toma como base de referencia las buenas prácticas aceptadas y aplicadas de marcos de trabajo aplicables a entornos VoIP y COBIT 4.1 de ISACA, VoIPSAM incluye el tratamiento de la ingeniería social mediante la definición y monitoreo de un plan de cultura de seguridad.

Resumen ejecutivo de auditoría de seguridad VoIP

VoIP

La Voz sobre el Protocolo de Internet VoIP es un término genérico en los ámbitos de tecnologías, protocolos de comunicación y técnicas de transmisión para ofrecer sesiones de voz y multimedia bidireccionales a través de redes IP. Similar a la data de IP, VoIP está basada en paquetes; las señales de voz analógicas emanadas de una llamada telefónica se digitalizan (en unos y ceros binarios), luego se codifican y transmiten como "paquetes" IP a través de una red de conmutación de paquetes. En el lado receptor, se produce un conjunto similar de pasos en orden inverso para convertir los paquetes IP de nuevo en voz, texto o video.

Entre los términos comunes relacionados con VoIP se incluye telefonía por internet, telefonía IP, banda ancha de telefonía y voz sobre banda ancha, términos que hacen mención de la forma en que se utiliza VoIP y debe considerarse como una referencia a las tecnologías VoIP, en lugar de ser sinónimos de VoIP.

La telefonía tradicional basada en circuitos analógicos y PSTN pertenecen y son operadas por las compañías locales e internacionales tradicionales, y se refieren como “telecomunicaciones”. La PSTN está basada en conmutación de circuitos por multiplexación por división de tiempo (TDM), también conocido como servicio telefónico

tradicional (POTS). VoIP proporciona un canal efectivo para comunicaciones de voz y multimedia a un costo menor y con una mayor flexibilidad.

VoIP se ha convertido en un importante componente de las comunicaciones corporativas modernas y muchas empresas dependen completamente de VoIP para voz y multimedia. Al igual que con la mayoría de las nuevas tecnologías, existen oportunidades y riesgos de seguridad con VoIP. El riesgo incluye la instalación incorrecta o inadecuada, la combinación de voz y datos en los mismos circuitos, la calidad de servicio (QoS) y la probabilidad de ataques a la seguridad en las redes VoIP. Las oportunidades incluyen aprovechar las infraestructuras de seguridad de la información existentes para proteger los flujos de paquetes VoIP (por ejemplo, firewalls) y el uso de cifrado para proteger la confidencialidad de las comunicaciones de voz y multimedia.

Los sistemas VoIP incluyen teléfonos tradicionales, unidades de conferencia y dispositivos móviles, así como otros componentes como procesadores de llamadas, gateways, enrutadores, cortafuegos y varios protocolos VoIP. Debido a la alta demanda de rendimiento de voz, VoIP (especialmente voz y video) el hardware y software estándar de red se suelen complementar con componentes especiales de VoIP.

Una gran ventaja de VoIP inalámbrico es que los teléfonos IP que funcionan en redes Wi-Fi pueden usarse en lugar de teléfonos celulares, en muchos casos. Los puntos de acceso (hotspots) públicos 802.11 a menudo son gratuitos o están disponibles a un costo diario bajo para el usuario final. Al conectarse a una red Wi-Fi para web y acceso al correo electrónico, no existe costo adicional para realizar llamadas VoIP que no sea el costo del servicio de VoIP de los usuarios. El servicio de VoIP generalmente cuesta mucho menos que el servicio de telefonía celular y puede ofrecer llamadas internacionales ilimitadas y gratuitas, algunos usuarios no obtienen este beneficio con la mayoría de los planes de telefonía celular.

Impacto y riesgo empresarial

El uso de VoIP se ha convertido en el componente principal de las comunicaciones electrónicas empresariales, es el conducto para todas las comunicaciones electrónicas multimedia, incluyendo voz, servicio de mensajes cortos (SMS), texto y video. La no entrega de requisitos de QoS consistentes (llamadas caídas, vídeo ilegible, etc.) tiene un evidente impacto negativo en las operaciones diarias a través de la empresa, desde oficinas de la planta de producción hasta suites ejecutivas.

Desde que VoIP utiliza el protocolo IP, es vulnerable a los ataques habituales de piratas informáticos, malware, entre otros; además, la falta de aplicación de una separación adecuada entre los circuitos de voz y datos implica que, si uno de ellos estuviera en peligro, la empresa estaría expuesta a la pérdida parcial o completa de ambas funciones críticas.

A diferencia de la PSTN, que utiliza el 100% del ancho de banda asignado (por lo general, 64 Kbits/seg), las conexiones VoIP son enrutadas por la red IP subyacente utilizando los mejores medios posibles en ese momento en particular. Es posible por lo tanto experimentar una QoS más baja debido a la congestión de la red VoIP, en este sentido la calidad de la llamada será una función de la calidad de la red subyacente. Por ejemplo, en las llamadas de VoIP realizadas sobre un ancho de banda bajo, la conexión a internet será de una calidad inferior a la de la red de área local (LAN) de alta velocidad de una empresa (por ejemplo, clase T1 o superior) o la red de área amplia (WAN).

La dependencia de las comunicaciones VoIP implica un impacto directo o indirecto en:

- Comunicaciones, tanto dentro de la empresa como con el mundo externo
- Operaciones comerciales en curso
- Relaciones con los clientes
- Mesa de ayuda y soporte técnico
- Cuestiones contractuales

- Problemas legales y de cumplimiento (por ejemplo, el riesgo de transmitir información de identificación personal sensible mediante mensajes VoIP o sesiones de chat, en violación de alguna ley)

Las comunicaciones de voz y multimedia generalmente contienen o se relacionan con información crítica para el negocio, que incluye:

- Propiedad intelectual (por ejemplo, patentes, material con derechos de autor)
- Material corporativo sensible, que incluye datos relacionados con finanzas, marketing y planificación estratégica, información personal sensible, ventas y marketing, y operaciones comerciales diarias.
- Comunicaciones con terceros, tales como clientes, autoridades gubernamentales, asesores legales externos, socios de empresas conjuntas, accionistas, corredores de bolsa y auditores externos.
- Documentos de trabajo de auditoría
- Monitoreo de problemas
- Control interno de documentación y pruebas.

Si no se diseñan y administran controles VoIP efectivos, se podrían producir:

- Destrucción o pérdida de datos empresariales debido a la penetración de redes VoIP no protegidas
- Divulgación de información confidencial enviada sin cifrar a través de redes públicas
- Divulgación de información confidencial o mala publicidad relacionada, lo que conlleva riesgos para la reputación y pérdida de confianza por parte de las partes interesadas, las empresas, los inversores y los clientes.
- Pérdida o robo de secretos comerciales y activos digitales.
- Robo de activos informáticos
- Pérdida de productividad debido a la falta de disponibilidad de activos electrónicos críticos, como correo electrónico, comunicaciones de voz y mensajería instantánea

- Multas y vínculos penales, debido al incumplimiento o al uso de las redes de VoIP corporativas para actividades indeseables como el acoso, el contenido indeseable y el espionaje industrial.
- Violaciones de seguridad debido a malware transportado por mensajería instantánea
- Pérdida de ventas debido a la incapacidad de los clientes para llegar al personal de ventas
- Daños de marca y pérdida de ventaja competitiva.
- Demandas de terceros perjudicados si los piratas informáticos logran utilizar servidores VoIP comprometidos para atacar otros sitios
- Incapacidad para cumplir con las demandas legales de descubrimiento.
- Incapacidad para restaurar la comunicación de voz o multimedia dentro de un marco de tiempo razonable.

Objetivos y alcance

Una red VoIP típica comprende una serie compleja de protocolos de cooperación, redes (inalámbricas y cableadas), servidores, arquitecturas de seguridad, servicios especiales (como E-911), sistemas de respaldo y recuperación, e interfaces a la PSTN.

Dependiendo de la implementación específica, incluye:

- Evaluación de la gobernanza, políticas y supervisión relacionada con VoIP
- Políticas de clasificación de datos y gestión
- El caso de negocio adecuado de VoIP, los procesos de implementación o actualización reales, la estrategia y los controles de implementación
- Arquitecturas técnicas, incluidos sistemas de seguridad, plataformas múltiples (diferentes proveedores que suministran y/o soportan VoIP), interfaces con redes de datos, respaldo y recuperación, política de retención y destrucción de datos, y tecnología
- Evaluaciones de la infraestructura de TI y el personal para respaldar las arquitecturas de VoIP.
- Configuraciones de línea base de hardware y software desplegados

- Problemas relacionados con los servidores de VoIP descentralizados, como diferentes estándares de seguridad
- Problemas relacionados con la agrupación en clúster de conmutación por error, cuando corresponda

Las consideraciones de seguridad para la PSTN o el acceso telefónico están fuera del alcance de VoIPSAM.

Habilidades mínimas de auditoría

VoIP es usualmente una arquitectura compleja y un conjunto de protocolos que requieren conocimientos técnicos y comprensión adecuados, así como la capacidad de evaluar el contenido y las vulnerabilidades. El profesional de auditoría y aseguramiento debe tener el conocimiento requerido de arquitecturas, protocolos, riesgos y controles VoIP.

4.6.2. Documentos guías de auditoría

Las guías de auditoría son documentos que proporcionan directrices específicas y estandarizadas para llevar a cabo auditorías de manera consistente y efectiva, las guías detallan los pasos, métodos y criterios que los auditores deben seguir para evaluar el cumplimiento de los procesos bajo revisión.

El objetivo es asegurar que las auditorías se realicen de acuerdo con las mejores prácticas y normas establecidas, garantizando la calidad y la fiabilidad de los resultados obtenidos.

Las guías de Auditoría VoIPSAM con sus correspondientes procedimientos de control se encuentran detalladas en el **Anexo E Guías de auditoría VoIPSAM**.

A continuación se especifican los procedimientos por cada guía de auditoría.

a) PGA-1 Plan general de auditoría de seguridad VoIPSAM

El plan establece los procedimientos necesarios para identificar, analizar y mitigar los riesgos de seguridad específicos asociados con VoIP, asegurando que las comunicaciones sean protegidas contra vulnerabilidades como la intercepción, la manipulación de datos y los ataques de ingeniería social, los procedimientos asociados al plan se muestran en la Tabla 31.

Tabla 31. **PGA-1 Plan General de Auditoría VoIPSAM.**

PGA-1						
Plan General de Auditoría VoIPSAM						
Objetivo:	Evaluar el cumplimiento de las políticas corporativas en cuanto a la gestión de la seguridad VoIP					
Naturaleza:	Procedimientos internos					
Alcance:	Nombre de la organización					
Plazo:	Tiempo estimado					
No.	**Procedimiento**	**Referencia Guía de Auditoría**	**Papel de Trabajo**	**Nombre Auditor**	**Fecha Inicio**	**Tiempo efectivo minutos**
1	PLANIFICACIÓN Y ALCANCE DE LA AUDITORÍA	GA-1				
2	PASOS PREPARATORIOS	GA-2	PT-GA-2			
3	GOBERNANZA	GA-3	PT-GA-3			
4	CONFIGURACIÓN DE SERVIDORES	GA-4	PT-GA-4			
5	RED	GA-5	PT-GA-5			
6	PLANIFICACIÓN DE CONTINGENCIAS	GA-6	PT-GA-6			
7	CULTURA DE SEGURIDAD	GA-7	PT-GA-7			
8	EVALUACIÓN DE MADUREZ	GA-8				
					Total	

Fuente: Elaborada por el autor.

b) GA-1. Planificación y alcance de la auditoría

La guía para planificación y alcance de la auditoría contiene todos los procedimientos necesarios que permitan determinar los objetivos de la auditoría de seguridad. La guía de auditoría GA-1 se puede apreciar en la Tabla 32.

Tabla 32. **GA-1. Planificación y alcance de la auditoría.**

Guía de Auditoría VoIPSAM					**Guía de Auditoría**
1. PLANIFICACIÓN Y ALCANCE DE LA AUDITORÍA					
Objetivo:	Definir los objetivos de la auditoría de seguridad. Los objetivos de auditoría de seguridad son de alto nivel y describen los objetivos generales de auditoría				**GA-1**
No.	**Procedimiento de control**	**% Cumplimiento**	**Nombre Auditor**	**Fecha**	**Tiempo efectivo minutos**

Fuente: Elaborada por el autor.

- **No.** Número del procedimiento
- **Procedimiento de control.** Técnicas, procesos y métodos que utilizan los auditores para obtener pruebas de auditoría fiables que les permitan formarse un juicio sólido sobre la situación real de una organización.
- **% Cumplimiento:** Corresponde al porcentaje de cumplimiento del procedimiento de control
- **Nombre Auditor:** Nombre de la persona que realiza el procedimiento de auditoría
- **Fecha:** Correspondiente a la aplicación del procedimiento de auditoría
- **Tiempo efectivo minutos:** Cantidad de minutos empleados en la aplicación del procedimiento.

c) GA-2. Pasos preparatorios

La guía GA-2 para los pasos preparatorios contiene todos los procedimientos necesarios para obtener y revisar los organigramas actuales relacionados con las comunicaciones VoIP. La guía de auditoría GA-2 se puede apreciar en la Tabla 33.

Tabla 33. **GA-2. Pasos preparatorios.**

Guía de Auditoría VoIPSAM			**Guía de Auditoría**			
2. PASOS PREPARATORIOS						
Objetivo:	Obtener y revisar los organigramas actuales relacionados con las comunicaciones VoIP		**GA-2**			
Papel de Trabajo:		**PT-GA-2**				
No.	**Procedimiento de control**		**% Cumplimiento**	**Nombre Auditor**	**Fecha**	**Tiempo efectivo minutos**

Fuente: Elaborada por el autor.

VoIPSAM cuenta además con las siguientes guías de auditoría que incluyen las referencias al modelo:

- GA-3. Gobernanza
- GA-4. Configuración de servidores
- GA-5. Red
- GA-6. Planificación de contingencias
- GA-7. Cultura de seguridad
- GA-8. Evaluación de madurez

d) GA-3. Gobernanza

La guía de auditoría GA-3 se puede apreciar en la Tabla 34.

Tabla 34. **GA-3. Gobernanza.**

Guía de Auditoría VoIPSAM					**Guía de Auditoría**		
3. GOBERNANZA							
Objetivo:	Determinar que la infraestructura inicial del servidor VoIP y las aplicaciones VoIP están respaldadas por un caso de negocio documentado que describe el retorno de la inversión y otros beneficios directos e indirectos				**GA-3**		
Papel de Trabajo:		**PT-GA-3**					
No.	**Procedimiento de control**	**Referencia Cobit**	**Referencia VoIPSAM**	**% Cumplimiento**	**Nombre Auditor**	**Fecha**	**Tiempo efectivo minutos**

Fuente: Elaborada por el autor.

e) GA-4. Configuración de servidores

La guía de auditoría GA-4 se puede apreciar en la Tabla 35.

Tabla 35. **GA-4. Configuración de servidores.**

Guía de Auditoría VoIPSAM					**Guía de Auditoría**		
4. CONFIGURACIÓN DE SERVIDORES							
Objetivo:	Determinar si los servidores VoIP que se ejecutan en un entorno virtualizado están completamente separados de otros servidores que se ejecutan en el mismo hardware físico				**GA-4**		
Papel de Trabajo:		**PT-GA-4**					
No.	**Procedimiento de control**	**Referencia Cobit**	**Referencia VoIPSAM**	**% Cumplimiento**	**Nombre Auditor**	**Fecha**	**Tiempo efectivo minutos**

Fuente: Elaborada por el autor.

f) GA-5. Red

La guía de auditoría GA-5 se puede apreciar en la Tabla 36.

Tabla 36. **GA-5. Red.**

Guía de Auditoría VoIPSAM					**Guía de Auditoría**		
5. RED							
Objetivo:	Determinar el estado de la red utilizada por el entorno del servidor VoIP para verificar el nivel de protección contra el acceso no autorizado e intrusiones				**GA-5**		
Papel de Trabajo:		**PT-GA-5**					
No.	**Procedimiento de control**	**Referencia Cobit**	**Referencia VoIPSAM**	**% Cumplimiento**	**Nombre Auditor**	**Fecha**	**Tiempo efectivo minutos**

Fuente: Elaborada por el autor.

g) GA-6. Planificación de contingencias

La guía de auditoría GA-6 se puede apreciar en la Tabla 37.

Tabla 37. **GA-6. Planificación de contingencias.**

Guía de Auditoría VoIPSAM					**Guía de Auditoría**		
6. PLANIFICACIÓN DE CONTINGENCIAS							
Objetivo:	Determinar si los servicios esenciales del servidor VoIP están incluidos en el Plan de Contingencia de TI / Plan de Continuidad del Negocio				**GA-6**		
Papel de Trabajo:		**PT-GA-6**					
No.	**Procedimiento de control**	**Referencia Cobit**	**Referencia VoIPSAM**	**% Cumplimiento**	**Nombre Auditor**	**Fecha**	**Tiempo efectivo minutos**

Fuente: Elaborada por el autor.

h) GA-7. Cultura de seguridad

La guía de auditoría GA-7 se puede apreciar en la Tabla 38.

Tabla 38. **GA-7. Cultura de seguridad.**

Guía de Auditoría VoIPSAM							**Guía de Auditoría**
7. CULTURA DE SEGURIDAD							
Objetivo:	Determinar la existencia de un Plan de cultura de seguridad que permita combatir los ataques de ingeniería social y la mitigación de los riesgos asociados						**GA-7**
Papel de Trabajo:		**PT-GA-7**					
No.	**7. CULTURA DE SEGURIDAD** **Procedimiento de control**	**Referencia VoIPSAM**	**% Cumplimiento**	**Nombre Auditor**	**Fecha**	**Tiempo efectivo minutos**	

Fuente: Elaborada por el autor.

i) GA-8. Evaluación de madurez

La evaluación de madurez permite al auditor evaluar la madurez de los procesos auditados, en base a los resultados de la revisión de la auditoría de seguridad y las observaciones del auditor, asigne un nivel de madurez a cada uno de los objetivos de control. El empleo de herramientas de evaluación hacia la administración de permite obtener una medición relativa de dónde se encuentra la organización, una manera de decidir hacia dónde ir de forma eficiente, y una herramienta para medir el avance contra la meta.

Los modelos de madurez para el control de los procesos de TI aplican un método de puntaje de modo que una organización pueda calificarse a sí misma desde inexistente hasta optimizada (de 0 a 5), se consideran varios estados:

- El estado actual de la organización (dónde está la organización actualmente)

- El estado actual de la industria (la mejor de su clase en) - la comparación
- El estado actual de los estándares internacionales - comparación adicional
- La estrategia de la organización para mejoramiento - dónde quiere estar la organización.

El nivel de madurez evaluada y objetivo con su correspondiente estado se describe en la Tabla 39.

Tabla 39. **Nivel de madurez – Estado.**

Nivel de Madurez	Estado
0 Inexistente	Carencia completa de cualquier proceso reconocible
1 Inicial	Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos
2 Repetible	Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea
3 Definido	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento
4 Administrado	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva
5 Optimizado	Los procesos se han refinado hasta un nivel de mejor práctica se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas

Fuente: Elaborada por el autor.

La determinación de los niveles de madurez evaluada y objetivo garantiza una evaluación estructurada y objetiva del estado actual de la organización y la meta considerando los niveles de madurez que se desean alcanzar. El proceso para el cálculo de las ponderaciones y calificaciones de la madurez evaluada y de la madurez objetivo en un control específico de VoIPSAM se detallan a continuación.

Identificación de áreas clave de control. Cada control de seguridad VoIP abarca diferentes áreas o dominios clave, como gobernanza, configuración de servidores, red, planificación de contingencias y cultura de seguridad; áreas necesarias para garantizar el cumplimiento de los requisitos del control.

Asignación de ponderaciones. La ponderación para cada área se asigna en función de su importancia relativa al control específico que se está evaluando. Por ejemplo, en un control relacionado con el "Aseguramiento positivo del cumplimiento", la Gobernanza puede recibir una mayor ponderación pues es crucial para establecer políticas y procesos de cumplimiento como se puede apreciar la Tabla 40.

Tabla 40. **Ponderación por área clave.**

Área/procedimiento	**Ponderación**	**Justificación**
Gobernanza	alta (30%)	Impacto en la gestión y supervisión del cumplimiento
Configuración de servidores	media (25%)	Influye directamente en la seguridad de la infraestructura tecnológica
Red	media o baja (20%)	Dependiendo de su relevancia para el control específico
Planificación de contingencias	menor (15%)	Es importante pero no siempre central para todos los controles
Cultura de seguridad	menor (10%)	Representa un apoyo general al cumplimiento

Fuente: Elaborada por el autor.

Evaluación de cumplimiento y calificación de la madurez evaluada. Para cada área clave, considerar los valores de los porcentajes de cumplimiento reportados, los cuales serán utilizados para determinar la calificación de madurez en una escala de 0 a 5, conforme la interpretación de la Tabla 41.

Tabla 41. **Porcentaje de cumplimiento por nivel de madurez.**

Valor	Nivel de madurez	% Cumplimiento	Estado
0	**Inexistente**	< 10%	No existen procesos claros
1	**Inicial**	10% - 30%	Reconocimiento del problema, pero sin procesos establecidos
2	**Repetible**	30% - 50%	Algunos procesos existen, pero no están estandarizados
3	**Definido**	50% - 70%	Procesos documentados y en práctica
4	**Administrado**	70% - 90%	Procesos monitoreados y controlados
5	**Optimizado**	> 90%	Procesos optimizados y mejorados continuamente

Fuente: Elaborada por el autor.

Ejemplo. Gobernanza (Ponderación: 30%)

Caso de negocio: 100%. Peso alto en Gobernanza.

Políticas de VoIP: 27.01%. Problema identificado, pero sin proceso.

Vigilancia: 0%. No hay supervisión.

Calificación: 1 Inicial

Pese a un alto cumplimiento en caso de negocio, el bajo cumplimiento en políticas y vigilancia reduce la calificación.

Madurez evaluada global. Las calificaciones de madurez de cada área se ponderan según su peso relativo y se calcula un promedio ponderado para obtener la calificación global de la madurez evaluada.

Fórmula para la madurez evaluada:

Madurez Evaluada = $\sum$ (Ponderación del área x Calificación del área)

Ejemplo:

Gobernanza: 1 (Ponderación 30%)

Configuración de Servidores: 2 (Ponderación 25%)

Red: 0 (Ponderación 20%)

Planificación de Contingencias: 1 (Ponderación 15%)

Cultura de Seguridad: 0 (Ponderación 10%)

Madurez Evaluada = (1×0.30) + (2×0.25) + (0×0.20) + (1×0.15) + (0×0.10) =0.95 ≈ 1 (Inicial)

Madurez objetivo. La madurez objetivo se establece en función del nivel deseado de madurez que la organización aspira alcanzar para cumplir con los estándares de la industria y mitigar los riesgos identificados, para áreas críticas como Gobernanza, se fija un objetivo de madurez alto (4 o 5), para áreas menos críticas, la meta puede ser una madurez intermedia (3 o 4), dependiendo de la importancia estratégica:

- **Gobernanza:** Madurez objetivo 4 (Administrado) para garantizar que las políticas se implementen y monitoreen consistentemente.
- **Cultura de Seguridad:** Madurez objetivo 3 (Definido) para asegurar que se implementen procesos básicos de concienciación y formación.

La guía de auditoría GA-8 se puede apreciar en la Tabla 42.

Tabla 42. **GA-8. Evaluación de madurez.**

Guía de Auditoría VoIPSAM								**Guía de Auditoría**
8. EVALUACIÓN DE MADUREZ								
Objetivo:	Evaluar la madurez de los procesos revisados. Con base en los resultados de la revisión de la auditoría de seguridad y las observaciones del revisor, asigne un nivel de madurez a cada uno de los procedimientos de control							**GA-8**
No.	**8. EVALUACIÓN DE MADUREZ Procedimiento de Control**	**Referencia Cobit**	**Referencia VoIPSAM**	**Madurez evaluada**	**Madurez objetivo**	**Nombre Auditor**	**Fecha**	**Tiempo efectivo minutos**

Fuente: Elaborada por el autor.

4.6.3. PT. Papeles de trabajo

El auditor debe crear papeles de trabajo PT acorde a las guías de auditoría GA, los cuales permitirán registrar el trabajo realizado considerando el porcentaje de cumplimiento, hallazgos, condiciones, criterio, causa, efecto, comentarios y recomendaciones. El sistema de numeración de la guía proporciona el esquema de numeración correspondiente a los papeles de trabajo.

La guía de auditoría GA-1 Planificación y alcance de la auditoría, así como la guía de auditoría GA-8 Evaluación de madurez, no requieren papeles de trabajo relacionados por su naturaleza. Las demás guías de auditoría tienen referencia al papel de trabajo respectivo como se muestra en la Tabla 43.

Tabla 43. **Papel de trabajo de la guía de auditoría.**

<table>
<tr><td colspan="10">Papel de Trabajo</td><td colspan="2">PT-GA-2</td></tr>
<tr><td colspan="10">Guía de Auditoría VoIPSAM</td><td rowspan="2">Guía de Auditoría</td><td rowspan="2">GA-2</td></tr>
<tr><td colspan="10">2. PASOS PREPARATORIOS</td></tr>
<tr><td rowspan="2">No</td><td rowspan="2">Procedimiento</td><td rowspan="2">% Cumplimiento</td><td rowspan="2">Hallazgo</td><td rowspan="2">Condición</td><td rowspan="2">Criterio</td><td rowspan="2">Causa</td><td rowspan="2">Efecto</td><td rowspan="2">Nombre Auditor</td><td rowspan="2">Fecha</td><td rowspan="2">Comentarios</td><td colspan="2">Recomendación</td></tr>
<tr><td>Dirigido a:</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Fuente: Elaborada por el autor.

- **No.** Número del procedimiento, corresponde al que consta en la guía de auditoría respectiva.
- **Procedimiento.** Técnicas, procesos y métodos que utilizan los auditores para obtener pruebas de auditoría fiables que les permitan formarse un juicio sólido sobre la situación real de una organización. El procedimiento corresponde al que consta en la guía de auditoría respectiva.
- **% Cumplimiento.** Corresponde al porcentaje de cumplimiento del procedimiento de control, el cual consta en la guía de auditoría respectiva.
- **Hallazgo.** Es la conclusión del auditor sobre una discrepancia entre la información auditada y los criterios establecidos. Puede ser positivo o negativo y puede tener impacto en la opinión final de la auditoría
- **Condición.** Es la situación o circunstancia que se ha encontrado durante la auditoría. Esta puede ser tanto una situación positiva como negativa que se evalúa contra los criterios establecidos.

- **Criterio.** Son los estándares o normas utilizados para evaluar la información auditada. El auditor utiliza los criterios para comparar la información auditada con las expectativas y requisitos de la organización.
- **Causa.** Es la razón por la cual se ha producido la condición observada durante la auditoría. El auditor busca identificar la causa raíz para poder proporcionar recomendaciones efectivas.
- **Efecto.** Es el resultado o consecuencia de la condición observada durante la auditoría. El auditor evalúa el impacto que la condición puede tener en la organización.
- **Nombre Auditor.** Nombre de la persona que realiza el procedimiento de auditoría.
- **Fecha.** Correspondiente a la aplicación del procedimiento de auditoría.
- **Comentarios.** Se puede utilizar para indicar la renuncia de un paso u otras anotaciones.
- **Recomendación.** Sugerencia o propuesta que realiza el auditor para corregir o mejorar la situación encontrada durante la auditoría. Las recomendaciones deben ser específicas, prácticas y basadas en criterios sólidos.

En forma adicional se puede documentar la siguiente información en forma complementaria:

- El resumen de la auditoría de seguridad aplicada
- Identificación de los procesos asociados con la finalización y revisión de los papeles de trabajo
- Preparación de problemas y recomendaciones
- Redacción de informes

NOTA. El auditor puede incluir por cada ítem la información según su criterio y necesidad, generando la referencia según la numeración de la actual guía para auditoría.

4.7. Relación integral de los componentes del modelo VoIPSAM

Una vez descritos los elementos fundamentales del modelo, así como la propuesta metodológica para su aplicación a través de la guía de auditoría, es necesario comprender cómo se interrelacionan los componentes desarrollados para garantizar una ejecución coherente y efectiva en entornos reales de auditoría de seguridad VoIP.

Los componentes estructurales del modelo VoIPSAM se articulan de forma secuencial e interdependiente para cubrir de manera integral el ciclo de auditoría de seguridad en entornos VoIP. Cada uno de los dominios representa un eje fundamental en el proceso de gestión y control de la seguridad:

- El Dominio A (Planear y Organizar) establece la base estratégica del modelo, definiendo la planificación, alineación institucional, arquitectura de información, políticas y responsabilidades en materia de seguridad para entornos VoIP.

- El Dominio B (Adquirir e Implementar) traduce la planificación en acciones concretas, mediante la identificación, adquisición, prueba e instalación de soluciones tecnológicas que cumplan con los requisitos de seguridad definidos.

- El Dominio C (Entrega y Soporte) se encarga de mantener operativos los servicios VoIP con estándares de seguridad, garantizando la disponibilidad, continuidad, control de incidentes y soporte adecuado, incluyendo la gestión segura de datos y configuraciones.

- Finalmente, el Dominio D (Monitorear y Evaluar) proporciona los mecanismos para verificar el cumplimiento, evaluar el desempeño de los controles implementados y retroalimentar el sistema para la mejora continua.

A estos dominios se integra de manera transversal el Plan de Cultura de Seguridad para VoIP, el cual fortalece el componente humano de la seguridad. Este plan no se concibe como un elemento autónomo, sino como un componente transversal que incide de manera estratégica en la implementación y eficacia de cada uno de los dominios del modelo.

En el Dominio A, incide en la planificación de políticas educativas y de concienciación; en el Dominio B, guía el diseño de controles técnicos y sociales que consideren el comportamiento del usuario; en el Dominio C, refuerza prácticas seguras operativas y de reporte de incidentes; y en el Dominio D, provee criterios de evaluación del comportamiento organizacional en torno a la seguridad.

Complementando la estructura funcional del modelo, se presenta la Guía de Auditoría de Seguridad VoIPSAM, que consolida los componentes desarrollados en un conjunto de instrumentos aplicables a un entorno real de auditoría. Esta guía incluye la referencia, documentos de auditoría y papeles de trabajo adaptados específicamente al contexto VoIP, permitiendo que el modelo sea no solo teórico, sino plenamente operativo. Su propósito es facilitar la aplicación estructurada del modelo VoIPSAM en organizaciones reales, asegurando trazabilidad, consistencia metodológica y efectividad en la detección de riesgos y brechas de seguridad.

En conjunto, estos elementos conforman un modelo robusto, adaptado a las necesidades actuales de seguridad en entornos de comunicación por VoIP, con enfoque técnico, organizacional y humano, que permite ejecutar auditorías especializadas de forma eficiente, coherente y contextualizada.

4.8. Aplicación práctica del modelo. Estudio de caso

4.8.1. Introducción

El modelo de auditoría de seguridad VoIPSAM considera procesos que permiten mitigar los riesgos derivados de los problemas de seguridad detectados en frameworks y estándares para auditoría mediante la especificación de políticas de seguridad para VoIP. La Escuela Superior Politécnica de Chimborazo ESPOCH, ubicada en Riobamba, Ecuador, utiliza un sistema de comunicaciones VoIP para sus operaciones internas y académicas, frente a la creciente preocupación por la seguridad en sus comunicaciones digitales, se aplicó VoIPSAM para evaluar la protección de su infraestructura.

La ESPOCH es una institución educativa de nivel superior que ofrece una amplia gama de programas académicos, cuenta con una infraestructura tecnológica avanzada, incluyendo un sistema VoIP que conecta múltiples departamentos y edificios dentro del campus. La Dirección de Tecnologías de la Información y Comunicación DTIC-ESPOCH se encarga de planificar, gestionar y monitorear la infraestructura tecnológica de la institución garantizando la disponibilidad de los servicios informáticos y adoptando estándares de tecnologías actuales para satisfacer las necesidades de la comunidad politécnica.

El sistema VoIP de la ESPOCH está compuesto por servidores de comunicaciones, teléfonos IP y una red de datos que soporta tanto la telefonía como otros servicios digitales; la infraestructura incluye componentes críticos como firewalls, sistemas de detección de intrusiones IDS y software de gestión de llamadas. La aplicación de VoIPSAM permitió evaluar la efectividad del modelo de auditoría de seguridad VoIP propuesto, determinando su capacidad para identificar y mitigar riesgos de seguridad en el entorno VoIP de la institución.

VoIPSAM se basa en principios de seguridad de la información y estándares para auditoría de sistemas, con un enfoque específico en la seguridad VoIP, que aborda la integridad, confidencialidad y disponibilidad de las comunicaciones. El modelo de auditoría VoIP incluye componentes clave como la evaluación de la configuración de seguridad, pruebas de penetración específicas para VoIP, análisis de vulnerabilidades y la verificación de políticas de seguridad relacionadas con la protección contra ataques de ingeniería social.

4.8.2. Metodología

El estudio se desarrolló mediante un enfoque cualitativo y cuantitativo, en el cual se aplicaron técnicas de auditoría específicas al entorno VoIP de la ESPOCH. Se realizó todo el proceso formal que permita obtener la autorización para la aplicación del modelo VoIPSAM, los documentos al respecto se pueden revisar en el **Anexo F Solicitud y aprobación de aplicación del modelo VoIPSAM**.

Se realizaron 2 auditorías por separado, el grupo de expertos de la DTIC- ESPOCH (perfiles validados) se dividió en 2 equipos de trabajo, el primer equipo aplicó la auditoría de seguridad VoIP utilizando la forma tradicional (COBIT 4.1, el equipo desconoce el modelo propuesto VoIPSAM), mientras que el segundo equipo aplicó el modelo propuesto VoIPSAM utilizando la guía de auditoría de seguridad VoIPSAM. Los modelos de auditoría se implementaron en tres fases: planificación de la auditoría, pasos preparatorios y evaluación de 5 áreas clave: gobernanza, configuración de servidores, red, planificación de contingencias y cultura de seguridad; en cada caso se generó la evaluación de madurez respectiva. Luego de la aplicación de la auditoría se aplicaron encuestas a los expertos de la DTIC para la validación del estudio de caso, la encuesta contempló la evaluación sobre cuatro dominios: Planificación y organización, Adquisición e implementación, Entrega y soporte, y Monitoreo y evaluación. La encuesta se muestra en el **Anexo G Encuesta B2CE. Auditoría de Seguridad VoIP (estudio de caso)**.

La comparación COBIT 4.1 – VoIPSAM es válida porque ambos funcionan como modelos de evaluación de auditoría. COBIT 4.1 incluye un modelo de madurez formal, igualmente aplicable como modelo analítico. VoIPSAM se construye como modelo específico, derivado de las limitaciones de frameworks en el dominio VoIP. La comparación se basa en criterios comunes y mensurables. La literatura valida explícitamente que los modelos pueden compararse según su eficacia en contextos particulares.

En consecuencia, existe sustento suficiente para establecer que COBIT 4.1 opera como un modelo evaluativo, permitiendo su comparación metodológica con VoIPSAM dentro de un mismo nivel funcional. El análisis comparativo realizado en esta investigación se fundamenta en criterios homogéneos y en evidencia empírica documentada, lo que garantiza la validez interna y rigor metodológico del estudio.

4.8.3. Perfiles de expertos

En este apartado se presentan los perfiles del grupo de expertos de la DTIC-ESPOCH.

Auditoría de Seguridad VoIP mediate COBIT 4.1

Experto 1.

Cargo: Analista de Infraestructura de Tecnologías de la Información y la Comunicación DTIC – ESPOCH

Preparación Académica: Ingeniero en Sistemas, Magister en Interconectividad de Redes, Tecnólogo Superior en Desarrollo de Software

Certificaciones: CCNA Collaboration (Cisco Certified Network Associate Collaboration)

Experiencia Profesional (roles, experiencia):

- Diseño, planificación, análisis, evaluación y aseguramiento de infraestructuras TIC
- Especialista en gestión y optimización de infraestructura y redes
- Gestión de servidores y almacenamiento

- Automatización y monitoreo
- Integración de servicios en la nube
- Gestión de proveedores y presupuestos
- Cumplimiento y auditorías
- Documentación y capacitación

Experto 2.

Cargo: Analista de Soporte y Mantenimiento DTIC – ESPOCH

Preparación Académica: Ingeniero en Sistemas Informáticos, Magister en Software

Certificaciones: Microsoft Certified: Microsoft 365 Security Administrator Associate

Experiencia Profesional (roles, experiencia):

- Soporte Técnico
- Monitoreo y gestión de sistemas
- Gestión de incidentes
- Mantenimiento preventivo y correctivo de hardware y software
- Gestión de actualizaciones
- Gestión de la seguridad y cumplimiento
- Documentación, capacitación y soporte proactivo
- Gestión de proveedores
- Gestión de inventario
- Implementación de nuevas tecnologías
- Gestión de proyectos tecnológicos
- Soporte hardware y software

Auditoría de Seguridad VoIP mediante VoIPSAM

Experto 3.

Cargo: Analista de Seguridad Informática

Preparación Académica: Analista en Sistemas Informáticos, Ingeniero en Sistemas Informáticos, Magíster en Informática Educativa, Diploma Superior en Formulación de Evaluación de Proyectos de Investigación

Certificaciones: CISM (Certified Information Security Manager)

Experiencia Profesional (roles, experiencia):

- Monitoreo y detección de amenazas
- Implementación de medidas de seguridad
- Análisis de vulnerabilidades y pruebas de penetración
- Gestión de incidentes de seguridad
- Control de acceso y gestión de identidades
- Cumplimiento normativo y auditoría
- Capacitación y concienciación de usuarios
- Gestión de riesgos de seguridad
- Desarrollo de sistemas
- Gestión de servidores
- Evaluación de vulnerabilidades (Nessus)
- Auditoría de TI
- Auditorías de seguridad
- Microsoft SQL Server

Experto 4.

Cargo: Analista de Automatización de Procesos 3

Preparación Académica: Ingeniero de Sistemas Informáticos, Magister en Formulación, Evaluación y Gerencia de Proyectos para el Desarrollo

Certificaciones: Microsoft Certified: SQL Server Database Administrator, SCRUM

Experiencia Profesional (roles, experiencia):

- Análisis de Procesos
- Diseño e implementación de soluciones de automatización
- Gestión de proyectos de automatización
- Integración de sistemas
- Monitoreo y optimización continua
- Formación y soporte a usuarios
- Cumplimiento y seguridad
- Desarrollo de software
- Gestión en infraestructura y redes LAN y WAN

- Administración de análisis de infraestructura
- Coordinación de proyectos informáticos

4.8.4. Resultados

Con el propósito de validar la propuesta del modelo VoIPSAM, se llevó a cabo un estudio de caso aplicado en un entorno real de infraestructura tecnológica. Esta metodología permitió observar y analizar el comportamiento del modelo propuesto frente a un modelo tradicional (COBIT 4.1), mediante su aplicación práctica en auditorías reales desarrolladas en una institución pública. El estudio de caso facilitó la recolección de datos empíricos y permitió evaluar la eficiencia temporal, relevancia de componentes y aplicabilidad del modelo en un contexto organizacional específico, sirviendo como base para la validación de las hipótesis planteadas en esta investigación. Los resultados de la aplicación del modelo propuesto mediante el estudio de caso en la Espoch se muestran en el **Anexo H Resultados de auditorías aplicadas**.

CAPÍTULO 5: RESULTADOS Y DISCUSIÓN

El presente capítulo expone los resultados obtenidos a partir de la aplicación del modelo propuesto VoIPSAM (Modelo de Auditoría de Seguridad específico para sistemas VoIP), así como la comprobación de las hipótesis formuladas en esta investigación.

En primer lugar, se presenta la validación del estudio de caso, analizando la aplicabilidad, operatividad y resultados generales obtenidos. Esta sección permite evaluar el desempeño del modelo VoIPSAM en un entorno real, considerando su efectividad para identificar vulnerabilidades y su capacidad para optimizar el proceso de auditoría de seguridad en sistemas VoIP.

A continuación, se desarrolla la validación de las hipótesis específicas, cada una de las cuales aborda aspectos fundamentales del modelo propuesto. Estas hipótesis evalúan la influencia de componentes clave como los requerimientos de seguridad específicos, la integración de elementos particulares para VoIP, la incorporación de un plan de cultura de seguridad orientado a la ingeniería social y la operatividad de un procedimiento especializado en la guía de auditoría.

Posteriormente, se expone la validación de la hipótesis principal, la cual sintetiza los resultados parciales y permite determinar si la implementación del modelo VoIPSAM mejora la eficiencia temporal durante la ejecución de auditorías en comparación con los modelos tradicionales.

Finalmente, se realiza una discusión integral de los resultados, relacionando los hallazgos con los objetivos de la investigación, la literatura revisada y las implicaciones

prácticas y teóricas derivadas del estudio. Esta sección permite reflexionar sobre la relevancia del modelo propuesto y sus posibles aplicaciones en el ámbito de la auditoría de seguridad VoIP.

5.1. Presentación de resultados

Con el objetivo de validar la eficacia y aplicabilidad del modelo de auditoría de seguridad propuesto para entornos VoIP, se procedió a su implementación en un entorno real mediante un estudio de caso desarrollado en una institución pública de educación superior. Esta aplicación permitió evaluar el desempeño operativo del modelo VoIPSAM frente a un enfoque tradicional, considerando variables clave como el tiempo efectivo de ejecución, la cobertura de procedimientos y la capacidad para identificar vulnerabilidades técnicas y humanas. La ejecución del estudio de caso incluyó la planificación, desarrollo y registro sistemático de las auditorías realizadas, bajo condiciones controladas, utilizando métricas cuantificables y herramientas de recolección de datos estructuradas. Los resultados obtenidos constituyen la base para el análisis comparativo y la validación empírica de las hipótesis formuladas en la presente investigación.

5.1.1. Resultados de la aplicación del modelo tradicional COBIT 4.1

En este apartado se presentan los resultados obtenidos tras la aplicación del modelo tradicional COBIT 4.1 en el proceso de auditoría de seguridad del sistema VoIP seleccionado como caso de estudio. La aplicación del modelo permitió evaluar el desempeño de un enfoque general de auditoría, identificando las principales observaciones, tiempos de ejecución y limitaciones encontradas al abordar un entorno tecnológico con características específicas VoIP. La Tabla 44 muestra los resultados de los procedimientos evaluados, el porcentaje de cumplimiento respecto a las áreas Planificación y alcance de la auditoría, y Evaluación de madurez no aplican ya que son actividades propias del proceso de auditoría. Los resultados de la aplicación de las

auditorías de seguridad VoIP se encuentran en el **Anexo H Resultados de auditorías aplicadas**.

Tabla 44. **Resultados de los procedimientos evaluados – cumplimiento. COBIT 4.1.**

No.	Área/Etapa	Procedimientos evaluados	Ítems evaluados	% Cumplimiento	Fecha Inicio	Tiempo efectivo minutos
1	PLANIFICACIÓN Y ALCANCE DE LA AUDITORÍA	8	16	N/A	01/04/2024	1870
2	PASOS PREPARATORIOS	5	9	76,25	06/05/2024	765
3	GOBERNANZA	1	20	19	15/05/2024	1745
4	CONFIGURACIÓN DE SERVIDORES	1	8	6,25	24/06/2024	1200
5	RED	1	2	0	10/07/2024	260
6	PLANIFICACIÓN DE CONTINGENCIAS	1	2	0	16/07/2024	240
7	CULTURA DE SEGURIDAD	0	0	0	22/07/2024	360
8	EVALUACIÓN DE MADUREZ	12	31	N/A	23/07/2024	1400
	Total	**29**	**100**	**16,92**	**Total Tiempo**	**7840 minutos**
	Madurez evaluada:				**0 – Inexistente**	
	Madurez objetivo:				**3 – Definido**	

Fuente: Auditores ESPOCH.

5.1.2. Resultados de la aplicación del modelo propuesto VoIPSAM

En este apartado se presentan los resultados obtenidos tras la aplicación del modelo propuesto VoIPSAM en la auditoría de seguridad del sistema VoIP analizado. La Tabla 45 muestra los resultados de los procedimientos evaluados, el porcentaje de cumplimiento

respecto a las áreas Planificación y alcance de la auditoría, y Evaluación de madurez no aplican ya que son actividades propias del proceso de auditoría.

Tabla 45. **Resultados de los procedimientos evaluados – cumplimiento. VoIPSAM.**

No.	Área/Etapa	Procedimientos evaluados	Ítems evaluados	% Cumplimiento	Fecha Inicio	Tiempo efectivo minutos
1	PLANIFICACIÓN Y ALCANCE DE LA AUDITORÍA	8	16	N/A	01/04/2024	1750
2	PASOS PREPARATORIOS	5	9	65,50	30/04/2024	645
3	GOBERNANZA	3	71	42,34	08/05/2024	1625
4	CONFIGURACIÓN DE SERVIDORES	7	84	77	11/06/2024	1075
5	RED	2	7	16,67	26/06/2024	125
6	PLANIFICACIÓN DE CONTINGENCIAS	2	11	8,33	01/07/2024	80
7	CULTURA DE SEGURIDAD	7	42	0	02/07/2024	280
8	EVALUACIÓN DE MADUREZ	12	41	N/A	08/07/2024	830
	Total	**46**	**281**	**34,97**	**Total Tiempo**	**6410 minutos**
				Madurez evaluada:	1 (Inicial)	
				Madurez objetivo:	4 (Administrado)	

Fuente: Auditores ESPOCH

5.1.3. Resultados de encuestas a expertos sobre los modelos de auditoría

La Tabla 46 muestra los resultados de la aplicación de la encuesta B2CE. Auditoría de Seguridad VoIP (estudio de caso) a expertos.

Tabla 46. **Resultados de la aplicación de la encuesta B2CE.**

Sección	Pregunta	Experto 1. COBIT 4.1	Experto 2. COBIT 4.1	Experto 3. VoIPSAM	Experto 4. VoIPSAM
A	A1	3	4	4	5
	A2	4	3	5	4
	A3	4	4	5	5
	A4	1	1	3	3
	A5	3	4	4	5
	A6	3	4	5	4
	A7	3	4	4	5
B	B1	2	3	4	4
	B2	3	4	5	5
	B3	2	3	5	5
C	C1	3	4	4	5
	C2	3	4	4	5
	C3	4	5	5	5
	C4	4	4	5	5
	C5	3	4	4	5
D	D1	3	3	4	4
	D2	4	3	5	4
	D3	4	4	4	5
	D4	4	3	5	5
	D5	1	1	4	4
E	E1	3	4	4	5
	E2	3	4	4	5
	E3	4	5	5	5
	E4	4	5	5	5
	E5	4	3	5	4
	E6	4	3	5	5
	E7	2	3	4	4

Fuente: Elaborada por el autor.

5.2. Validación del estudio de caso

La validación del estudio de caso se realizó a través de la evaluación de expertos en seguridad de la información con experiencia en auditoría y operación de sistemas VoIP. La selección de los expertos se basó en su perfil técnico y profesional, priorizando la idoneidad y competencia en el área de estudio, con el objetivo de garantizar la rigurosidad y pertinencia del proceso de validación.

La población estuvo conformada por cuatro (4) expertos de la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la ESPOCH, cuya experiencia profesional incluye la realización de auditorías de seguridad bajo marcos de referencia como COBIT 4.1 y la gestión de infraestructuras VoIP en entornos reales. Los expertos seleccionados poseen formación académica de cuarto nivel y certificaciones internacionales reconocidas en seguridad de la información, redes e infraestructura, lo que asegura su capacidad para emitir criterios fundamentados en estándares y buenas prácticas internacionales.

Si bien la totalidad de los expertos pertenece a una misma institución, se garantizó la objetividad y minimización de sesgos mediante la aplicación de instrumentos de evaluación estructurados y criterios técnicos claramente definidos. Este procedimiento permitió mantener la trazabilidad de las valoraciones emitidas y asegurar que los juicios realizados se fundamenten en la experiencia técnica y el conocimiento especializado de los participantes, más allá de su vínculo institucional.

La utilización de una muestra equivalente a la población total se justifica plenamente, dado el carácter reducido y especializado de la misma. En este contexto, la literatura respalda que en estudios de validación técnica la participación de tres a cinco expertos resulta adecuada para garantizar la representatividad y confiabilidad de los resultados (Faulkner, 2003). Dichos expertos cumplen con el perfil requerido y poseen la experiencia práctica indispensable para evaluar la aplicabilidad y efectividad del modelo

propuesto en entornos VoIP. En consecuencia, la validación del estudio de caso por parte de los expertos se considera metodológicamente válida y suficiente, permitiendo obtener resultados confiables sobre la pertinencia, relevancia y aplicabilidad del modelo de auditoría desarrollado.

5.2.1. Fiabilidad de la encuesta

Conforme la aplicación de la encuesta a expertos (Ver Anexo G Encuesta B2CE. Auditoría de Seguridad VoIP - estudio de caso), en la Tabla 47 se consolidan las respuestas de los expertos encuestados para las diferentes preguntas agrupadas en 5 secciones, el conjunto de datos contiene 27 preguntas conforme la Tabla 46.

Tabla 47. **Resultados de la aplicación de la encuesta B2CE.**

Sección / Experto	A							B			C					D					E						
	P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**P12**	**P13**	**P14**	**P15**	**P16**	**P17**	**P18**	**P19**	**P20**	**P21**	**P22**	**P23**	**P24**	**P25**	**P26**	**P27**
Exp 1. COBIT 4.1	3	4	4	1	3	3	3	2	3	2	3	3	4	4	3	3	4	4	4	1	3	3	4	4	4	4	2
Exp 2. COBIT 4.1	4	3	4	1	4	4	4	3	4	3	4	4	5	4	4	3	3	4	3	1	4	4	5	5	3	3	3
Exp 3. VoIP SAM	4	5	5	3	4	5	4	4	5	5	4	4	5	5	4	4	5	4	5	4	4	4	5	5	5	5	4
Exp 4. VoIP SAM	5	4	5	3	5	4	5	4	5	5	5	5	5	5	5	4	4	5	5	4	5	5	5	5	4	5	4

Fuente: Elaborada por el autor.

El alfa de Cronbach calculado para la encuesta usando IBM SPSS Statistics es 0.978, de acuerdo con la Tabla 28. Fiabilidad de George y Mallery, este valor indica una "excelente" consistencia interna de las preguntas en la encuesta, es decir las preguntas están bien alineadas y miden de manera consistente el constructo subyacente que se desea evaluar.

Cada sección de la encuesta está diseñada para medir un aspecto específico, se procede a calcular el alfa de Cronbach por sección para evaluar la consistencia interna de las preguntas dentro de cada aspecto específico.

La Tabla 48 muestra los resultados del alfa de Cronbach por secciones, que permite observar una medida más precisa de la fiabilidad por cada grupo de preguntas.

Tabla 48. **Resultados del alfa de Cronbach por sección.**

Sección	**Valor alfa de Cronbach**	**Consistencia interna**
A	0.913	Excelente
B	0.971	Excelente
C	0.954	Excelente
D	0.870	Buena
E	0.886	Buena

Fuente: Elaborada por el autor.

Los resultados del alfa de Cronbach global y por sección obtenidos mediante SPSS se muestran en el **Anexo I Alfa de Cronbach global y por sección obtenidos mediante SPSS.**

5.2.2. Análisis de diferencias de Medias

En este apartado se analiza la diferencia de medias entre los modelos evaluados para determinar la existencia de variaciones significativas. La Tabla 49 muestra los valores de la media por sección.

Tabla 49. **Media por sección.**

Sección	Media COBIT 4.1	Media VoIPSAM	Diferencia de medias
A	3,214	4,357	-1,1429
B	2,83	4,67	-1,833
C	3,80	4,70	-0,900
D	3,00	4,40	-1,400
E	3,64	4,64	-1,000

Fuente: Elaborada por el autor.

Las medias de las respuestas para el modelo VoIPSAM son consistentemente más altas que para COBIT 4.1 en todas las secciones.

5.2.3. Prueba t para comparación entre modelos

Se considera una prueba t para muestras independientes para determinar si existen diferencias significativas en la valoración de las secciones entre el modelo COBIT 4.1 y VoIPSAM.

El valor t es el resultado del cálculo del estadístico t en la prueba t, mide la diferencia entre las medias de los dos grupos en relación con la variabilidad de las muestras. El valor p indica la probabilidad de que esa diferencia sea debida al azar y se

usa para decidir si la diferencia es estadísticamente significativa. Los resultados del valor t y del valor p se muestran en la Tabla 50.

Tabla 50. **Comparación entre modelos. Resultados del valor t y del valor p.**

Sección	**t**	**p**
A	-3,320	0,003
B	-4,919	0,001
C	-3,576	0,002
D	-3,500	0,004
E	-3,827	0,001

Fuente: Elaborada por el autor.

Los resultados de la prueba t por sección obtenidos mediante SPSS se muestran en el **Anexo J Prueba T Estudio de caso**. No se asume igualdad de varianzas ya que los valores de p en todas las secciones son menores a 0.05, lo que indica que hay diferencias significativas entre las valoraciones de los modelos COBIT 4.1 y VoIPSAM en cada sección.

5.2.4. Validación externa de los resultados del estudio de caso

Con el propósito de fortalecer la validez de la investigación se incorporó una fase adicional de validación de los resultados del estudio de caso mediante la participación de expertos externos a la institución donde se ejecutaron las auditorías.

Esta validación tuvo como objetivo evaluar, desde una perspectiva independiente, la coherencia metodológica, la consistencia interna, la pertinencia de los indicadores utilizados, la correspondencia entre los modelos aplicados y los resultados obtenidos, así

como la posibilidad de transferir dichos resultados a otros contextos organizacionales con infraestructuras VoIP.

Selección de expertos

La validación externa contó con la participación de cinco expertos de perfil académico-investigador, con formación doctoral en universidades de México, Perú, Colombia, Ecuador y Argentina. Los criterios de selección incluyeron:

- Grado académico de Doctor o formación equivalente en áreas afines a tecnologías de la información o seguridad informática.

- Experiencia mínima comprobable en seguridad de la información.

- Conocimiento o experiencia en entornos VoIP.

- Participación independiente respecto al proceso de auditoría realizado en la institución objeto del estudio de caso.

Se solicitó a cada experto declarar su imparcialidad, confirmando que su evaluación se realizó con criterio técnico y académico independiente.

Perfil de Expertos

El perfil de los expertos para la validación externa de los resultados del estudio de caso se muestra en la Tabla 51.

Tabla 51. **Perfil expertos. Validación externa de los resultados del estudio de caso**

Exp	**País y Universidad de formación doctoral y/o actividad profesional actual**	**Rol principal que desempeña actualmente**	**Años de experiencia en seguridad informática**	**Experiencia específica en VoIP**	**Certificaciones relevantes en seguridad de la información o TI**
1	México. Universitam	Investigador	Más de 10 años	Auditoría	CISA, CISSP
2	Perú. Universidad Nacional Mayor de San Marcos	Docente universitario	6–10 años	Gestión / administración	CCNA/CCNP Security
3	Colombia. Universidad Nacional de Colombia	Investigador	Más de 10 años	Investigación	CRISC
4	Ecuador, Universidad Politécnica Salesiana	Auditor de sistemas	Más de 10 años	Auditoría	CCNA Voice / Collaboration, COBIT Foundation
5	Argentina. Universidad Nacional de La Plata	Investigador	6–10 años	Investigación	OSCP. GWAPT – GIAC

Fuente: Expertos Externos.

La validación externa se realizó con la participación de cinco expertos internacionales con formación doctoral o actividad académica y profesional en México, Perú, Colombia, Ecuador y Argentina. Los participantes desempeñan roles como investigadores, docentes universitarios y auditores de sistemas, y cuentan con una experiencia en seguridad informática que oscila entre 6 y más de 10 años. Su experiencia específica en entornos VoIP se concentra en áreas de auditoría, investigación y gestión de tecnologías de comunicación. Además, poseen certificaciones reconocidas en seguridad de la información y tecnologías de la información, tales como CISA, CISSP, CRISC,

CCNA/CCNP Security, CCNA Voice/Collaboration, COBIT Foundation, OSCP, GWAPT y GIAC, lo que respalda su idoneidad técnica para la validación externa de los resultados del estudio de caso.

Información suministrada a los expertos

Para permitir una evaluación fundamentada, los expertos recibieron un dossier de validación que incluyó:

- Resultados completos del estudio de caso
- Resultados numéricos consolidados de las auditorías realizadas con COBIT 4.1 y con el modelo VoIPSAM.
- Tablas comparativas de tiempos, procedimientos e ítems evaluados.
- Guía de auditoría VoIPSAM y COBIT 4.1.

Esta información permitió a los expertos analizar tanto el proceso seguido como los resultados obtenidos, sin haber participado en su ejecución.

Instrumento de validación

Se diseñó una encuesta estructurada para validación por expertos externos de los resultados del estudio de caso la cual se puede apreciar en el Anexo O, organizada en cinco ejes temáticos:

- Coherencia entre metodología y resultados.
- Consistencia interna de los resultados.
- Adecuación de los indicadores utilizados.

- Correspondencia entre los modelos aplicados y los resultados obtenidos.

- Transferibilidad de los resultados a otros contextos organizacionales.

Cada eje estuvo compuesto por tres ítems, totalizando quince preguntas cerradas, valoradas mediante una escala Likert de cinco niveles, desde “Muy en desacuerdo” hasta “Muy de acuerdo”. Previamente, se incluyó una sección de caracterización del experto orientada a documentar su perfil académico y profesional.

Procedimiento de aplicación

La encuesta fue aplicada de forma remota. Los expertos analizaron previamente la documentación proporcionada y posteriormente respondieron el instrumento de validación. El proceso se realizó de manera individual, sin interacción entre los participantes, para evitar influencias cruzadas en las respuestas.

Las respuestas fueron consolidadas en matrices de datos para su análisis estadístico descriptivo, considerando medias por ítem, medias por eje y porcentaje de respuestas con valores iguales o superiores a 4.

Resultados de la validación externa

Los resultados de la aplicación de las encuestas a expertos externos respecto al estudio de caso se muestran en la Tabla 52.

Tabla 52. **Resultados de la validación externa del estudio de caso**

Ítem	Exp1	Exp2	Exp3	Exp4	Exp5	Media	Desviación estándar	Porcentaje de acuerdo (≥ 4 puntos)
P1	5	4	5	4	5	**4.6**	0.49	**100%**
P2	4	4	5	4	4	**4.2**	0.40	**100%**
P3	4	3	4	4	4	3.8	0.40	80%
P4	5	4	4	4	5	**4.4**	0.49	**100%**
P5	4	4	4	3	4	3.8	0.40	80%
P6	4	5	4	4	4	**4.2**	0.40	**100%**
P7	5	4	5	4	4	**4.4**	0.49	**100%**
P8	4	4	4	4	3	3.8	0.40	80%
P9	4	4	5	4	4	**4.2**	0.40	**100%**
P10	4	5	4	4	4	**4.2**	0.40	**100%**
P11	5	4	4	4	4	**4.2**	0.40	**100%**
P12	4	4	4	3	4	3.8	0.40	80%
P13	4	4	3	4	4	3.8	0.40	80%
P14	4	5	4	4	4	**4.2**	0.40	**100%**
P15	4	4	4	3	4	3.8	0.40	80%

Fuente: Expertos Externos.

Los resultados por eje de validación externa se muestran a continuación:

- Eje 1. Coherencia método–resultado (P1–P3)

Medias: 4.6, 4.2, 3.8

Media del eje: 4.20

% respuestas ≥ 4: 93.33%

Interpretación:

Los expertos consideran que existe alta coherencia entre el método comparativo aplicado y los resultados obtenidos.

- Eje 2. Consistencia interna de los resultados (P4–P6)

Medias: 4.4, 3.8, 4.2

Media del eje: 4.13
% respuestas ≥ 4: 93.33%

Interpretación:
Se valida que los resultados presentan estabilidad y coherencia interna entre fases y mediciones.

- Eje 3. Adecuación de los indicadores utilizados (P7–P9)

Medias: 4.4, 3.8, 4.2
Media del eje: 4.13
% respuestas ≥ 4: 93.33%

Interpretación:
Los indicadores empleados son considerados adecuados para evaluar eficiencia, relevancia y vulnerabilidad.

- Eje 4. Correspondencia modelo–resultado (P10–P12)

Medias: 4.2, 4.2, 3.8
Media del eje: 4.07
% respuestas ≥ 4: 93.33%

Interpretación:
Existe una correspondencia clara entre los componentes de VoIPSAM/COBIT y los resultados observados.

- Eje 5. Transferibilidad de los resultados (P13–P15)

Medias: 3.8, 4.2, 3.8
Media del eje: 3.93

% respuestas ≥ 4: 86.67%

Interpretación:
Los resultados son considerados mayoritariamente transferibles a otros contextos, aunque con mayor cautela que en los otros ejes.

Los resultados mostraron medias entre 3.93 y 4.20 en todos los ejes evaluados, con porcentajes de acuerdo (respuestas ≥ 4) entre 86.67% y 93.33%. Estos valores evidencian una alta aceptación de los resultados del estudio de caso desde una perspectiva externa e independiente.

Los resultados de la validación externa evidencian un alto nivel de acuerdo entre los expertos internacionales. 9 de los 15 ítems alcanzan medias iguales o superiores a 4.2, con el 100% de las respuestas ubicadas en las categorías "de acuerdo" o "muy de acuerdo", mientras que los seis ítems restantes presentan medias de 3.8 y un 80% de respuestas en dichas categorías, lo que refleja una aceptación generalizada. La baja dispersión de los datos, con desviaciones estándar entre 0.40 y 0.49, confirma la coherencia entre las valoraciones de los expertos y respalda la consistencia y validez externa de los resultados del estudio de caso.

De manera específica, los expertos confirmaron:

- Coherencia entre la metodología aplicada y los resultados obtenidos.

- Consistencia interna entre las diferentes fases de la auditoría.

- Pertinencia de los indicadores empleados para medir eficiencia, relevancia y percepción de vulnerabilidad.

- Correspondencia lógica entre los componentes de los modelos evaluados y los resultados observados.

- Posibilidad de transferir los resultados a otros entornos con infraestructuras VoIP, considerando ajustes contextuales.

Síntesis de la validación

La validación externa internacional permitió corroborar, desde una perspectiva independiente, que los resultados del estudio de caso no responden únicamente a condiciones institucionales particulares, sino que presentan coherencia metodológica, solidez interna y potencial de aplicación en otros contextos organizacionales.

Esta fase complementa la validación interna realizada durante el estudio de caso y refuerza la credibilidad científica del modelo VoIPSAM y de los resultados obtenidos.

5.3. Validación de las hipótesis secundarias

5.3.1. Validación de la hipótesis secundaria HS1

- **Hipótesis Secundaria HS1:** La incorporación funcional de los requerimientos de seguridad específicos para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad.
- **Variable Independiente (VI):** Incorporación funcional de requerimientos de seguridad específicos para VoIP.
- **Variable Dependiente (VD):** Eficiencia temporal en la ejecución de auditorías de seguridad.

- **Hipótesis Nula (H_0):**

  La incorporación funcional de los requerimientos de seguridad específicos para sistemas VoIP no mejora la eficiencia temporal en la ejecución de auditorías de seguridad.

- **Hipótesis Alternativa (H_1):**

  La incorporación funcional de los requerimientos de seguridad específicos para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad.

Metodología de Validación:

Se realizó un análisis comparativo de los tiempos de ejecución de auditorías en dos escenarios:

- **Escenario A:** Auditoría bajo un enfoque tradicional con requerimientos generales de seguridad.
- **Escenario B:** Auditoría con la incorporación funcional de los requerimientos de seguridad específicos para sistemas VoIP.

El análisis comparativo se centró en los tiempos efectivos de ejecución de las auditorías de seguridad realizadas con COBIT 4.1 y VoIPSAM en las áreas de gobernanza, configuración de servidores, red y planificación de contingencias como se muestra en la Tabla 53, donde el modelo VoIPSAM incorpora de manera funcional los requerimientos de seguridad específicos para sistemas VoIP.

Tabla 53. **Resultados de los procedimientos evaluados COBIT 4.1 y VoIPSAM.**

No.	Área	COBIT 4.1			VoIPSAM		
		Procedimientos evaluados	Ítems evaluados	Tiempo efectivo minutos	Procedimientos evaluados	Ítems evaluados	Tiempo efectivo minutos
3	GOBERNANZA	1	20	1745	3	71	1625
4	CONFIGURACIÓN DE SERVIDORES	1	8	1200	7	84	1075
5	RED	1	2	260	2	7	125
6	PLANIFICACIÓN DE CONTINGENCIAS	1	2	240	2	11	80
	Total	**4**	**32**	**3445 minutos**	**14**	**173**	**2905 minutos**

Fuente: Auditores ESPOCH.

Se aplicó una prueba t para muestras relacionadas para evaluar el efecto sobre la eficiencia temporal.

Resultados

La prueba t arrojó los siguientes resultados:

- **Estadístico t:** 15.173
- **Valor p:** 0.001
- **Nivel de significancia:** $\alpha = 0.05$

Interpretación

La prueba t para muestras relacionadas arrojó un valor p = 0.001, indicando una diferencia significativa entre los tiempos de ejecución de los modelos COBIT 4.1 y VoIPSAM, con un nivel de confianza del 95%.

Dado que el valor p es menor a 0.05, se rechaza la hipótesis nula y se acepta la hipótesis específica HS1. La incorporación funcional de los requerimientos de seguridad

específicos para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad.

Los resultados de la prueba de la Prueba t para muestras relacionadas generados mediante SPSS para HS1 se pueden apreciar en el **Anexo K. Prueba t - HS1**.

Discusión

La validación de esta hipótesis demuestra que los requerimientos de seguridad diseñados específicamente para entornos VoIP permiten optimizar el proceso de auditoría al enfocarse en aspectos críticos y particulares de esta tecnología. Esto reduce los tiempos de análisis y evaluación frente a metodologías tradicionales. Este resultado respalda el objetivo específico 1 de la investigación, confirmando que la determinación de los requerimientos de seguridad específicos para VoIP mejora la eficiencia de las auditorías en escenarios VoIP.

Los resultados evidencian una diferencia sustancial en la cobertura y profundidad de la auditoría al comparar los modelos COBIT 4.1 y VoIPSAM. Mientras que el modelo tradicional evaluó únicamente 4 procedimientos y 32 ítems en las áreas de Gobernanza, Configuración de Servidores, Red y Planificación de Contingencias, el modelo VoIPSAM examinó 14 procedimientos y 173 ítems en esas mismas áreas, lo cual representa un incremento significativo en la especificidad y alcance de la evaluación de seguridad.

A pesar de esta ampliación en el número de componentes evaluados, el tiempo efectivo total requerido por VoIPSAM (2.905 minutos) fue inferior al registrado por COBIT 4.1 (3.445 minutos), lo que sugiere no solo una mayor profundidad técnica, sino también una mayor eficiencia en la ejecución.

5.3.2. Validación de la hipótesis secundaria HS2

- **Hipótesis Secundaria HS2:** La integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP incrementa la relevancia de las evaluaciones de seguridad en dichos sistemas.
- **Variable Independiente (VI):** Integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP.
- **Variable Dependiente (VD):** Relevancia de las evaluaciones de seguridad en sistemas VoIP.

- **Hipótesis Nula (H_0):**

  La integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP no incrementa la relevancia de las evaluaciones de seguridad en dichos sistemas.

- **Hipótesis Alternativa (H_1):**

  La integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP incrementa la relevancia de las evaluaciones de seguridad en dichos sistemas.

Metodología de Validación

Se aplicó una encuesta a expertos, quienes valoraron la relevancia de los componentes de seguridad sobre dos modelos de auditoría (ver Tabla 46. Resultados de la aplicación de la encuesta B2CE):

- Modelo COBIT 4.1: sin componentes específicos para VoIP.
- Modelo VoIPSAM: con integración operativa de componentes específicos adaptados a las particularidades de sistemas VoIP.

Se compararon las puntuaciones asignadas a los componentes de cada sección de ambos modelos, aplicando una prueba t de muestras independientes sobre los resultados (ver Tabla 50. Comparación entre modelos. Resultados del valor t y del valor p).

Resultados

La prueba estadística aplicada determinó que el valor p en todas las secciones evaluadas fue menor a 0.05, lo que indica diferencias significativas en la percepción de relevancia entre ambos modelos. Los resultados de la prueba t por sección se muestran a continuación y los estadísticos generados en SPSS se pueden apreciar en el **Anexo J Prueba T Estudio de caso**.

- Sección A: p = 0,003
- Sección B: p = 0,001
- Sección C: p = 0,002
- Sección D: p = 0,004
- Sección E: p = 0,001

Interpretación

Dado que el valor p es menor a 0.05 en todas las secciones evaluadas, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alternativa (H_1). La integración operativa de componentes específicos en el modelo de auditoría de seguridad VoIPSAM incrementa la relevancia de las evaluaciones de seguridad en sistemas VoIP, según la valoración de los expertos participantes.

Discusión

Los resultados refuerzan la importancia práctica y metodológica de incorporar componentes específicos que atiendan las particularidades de los sistemas VoIP dentro de un modelo de auditoría. La validación de esta hipótesis específica respalda el diseño del modelo VoIPSAM, evidenciando que dichos componentes aportan mayor valor y pertinencia en las evaluaciones de seguridad frente a modelos tradicionales como COBIT 4.1. Este hallazgo también respalda el cumplimiento del objetivo específico 2 de la investigación, orientado a implementar componentes específicos en el modelo de auditoría que incrementen la relevancia de las evaluaciones de seguridad en entornos VoIP.

En la validación de la hipótesis HS2, uno de los elementos diferenciadores entre los modelos comparados fue el número de componentes específicos evaluados durante la auditoría de seguridad. El modelo tradicional COBIT 4.1 consideró un total de 29 procedimientos y 100 ítems evaluados, mientras que el modelo propuesto VoIPSAM integró 46 procedimientos y 281 ítems evaluados. Esta diferencia sustancial refleja una mayor cobertura y especificidad por parte de VoIPSAM frente a las particularidades del entorno VoIP.

La incorporación de componentes especializados permitió abordar aspectos críticos como configuración de servidores, seguridad de red, gobernanza y cultura de seguridad, los cuales no fueron cubiertos o fueron considerados de forma superficial en el modelo tradicional. Este incremento en la cantidad de componentes evaluados, orientados específicamente al contexto VoIP, respalda la percepción de los expertos de que el modelo VoIPSAM ofrece una mayor relevancia en las evaluaciones de seguridad, al considerar dimensiones clave que inciden directamente en la protección de este tipo de sistemas.

Así, el mayor número de componentes específicos abordados por VoIPSAM no solo representa una mejora cuantitativa en la estructura de auditoría, sino también una mejora cualitativa en la capacidad del modelo para generar evaluaciones más pertinentes y alineadas a los riesgos reales de los entornos VoIP.

5.3.3. Validación de la hipótesis secundaria HS3

- **Hipótesis Secundaria HS3:** La incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP reduce la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano.
- **Variable Independiente (VI):** Incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP.
- **Variable Dependiente (VD):** Percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano.

- **Hipótesis Nula (H_0):**

  La incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP no reduce la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano.

- **Hipótesis Alternativa (H_1):**

  La incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP reduce la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano.

Metodología de Validación

Se aplicó una encuesta a expertos en auditoría y seguridad VoIP, quienes valoraron la relevancia del componente "plan de cultura de seguridad e ingeniería social" en dos modelos de auditoría:

- Modelo COBIT 4.1: sin componentes específicos sobre cultura de seguridad e ingeniería social.
- Modelo VoIPSAM: con incorporación funcional del plan de cultura de seguridad orientado a ingeniería social.

Se compararon las valoraciones promedio de las preguntas P4, P10, P12, P14, P20, P24 que constan en Tabla 47 Resultados de la aplicación de la encuesta B2CE. Se aplicó una prueba t de muestras independientes para comparar los puntajes de percepción de vulnerabilidad asignados por los expertos al evaluar los modelos COBIT 4.1 y VoIPSAM.

Resultados

La prueba t arrojó los siguientes resultados:

- Estadístico t: -3.43
- Valor p: 0.003
- Nivel de significancia: $\alpha = 0.05$

Los resultados de la prueba t de muestras independientes generados mediante SPSS para HS3 se pueden apreciar en el **Anexo L. Prueba t – HS3**.

Interpretación

Dado que el valor p es menor al nivel de significancia establecido 0.05, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alternativa (H_1). La incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP reduce la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano.

Discusión

Estos resultados evidencian que la inclusión de un plan de cultura de seguridad como componente específico en el modelo VoIPSAM es percibida por los expertos como una medida relevante y efectiva para reducir la percepción de vulnerabilidad organizacional ante ataques basados en ingeniería social. La validación de esta hipótesis específica respalda el diseño del modelo y el cumplimiento del objetivo específico 3 de la investigación, confirmando que la cultura de seguridad es un elemento esencial para reducir riesgos humanos en la seguridad de sistemas VoIP.

5.3.4. Validación de la hipótesis secundaria HS4

- **Hipótesis Secundaria HS4:** La integración operativa de un procedimiento especializado en una guía de auditoría específica para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad.
- **Variable Independiente (VI):** Integración operativa de un procedimiento especializado en una guía de auditoría específica para sistemas VoIP.
- **Variable Dependiente (VD):** Eficiencia temporal en la ejecución de auditorías de seguridad.

- **Hipótesis Nula (H_0):**

  La integración operativa de un procedimiento especializado en una guía de auditoría específica para sistemas VoIP no mejora la eficiencia temporal en la ejecución de auditorías de seguridad.

- **Hipótesis Alternativa (H_1):**

  La integración operativa de un procedimiento especializado en una guía de auditoría específica para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad.

Metodología de Validación

Se compararon los tiempos de ejecución de auditorías de seguridad aplicando dos modelos:

- Modelo COBIT 4.1: sin procedimiento especializado para VoIP.
- Modelo VoIPSAM: integrando operativamente el procedimiento especializado en la guía de auditoría.

Se registraron los tiempos efectivos de auditoría en cada caso (ver Tabla 44 y Tabla 45) y se aplicó una prueba t para muestras relacionadas.

Resultados

La prueba t arrojó los siguientes resultados:

- Estadístico t: 3.168
- Valor p: 0.016
- Nivel de significancia: $\alpha = 0.05$

Los resultados de la prueba de Shapiro-Wilk y Prueba t para muestras relacionadas generados mediante SPSS se pueden apreciar en el **Anexo M. Eficiencia Shapiro-Wilk - Prueba t**.

Interpretación

Dado que el valor p es menor a 0.05, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alternativa (H_1). La integración operativa de un procedimiento especializado en la guía de auditoría VoIPSAM mejora la eficiencia temporal en la ejecución de auditorías de seguridad en sistemas VoIP.

Discusión

Este resultado respalda el diseño del modelo VoIPSAM y su enfoque específico en sistemas VoIP. La incorporación de un procedimiento especializado permite optimizar tiempos y facilitar la ejecución de auditorías al centrarse en los aspectos críticos de la tecnología VoIP. La validación de esta hipótesis respalda el cumplimiento del objetivo específico 4 de la investigación, confirmando que el procedimiento propuesto aporta eficiencia y efectividad frente a modelos tradicionales.

La comparación de los tiempos efectivos de ejecución entre los dos modelos aplicados evidenció una diferencia significativa. El modelo tradicional COBIT 4.1 registró un tiempo total de 7.840 minutos, mientras que el modelo propuesto VoIPSAM, que incorpora el procedimiento especializado en una guía de auditoría específica para VoIP, presentó un tiempo total de 6.410 minutos. Esta diferencia representa una reducción aproximada del 18,27 % en el tiempo de ejecución, lo cual respalda la mejora en la eficiencia temporal atribuida al modelo propuesto.

Una vez validadas las hipótesis secundarias, se procede a la comprobación de la hipótesis principal de la presente investigación.

5.4. Validación de la Hipótesis Principal HP

- **Hipótesis Principal HP.** La implementación de un modelo de auditoría de seguridad específico para sistemas VoIP mejora la eficiencia temporal durante la ejecución de auditorías respecto de los modelos tradicionales.
- **Variable Independiente (VI):** Implementación de un modelo de auditoría de seguridad específico para sistemas VoIP.
- **Variable Dependiente (VD):** Eficiencia temporal durante la ejecución de auditorías.

VoIPSAM: Modelo de auditoría de seguridad específico para sistemas VoIP.
COBIT 4.1: Modelo de auditoría tradicional utilizado como referencia.

- **Hipótesis Nula (H_0)**
  La implementación de un modelo de auditoría de seguridad específico para sistemas VoIP no mejora la eficiencia temporal durante la ejecución de auditorías respecto de los modelos tradicionales.

- **Hipótesis Alternativa (H_1)**
  La implementación de un modelo de auditoría de seguridad específico para sistemas VoIP mejora la eficiencia temporal durante la ejecución de auditorías respecto de los modelos tradicionales.

Prueba de normalidad.

Se aplicó la prueba de Shapiro-Wilk para determinar si los tiempos de ambos modelos siguen una distribución normal con los siguientes resultados:

- **COBIT 4.1.** p = 0.245
- **VoIPSAM.** p = 0.372

Ambos valores son mayores a 0.05, por lo que se concluye que los datos siguen una distribución normal y es posible aplicar pruebas paramétricas.

Prueba t para muestras relacionadas.

Se aplicó una prueba t para muestras relacionadas, dado que los datos son dependientes (los tiempos de ambos modelos provienen de las mismas auditorías).

- **Estadístico t**: 3.168
- **Valor p**: 0.016

El valor p menor a 0.05 indica una diferencia significativa en los tiempos de ejecución entre los dos modelos. Los resultados de la prueba de Shapiro-Wilk y Prueba t

para muestras relacionadas generados mediante SPSS se pueden apreciar en el **Anexo M. Eficiencia Shapiro-Wilk - Prueba t**.

Resultado del análisis.

Dado que el valor **p = 0.016** es menor al nivel de significancia (α = 0.05), se **rechaza la hipótesis nula (H_0)**. En consecuencia, se **acepta la hipótesis alternativa (H_1)**, lo que confirma que **la implementación de un modelo de auditoría de seguridad específico para sistemas VoIP mejora la eficiencia temporal durante la ejecución de auditorías respecto de los modelos tradicionales**.

El análisis estadístico respalda la hipótesis de esta investigación, demostrando que la aplicación de un modelo de auditoría de seguridad específico para sistemas VoIP mejora la eficiencia temporal respecto de los modelos tradicionales. Por lo tanto, la implementación del modelo VoIPSAM mejora la eficiencia temporal durante la ejecución de auditorías en comparación con el modelo COBIT 4.1.

Los resultados evidencian que las auditorías realizadas con VoIPSAM se completan en menos tiempo que las realizadas con COBIT 4.1, validando así la superioridad temporal de VoIPSAM en la ejecución de auditorías de seguridad VoIP.

Además, la implementación del modelo permitió detectar problemas críticos de seguridad, proporcionando una base sólida para fortalecer la protección del sistema VoIP en la ESPOCH. La aplicación del modelo destacó la importancia de la formación continua del personal y la necesidad de implementar políticas más estrictas para garantizar la seguridad de la infraestructura VoIP. La Tabla 54 muestra la validación de la hipótesis general.

Tabla 54. **Validación de la hipótesis general.**

Elemento evaluado	Modelo COBIT 4.1	Modelo VoIPSAM	Diferencia observada	Interpretación
Duración total de la auditoría (percepción de los expertos)	Alta (más tiempo requerido)	Baja (menos tiempo requerido)	VoIPSAM reduce el tiempo total	Mejora de la eficiencia temporal
Tiempo por etapa	Mayor tiempo por etapa	Menor tiempo por etapa	Se optimiza la ejecución en cada fase con VoIPSAM	Ventaja operativa de VoIPSAM
Claridad metodológica	Parcial	Alta	VoIPSAM tiene una guía más específica	Facilita el desarrollo del proceso
Adaptación al contexto VoIP	Baja	Alta	COBIT no aborda especificidades de VoIP	VoIPSAM cubre mejor el dominio específico
Opinión global sobre eficiencia temporal	Baja	Alta	VoIPSAM mejora la eficiencia temporal	Soporte empírico a la hipótesis

Fuente: Elaborada por el autor.

Interpretación de resultados en función de las variables y los objetivos

La variable independiente (VI) considerada en esta investigación es la implementación de un modelo de auditoría de seguridad VoIP (VoIPSAM). La variable dependiente (VD) es la eficiencia temporal en la ejecución de auditorías.

Los resultados obtenidos evidencian que la implementación de VoIPSAM tiene un efecto significativo sobre la eficiencia temporal (VD), reduciendo los tiempos de ejecución de las auditorías en comparación con el modelo tradicional COBIT 4.1.

Este resultado está alineado con el objetivo general de la investigación, que es implementar un modelo de auditoría de seguridad específico para sistemas VoIP que mejore la eficiencia temporal durante la ejecución de auditorías frente a los modelos tradicionales.

Asimismo, se respalda el cumplimiento del objetivo general relacionado con la validación de la eficiencia temporal del modelo VoIPSAM frente a un modelo tradicional, demostrando su superioridad en términos de tiempo de ejecución.

5.5. Comparación de resultados y evaluación de madurez

En esta sección se presenta el análisis comparativo de los resultados y la evaluación de madurez obtenidos tras la aplicación de los modelos COBIT 4.1 y VoIPSAM en la auditoría de seguridad del sistema VoIP. El análisis considera los tiempos efectivos de ejecución, los porcentajes de cumplimiento, el alcance de los procedimientos e ítems evaluados y el nivel de madurez alcanzado.

El modelo propuesto VoIPSAM demostró una mejora significativa en la eficiencia temporal, al reducir el tiempo total de auditoría de 7840 minutos (COBIT 4.1) a 6410 minutos, lo que representa una reducción de 1430 minutos, equivalentes a 23.8 horas menos de ejecución. Esta mejora evidencia la optimización de los procedimientos al estar adaptados específicamente a las particularidades de los sistemas VoIP.

En cuanto al porcentaje total de cumplimiento, VoIPSAM alcanzó un 34,97%, superando el 16,92% logrado por COBIT 4.1. Esto representa una mejora de +18,05% en la cobertura de aspectos relevantes y específicos de la seguridad VoIP, lo que refuerza la efectividad del modelo propuesto en la identificación y evaluación de riesgos en este tipo de entornos.

Entre las áreas donde VoIPSAM evidenció mayor ventaja destacan:

- Gobernanza: mejora de cumplimiento de 19% a 42,34% y reducción de tiempo.
- Configuración de Servidores: incremento de 6,25% a 77% en cumplimiento y menor tiempo de ejecución.

- Red: pasa de 0% a 16,67% de cumplimiento y reduce a la mitad el tiempo invertido.
- Evaluación de Madurez: optimización de tiempo en 570 minutos.
- Planificación de Contingencias: pasa de 0% a 8,33% de cumplimiento y reducción de tiempo.

Adicionalmente, se destaca la diferencia en la cantidad de procedimientos e ítems evaluados, lo cual refleja la profundidad y cobertura de la auditoría en cada modelo:

- COBIT 4.1 evaluó un total de 29 procedimientos y 100 ítems.
- VoIPSAM evaluó un total de 46 procedimientos y 281 ítems.

Esta diferencia evidencia que VoIPSAM, al estar diseñado específicamente para sistemas VoIP, incorpora mayor detalle y profundidad en la auditoría, cubriendo un número superior de procedimientos y evaluando más ítems relacionados con la seguridad y particularidades de los sistemas VoIP.

A pesar de esta mayor carga de evaluación (un 58% más de procedimientos y 181 ítems adicionales), VoIPSAM logra reducir el tiempo total de auditoría, lo cual confirma su eficiencia y enfoque especializado. Esto valida no solo la mejora en tiempo y cumplimiento, sino también en la capacidad operativa del modelo propuesto para realizar auditorías más completas y específicas en sistemas VoIP.

La evaluación de madurez permite determinar el nivel de formalización y control en los procesos de seguridad evaluados.

La aplicación de COBIT 4.1 determinó que el nivel de madurez del sistema VoIP auditado es 0 (Inexistente), lo que evidencia que los procesos de seguridad evaluados no están documentados ni se aplican de manera formal. Este resultado resalta una brecha significativa que la organización debe cerrar, ya que actualmente no se están llevando a cabo prácticas relacionadas con este control, lo cual representa un estado de riesgo. No

obstante, la organización se ha planteado un objetivo razonable y alcanzable al aspirar a desarrollar y establecer procesos documentados y bien entendidos (nivel 3 - Definido).

Para alcanzar este nivel, será necesario un esfuerzo considerable que implique la creación de políticas, la documentación de procedimientos, la capacitación del personal y la implementación de nuevas tecnologías y herramientas de soporte.

Por su parte, la aplicación del modelo VoIPSAM permitió elevar la valoración de la madurez a 1 (Inicial), lo que indica la existencia de ciertos procesos básicos que, si bien no están plenamente formalizados ni controlados, comienzan a ser reconocidos dentro del sistema auditado. La organización se encuentra en un estado donde los procesos se gestionan de forma informal, sin estructura definida, y se ha planteado como meta alcanzar el nivel 4 - Administrado, en el que los procesos estén completamente documentados, monitoreados y gestionados.

Esta brecha significativa refleja la necesidad de una transformación profunda que involucra la formalización de procesos, la implementación de herramientas de monitoreo y el desarrollo de capacidades para medir y ajustar los procesos en función de su rendimiento. Aunque el desafío es considerable, avanzar hacia un nivel Administrado permitirá mejorar la eficiencia operativa, reducir riesgos y garantizar un mejor cumplimiento normativo, sentando una base sólida para futuras optimizaciones.

El modelo VoIPSAM permite avanzar un nivel en la madurez evaluada respecto a COBIT 4.1, evidenciando su capacidad para detectar y formalizar procesos incipientes de seguridad en sistemas VoIP. Además, el planteamiento de un objetivo de madurez más alto por parte de VoIPSAM refuerza su enfoque orientado a la mejora continua y a la consolidación de prácticas de seguridad más robustas y controladas en este tipo de entornos tecnológicos.

5.6. Discusión general de resultados

La presente sección integra y reflexiona sobre los principales hallazgos obtenidos durante la validación del estudio de caso y la comprobación de las hipótesis específicas y principal. Los resultados obtenidos permiten discutir la pertinencia, efectividad y aplicabilidad del modelo en el contexto de la auditoría de seguridad para sistemas VoIP.

El estudio de caso fue validado mediante dos niveles complementarios. En una primera fase, los resultados de las auditorías realizadas con COBIT 4.1 y VoIPSAM en la ESPOCH fueron evaluados por expertos internos que participaron directamente en la ejecución del caso, utilizando encuestas estructuradas y análisis estadístico, lo que permitió comprobar empíricamente la mejora en eficiencia temporal, cobertura y relevancia técnica. En una segunda fase, estos mismos resultados consolidados incluyendo tablas comparativas, tiempos de auditoría y aplicación de la guía VoIPSAM fueron sometidos a validación por expertos externos internacionales, independientes de la institución de estudio. La alta coincidencia en las valoraciones, con medias cercanas o superiores a 4 y porcentajes de acuerdo mayores al 80%, confirmó que los hallazgos no dependen del contexto institucional, sino que son consistentes, técnicamente coherentes y transferibles, fortaleciendo la validez interna y externa del estudio de caso.

La validación de las hipótesis específicas permitió evidenciar que cada uno de los componentes diseñados dentro del modelo VoIPSAM aporta mejoras significativas en comparación con modelos tradicionales como COBIT 4.1. La inclusión de requerimientos de seguridad específicos para VoIP optimizó la eficiencia temporal al enfocar la auditoría en aspectos técnicos relevantes para esta tecnología. Este hallazgo coincide con la necesidad de adaptar los marcos de auditoría a las particularidades de los entornos tecnológicos, como señala la literatura en el ámbito de la seguridad de las comunicaciones.

Asimismo, la integración operativa de componentes específicos en el modelo incrementó la relevancia de las evaluaciones de seguridad, lo que fue confirmado por los

expertos participantes. Esta percepción refuerza la importancia de adaptar los modelos de auditoría a las características técnicas de VoIP, mejorando la capacidad de los auditores para identificar riesgos y vulnerabilidades propias de estos entornos.

Otro aspecto relevante fue la incorporación de un plan de cultura de seguridad orientado al tratamiento de la ingeniería social, el cual demostró reducir la percepción de vulnerabilidad de las organizaciones frente a ataques que explotan el factor humano. Este resultado resalta la necesidad de fortalecer la conciencia y el comportamiento seguro de los usuarios como parte integral de cualquier proceso de auditoría de seguridad en VoIP, alineándose con las recomendaciones de diversos estudios sobre la importancia del factor humano en la seguridad de la información.

Finalmente, la integración operativa de un procedimiento especializado en la guía de auditoría permitió mejorar la eficiencia temporal en la ejecución de auditorías. La reducción de tiempos de ejecución valida la premisa de que contar con una guía específica para VoIP optimiza el trabajo de los auditores y focaliza los esfuerzos en los aspectos más críticos de este tipo de sistemas.

La validación de la hipótesis principal consolidó estos resultados parciales, demostrando que el modelo VoIPSAM mejora de manera significativa la eficiencia temporal en la ejecución de auditorías de seguridad respecto de los modelos tradicionales. Este hallazgo cumple con el objetivo general de la investigación y aporta un modelo específico que atiende las particularidades de la tecnología VoIP, superando las limitaciones de los marcos de auditoría generales.

En términos de aporte académico y práctico, los resultados obtenidos fortalecen la línea de investigación en auditoría de seguridad específica para sistemas VoIP e incorporan el tratamiento de riesgos asociados a la ingeniería social, una amenaza creciente en el ámbito de las comunicaciones digitales. La propuesta del modelo VoIPSAM y su validación práctica representan un avance en la generación de metodologías adaptadas a las necesidades actuales de las organizaciones.

CONCLUSIONES

La implementación del modelo de auditoría de seguridad específico para sistemas VoIP (VoIPSAM) cumplió el objetivo general de la investigación, al demostrar una mejora en la eficiencia temporal frente a un modelo tradicional. La validación empírica, realizada mediante un diseño cuasiexperimental en una institución pública, evidenció una reducción total de 1,430 minutos (23.8 horas) en el tiempo de ejecución de la auditoría, al pasar de 7,840 minutos con COBIT 4.1 a 6,410 minutos con VoIPSAM, lo que representa una mejora del 18.27%. Esta diferencia fue estadísticamente significativa según la prueba t de Student para muestras relacionadas ($p = 0.016$), confirmando que un modelo especializado permite ejecutar auditorías más eficientes, incluso evaluando un mayor número de procedimientos (46 frente a 29) e ítems (281 frente a 100), y logrando además un avance en el nivel de madurez de los procesos auditados.

La identificación, incorporación e implementación de requerimientos de seguridad específicos para sistemas VoIP permitió optimizar los tiempos de auditoría en áreas críticas del proceso, particularmente en Gobernanza, Configuración de servidores, Red y Planificación de contingencias. La comparación entre el enfoque tradicional y VoIPSAM evidenció una reducción de 540 minutos, diferencia que resultó estadísticamente significativa según la prueba t para muestras relacionadas ($p = 0.001$). Asimismo, estos requerimientos posibilitaron una mayor focalización del proceso de auditoría, al ampliar la evaluación a 14 procedimientos y 173 ítems, frente a 4 procedimientos y 32 ítems del modelo tradicional, confirmando que la implementación de requerimientos específicos mejora la eficiencia operativa sin afectar la cobertura ni la profundidad técnica.

El diseño, integración e implementación de componentes específicos en el modelo de auditoría VoIPSAM permitió incrementar la relevancia de las evaluaciones de seguridad en entornos VoIP, según la valoración de expertos. La medición realizada mediante una escala Likert de cinco niveles evidenció medias consistentemente superiores para VoIPSAM en todas las secciones evaluadas. Estas diferencias fueron estadísticamente significativas conforme a la prueba t para muestras independientes ($p < 0.05$, con valores entre 0.001 y 0.004), confirmando que la implementación de componentes adaptados a las particularidades de VoIP mejora la pertinencia técnica del proceso de auditoría y su capacidad para identificar riesgos específicos que no son abordados de forma adecuada por modelos tradicionales.

La implementación de un plan de cultura de seguridad orientado a la ingeniería social permitió reducir significativamente la percepción de vulnerabilidad organizacional frente a ataques que explotan el factor humano en entornos VoIP. La validación realizada mediante juicio de expertos, a partir del análisis de los ítems P4, P10, P12, P14, P20 y P24 de la encuesta, evidenció valoraciones superiores para el modelo VoIPSAM en comparación con el enfoque tradicional. Esta diferencia fue estadísticamente significativa conforme a la prueba t para muestras independientes ($p = 0.003$), confirmando que la integración de una estrategia de concienciación y comportamiento seguro constituye un componente efectivo para mitigar amenazas de ingeniería social que no pueden ser abordadas únicamente mediante controles técnicos.

La implementación de una guía de auditoría específica para sistemas VoIP, que incorpora un procedimiento especializado, demostró ser efectiva para mejorar la eficiencia temporal del proceso de auditoría frente a enfoques tradicionales. La comparación empírica entre ambos modelos evidenció una reducción significativa del tiempo de ejecución, validada estadísticamente mediante la prueba t para muestras relacionadas ($p = 0.016$). Asimismo, el procedimiento especializado permitió estructurar la auditoría en función de aspectos técnicos críticos de VoIP, facilitando una evaluación más focalizada y profunda, lo que confirma que la guía diseñada optimiza la ejecución del proceso sin sacrificar alcance ni rigor técnico.

RECOMENDACIONES

Se recomienda la adopción del modelo VoIPSAM en instituciones que cuenten con infraestructuras VoIP, dado que su aplicación demostró una mejora en la eficiencia temporal de las auditorías, una mayor cobertura de procedimientos y una capacidad superior para identificar vulnerabilidades específicas que no son abordadas con suficiente profundidad por modelos tradicionales.

Es recomendable incorporar requerimientos y controles diseñados específicamente para entornos VoIP dentro de los procedimientos de auditoría, ya que estos permiten focalizar la evaluación en áreas críticas de seguridad, optimizando el tiempo de ejecución sin comprometer la profundidad ni el rigor técnico del proceso.

Se sugiere integrar componentes específicos orientados a la arquitectura, protocolos y riesgos inherentes a VoIP en los modelos de auditoría de seguridad, con el propósito de incrementar la relevancia y precisión de las evaluaciones y mejorar la identificación de riesgos técnicos propios de este tipo de sistemas.

Las organizaciones deberían implementar planes continuos de cultura de seguridad, que incluyan formación, concienciación y simulacros, orientados a mitigar los riesgos asociados al factor humano, especialmente aquellos derivados de técnicas de ingeniería social en entornos VoIP, como el vishing.

Se recomienda utilizar la guía de auditoría desarrollada como documento base en auditorías de seguridad VoIP, ya que su estructura permite sistematizar el proceso,

asegurar una cobertura específica de los aspectos técnicos críticos y mejorar los tiempos de ejecución, contribuyendo a una gestión de la seguridad más eficiente.

Se recomienda desarrollar investigaciones orientadas a la integración de técnicas automatizadas y herramientas de análisis especializado dentro del modelo VoIPSAM, tales como mecanismos de monitoreo de tráfico SIP/RTP, detección de anomalías y análisis automatizado de configuraciones, con el propósito de evaluar su impacto en la optimización adicional de los tiempos de auditoría y en la precisión de la identificación de vulnerabilidades en entornos VoIP. Este enfoque permitiría analizar el potencial de la automatización como complemento del modelo propuesto, fortaleciendo su aplicabilidad en escenarios con infraestructuras de mayor complejidad.

Como proyección de trabajos futuros, se propone la incorporación de técnicas de Inteligencia Artificial y Machine Learning en el modelo de auditoría VoIPSAM, con el fin de analizar su aporte en la detección automatizada de patrones anómalos, amenazas emergentes y comportamientos asociados a ataques en entornos VoIP.

BIBLIOGRAFÍA

Abubaker, A. A., Eleyan, D., Eleyan, A., Bejaoui, T., Katuk, N., & Al-Khalidi, M. (2023). Social Engineering in Social Network: A Systematic Literature Review. *2023 International Symposium on Networks, Computers and Communications (ISNCC)*, 1-7. https://doi.org/10.1109/ISNCC58260.2023.10323826

Al-Ashmoery, Y., Haider, H., Haider, A., Nasser, N., & Al-Sarem. (2021). Impact of IT Service Management and ITIL Framework on the Businesses. *2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI)*, 1-5. https://doi.org/10.1109/MTICTI53925.2021.9664763

Alger, J. (2025). *Vishing attacks increased by 442% in the second half of 2024*. Security Magazine. https://www.securitymagazine.com/articles/101439-vishing-attacks-increased-by-442-in-the-second-half-of-2024

Almutairi, B., & Alghamdi, A. (2022). *The Role of Social Engineering in Cybersecurity and Its Impact*. https://doi.org/10.4236/jis.2022.134020

Alratrout, M., Thani, B., Taleb, N., & Said, R. (2022). The Challenges of Compliance it Governance Frameworks in the UAE. *International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence*, *1*, 56-66. https://doi.org/10.54938/ijemdcsai.2022.01.2.140

Alvanos, D., Limniotis, K., & Stavrou, S. (2018). On the Cryptographic Features of a VoIP Service. *Cryptography*, *2*(1), 3. https://doi.org/10.3390/cryptography2010003

Amorim, A. C., Mira da Silva, M., Pereira, R., & Gonçalves, M. (2021). Using agile methodologies for adopting COBIT. *Information Systems*, *101*, 101496. https://doi.org/10.1016/j.is.2020.101496

Ariyadi, D., & Dirgahayu, T. (2015). Assessment to COBIT 4.1 maturity model based on process attributes and control objectives. *International Conference on Science in Information Technology (ICSITech)*, 343-347. https://doi.org/10.1109/ICSITech.2015.7407829

Awaludin Rizal, R., Sarno, R., & Rossa Sungkono, K. (2020). COBIT 5 for Analysing Information Technology Governance Maturity Level on Masterplan E-Government. *2020 International Seminar on Application for Technology of Information and Communication (iSemantic)*, 517-522. https://doi.org/10.1109/iSemantic50169.2020.9234301

Babilonia, G. (2023). Beneficios de las normas ISO 27000. *High Tech-Engineering Journal*, *3*(2), Article 2. https://doi.org/10.46363/high-tech.v3i2.4

Basicevic, I., Popovic, M., & Kukolj, D. (2008). Comparison of SIP and H.323 Protocols. *2008 The Third International Conference on Digital Telecommunications (icdt 2008)*, 162-167. https://doi.org/10.1109/ICDT.2008.14

Batchelor, J., Spivey, T., & McIlveene, T. (2023). *To Fear or Not to Fear How to Create an Optimal Security Culture*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/to-fear-or-not-to-fear-how-to-create-an-optimal-security-culture

Beckers, K., Krautsevich, L., & Yautsiukhin, A. (2015). Analysis of Social Engineering Threats with Attack Graphs. En J. Garcia-Alfaro, J. Herrera-Joancomartí, E. Lupu, J. Posegga, A. Aldini, F. Martinelli, & N. Suri (Eds.), *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance* (pp. 216-232). Springer International Publishing. https://doi.org/10.1007/978-3-319-17016-9_14

Behan, L., Rozhon, J., Safarik, J., Rezac, F., & Voznak, M. (2022). Efficient Detection of Spam Over Internet Telephony by Machine Learning Algorithms. *IEEE Access*, *10*, 133412-133426. IEEE Access. https://doi.org/10.1109/ACCESS.2022.3231384

Bella, G., Biondi, P., & Bognanni, S. (2022). Multi-service threats: Attacking and protecting network printers and VoIP phones alike. *Internet of Things*, *18*, 100507. https://doi.org/10.1016/j.iot.2022.100507

Bellavista, P., Corradi, A., & Stefanelli, C. (1999). An Open Secure Mobile Agent Framework for Systems Management | SpringerLink. *Journal of Network and Systems Management*. https://doi.org/10.1023/A:1018775413054

Bin Adam, W. A., Xuan Tan, I. Y., Lai, C. S., Rahim, N. T., Bin Tham, B. Y., & Guo, H. (2023). VishingDefender: An Advanced Vishing Defence System Against Vishing Attacks. *2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, 1-8. https://doi.org/10.1109/SOLI60636.2023.10425272

Biondi, P., Bognanni, S., & Bella, G. (2020). *VoIP Can Still Be Exploited—Badly*. 237-243. https://doi.org/10.1109/FMEC49853.2020.9144875

Brahmbhatt, N., Mann, P., & Rawat, A. (2017). Design and implementation of compatible VoIP. *2017 6th International Conference on Computer Applications In Electrical Engineering-Recent Advances (CERA)*, 103-107. https://doi.org/10.1109/CERA.2017.8343309

Budiyanto, S., & Gunawan, D. (2023). *Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol*. *11*, 60853-60865. https://doi.org/10.1109/ACCESS.2023.3286032

Burgemeestre, B., Hulstijn, J., & Tan, Y.-H. (2011). Value-based argumentation for justifying compliance. *Artificial Intelligence and Law*, *19*(2), 149. https://doi.org/10.1007/s10506-011-9113-4

Burgemeestre, B., Hulstijn, J., & Tan, Y.-H. (2013). Value-based argumentation for designing and auditing security measures. *Ethics and Information Technology*, *15*(3), 153-171. https://doi.org/10.1007/s10676-013-9325-2

Carrillo, J., Martinez, J. L., & Suarez-Tangil, G. (2022). On how VoIP attacks foster the malicious call ecosystem. *Computers & Security*, *119*, 102758. https://doi.org/10.1016/j.cose.2022.102758

Chiappetta, S., Mazzariello, C., Presta, R., & Romano, S. P. (2013). An anomaly-based approach to the analysis of the social behavior of VoIP users. *Computer Networks*, *57*(6), 1545-1559. https://doi.org/10.1016/j.comnet.2013.02.009

Cole, J. M. (2016). Challenges of implementing substation hardware upgrades for NERC CIP version 5 compliance to enhance cybersecurity. *IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, 1-5. https://doi.org/10.1109/TDC.2016.7519964

Cots, S., Casadesús, M., & Marimon, F. (2016). Benefits of ISO 20000 IT service management certification. *Information Systems and E-Business Management*, *14*(1), 1-18. https://doi.org/10.1007/s10257-014-0271-2

Cuaresma, J. C. (2002). *The Gramm-Leach-Bliley Act* (SSRN Scholarly Paper 3409888). Social Science Research Network. https://doi.org/10.2139/ssrn.3409888

Debreceny, R. S., & Gray, G. L. (2013). IT Governance and Process Maturity: A Multinational Field Study. *Journal of Information Systems*, *27*(1), 157-188. https://doi.org/10.2308/isys-50418

Draxler, S., & Stevens, G. (2011). Supporting the Collaborative Appropriation of an Open Software Ecosystem. *Computer Supported Cooperative Work (CSCW)*, *20*(4), 403-448. https://doi.org/10.1007/s10606-011-9148-9

Dupuis, M. J., Bejan, C., Bishop, M., David, S., & Lagesse, B. (2019). Design Patterns for Compensating Controls for Securing Financial Sessions. *2019 IEEE SmartWorld,*

Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 1437-1443. https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00260

Dwivedi, H. (2009). *Hacking VoIP: Protocols, attacks, and countermeasures*. No Starch Press.

Elluri, L., Nagar, A., & Joshi, K. P. (2018). An Integrated Knowledge Graph to Automate GDPR and PCI DSS Compliance. *2018 IEEE International Conference on Big Data (Big Data)*, 1266-1271. https://doi.org/10.1109/BigData.2018.8622236

Esparza, D. E. I., Díaz, F. J., Egas, M. B. R., Sinchiguano, F. A. C., & Misacango, R. A. L. (2020). Evaluation model of computer audit methodologies based on inherent risk. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 1-7. https://doi.org/10.23919/CISTI49556.2020.9140877

Fasihuddin, H., Alharbi, S., Alshehri, A., Alzahrani, A., & Fatani, H. (2022). Measuring the maturity of Information Technology Governance based on COBIT. *Romanian Journal of Information Technology and Automatic Control*, *32*(2), 65-78. https://doi.org/10.33436/v32i2y202205

Faulkner, L. (2003). Beyond the five-user assumption: Benefits of increased sample sizes in usability testing. *Behavior Research Methods, Instruments, & Computers*, *35*(3), 379-383. https://doi.org/10.3758/BF03195514

Figueiredo, J., Carvalho, A., Castro, D., Gonçalves, D., & Santos, N. (2024). *On the Feasibility of Fully AI-automated Vishing Attacks*. https://doi.org/10.48550/arXiv.2409.13793

Fox, M., Hammad, E., Magnussen, W., & Schulzrinne, H. (2023). *Towards Zero-Trust VoIP Architecture: A Testbed Implementation, Approach, and Lessons Learned*. https://doi.org/10.1109/FNWF58287.2023.10520531

Fraga, C., Abelém, A., Borges, V., Pinheiro, B., & Cordeiro, W. (2024). A Blockchain-based Approach for Continuous Auditing in IT Change Management. *NOMS 2024-2024 IEEE*

Network Operations and Management Symposium, 1-4. https://doi.org/10.1109/NOMS59830.2024.10575576

Freire, E. (2020). La búsqueda de información científica en las bases de datos académicas. *Revista Metropolitana de Ciencias Aplicadas*, *3*(1), Article 1. https://doi.org/10.62452/z5re7v21

Gavilanez, O., & Rodriguez, G. (2022). VoIP security auditing model based on COBIT 4.1. *International Journal of Security and Networks*, *17*(2), 63-76. https://doi.org/10.1504/IJSN.2022.123293

Gavilanez, O., Rodriguez, G., & Gavilanez, F. (2017). *Audit Analysis Models, Security Frameworks and Their Relevance for VoIP*. https://doi.org/10.48550/arXiv.1704.02440

Geneiatakis, D., Lambrinoudakis, C., & Kambourakis, G. (2008). An ontology-based policy for deploying secure SIP-based VoIP services. *Computers & Security*, *27*(7), 285-297. https://doi.org/10.1016/j.cose.2008.07.002

George, D., & Mallery, P. (2021). *IBM SPSS Statistics 27 Step by Step: A Simple Guide and Reference* (17th ed.). Allyn & Bacon, Inc.

Goldstein, A., & Frank, U. (2016). Components of a multi-perspective modeling method for designing and managing IT security systems. *Information Systems and E-Business Management*, *14*(1), 101-140. https://doi.org/10.1007/s10257-015-0276-5

Gonzalez, N., Miers, C., Redígolo, F., Simplício, M., Carvalho, T., Näslund, M., & Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *1*(1), 11. https://doi.org/10.1186/2192-113X-1-11

Guo, Z., Cho, J.-H., Chen, I.-R., Sengupta, S., Hong, M., & Mitra, T. (2021). *Online Social Deception and Its Countermeasures: A Survey*. 1770-1806. https://doi.org/10.1109/ACCESS.2020.3047337

Hashmi, S., George, N., Saqib, E., Ali, F., Siddique, N., & Kashif, S. (2023). *Training Users to Recognize Persuasion Techniques in Vishing Calls*. https://doi.org/10.1145/3544549.3585823

Huseinović, A., Mrdović, S., Bicakci, K., & Uludag, S. (2020). *A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid*. https://doi.org/10.1109/ACCESS.2020.3026923

Imran, M., Hamid, S., & Ismail, M. A. (2023). Advancing Process Audits With Process Mining: A Systematic Review of Trends, Challenges, and Opportunities. *IEEE Access*, *11*, 68340-68357. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3292117

Irarrázaval, M. E., Maldonado, S., Pérez, J., & Vairetti, C. (2021). Telecom traffic pumping analytics via explainable data science. *Decision Support Systems*, *150*, 113559. https://doi.org/10.1016/j.dss.2021.113559

ISACA. (2007). *COBIT® 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models*. ISACA.

ISACA. (2024). *Nearly Two thirds of Cybersecurity Pros Say Job Stress Is Growing According to New ISACA Research*. ISACA. https://www.isaca.org/about-us/newsroom/press-releases/2024/nearly-two-thirds-of-cybersecurity-pros-say-job-stress-is-growing-according-to-new-isaca-research

ISACA. (2025). *IT/IS Audit Programs & Tools | IT Professional Resources | ISACA*. https://www.isaca.org/resources/insights-and-expertise/audit-programs-and-tools

ISO. (2022). *ISO - ISO/IEC 27000 family—Information security management*. ISO. https://www.iso.org/standard/iso-iec-27000-family

ISO/IEC 27001:2022. (2022). ISO. https://www.iso.org/standard/27001

IT Governance. (2025). *The Calder-Moir IT Governance Framework*. https://www.itgovernance.eu/es-es/calder-moir-es

Jaafar, M. A., & Al-Daamy, A. M. M. (2024). Impact of Strategic Audit on Enhancing the Efficiency of the Internal Control System: A Study of Industrial Companies in Iraq. *Technium Social Sciences Journal*, *56*, 1-13. https://doi.org/10.47577/tssj.v56i1.10845

Jaber, A. (2022). *Competitive Study on Public and Private Key Usage in Voice over Internet Protocol*. https://doi.org/10.1109/ISEC54952.2022.10025239

Joint Task Force. (2022). *Assessing security and privacy controls in information systems and organizations* (NIST SP 800-53Ar5; p. NIST SP 800-53Ar5). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-53Ar5

Kara, M., Merzeh, H., Aydın, M., & Balık, H. (2023). *VoIPChain: A decentralized identity authentication in Voice over IP using Blockchain*. *198*, 247-261. https://doi.org/10.1016/j.comcom.2022.11.019

Kartika, A., & Aprilinda, Y. (2019). Maturity rating of information technology governance for State Owned Enterprises (SOE). *Control Theory and Informatics*, *8*(0), 72. https://doi.org/10.7176/CTI/8-07

Kerr, D. S., & Murthy, U. S. (2013). The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: An international survey. *Information & Management*, *50*(7), 590-597. https://doi.org/10.1016/j.im.2013.07.012

Khan, H. M. A., Inayat, U., Zia, M. F., Ali, F., Jabeen, T., & Ali, S. M. (2021). Voice Over Internet Protocol: Vulnerabilities and Assessments. *2021 International Conference on Innovative Computing (ICIC)*, 1-6. https://doi.org/10.1109/ICIC53490.2021.9692955

Kishore, M., Lavanya, D., Dennypau, K., Bhavani, G., & Manikanteswarao, S. (2024). A comprehensive review of VoIP technologies and performance metrics. *Journal of Electrical Systems*, *20*(3), 9643-9650. https://doi.org/10.52783/jes.8536

Kondoth, L., Shankaran, R., Sheng, Q., & Han, R. (2023). *Wireless Network-on-Chip Security Review: Attack Taxonomy, Implications, and Countermeasures*. *11*, 122876-122892. https://doi.org/10.1109/ACCESS.2023.3329572

Kuhn, D. R., Walsh, T. J., & Fries, S. (2005). *Security considerations for Voice Over IP Systems* (NIST SP 800-58; 0 ed., p. NIST SP 800-58). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-58

Kumar, V., & Roy, O. P. (2021). Security and Challenges in Voice over Internet Protocols: A Survey. *IOP Conference Series: Materials Science and Engineering*, *1020*(1), 012020. https://doi.org/10.1088/1757-899X/1020/1/012020

Laurens, R., Christianto, E., Caulkins, B., & Zou, C. C. (2022). Side-Channel VoIP Profiling Attack against Customer Service Automated Phone System. *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, 6091-6096. https://doi.org/10.1109/GLOBECOM48099.2022.10001537

Lu, K.-C., Liu, I.-H., Chang, K.-H., & Li, J.-S. (2024). *VoWi-Fi security threats: Address resolution protocol attack and countermeasures*. https://doi.org/10.1049/ntw2.12113

Malhotra, Y. (2018). *Bridging networks, systems and controls frameworks for cybersecurity curriculums and standards development*. https://doi.org/10.21314/JOP.2018.201

Mcinnes, N., & Wills, G. (2025). *The VoIP PBX Honeypot Advance Persistent Threat Analysis*. 70-80. http://dx.doi.org/10.5220/0010443500700080

Mishra, M., Jain, S., Patel, S., Mani, S., Boragule, A., Sahni, N., & Chirakarotur. (2024). Multimodal Strategy To Defend Mobile Devices Against Vishing Attacks. *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*. https://doi.org/10.1145/3636534.3690683

Motl, J., & Kordík, P. (2021). Fast and exact audit scheduling optimization. *SN Applied Sciences*, *3*(10), 794. https://doi.org/10.1007/s42452-021-04778-z

Nazih, W., Alnowaiser, K., Eldesouky, E., & Youssef Atallah, O. (2023). Detecting SPIT Attacks in VoIP Networks Using Convolutional Autoencoders: A Deep Learning Approach. *Applied Sciences*, *13*(12), 6974. https://doi.org/10.3390/app13126974

Neto, J., & Ferreira, A. (2013). *Metamodel of the IT Governance Framework Cobit | Journal of Information Systems and Technology Management*. *3*(10). https://doi.org/10.4301/s1807-17752013000300004

Nielsen, J., & Landauer, T. K. (1993). A mathematical model of the finding of usability problems. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '93*, 206-213. https://doi.org/10.1145/169059.169166

Nyassi, V., Tchakount, F., Yenk, B. O., Danga, D. E. H., Ngoran, M. D., & Fendji, J. L. K. E. (2024). Emoti-Shing: Detecting Vishing Attacks by Learning Emotion Dynamics through Hidden Markov Models. *Journal of Intelligent Learning Systems and Applications*, *16*(3), 274-315. https://doi.org/10.4236/jilsa.2024.163015

Oliinyk, B. M., & Oleksiuk, V. P. (2024). Social engineering as a component of professional competence in information security of future computer science teachers. *Educational Dimension*, *11*, 129-145. https://doi.org/10.55056/ed.778

Ramly, M., Ng, Z., Khamayseh, Y., Kwan, C., Amphawan, A., & Neo, T.-K. (2024). Review and Enhancement of VoIP Security: Identifying Vulnerabilities and Proposing Integrated Solutions. *Journal of Telecommunications and the Digital Economy*, *12*, 109-136. https://doi.org/10.18080/jtde.v12n4.1022

Rosenberg, J., Schulzrinne, H., Johnston, A., Camarillo, G., Peterson, J., Sparks, R., Handley, M. J., & Schooler, E. (2002). *SIP: Session Initiation Protocol* (Request for Comments RFC 3261). Internet Engineering Task Force. https://doi.org/10.17487/RFC3261

Ryoo, J., Rizvi, S., Aiken, W., & Kissell, J. (2014). Cloud Security Auditing: Challenges and Emerging Approaches. *IEEE Security & Privacy*, *12*(6), 68-74. IEEE Security & Privacy. https://doi.org/10.1109/MSP.2013.132

Sadgrove, K. (2016). *The Complete Guide to Business Risk Management*. Routledge.

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Salas, J. A., & Reyes, N. M. (2015). Modelo propuesto para la detección de fraudes por parte de los auditores internos basado en las Normas Internacionales de Auditoría. *Cuadernos de Contabilidad*, *16*(SPE42), 579-623. https://doi.org/10.11144/Javeriana.cc16-42.mpdf

Salihu, A., & Hoti, H. (2022). Managers' Perception on the IT Audit Recommendations: The Effect of Risk Significance, Ease of Implementation and Added Value on Implementation of Recommendations. *Journal of ICT Standardization*, *10*(2), 105-124. Journal of ICT Standardization. https://doi.org/10.13052/jicts2245-800X.1021

Santoso, F., & Finn, A. (2024). *Trusted Operations of a Military Ground Robot in the Face of Man-in-the-Middle Cyberattacks Using Deep Learning Convolutional Neural Networks: Real-Time Experimental Outcomes | IEEE Journals & Magazine | IEEE Xplore*. *21*, 2273-2284. https://doi.org/10.1109/TDSC.2023.3302807

Schmitt, M. (2022). *Mobile Security for the modern CEO: Attacks, Mitigations, and Future Trends* (arXiv:2207.08105). arXiv. https://doi.org/10.48550/arXiv.2207.08105

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences*, *12*(12), Article 12. https://doi.org/10.3390/app12126042

Sreenivasulu, V., & Ravikumar, C. (2025). FractalNet-based key generation for authentication in Voice over IP using Blockchain. *Ain Shams Engineering Journal*, *16*(3), 103286. https://doi.org/10.1016/j.asej.2025.103286

Stanescu, C., Gabriel, M. E., Gabriel, P., Denisa, C. L., Nicoleta, A., & Constantin, P. D. (2023). VoIP system for Wi-Fi Networks and Smart Terminals. *2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 01-06. https://doi.org/10.1109/ECAI58194.2023.10194061

Sun, C.-M., Wang, Y.-Y., & Yang, C.-B. (2022). *Information Security Assurance and the Role of Security Configuration Management: Substantive and Symbolic Perspectives*. https://doi.org/10.2308/ISYS-2020-065

Sun, Y., Li, J., Lu, M., & Guo, Z. (2024). *Study of the Impact of the Big Data Era on Accounting and Auditing* (arXiv:2403.07180). arXiv. https://doi.org/10.48550/arXiv.2403.07180

Suthar, D., & Rughani, P. H. (2020). A Comprehensive Study of VoIP Security. *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, 812-817. https://doi.org/10.1109/ICACCCN51052.2020.9362943

Syafitri, W., Shukur, Z., Mokhtar, U., Sulaiman, R., & Ibrahim, M. (2022). *Social Engineering Attacks Prevention: A Systematic Literature Review*. *10*, 39325-39343. https://doi.org/10.1109/ACCESS.2022.3162594

Tan, E. N., Garg, M., Jeter, D., Kirubaharan, D., & Naiker, V. (2025). Audit Office Effectiveness and Efficiency. *AUDITING: A Journal of Practice & Theory*, *44*(2), 181-209. https://doi.org/10.2308/AJPT-2020-064

Tas, M., & Baktir, S. (2024). *Blockchain-Based Caller-ID Authentication (BBCA): A Novel Solution to Prevent Spoofing Attacks in VoIP/SIP Networks*. *12*, 60123-60137. https://doi.org/10.1109/ACCESS.2024.3393487

Thomas, C., Fraga-Lamas, P., & Fernández-Caramés, T. M. (2020). *Computer Security Threats*. BoD – Books on Demand.

Tjhin, V. U. (2014). Audit Domain Acquire And Implement dengan Cobit 4.1 pada PT Erajaya Swasembada Tbk. *ComTech: Computer, Mathematics and Engineering Applications*, *5*(2), 1086-1095. https://doi.org/10.21512/comtech.v5i2.2373

Tsai, Hsieh, C.-L., Wang, C.-W., Chen, C.-T., & Li, W.-H. (2015). The impact of IT management process of COBIT 5 on internal control, information quality, and business

value. *IEEE International Conference on Industrial Engineering and Engineering Management*, 631-634. https://doi.org/10.1109/IEEM.2015.7385724

Tsiatsikas, Z., Geneiatakis, D., Kambourakis, G., & Keromytis, A. D. (2013). A Privacy-Preserving Entropy-Driven Framework for Tracing DoS Attacks in VoIP. *2013 International Conference on Availability, Reliability and Security*, 224-229. https://doi.org/10.1109/ARES.2013.30

Vasilomanolakis, E., Karuppayah, S., Kikiras, P., & Mühlhäuser, M. (2015). *A honeypot-driven cyber incident monitor: Lessons learned and steps ahead*. https://doi.org/10.1145/2799979.2799999

Vilarinho, S., & da Silva, M. M. (2011). Risk Management Model in ITIL. En M. M. Cruz-Cunha, J. Varajão, P. Powell, & R. Martinho (Eds.), *ENTERprise Information Systems* (pp. 306-314). Springer. https://doi.org/10.1007/978-3-642-24355-4_31

Vrhovec, S. (2021). *Survey about social engineering and the Varni na internetu awareness campaign, 2020* (arXiv:2109.00837). arXiv. https://doi.org/10.48550/arXiv.2109.00837

Waelchli, S., & Walter, Y. (2025). Reducing the risk of social engineering attacks using SOAR measures in a real world environment: A case study. *Computers & Security*, *148*, 104137. https://doi.org/10.1016/j.cose.2024.104137

Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access*, *8*, 85094-85115. IEEE Access. https://doi.org/10.1109/ACCESS.2020.2992807

Wang, Z., Zhu, H., Liu, P., & Sun, L. (2021). Social engineering in cybersecurity: A domain ontology and knowledge graph application examples. *Cybersecurity*, *4*(1), 31. https://doi.org/10.1186/s42400-021-00094-6

Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, *4*, 100126. https://doi.org/10.1016/j.chbr.2021.100126

Wolden, M., Valverde, R., & Talla, M. (2015). *The effectiveness of COBIT 5 Information Security Framework for reducing Cyber Attacks on Supply Chain Management System*. https://doi.org/10.1016/j.ifacol.2015.06.355

Yakubova, M., Manankova, O., Mukasheva, A., Baikenov, A., & Serikov, T. (2023). The Development of a Secure Internet Protocol (IP) Network Based on Asterisk Private Branch Exchange (PBX). *Applied Sciences*, *13*(19), 10712. https://doi.org/10.3390/app131910712

Yasar, A., & Yazicigil, R. (2023). *Physical-Layer Security for Energy-Constrained Integrated Systems: Challenges and Design Perspectives*. *3*, 262-273. https://doi.org/10.1109/OJSSCS.2023.3327326

Younes, O., & Albalawi, U. (2022). Securing Session Initiation Protocol. *Sensors*, *22*(23), 9103. https://doi.org/10.3390/s22239103

Youness, O. (2023). Secure and Efficient Authentication Scheme for VoIP Communications. *International Journal of Computers and Information*, *10*(3). https://doi.org/10.21608/ijci.2023.236399.1142

Zhai, H., Zhang, Q., Zhai, Q., Bian, R., Liu, B., & Zhang, Y. (2024). *Dual Authentication Mechanism of Reliable Session Initiation Protocol | IEEE Conference Publication | IEEE Xplore*. https://ieeexplore.ieee.org/document/10869742

Zhang, G., & Fischer, S. (2019). A survey on anonymous voice over IP communication: Attacks and defenses. *Electronic Commerce Research*, *19*(3), 655-687. https://doi.org/10.1007/s10660-019-09369-0

Zhang, L., Tang, S., & Zhu, S. (2016). A lightweight privacy preserving authenticated key agreement protocol for SIP-based VoIP. *Peer-to-Peer Networking and Applications*, *9*(1), 108-126. https://doi.org/10.1007/s12083-014-0317-8

Zumba, C., Garcia, D., & Bolanos, F. (2018). Proposal of a framework for the internal audit to the service management of the department of information technologies. *2018 13th*

Iberian Conference on Information Systems and Technologies (CISTI), 1-5. https://doi.org/10.23919/CISTI.2018.8399441

Žvanut, B., Burnik, M., Kolnik, T. Š., & Pucer, P. (2020). The applicability of COBIT processes representation structure for quality improvement in healthcare: A Delphi study. *International Journal for Quality in Health Care*, *32*(9), 577-584. https://doi.org/10.1093/intqhc/mzaa096

ANEXOS

Anexo A. Matriz de Consistencia

Problema de Investigación	**Pregunta de Investigación**	**Objetivo de Investigación**	**Hipótesis**	**Variables (VI - VD)**	**Método y Técnicas**
PG: ¿La ausencia de un modelo de auditoría de seguridad específico para sistemas VoIP limita la eficiencia temporal durante la ejecución de auditorías respecto de los modelos tradicionales?	¿La implementación de un modelo de auditoría de seguridad específico para sistemas VoIP mejora la eficiencia temporal durante la ejecución de auditorías respecto de los modelos tradicionales?	Implementar un modelo de auditoría de seguridad específico para sistemas VoIP que mejore la eficiencia temporal durante la ejecución de auditorías frente a los modelos tradicionales	La implementación de un modelo de auditoría de seguridad específico para sistemas VoIP mejora la eficiencia temporal durante la ejecución de auditorías respecto de los modelos tradicionales	**VI:** Implementación de un modelo de auditoría de seguridad específico para sistemas VoIP **VD:** Eficiencia temporal durante la ejecución de auditorías	**Método**: Cuantitativo – Comparativo (con validación por juicio experto) **Técnicas**: **Técnica de investigación:** - Estudio de caso **Técnicas de recolección de datos:** - Encuesta estructurada a expertos en seguridad VoIP - Registro técnico del tiempo efectivo durante la auditoría

Problema de Investigación	Pregunta de Investigación	Objetivo de Investigación	Hipótesis	Variables (VI - VD)	Método y Técnicas
					Técnicas de análisis de datos: - Prueba de normalidad Shapiro-Wilk - Prueba t de Student para muestras independientes - Prueba t de Student para muestras relacionadas
PE1: ¿La insuficiente especificación de los requerimientos de seguridad para sistemas VoIP limita la eficiencia temporal en la ejecución de auditorías de seguridad?	¿La incorporación funcional de los requerimientos de seguridad específicos para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad?	Determinar los requerimientos de seguridad específicos para sistemas VoIP que mejoren la eficiencia temporal en la ejecución de auditorías de seguridad	La incorporación funcional de los requerimientos de seguridad específicos para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad	**VI:** Incorporación funcional de los requerimientos de seguridad específicos para sistemas VoIP **VD:** Eficiencia temporal en la ejecución de auditorías de seguridad	**Método**: Cuantitativo – Descriptivo **Técnicas**: **Técnicas de recolección de datos:** - Registro de procedimientos integrados - Registro de ítems evaluados por procedimiento - Registro técnico del tiempo efectivo durante la auditoría

Problema de Investigación	Pregunta de Investigación	Objetivo de Investigación	Hipótesis	Variables (VI - VD)	Método y Técnicas
					Técnicas de análisis de datos: - Análisis comparativo entre modelos - Observación directa mediante el instrumento de evaluación aplicado - Prueba t de Student para muestras relacionadas - Análisis comparativo de tiempos efectivos
PE2: ¿La ausencia de componentes específicos en los modelos de auditoría tradicionales limita la relevancia de las evaluaciones de seguridad en sistemas VoIP?	¿La integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP incrementa la relevancia de las evaluaciones de seguridad en dichos sistemas?	Implementar componentes específicos en el modelo de auditoría de seguridad propuesto para sistemas VoIP que incrementen la relevancia de las evaluaciones de seguridad	La integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP incrementa la relevancia de las evaluaciones de seguridad en dichos sistemas	**VI:** Integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP **VD:** Relevancia de las evaluaciones de seguridad en sistemas VoIP	**Método**: Cuantitativo – Comparativo (con validación por juicio experto) **Técnicas**: **Técnicas de recolección de datos:** - Registros de auditoría - Encuesta estructurada aplicada a expertos

Problema de Investigación	Pregunta de Investigación	Objetivo de Investigación	Hipótesis	Variables (VI - VD)	Método y Técnicas
					Técnicas de análisis de datos: - Prueba t de Student para muestras independientes
PE3: ¿La ausencia de un plan de cultura de seguridad que aborde integralmente la ingeniería social en entornos VoIP incrementa la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano?	¿La incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP reduce la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano?	Implementar un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP orientado a la reducción de la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano	La incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP reduce la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano	**VI:** Incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería social en entornos VoIP **VD:** Percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano	**Método**: Mixto - Documental, descriptivo y validación cuantitativa **Técnicas**: **Técnicas de recolección de datos:** - Registros de auditoría - Encuesta estructurada aplicada a expertos **Técnicas de análisis de datos:** - Prueba t de Student para muestras independientes
PE4: ¿La ausencia de un procedimiento especializado para	¿La integración operativa de un procedimiento especializado en una	Implementar una guía de auditoría específica para sistemas VoIP que	La integración operativa de un procedimiento especializado en una	**VI:** Integración operativa de un procedimiento especializado en una	**Método**: Cuantitativo – Comparativo

Problema de Investigación	**Pregunta de Investigación**	**Objetivo de Investigación**	**Hipótesis**	**Variables (VI - VD)**	**Método y Técnicas**
auditar sistemas VoIP limita la eficiencia temporal en la ejecución de auditorías de seguridad?	guía de auditoría específica para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad?	incorpore un procedimiento especializado orientado a la mejora de la eficiencia temporal en la ejecución de auditorías de seguridad	guía de auditoría específica para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad	guía de auditoría específica para sistemas VoIP **VD:** Eficiencia temporal en la ejecución de auditorías de seguridad	**Técnicas**: **Técnicas de recolección de datos:** - Guía de auditoría - Registro técnico de tiempos efectivos de auditoría **Técnicas de análisis de datos:** - Prueba t de Student para muestras relacionadas

Fuente: Elaborada por el autor.

Anexo B. Operacionalización de Variables

Hipótesis	Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Instrumentos de medición	Escala	Técnica de análisis
HP: La implementación de un modelo de auditoría de seguridad específico para sistemas VoIP mejora la eficiencia temporal durante la ejecución de auditorías respecto de los modelos tradicionales	**VI:** Implementación de un modelo de auditoría de seguridad específico para sistemas VoIP	Marco metodológico orientado a atender las necesidades y amenazas específicas de los sistemas VoIP, considerando tanto vulnerabilidades técnicas como amenazas de origen humano	Implementación del modelo de auditoría de seguridad específico para sistemas VoIP derivado de la revisión bibliográfica y aplicado de forma práctica en auditorías reales	Incorporación funcional de requerimientos de seguridad específicos para sistemas VoIP	Número de procedimientos evaluados por modelo Número de ítems evaluados por modelo	Registro de procedimientos integrados Registro de ítems evaluados por procedimiento	Conteo absoluto (número de procedimientos e ítems evaluados por área)	Análisis comparativo entre modelos Observación directa mediante el instrumento de evaluación aplicado
				Integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP	Número de componentes específicos evaluados por el modelo	Registros de auditoría Encuesta estructurada aplicada a expertos	Cualitativa nominal (componentes por modelo)	Prueba t de Student para muestras independientes
				Incorporación funcional de un plan de cultura de seguridad que integre el tratamiento de la ingeniería	Evaluación de componentes del plan de cultura de seguridad en el modelo	Registros de auditoría Encuesta estructurada aplicada a expertos	Cualitativa nominal Cuantitativa ordinal (escala de Likert 1-5)	Prueba t de Student para muestras independientes

Hipótesis	Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Instrumentos de medición	Escala	Técnica de análisis
				social en entornos VoIP Integración operativa de un procedimiento especializado en una guía de auditoría específica para sistemas VoIP	Presencia del procedimiento especializado en la guía de auditoría	Guía de auditoría	Escala cuantitativa de razón (minutos de ejecución)	Prueba t de Student para muestras relacionadas
	VD: Eficiencia temporal durante la ejecución de auditorías	Capacidad de completar un proceso de auditoría de forma efectiva utilizando la menor cantidad de tiempo posible sin sacrificar la calidad del trabajo	Tiempo efectivo registrado en minutos para la ejecución de cada auditoría, permitiendo comparar la duración entre el modelo tradicional y el modelo propuesto bajo condiciones similares	Tiempo efectivo total de ejecución de auditorías	Tiempo efectivo de auditoría (en minutos) por modelo	Registro técnico del tiempo efectivo durante la auditoría	Cuantitativa – razón (minutos de ejecución)	Prueba de normalidad Shapiro-Wilk Prueba t de Student para muestras relacionadas

Hipótesis	Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Instrumentos de medición	Escala	Técnica de análisis
HS1: La incorporación funcional de los requerimientos de seguridad específicos para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad.	**VI:** Incorporación funcional de los requerimientos de seguridad específicos para sistemas VoIP	Aplicación práctica de un conjunto estructurado de requisitos técnicos y organizativos orientados a mitigar amenazas y vulnerabilidades inherentes a los entornos VoIP	Inclusión efectiva de los requerimientos de seguridad específicos dentro del modelo propuesto y su aplicación en auditorías reales	Cobertura de requerimientos (áreas)	Número de procedimientos evaluados por modelo Número de ítems evaluados por modelo	Registro de procedimientos integrados Registro de ítems evaluados por procedimiento	Conteo absoluto (número de procedimientos e ítems evaluados por área)	Análisis comparativo entre modelos Observación directa mediante el instrumento de evaluación aplicado
	VD: Eficiencia temporal en la ejecución de auditorías de seguridad	Habilidad para ejecutar un proceso de auditoría de manera eficiente, optimizando el tiempo empleado sin comprometer la calidad de los resultados obtenidos	Tiempo total requerido (en minutos) para ejecutar auditorías completas con cada modelo	Tiempo efectivo total de ejecución de auditorías por etapa	Tiempo efectivo de auditoría (en minutos) por cada área evaluada Reducción porcentual del tiempo de ejecución respecto al modelo tradicional	Registro técnico del tiempo efectivo durante la auditoría	Cuantitativa – razón (minutos de ejecución)	Prueba t de Student para muestras relacionadas Análisis comparativo de tiempos efectivos

Hipótesis	Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Instrumentos de medición	Escala	Técnica de análisis
HS2: La integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP incrementa la relevancia de las evaluaciones de seguridad en dichos sistemas.	**VI:** Integración operativa de componentes específicos en el modelo de auditoría de seguridad para sistemas VoIP	Inclusión funcional de componentes diseñados exclusivamente para abordar amenazas y características propias de sistemas VoIP dentro del modelo de auditoría	Incorporación efectiva de componentes VoIP en el modelo de auditoría de seguridad específico para sistemas VoIP	Integración de componentes específicos	Número de componentes específicos evaluados por el modelo	Registros de auditoría Encuesta estructurada aplicada a expertos	Cualitativa nominal (componentes por modelo)	Prueba t de Student para muestras independientes
	VD: Relevancia de las evaluaciones de seguridad en sistemas VoIP	Nivel de utilidad y especificidad de la auditoría para abordar aspectos clave de seguridad VoIP	Valoración de expertos sobre aspectos evaluados	Relevancia de los resultados de auditoría	Pertinencia de los resultados obtenidos frente a las particularidades del entorno VoIP	Encuesta estructurada aplicada a expertos	Cuantitativa ordinal (escala de Likert 1-5)	Prueba t de Student para muestras independientes
HS3: La incorporación funcional de un plan de cultura de seguridad que integre el	**VI:** Incorporación funcional de un plan de cultura de seguridad que integre el	Integración práctica y sistemática de un conjunto de políticas, acciones y capacitacione	Diseño e inclusión del plan de cultura de seguridad en el modelo de auditoría	Presencia funcional del plan de cultura de seguridad en los procesos de auditoría	Evaluación de componentes del plan de cultura de seguridad en el modelo	Registros de auditoría Encuesta estructurada aplicada a expertos	Cualitativa nominal Cuantitativa ordinal (escala de Likert 1-5)	Prueba t de Student para muestras independientes

Hipótesis	Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Instrumentos de medición	Escala	Técnica de análisis
tratamiento de la ingeniería social en entornos VoIP reduce la percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano	tratamiento de la ingeniería social en entornos VoIP	s orientadas a concienciar sobre los riesgos de ingeniería social en entornos VoIP	de seguridad VoIP propuesto cuya percepción de relevancia se compara con un modelo tradicional					
	VD: Percepción de vulnerabilidad organizacional ante ataques que explotan el factor humano	Nivel de exposición que los evaluadores perciben que posee una organización frente a amenazas de ingeniería social que comprometen la seguridad de los sistemas VoIP	Valoración experta sobre el nivel de percepción de vulnerabilidad organizacional ante ataques de ingeniería social	Nivel percibido de exposición organizacional frente a ataques de ingeniería social	Percepción de efectividad del modelo para prevenir ataques de ingeniería social	Encuesta estructurada aplicada a expertos	Escala ordinal tipo Likert	Prueba t de Student para muestras independientes
HS4: La integración operativa de un procedimiento	**VI:** Integración operativa de un	Aplicación estructurada de un conjunto de	Implementación del procedimiento detallado	Aplicación del procedimiento especializado integrado en la	Presencia del procedimiento especializado	Guía de auditoría	Escala cuantitativa de razón (minutos	Prueba t de Student para muestras relacionadas

Hipótesis	Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Instrumentos de medición	Escala	Técnica de análisis
especializado en una guía de auditoría específica para sistemas VoIP mejora la eficiencia temporal en la ejecución de auditorías de seguridad	procedimiento especializado en una guía de auditoría específica para sistemas VoIP	pasos específicos dentro de una guía de auditoría orientada a mejorar el desempeño temporal del proceso de auditoría	incluido en la guía de auditoría, aplicado en auditorías reales comparadas con procesos tradicionales	guía de auditoría	en la guía de auditoría		de ejecución)	
	VD: Eficiencia temporal en la ejecución de auditorías de seguridad	Capacidad para llevar a cabo una auditoría maximizando la eficiencia en el tiempo, asegurando integridad y calidad de los hallazgos obtenidos	Tiempo total requerido (en minutos) para ejecutar auditorías completas con cada modelo	Tiempo efectivo de ejecución de auditoría	Tiempo efectivo total de la auditoría (en minutos) Diferencia porcentual entre modelos	Registro técnico de tiempos efectivos de auditoría	Cuantitativa – razón (minutos de ejecución)	Prueba t de Student para muestras relacionadas

Fuente: Elaborada por el autor.

Anexo C. Encuesta A1. Aspectos Ingeniería Social (Modelo Auditoría de Seguridad VoIP)

Introducción

La presente encuesta determinará la relevancia (pertinencia) de varios aspectos de Ingeniería Social considerados en un Modelo de Auditoría de Seguridad VoIP que evalúe la seguridad en cuanto a Confidencialidad, Integridad y Disponibilidad. La encuesta le tomará pocos minutos y sus respuestas son totalmente confidenciales.
Solo puede responder la encuesta una vez; no obstante, puede editar las respuestas hasta el cierre de la encuesta. Todas las preguntas requieren respuesta.

Si desea realizar alguna pregunta sobre la encuesta, envíe un correo electrónico a: oscar.gavilanez@gmail.com

¡Valoramos sus comentarios!

Nombre completo
Por favor ponga sus nombre y apellidos completos

Perfil
Por favor indique su perfil profesional. Ingeniero en Sistemas Informáticos, Ingeniero en Electrónica y Telecomunicaciones, Psicofisiólogo Forense, Especialista en Detección y Prevención de Fraudes Informáticos, Consultor de seguridad, Auditor de seguridad, Experto Ingeniería Social, perfiles relacionados
---

e-mail

Cargo

Por favor indique su cargo. Administrador TI, Administrador VoIP, Consultor de seguridad, Auditor de seguridad, perfiles relacionados

---

Institución a la que pertenece

Ingeniería Social en el Modelo de auditoría de seguridad para sistemas VoIP. Se requiere determinar ¿Qué tan de acuerdo es que los ítems considerados sobre Ingeniería Social sean adecuados para el Modelo de auditoría de seguridad en sistemas VoIP?

a) Incentivos y motivadores en Ingeniería Social

La ingeniería social se basa en la psicología. Existen diferentes incentivos y motivadores en las personas que permiten a los ingenieros sociales llevar a su víctima a actuar

A1. ¿Es adecuado incluir en un modelo de auditoría de seguridad para sistemas VoIP los Incentivos y motivadores en Ingeniería Social?

Incentivos y motivadores en Ingeniería Social: reciprocidad (Sentir que le debemos un favor a quien hace algo por nosotros), orientación social (Buscar a una persona que nos diga que tenemos que hacer.), consistencia/compromiso (Desarrollo de patrones de conducta que se convierten en hábitos), aceptación (Aceptar una situación molesta o desagradable de determinada manera y dejarse persuadir más fácilmente por personas que nos gustan), autoridad (Ser receptivo a las órdenes y peticiones de las figuras de autoridad) y tentación (Tener más motivación para perseguir lo exclusivo o limitado)

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

b) Pruebas de seguridad de penetración mediante ingeniería social.

Técnicas de ingeniería social que los atacantes pueden usar para probar la seguridad de la organización: phishing/vishing, pretexting, media dropping y tailgating

A2. ¿Es adecuado incluir en un modelo de auditoría de seguridad para sistemas VoIP la prueba de seguridad de penetración Phishing/Vishing?

Phishing: El objetivo de este ataque de prueba debería ser que el usuario haga clic en algo y después registrar esa actividad, o incluso instalar un programa como parte de un programa de pruebas mucho más extenso. En última instancia pueden instalar exploit adaptados al software del cliente para verificar problemas con los navegadores, contenido dinámico, plugins o software instalado. Vishing: se trata de un ciberdelito que ofrece a la víctima un número de teléfono al que comunicarse en vez de un link, en el caso del phishing.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A3. ¿Es adecuado incluir en un modelo de auditoría de seguridad para sistemas VoIP la prueba de seguridad de penetración Pretexting?

El pretexting (pretextos) implica llamar por teléfono al usuario y pedirle cierta información, generalmente simulando ser alguien que precisa su ayuda. Esta técnica puede funcionar bien si se usa mediante aquellos usuarios de bajo nivel técnico y que tengan acceso a información sensible.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A4. ¿Es adecuado incluir en un modelo de auditoría de seguridad para sistemas VoIP la prueba de seguridad de penetración Media dropping?

La descarga en medios suele implicar la presencia de un disco USB en un lugar razonable, como un aparcamiento o la entrada al edificio. El ingeniero social busca el interés de la persona que, al utilizar esta unidad flash, lanza un ataque contra el equipo donde se conecta.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A5. ¿Es adecuado incluir en un modelo de auditoría de seguridad para sistemas VoIP la prueba de seguridad de penetración Tailgating?

Supone lograr acceso a una instalación física mediante engaño a su personal, o simplemente colándose dentro. El objetivo de este test es demostrar que el atacante puede superar a la seguridad física.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

c) Plan de Cultura de Seguridad

Combinación de los valores, actitudes, competencias y modos de comportamiento, tanto individuales como de grupo, que determinan el compromiso, modelo y competencia de la gestión de la seguridad en la organización

A6. ¿Es adecuado incluir en el plan de cultura de seguridad del modelo de auditoría VoIP la revisión de las políticas de Seguridad (de la información) vigentes?

Describe cuáles son los activos críticos de la empresa y cómo deben protegerse. Proporcionar una breve descripción general del uso aceptable de cualquiera de los Activos de la información.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo

- De acuerdo
- Muy de acuerdo

A7. ¿Es adecuado incluir en el plan de cultura de seguridad del modelo de auditoría VoIP la evaluación del cumplimiento de las políticas de seguridad?

Comprende la percepción y actitud de un individuo hacia la seguridad de la información

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A8. ¿Es adecuado incluir en el plan de cultura de seguridad del modelo de auditoría VoIP la evaluación de Recursos Humanos?

Evaluación del componente humano en cuanto a roles y estilo de aprendizaje

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A9. ¿Es adecuado incluir en el plan de cultura de seguridad del modelo de auditoría VoIP la definición de un Plan de Desarrollo de Cultura de Seguridad?

Proporciona los conocimientos necesarios y sentar las bases para los supuestos tácitos compartidos (creencias y valores de los individuos)

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

d) Aspectos a ser evaluados dentro de la Seguridad de la Información

A10. ¿Es adecuado incluir en el plan de cultura de seguridad del modelo de auditoría VoIP la evaluación de valores clave que afectan a la cultura de seguridad de la organización?

Proporciona los conocimientos necesarios y sentar las bases para los supuestos tácitos compartidos (creencias y valores de los individuos)

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A11. ¿Es adecuado incluir en el plan de cultura de seguridad del modelo de auditoría VoIP la evaluación de la división de la responsabilidad y la autoridad, e incorporación de esos valores en las jerarquías y divisiones organizacionales?

Los hábitos de trabajo organizacionales definen la mayoría de los aspectos del comportamiento organizacional mediante la creación y el fomento de algunas formas de comunicación e interacción entre los miembros, a la vez que limitan y desalientan a los demás. Con el tiempo, estos comportamientos se vuelven arraigados e instintivos, a medida que la "forma" de la organización se convierte en parte de la cultura.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A12. ¿Es adecuado incluir en el plan de cultura de seguridad del modelo de auditoría VoIP la evaluación de conceptualización de la seguridad de la información por parte de la organización?

Al hablar de seguridad se habla de la necesidad de que todos estén activos y participantes en la protección de la organización.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo

- De acuerdo
- Muy de acuerdo

A13. ¿Es adecuado incluir en el plan de cultura de seguridad del modelo de auditoría VoIP la evaluación de la descripción de la gestión y el control de la información como un recurso compartido?

El control de la información no es necesariamente de seguridad específica, pero la forma en que una organización ve la información como una herramienta y un producto tiene una relación directa con la forma en que la organización se siente al restringir el acceso a ella y al controlar los usos de la información por motivos de seguridad.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A14. ¿Es adecuado incluir en el plan de cultura de seguridad del modelo de auditoría VoIP la evaluación de la selección y priorización de las actividades funcionales cotidianas de la organización, incluidas tareas, interacciones, decisiones y evaluaciones?

Genera datos sobre dónde se encuentra el entorno operacional, incluidos los hábitos y las normas que representa

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A15. ¿Es adecuado incluir en el plan de cultura de seguridad del modelo de auditoría VoIP la evaluación de la gestión de la tecnología como un recurso organizacional?

La tecnología está sujeta a más o menos control, y si se usa para aumentar el éxito de las partes interesadas internas o partes interesadas externas. La gestión de la tecnología puede tener

profundas implicaciones para la cultura de seguridad, agregando tanto libertades como restricciones a los miembros de toda la organización

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A16. ¿Es adecuado incluir en el plan de cultura de seguridad del modelo de auditoría VoIP la evaluación de los siguientes ítems?: a) Cómo las personas son tratadas y utilizadas como un recurso dentro de la organización. b) Comprensión y gestión del riesgo dentro de la organización. c) Formas en que la organización entiende y asume la responsabilidad. d) Desempeño y responsabilidad como requisito básico para la organización?

a) Entorno más parecido a una familia, una comunidad o un movimiento social, donde las personas se elevan por encima de otros componentes de la organización y se les da un enfoque y privilegio especial. b) Explora cómo la administración de riesgos puede diferir entre las categorías culturales dentro de la cultura de seguridad y documenta los medios por los cuales la organización aborda los riesgos y oportunidades en la conducción de sus negocios. c) Dependiendo de la cultura, la rendición de cuentas puede ser mecánica y el producto de medidas estrictas, o puede ser más situacional y subjetiva. d) Definir los métodos mediante los cuales se realiza la evaluación, si los criterios de éxito son formalizados o ad hoc, impulsados o influenciados internamente por terceros y si el desempeño es una actividad organizacional compartida o más individualizada.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

Comentarios y Sugerencias

Anexo D. Encuesta B1. Modelo de auditoría de seguridad VoIP

Introducción

Se lleva a cabo una investigación sobre la importancia y aplicabilidad de un Modelo de auditoría de seguridad para sistemas VoIP, que evalúe la incidencia de los problemas de seguridad y que aborde los retos en cuanto a protección de recursos de TI como activos, tareas, procesos y sistemas de información corporativa. La información que Usted proporcione nos ayudará a realizar mejoras en el modelo propuesto y a priorizar nuevas funcionalidades. La encuesta le tomará pocos minutos y sus respuestas son totalmente confidenciales.

Solo puede responder la encuesta una vez; no obstante, puede editar las respuestas hasta el cierre de la encuesta. Todas las preguntas requieren respuesta.

Si desea realizar alguna pregunta sobre la encuesta, envíe un correo electrónico a: oscar.gavilanez@gmail.com

¡Valoramos sus comentarios!

Nombre completo

Por favor ponga sus nombre y apellidos completos

Perfil

Por favor indique su perfil profesional. Ingeniero en Sistemas Informáticos, Ingeniero en Electrónica y Telecomunicaciones, Psicofisiólogo Forense, Especialista en Detección y Prevención de Fraudes Informáticos, Consultor de seguridad, Auditor de seguridad, perfiles relacionados

---

e-mail

País

Institución a la que pertenece

Se requiere determinar qué tan de acuerdo está en que los ítems considerados son adecuados para incluirlos en un Modelo de auditoría de seguridad para sistemas VoIP

B1. Definir un Plan Estratégico de TI

La planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. La función de TI y los interesados del negocio son responsables de asegurar que el valor óptimo se consigue desde los proyectos y el portafolio de servicios. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido. La estrategia de negocio y prioridades se reflejarán en portafolios y se ejecutarán por los planes estratégicos de TI, que especifican objetivos concisos, planes de acción y tareas que están comprendidas y aceptadas tanto por el negocio como por TI

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B1.1. Gestión de Valor

Trabajar con la empresa para garantizar que la cartera de la empresa de las inversiones de TI habilitado contiene programas que tienen casos de negocio sólidos

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B1.2. Negocios – Alineación TI

Establecer procesos de educación bidireccional y la participación recíproca en la planificación estratégica para lograr la alineación de negocio e integración TI

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B2. Definir la Arquitectura de la Información

La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. Este proceso mejora la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias del negocio. Este proceso de TI también es necesario para incrementar la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de la información compartida a lo largo de las aplicaciones y de las entidades

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B2.1. Información del modelo de Arquitectura Empresarial

Información de Arquitectura Empresarial Modelo - Establecer y mantener un modelo de información de la empresa para permitir el desarrollo de aplicaciones y actividades de toma de apoyo, de acuerdo con los planes de TI

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B2.2. Esquema de Clasificación de Datos

Establecer un sistema de clasificación que se aplica en toda la empresa, basado en la criticidad y sensibilidad (por ejemplo, público, confidencial, secreta) de los datos empresariales. Este esquema debe incluir detalles sobre la propiedad de los datos; definición de los niveles de seguridad adecuados y controles de protección; y una breve descripción de la retención de datos y los requisitos de destrucción, la criticidad y sensibilidad. Debe ser utilizado como base para la aplicación de los controles, como controles de acceso, archivado o cifrado

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B3. Definir los procesos, organización y Relaciones

Una organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión. La organización está embebida en un marco de trabajo de procesos de TI que asegure la transparencia y el control, así como el involucramiento de los altos ejecutivos y de la gerencia del negocio. Un comité estratégico debe garantizar la vigilancia del consejo directivo sobre TI, y uno o más comités de dirección, en los cuales participen tanto el negocio como TI, deben determinar las prioridades de los recursos de TI alineados con las necesidades del negocio. Deben existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el

aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas y la segregación de funciones. Para garantizar el soporte oportuno de los requerimientos del negocio, TI se debe involucrar en los procesos importantes de decisión

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B3.1. Establecimiento de funciones y responsabilidades

Establecer y comunicar las funciones y responsabilidades del personal de TI y los usuarios finales que delimitan entre el personal de TI y la autoridad de los usuarios finales, las responsabilidades y la rendición de cuentas para satisfacer las necesidades de la organización

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B3.2. Responsabilidad sobre el Riesgo, Seguridad y Cumplimiento

Insertar propiedad y responsabilidad de los riesgos relacionados con las TI dentro de la empresa a un nivel superior adecuado. Definir y asignar roles críticos para la gestión de riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B3.3. Datos y Sistema de Propiedad

Proporcionar el negocio con los procedimientos y herramientas, lo que le permite hacer frente a sus responsabilidades en materia de propiedad de los datos y sistemas de información. Los propietarios deben tomar decisiones acerca de la clasificación de la información y sistemas y protegerlos de acuerdo con esta clasificación

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B4. Definir Plan de Cultura de seguridad

Diseño de un Plan de Cultura de Seguridad para luchar contra los ataques de ingeniería social, los procesos se deben diseñar con la ingeniería social en la mente

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B4.1. Configuración de seguridad establecida a partir de Políticas de Auditoría

Se establece configuración de seguridad para los usuarios y hacerlas cumplir a través de políticas asignadas a las unidades de la organización

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B4.2. Directivas de contraseña

Las directivas de contraseñas protegen adecuadamente a los usuarios y la privacidad de los correos electrónicos y aplicaciones

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B4.3. Controles de acceso de la aplicación

Aplicaciones (por ejemplo, centro de llamadas, autoservicio al cliente) Determinar si la utilización de la infraestructura de VoIP tiene la seguridad de acceso adecuada en alineación con las políticas de clasificación de datos y la cuenta de usuario

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B4.4. Controles de seguridad física

Los servidores PBX VoIP tienen protección física adecuada contra la manipulación no autorizada

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B4.5. Restricción de los detalles del sistema de VoIP implementado

Información sobre qué hardware y software de VoIP implementado está restringido sólo para uso interno

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B4.6. Establecimiento de directrices

Enfocar la atención en seguridad de la información para posibilitar que el público objetivo reconozca los temas de interés, estableciendo al inicio qué comportamientos se quieren reforzar, establecimiento de directrices

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B5. Administrar la calidad de servicio (QoS)

A medida que aumenta el tráfico en una red, es más importante para los departamentos de TI equilibrar el rendimiento de la red con el costo del servicio.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B5.1. Generar un plan de gestión para criterios de evaluación

La transmisión de los flujos VoIP es sensible para la calidad de servicio (QoS), Generar un plan de gestión para criterios de evaluación respecto a: retardo de extremo a extremo, retraso jitter y pérdida de paquetes

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B5.2. Equilibrar el rendimiento de la red con el costo del servicio

Las aplicaciones de misión crítica y sensible a la latencia deben competir por ancho de banda con tráfico de menor prioridad. Al mismo tiempo, algunos usuarios y equipos con el rendimiento de

red específico pueden requerir requisitos que diferencian los niveles de servicio. Con QoS basada en directivas, los administradores de TI pueden configurar y aplicar directivas de QoS que no se puede configurar en los conmutadores y enrutadores

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B6. Monitorear y Evaluar el Control Interno

Establecer un programa de control interno efectivo para TI requiere un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las autoevaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B6.1. Seguimiento del Marco de Control Interno

Seguimiento de forma continua, comparar y mejorar el ambiente de control de TI y el marco de trabajo de control de TI para satisfacer los objetivos organizacionales

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B6.2. Revisión de Supervisión

Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento, optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B6.3. Excepciones de Control

Identificar las excepciones de control, y analizar e identificar sus causas raíz subyacentes. Escalar las excepciones de control y reportar a los interesados apropiadamente. Establecer acciones correctivas necesarias

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B6.4. Control de Autoevaluación

Evaluar la completitud y efectividad de los controles de gerencia sobre los procesos, políticas y contratos de TI por medio de un programa continuo de autoevaluación

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B6.5. Acción Correctiva

Identificar, iniciar, rastrear e implementar acciones correctivas derivadas de los controles de evaluación y los informes

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B7. Garantizar el cumplimiento de los requisitos externos

Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento, optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B7.1. Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales

Identificar, sobre una base continua, leyes locales e internacionales, regulaciones, y otros requerimientos externos que se deben de cumplir para incorporar en las políticas, estándares, procedimientos y metodologías de TI de la organización

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B7.2. Optimización de la respuesta a los requerimientos externos

Revisar y ajustar las políticas, estándares, procedimientos y metodologías de TI para garantizar que los requisitos legales, regulatorios y contractuales son direccionados y comunicados

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B7.3. Evaluación del cumplimiento de los requisitos externos

Confirmar el cumplimiento de políticas, estándares, procedimientos y metodologías de TI con requerimientos legales y regulatorios

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B7.4. Aseguramiento Positivo del Cumplimiento

Obtener y reportar garantía de cumplimiento y adhesión a todas las políticas internas derivadas de directivas internas o requerimientos legales externos, regulatorios o contractuales, confirmando que se ha tomado cualquier acción correctiva para resolver cualquier brecha de cumplimiento por el dueño responsable del proceso de forma oportuna

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B8. Proporcionar Gobierno de TI

El establecimiento de un marco de trabajo de gobierno efectivo incluye la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales para garantizar así que las inversiones empresariales en TI estén alineadas y de acuerdo con las estrategias y objetivos empresariales

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B8.1. Establecimiento de un Marco de Gobierno de TI

Definir, establecer y alinear el marco de gobierno de TI con la visión completa del entorno de control y Gobierno Corporativo. Basar el marco de trabajo en un adecuado proceso de TI y modelo de control y proporcionar la rendición de cuentas y prácticas inequívocas para evitar una rotura en el control interno y la revisión. Confirmar que el marco de gobierno de TI asegura el cumplimiento con las leyes y regulaciones y que esta alineado, y confirma la entrega de, la estrategia y objetivos empresariales. Informa del estado y cuestiones de gobierno de TI

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B8.2. Entrega de valor

Administrar los programas de inversión habilitados con TI, así como otros activos y servicios de TI, para asegurar que ofrezcan el mayor valor posible para apoyar la estrategia y los objetivos empresariales. Asegurarse de que los resultados de negocio esperados de las inversiones habilitadas por TI y el alcance completo del esfuerzo requerido para lograr esos resultados esté bien entendido, que se generen casos de negocio integrales y consistentes, y que los aprueben los interesados, que los activos y las inversiones se administren a lo largo del ciclo de vida económico, y que se lleve a cabo una administración activa del logro de los beneficios, tales como la

contribución a nuevos servicios, ganancias de eficiencia y un mejor grado de reacción a los requerimientos de los clientes. Implementar un enfoque disciplinado de la administración del portafolio, programa y proyecto, enfatizando que el negocio asume la propiedad de todas las inversiones habilitadas con TI y que TI garantiza la optimización de los costos por la prestación de los servicios y capacidades de TI

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B9. Evaluar QoS Rentable

Evaluación de QoS rentable, mejora continua y disposición para cambios futuros

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B9.1. Evaluar QoS en base a la medición de parámetros según estándares de calidad

Evaluación de los flujos VoIP respecto a: retardo de extremo a extremo, retraso jitter y pérdida de paquetes

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B10. Monitorear Plan de Cultura de Seguridad

Monitorear el plan de Cultura de seguridad, el control se realiza sobre el plan y satisfacción de beneficios, costos y riesgos asociados, se logra mediante estrategias de evaluación y monitoreo del plan de seguridad

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B10.1. Administración de Supervisión de implementaciones y operaciones del servidor VoIP

Las implementaciones del servidor VoIP siguen el sistema de gestión de proyectos de la empresa, y cuando sea posible, la gestión y el ciclo de vida de desarrollo de los sistemas del proyecto

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B10.2. Preparar una muestra de las implementaciones de servidores VoIP recientes

Mejoras o nuevas implementaciones. Determinar si los servidores o redes VoIP específicas están bajo consideración para su inclusión en el ámbito de aplicación de la auditoría

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B10.3. Seleccionar implementaciones del servidor VoIP de alto riesgo o de alto perfil

Documentar las implementaciones VoIP y su configuración de seguridad

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B10.4. Obtener la documentación del proyecto

Revisar la documentación de configuración de seguridad actual, así como el control funcional y administrativo pertinente, para determinar si se han abordado temas previamente identificados

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B10.5. Determinar si el seguimiento del proyecto de servidor VoIP estaba / está en alineación con las normas de la empresa

Determinación de implementaciones y aplicaciones del servidor de VoIP objeto de seguimiento y presentación de informes periódicos, sobre la base de la criticidad y sensibilidad de los datos

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B10.6. Determinar si las operaciones del servidor de VoIP son monitoreadas de manera compatible con otros procesos operativos

Determinación del cumplimiento de los requisitos de supervisión de gestión y procesos operativos

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B10.7. Emisión del Monitoreo del Plan de seguridad

Las implementaciones y operaciones de servidor VoIP están sujetos a emitir el seguimiento y la escalada de los administradores apropiados en las unidades de TI y de negocios respecto al plan de seguridad

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B10.8. Evaluar la función de supervisión para la eficacia, integridad y escaladas apropiadas y oportunas

Emisión de informe de cumplimiento de eficacia, integridad y escaladas apropiadas y oportunas

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

Comentarios y Sugerencias

Anexo E. Guías de auditoría VoIPSAM

Guía de Auditoría GA-1. PLANIFICACIÓN Y ALCANCE DE LA AUDITORÍA

Guía de Auditoría VoIPSAM		**Guía de Auditoría**
1. PLANIFICACIÓN Y ALCANCE DE LA AUDITORÍA		
Objetivo:	Definir los objetivos de la auditoría de seguridad. Los objetivos de auditoría de seguridad son de alto nivel y describen los objetivos generales de auditoría	**GA-1**

No.	1. PLANIFICACIÓN Y ALCANCE DE LA AUDITORÍA Procedimiento de control	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
1.1	**Definir los objetivos de la auditoría de seguridad. Los objetivos de auditoría de seguridad son de alto nivel y describen los objetivos generales de auditoría**				
1.1.1	Revisar los objetivos de la auditoría de seguridad en el apartado "Objetivos y Alcance"				
1.2	**Definir el éxito de la tarea de auditoría. Los factores de éxito deben ser identificados. La comunicación entre el equipo de auditoría de seguridad de TI, otros equipos de aseguramiento y la empresa es esencial**				
1.2.1	Identificar los controladores (drivers) para una revisión exitosa. (estándares y procedimientos de la función de aseguramiento)				
1.2.2	Comunicar los atributos de éxito al propietario del proceso o parte interesada y obtener su consentimiento				
1.3	**Definir los límites de la revisión. La revisión debe tener un alcance definido. Comprenda las funciones y los requisitos de la aplicación para los servidores VoIP dentro del alcance**				
1.3.1	Obtener una lista de servidores VoIP y para cada uno, el correspondiente fabricante, proveedor y las versiones del software				
1.3.2	Identificar los criterios para seleccionar los servidores de VoIP para inclusión o exclusión en la revisión actual de la auditoría				

No.	1. PLANIFICACIÓN Y ALCANCE DE LA AUDITORÍA Procedimiento de control	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
1.4	**Identificar y documentar el riesgo de la auditoría. La evaluación de riesgos es necesaria para evaluar dónde deben enfocarse los recursos de auditoría. En la mayoría de las empresas, los recursos de auditoría no están disponibles para todos los procesos. El enfoque basado en el riesgo asegura la utilización de los recursos de auditoría de la manera más efectiva**				
1.4.1	Identificar el riesgo comercial asociado con el uso de VoIP bajo la consideración para la revisión de la auditoría				
1.4.2	Con base en la evaluación de riesgos, evaluar el factor de riesgo de auditoría general para realizar la revisión de auditoría				
1.4.3	Sobre la base de la evaluación de riesgos, identificar los cambios en el alcance				
1.4.4	Determinar el riesgo con la administración de TI y ajustar la evaluación de riesgos				
1.4.5	Sobre la base de la evaluación de riesgos, revisar el alcance				
1.5	**Definir el proceso de cambio de auditoría. El enfoque de auditoría inicial se basa en la comprensión del revisor del entorno operativo y el riesgo asociado. A medida que se realicen más investigaciones y análisis, se pueden producir cambios en el alcance y enfoque**				
1.5.1	Identificar la seguridad de TI y los recursos empresariales responsables de la revisión				
1.5.2	Establecer el proceso para sugerir e implementar cambios en el programa de auditoría de seguridad y las autorizaciones requeridas				
1.6	**Definir los recursos de auditoría de seguridad requeridos**				
1.6.1	Determinar las habilidades de auditoría de seguridad necesarias para la revisión				
1.6.2	Estimar los recursos totales para garantía de la auditoría (horas) y el plazo (fechas de inicio y finalización) necesarios para la revisión				
1.7	**Definir los entregables. Los entregables no se limitan al informe final. La comunicación entre los equipos de auditoría de seguridad y el propietario del proceso es esencial para el éxito de la asignación**				
1.7.1	Determinar los entregables provisionales, incluidos los hallazgos iniciales, los informes de estado, los informes preliminares, las fechas de vencimiento de las respuestas o reuniones y el informe final				

No.	1. PLANIFICACIÓN Y ALCANCE DE LA AUDITORÍA Procedimiento de control	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
1.8	**Comunicar el proceso de auditoría de seguridad claramente al consumidor/cliente**				
1.8.1	Conducir una conferencia de apertura para discutir: - Objetivos con los grupos de interés. - Documentación relevante (por ejemplo, políticas, procesos, comunicaciones de gestión, actas de reuniones, documentación de implementación) requerida para realizar la revisión de la auditoría - Alcance, limitaciones del alcance (límites de auditoría), presupuestos, fechas de vencimiento, líneas de tiempo, hitos y entregables - Recursos de seguridad de la información disponibles requeridos para ayudar con la revisión de auditoría				
	Total (promedio porcentajes de cumplimiento)		**Total** Tiempo efectivo en minutos		

Guía de Auditoría GA-2. PASOS PREPARATORIOS

Guía de Auditoría VoIPSAM			**Guía de Auditoría**
2. PASOS PREPARATORIOS			
Objetivo:	Obtener y revisar los organigramas actuales relacionados con las comunicaciones VoIP		**GA-2**
		Papel de Trabajo: **PT-GA-2**	

No.	**2. PASOS PREPARATORIOS** **Procedimiento de control**	**% Cumplimiento**	**Nombre Auditor**	**Fecha**	**Tiempo efectivo minutos**
2.1	**Obtener y revisar los organigramas actuales relacionados con las comunicaciones VoIP**				
2.1.1	Obtener el diagrama organizacional de la alta dirección que supervisa comunicaciones VoIP				
2.1.2	Obtener el diagrama organizacional de la infraestructura TI de soporte e interfaz con VoIP				
2.1.3	Obtener el diagrama organizacional para configuración y mantenimiento del usuario VoIP				
2.2	**Obtener las descripciones de trabajo del personal responsable de la infraestructura de VoIP, configuración y administración de usuarios**				
2.3	**Determinar si se han realizado revisiones de auditorías a la infraestructura de VoIP anteriormente**				
2.3.1	Si se han realizado revisiones de auditorías anteriores, obtener los documentos de trabajo pertinentes				
2.3.1.1	Revisar la documentación de la actual configuración de seguridad, así como el control funcional y administrativo relevante, que determine si previamente se han identificado problemas abordados				
2.3.1.2	Determinar si los servidores específicos VoIP o redes bajo esta consideración se incluyen en el alcance de esta revisión de auditoría y si se incluyeron en la revisión de auditoría				
2.3.1.3	Revisar cualquier prueba de penetración y evaluación de vulnerabilidad que se haya realizado				
2.4	**Seleccionar los servidores y redes VoIP que se incluirán en la auditoría**				

No.	2. PASOS PREPARATORIOS Procedimiento de control	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
2.4.1	Obtener una lista de los servidores y redes VoIP. Los servidores de medios VoIP pueden incluir cualquiera de los siguientes: - Media gateway, para la traducción de protocolos, generalmente PSTN a/desde protocolos locales - H.323 gatekeeper, el cual proporciona traducción de direcciones (alias a dirección IP) - Firewalls y gateways de la capa de aplicación para filtrado de direcciones y seguridad - Servidor de respuesta de voz interactiva (IVR) - Señalización del servidor de medios (controlador de media gateways) para manejar el control de llamadas - Distribución automatizada de llamadas (ACD) para recibir y distribuir llamadas en un centro de contacto - Servidor de medios de Conferencia para conferencias de voz y video - Servidor texto a voz (TTS), convierte el texto de e-mail a voz - Sistema automatizado de respuesta de voz a e-mail - Servidor de aplicaciones de voz o video. - Servidor de contenido de streaming - Servidor de fax bajo demanda				
2.4.2	Determinar las unidades de negocio asociadas con cada red o servidor VoIP. Seleccione las redes para su inclusión en una muestra de la población. Incluir en la muestra redes/servidores de alto perfil, los procesos que requieren recursos intensivos (como los dedicados a la videoconferencia) o IVR				
2.5	**Obtener documentos del servidor** Para que los servidores se incluyan en el alcance, obtener los siguientes documentos de cada servidor: - Documentos del servidor: configuración, versiones de software, hardware, protocolos VoIP desplegados, etc. - Documentos de seguridad - Políticas de documentos - Lista de administradores con acceso - Diagrama de Red VoIP				
	Total (promedio porcentajes de cumplimiento)		**Total** Tiempo efectivo en minutos		

Guía de Auditoría GA-3. GOBERNANZA

Guía de Auditoría VoIPSAM		**Guía de Auditoría**
3. GOBERNANZA		
Objetivo:	Determinar que la infraestructura inicial del servidor VoIP y las aplicaciones VoIP están respaldadas por un caso de negocio documentado que describe el retorno de la inversión y otros beneficios directos e indirectos	**GA-3**
Papel de Trabajo:	**PT-GA-3**	

No.	**3. GOBERNANZA** **Procedimiento de control**	**Referencia Cobit**	**Referencia VoIPSAM**	**% Cumplimiento**	**Nombre Auditor**	**Fecha**	**Tiempo efectivo minutos**
3.1	**Caso de negocio** **Objetivo de** la infraestructura inicial del servidor VoIP y las aplicaciones VoIP están respaldadas por un caso de negocio documentado que describe el retorno de la inversión y otros beneficios directos e indirectos.	PO1 PO1.1 PO1.2 PO2.1 AI1.3 AI3.1 DS11.1	PA1 PA1.1 PA1.2 PA2.1 PB1.2 PB2.1 PC5.1				
3.1.1	**Requisitos de caso de negocio de VoIP** **Control:** Un caso de negocio para respaldar la implementación de VoIP está completamente documentado y describe los beneficios que se deben realizar						
3.1.1.1	Obtener una copia del documento del caso de negocio que respalde la implementación de VoIP en la empresa para reemplazar la tecnología anterior (analógica)						
3.1.1.2	Determinar que el documento del caso de negocio describa adecuadamente los beneficios que se obtendrán de la implementación de VoIP en lugar de la tecnología analógica y debidamente autorizada						

No.	3. GOBERNANZA Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
3.1.1.3	Determinar que después de la implementación, los beneficios proyectados se alcanzaron o superaron						
3.1.1.4	Determinar si la conversión a VoIP se incluyó en cualquier plan de TI estratégico a corto o largo plazo						
3.2	**Políticas de VoIP**						
3.2.1	**Principios rectores** **Objetivo de auditoría de seguridad:** La implementación de VoIP se adhiere a los objetivos de la empresa o principios rectores						
3.2.1.1	**Documento de principios rectores de VoIP** **Control:** Se ha establecido un documento de principios rectores que aborda cuestiones clave del diseño, la implementación y las operaciones de VoIP	PO1.4 PO6 AI1.1 AI1.4 ME4	PA1.3 PA5 PB1.1 PB1.3 PD4				
3.2.1.1.1	Determinar si existen principios rectores o documentos con nombres similares que describan los objetivos de diseño específicos para una arquitectura o infraestructura de VoIP						
3.2.1.1.2	Obtener una copia del documento de principios rectores						
3.2.1.1.3	Determinar si los principios rectores abordan las políticas generales de la empresa relacionadas con la confidencialidad y la privacidad, la integridad de los datos y la disponibilidad, así como los derechos de autor, la retención de registros y la seguridad general						

No.	3. GOBERNANZA Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
3.2.1.1.4	Con referencia a la documentación formal (actas de reuniones, informes de progreso, etc.), determinar si los principios rectores se aplicaron durante la adquisición de la tecnología y el despliegue de VoIP						
3.2.1.1.5	**Diseño del sitio:** Verificar que los principios rectores requieren de los arquitectos de VoIP: - Usar un diseño consistente - Aprobar cambios basados en necesidad demostrada - Tener un propietario designado para cada red						
3.2.1.1.6	**Documentación de arquitectura:** Verifique que la documentación sea: - Almacenada en una ubicación y un formato que evite cambios no autorizados - Se actualiza regularmente a medida que ocurren los cambios. - Es accesible al personal autorizado						
3.2.2	**Políticas y normas** **Objetivo de auditoría de seguridad:** las políticas y normas se adhieren a las políticas y normas de la empresa.						
3.2.2.1	**Políticas y estándares de VoIP** **Control:** Las políticas de VoIP se definen, documentan y distribuyen a los administradores y usuarios relevantes de VoIP	PO6.4 PO6.5	PA5.1 PA5.2				
3.2.2.1.1	Determinar si existe un documento de políticas y estándares de VoIP						
3.2.2.1.2	Obtener el documento de políticas y estándares de VoIP y revisarlo como se indica en los siguientes pasos						

No.	3. GOBERNANZA Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
3.2.2.1.3	Determinar que las políticas y estándares de VoIP se revisen al menos anualmente y se actualicen según sea necesario						
3.2.2.1.4	Revisar el documento de políticas y estándares de VoIP y revisarlo como se indica en los siguientes pasos						
3.2.2.1.4.1	Los estándares de arquitectura incluyen los puntos indicados en los siguientes pasos						
3.2.2.1.4.1.1	Todos los teléfonos VoIP deben estar en una LAN virtual (VLAN) separada de cualquier VLAN de datos y deben usar direcciones no enrutables RFC 1918						
3.2.2.1.4.1.2	Las LAN y las VLAN de voz deben estar desconectadas del firewall desde cualquier VLAN/LAN de datos						
3.2.2.1.4.1.3	Se requieren mecanismos apropiados, como las listas de control de acceso (ACL), para evitar cualquier comunicación a través de VLANs						
3.2.2.1.4.1.4	Revisar las ACL para asegurar que proporcionan el aislamiento adecuado entre la VLAN de VoIP y otras VLAN de datos						
3.2.2.1.4.1.5	Las conexiones de los componentes de VoIP a internet están expresamente prohibidas						
3.2.2.1.4.1.6	En el caso de cualquier excepción a la política anterior, determine que el riesgo ha sido documentado y que se han implementado las medidas adecuadas (por ejemplo, firewalls adicionales compatibles con VoIP)						

No.	3. GOBERNANZA Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
3.2.2.1.4.1.7	Si a los teletrabajadores se les permite acceder a la PBX VoIP a través de internet, deben ingresar mediante un túnel VPN cifrado con una fuerte autenticación de usuario						
3.2.2.1.4.1.8	Se implementa un sistema de detección de intrusos (IDS) o un sistema de prevención de intrusos (IPS) para protección contra ataques externos de denegación de servicio (DoS)						
3.2.2.1.4.1.9	Los teléfonos habilitados para VoIP deben autenticarse cuando se conectan a la PBX mediante un proceso de desafío-respuesta						
3.2.2.1.4.1.10	En un entorno de alta seguridad, los teléfonos VoIP deben estar encriptados para evitar los ataques internos (por ejemplo, cuando una PC deshonesta está conectada a una red VoIP para interceptar paquetes de voz)						
3.2.2.1.4.1.11	Si se implementa el cifrado, se debe aplicar a/desde todos los teléfonos y entre el gateway y la PSTN externa						
3.2.2.1.4.1.12	Si se implementa el cifrado, se requiere un algoritmo de cifrado estándar de la industria como AES o 3DES. No se deben utilizar algoritmos patentados, suministrados por el vendedor o de otro tipo, debido a su efectividad desconocida						
3.2.2.1.4.1.13	Si se implementa conectividad inalámbrica (es decir, hacia/desde teléfonos celulares), se utiliza un protocolo de cifrado fuerte, como WPA2, no WEP u otro cifrado débil						

No.	3. GOBERNANZA Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
3.2.2.1.4.1.14	En un entorno regulado, Skype no está permitido debido a la facilidad de suplantación del usuario y la falta de protección HTTPS (cifrado)						
3.2.2.1.4.1.15	Cuando sea factible, la opción de enlace de MAC debe implementarse para garantizar que no se conecten dispositivos no autorizados a la VLAN de VoIP						
3.2.2.1.4.2	**Operaciones**						
3.2.2.1.4.2.1	Verificar que todas las contraseñas administrativas relacionadas con VoIP (y las claves de cifrado/descifrado, cuando corresponda) se hayan cambiado con respecto a los valores predeterminados del fabricante						
3.2.2.1.4.2.2	Verificar que las contraseñas administrativas y las claves de cifrado/descifrado sean conocidas solo por una lista restringida de personal de confianza						
3.2.2.1.4.2.3	Determinar que las copias de emergencia de todas las contraseñas administrativas y las claves de cifrado/descifrado se guardan en un lugar seguro con acceso restringido						
3.2.2.1.4.2.4	Determinar que las políticas y estándares de VoIP se revisen al menos anualmente y se actualizan según sea necesario						
3.2.2.1.4.3	**Contenido VoIP**						

No.	3. GOBERNANZA Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
3.2.2.1.4.3.1	El contenido de los mensajes instantáneos (IM) y chat están sujetos a revisión de acuerdo con la clasificación de datos empresariales y las políticas de uso aceptable						
3.2.2.1.4.3.2	Los datos de mensajería instantánea y de chat se conservan de acuerdo con las políticas de retención empresarial, con disposiciones para una política más estricta basada en la clasificación de los datos, el contenido de los datos o el grupo de usuarios (por ejemplo, los ejecutivos de C-suite)						
3.2.2.1.4.4	**Políticas de implementación**						
3.2.2.1.4.4.1	Las implementaciones de VoIP siguen un framework de proyecto prescrito, por ejemplo, la Biblioteca de infraestructura de TI (ITIL)						
3.2.2.1.4.4.2	Si se trata de una nueva implementación de VoIP o una actualización reciente de una versión anterior de VoIP, se seguirán las buenas prácticas documentadas del estándar de la industria						
3.2.2.1.4.4.3	El proceso de implementación incluye requisitos formales de seguridad y control, que incluyen arquitectura segura, seguridad de red, parches, definición de incidentes y desencadenadores de incidentes, cumplimiento, descubrimiento electrónico y cifrado						

No.	3. GOBERNANZA Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
3.2.2.1.4.4.4	Los requisitos de seguridad se definen de acuerdo con las políticas de seguridad de la empresa, la separación de tareas, las políticas de aprobación, el cumplimiento, la recuperación de desastres, la gestión de incidentes, etc.						
3.2.2.1.4.4.5	El proceso de implementación incluye métricas de rendimiento adecuadas para cuantificar el hardware necesario, en el presente y en el futuro						
3.2.2.1.4.4.6	El personal de operaciones de VoIP lleva a cabo una planificación adecuada y regular para determinar la capacidad de procesamiento futura prevista para satisfacer las necesidades comerciales esperadas						
3.2.2.1.4.5	**Políticas de la unidad organizativa específica**						
3.2.2.1.4.5.1	Las unidades organizativas específicas pueden alterar las políticas para exigir normas de seguridad y diseño más estrictas. Las políticas más flexibles que no cumplen con las normas y pautas de clasificación de datos deben ser aprobadas por la administración de seguridad de la información y el propietario de los datos de negocios						
3.2.2.1.4.5.2	Obtener evidencia documental de cualquier aprobación (s) reciente (s)						
3.2.2.1.4.6	**Políticas de auditoría**						
3.2.2.1.4.6.1	Las políticas de auditoría están alineadas con las políticas de auditoría empresarial basadas en la clasificación de datos						

No.	3. GOBERNANZA Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
3.2.2.1.4.6.2	Las políticas de auditoría incluyen la supervisión del acceso a los servidores de VoIP por parte de los administradores y otros usuarios privilegiados						
3.2.3	**Funciones y responsabilidades** Objetivo de auditoría de seguridad: las políticas y los estándares abordan los roles y las responsabilidades para implementar y mantener las instalaciones del servidor VoIP, incluida la pila de tecnología subyacente que admite el servidor VoIP						
3.2.3.1	**Descripción de roles y responsabilidades** Control: Un documento de políticas y roles del servidor VoIP describe las responsabilidades específicas de las funciones clave del trabajo	PO4.6 PO7	PA3.1 PA6				
3.2.3.1.1	Determine si existe un documento de funciones y responsabilidades del servidor VoIP						
3.2.3.1.2	Si existe un documento de roles y responsabilidades del servidor VoIP, evalúe la idoneidad de las descripciones para los siguientes roles: - Patrocinador ejecutivo (solicitudes) - Junta de gobierno o comité de dirección (a las solicitudes) - Administrador de tecnología - Equipo de soporte tecnológico - Administrador de VoIP - Arquitecto de redes - Administrador de la unidad organizativa						

No.	3. GOBERNANZA Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
3.2.3.1.3	Revise los roles con las siguientes responsabilidades para asegurarse de que estas responsabilidades se asignen a una función laboral y a personas específicas: - Gestión de la infraestructura técnica, incluidos servidores, redes, gestión de bases de datos, gestión de buzones, etc. - Gestión de la infraestructura del servidor VoIP. - Gestión de aplicaciones - Controles de acceso, es decir, provisioning del usuario. - Evaluación del desempeño - Continuidad del negocio y recuperación ante desastres						
3.3	**Vigilancia**						
3.3.1	**Vigilancia** **Objetivo de auditoría de seguridad:** Las implementaciones y aplicaciones del servidor VoIP están sujetas a un monitoreo y reporte regular, basado en la crítica y sensibilidad de los datos, y el cumplimiento de los requisitos de supervisión de la administración						
3.3.1.1	**Supervisión de la administración de las implementaciones y operaciones del servidor VoIP** **Control:** las implementaciones del servidor VoIP siguen el sistema de gestión de proyectos empresariales y, en su caso, el ciclo de vida de la gestión de proyectos						

No.	3. GOBERNANZA Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
3.3.1.1.1	Preparar una muestra de implementaciones recientes del servidor VoIP (actualizaciones o nuevas implementaciones)						
3.3.1.1.2	Seleccionar implementaciones de servidores VoIP de alto riesgo o de alto perfil						
3.3.1.1.3	Obtener documentación del proyecto del servidor VoIP						
3.3.1.1.4	Determinar si el monitoreo del servidor de VoIP está alineado con los estándares de la empresa						
3.3.1.1.5	Determinar si las operaciones del servidor VoIP se monitorean de manera consistente con otros procesos operativos						
3.3.1.2	**Monitoreo de problemas** **Control:** La implementación y las operaciones del servidor VoIP están sujetas al monitoreo y escalamiento de problemas para los gerentes apropiados en las unidades de negocios y TI	PO10 DS8 ME1 ME2 ME4	PA7 PC3 PD1 PD2 PD4				
3.3.1.2.1	Obtener informes de seguimiento de problemas						
3.3.1.2.2	Evaluar la función de monitoreo de problemas para verificar su efectividad, integridad y escalamiento adecuado y oportuno						
		Total (promedio porcentajes de cumplimiento)			**Total** Tiempo efectivo en minutos		

Guía de Auditoría GA-4. CONFIGURACIÓN DE SERVIDORES

Guía de Auditoría VoIPSAM		**Guía de Auditoría**
4. CONFIGURACIÓN DE SERVIDORES		
Objetivo:	Determinar si los servidores VoIP que se ejecutan en un entorno virtualizado están completamente separados de otros servidores que se ejecutan en el mismo hardware físico	**GA-4**
Papel de Trabajo:	**PT-GA-4**	

No.	**4. CONFIGURACIÓN DE SERVIDORES** **Procedimiento de control**	**Referencia Cobit**	**Referencia VoIPSAM**	**% Cumplimiento**	**Nombre Auditor**	**Fecha**	**Tiempo efectivo minutos**
4.1	**Virtualización** **Objetivo de auditoría de seguridad:** los servidores VoIP que se ejecutan en un entorno virtualizado están completamente separados de otros servidores que se ejecutan en el mismo hardware físico.						
4.1.1	**Segregación de virtualización** **Control:** los servidores de VoIP están separados de otros servidores en el grupo de virtualización.	PO2.1 DS5.1 DS9	PA2.1 PC2.1 PC4				
4.1.1.1	Obtener las especificaciones de virtualización del servidor y la documentación de la arquitectura.						
4.1.1.2	Determinar que los controles dentro de la configuración de virtualización aseguren una separación completa de los procesos del servidor VoIP y los derechos de acceso de otros entornos.						
4.1.1.3	Si se ha realizado una auditoría de virtualización, revisar los hallazgos y el monitoreo de problemas para identificar controles y planes de remediación.						
4.1.1.4	Si no se ha realizado una auditoría de virtualización reciente y los servidores de VoIP operan en un entorno virtualizado, considerar posponer la auditoría del servidor de VoIP hasta que se pueda realizar una auditoría de virtualización.						

No.	4. CONFIGURACIÓN DE SERVIDORES Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
4.2	**Fortalecimiento del sistema operativo** **Objetivo de auditoría de seguridad:** los sistemas operativos de los servidores host se fortalecen de acuerdo con las mejores prácticas						
4.2.1	Los sistemas operativos están configurados para el control de seguridad: los sistemas operativos están configurados para la máxima seguridad.	DS9	PC4				
4.2.1.1	Establecer si una auditoría reciente del sistema operativo se completó para el sistema operativo relevante. - Si es así, obtener una copia del informe y asegurarse que todos los problemas hayan sido remediados adecuadamente. - De lo contrario, considerar realizar una auditoría de la seguridad del sistema operativo subyacente y los controles						
4.2.1.2	Revisar si la organización tiene alguna línea de base de configuración de sistema operativo para servidores VoIP.						
4.2.1.3	Verificar que los servidores VoIP (virtuales y reales) estén dedicados únicamente a los procesos VoIP.						
4.2.1.4	Verificar que los servicios no esenciales no estén funcionando en los servidores.						
4.2.1.5	Verificar que solo los puertos necesarios para VoIP estén abiertos en el servidor de firewall.						

No.	4. CONFIGURACIÓN DE SERVIDORES Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
4.2.1.6	Verificar que los firewalls que protegen las VLAN y los servidores de VoIP estén configurados para evitar los escenarios de ataque de VoIP más comunes. La siguiente es una lista no exhaustiva de tales ataques: - DoS y ataques de denegación de servicio distribuido (DDoS) - Ataque de modificación de QoS - Inyección de paquetes VoIP - DoS en contra de servicios suplementarios (por ejemplo, protocolo de configuración dinámica de host) [DHCP] o sistema de nombres de dominio [DNS]) - DoS inalámbrico - Paquete de la muerte (Packet of Death) DoS: esencialmente una inundación aleatoria de paquetes del Protocolo de Control de Transmisión (TCP), UDP, o Protocolo de Mensajes de Control de Internet (ICMP) diseñados para bloquear servidores de VoIP - IP Phone Flood DoS: se envía un gran volumen de datos de llamadas a un único punto final de VoIP en un intento de agotar su unidad central de procesamiento (CPU), ancho de banda, sesiones TCP, etc. - Envenenamiento de DNS (DNS Poisoning) - Fraude de llamadas (Toll Fraud): uso de los servidores de VoIP para realizar llamadas no autorizadas a través de la PSTN						
4.3	**Políticas específicas de VoIP**						
4.3.1	**Las configuraciones de seguridad se establecen utilizando políticas.** **Objetivo de auditoría de seguridad:** las configuraciones de seguridad para los usuarios se establecen y aplican a través de políticas asignadas a las unidades organizativas y la raíz del directorio.						

No.	4. CONFIGURACIÓN DE SERVIDORES Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
4.3.1.1	**La configuración de las políticas de seguridad se establece mediante documentos de política.** **Control:** Las políticas de seguridad se establecen para los usuarios que utilizan el documento de políticas y se asigna a la unidad organizativa y, cuando sea necesario, a un individuo.	PO2.3 DS5.3 DS5.4 DS9	PA2.2 PC2.4 PC2.5 PC4				
4.3.1.1.1	Obtener el documento de políticas para cada servidor a su alcance						
4.3.1.1.2	Determinar si se han establecido políticas dentro de la jerarquía de directorios						
4.3.1.1.3	Determinar si las políticas asignadas explícitamente no crean una exposición para el acceso no autorizado						
4.3.2	**Políticas de contraseña** **Objetivo de auditoría de seguridad:** Las políticas de contraseña protegen adecuadamente a los usuarios y la privacidad de los correos electrónicos y las aplicaciones	DS5.3 DS5.4 DS9	PC2.4 PC2.5 PC4				
4.3.2.1	**Las políticas de contraseñas protegen la identidad y el acceso a correos electrónicos** **Control:** Las políticas de contraseña de VoIP / número de identificación personal (PIN) están alineadas con las políticas y prácticas de gestión de identidad empresarial						
4.3.2.1.1	Determinar que todos los usuarios deban configurar una contraseña privada para acceder a sus correos de voz						
4.3.2.1.2	Para una muestra de teléfonos VoIP, determinar que no se puede acceder al correo de voz sin una contraseña / PIN y que las contraseñas / PIN predeterminadas (por ejemplo, 0000, 1234) se han cambiado						
4.3.2.1.3	Verificar que las reglas básicas de firewall bloqueen cualquier acceso de los usuarios regulares (datos) a la VLAN VoIP desde sus estaciones de trabajo						

No.	4. CONFIGURACIÓN DE SERVIDORES Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
4.3.2.2	**Las políticas de contraseña / PIN protegen la configuración del teléfono VoIP** **Control:** Se requiere un PIN para acceder a la información de configuración en cada auricular/teléfono VoIP individual	DS5.3 DS5.4 DS9	PC2.4 PC2.5 PC4				
4.3.2.2.1	Determinar que se asigne un PIN de 4 dígitos o más a cada auricular/teléfono VoIP para acceder al menú de configuración del dispositivo						
4.3.3	**Controles de acceso a la aplicación** **Objetivo de auditoría de seguridad:** las aplicaciones (por ejemplo, centro de llamadas, autoservicio del cliente) que utilizan la infraestructura VoIP tienen una seguridad de acceso adecuada para alinearse con la clasificación de datos y las políticas de cuentas de usuario						
4.3.3.1	**Mantenimiento de Control de Acceso** **Control:** Los controles de acceso se mantienen para los procedimientos de aprovisionamiento, desaprovisionamiento y transferencia	DS5.3 DS5.4	PC2.4 PC2.5				
4.3.3.1.1	Obtener los procedimientos de aprovisionamiento, transferencia y terminación						
4.3.3.1.2	Evaluar los procedimientos para la efectividad del diseño						
4.3.3.1.3	Seleccionar una muestra de usuarios nuevos, usuarios terminados y transferidos. Verificar que el control de acceso a un conjunto de usuarios de muestra cumpla con los procedimientos de mantenimiento de control de acceso						
4.3.4	**Controles de seguridad física** **Objetivo de auditoría de seguridad:** Los servidores PBX de VoIP tienen una protección física adecuada contra la manipulación no autorizada						

No.	4. CONFIGURACIÓN DE SERVIDORES Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
4.3.4.1	**El acceso físico al hardware de la VLAN está restringido** **Control:** El acceso a dispositivos sensibles, como los conmutadores VLAN, está restringido a un pequeño número de personas confiables con una estricta "necesidad de saber"						
4.3.4.1.1	Seleccionar una muestra de conmutadores VLAN y otro hardware y determinar que todos se encuentran en gabinetes o salas con llave, a los que el acceso está limitado a un pequeño número de ingenieros de confianza						
4.3.4.1.2	Determinar que los controles de acceso electrónico sean apropiados, como lectores de tarjetas magnéticas, lectores de tarjetas inteligentes, escáneres biométricos (huella digital, geometría de la mano, iris, geometría facial, etc.), estén en su lugar para restringir dicho acceso						
4.3.5	**Los detalles del sistema VoIP implementado están restringidos** **Objetivo de auditoría de seguridad:** La información sobre el hardware y software VoIP implementados está restringida solo para uso interno						
4.3.5.1	**Limitaciones en la implementación de VoIP** **Control:** Los detalles específicos sobre el hardware y software VoIP implementados (como fabricante, proveedor, modelo, número de versión, etc.) están restringidos a los empleados internos en una base de "necesidad de saber"						
4.3.5.1.1	Determinar que la información confidencial anterior (que podría ser utilizada por los intrusos para planificar ataques en las redes VoIP) NO se muestra en sitios web externos o internos abiertos						

No.	4. CONFIGURACIÓN DE SERVIDORES Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
4.3.5.1.2	Determinar que el acceso a la documentación técnica relevante para las redes VoIP implementadas está restringido a un pequeño grupo de personas confiables, en función de la "necesidad de saber"						
4.3.5.1.3	Determinar que toda esa información se clasifica como "Confidencial, sólo para uso interno" o similar						
4.4	**Configuración del servidor VoIP**						
4.4.1	**Acceso de Administradores** **Objetivo de auditoría de seguridad:** los administradores tienen limitaciones en su capacidad para acceder y modificar las configuraciones del servidor						
4.4.1.1	**El acceso del administrador está definido** **Control:** Los administradores de VoIP están definidos y documentados por nivel de acceso	DS5.3	PC2.4				
4.4.1.1.1	Obtener las asignaciones de acceso de administrador						
4.4.1.1.2	Determinar que los derechos de acceso del administrador se han creado de una manera coherente con las políticas de seguridad de la empresa						
4.4.1.1.3	Determinar que las asignaciones de acceso definen los siguientes derechos de acceso de administrador de VoIP: - Administradores de acceso completo - Administradores (servidor específico) - Administradores de bases de datos - Administradores remotos de PBX - Administradores de solo lectura - Administrador de sistema						
4.4.1.2	**Los usuarios no autorizados no pueden asumir privilegios de administrador** **Control:** solo los administradores tienen acceso a las funciones de administrador privilegiado	DS9	PC4				

No.	4. CONFIGURACIÓN DE SERVIDORES Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
4.4.1.2.1	Obtener acceso e identificar perfiles, y verificar que solo los administradores autorizados teng an acceso al servidor VoIP y a las funciones de administración						
4.4.1.2.2	Determinar que, si se usan grupos, los miembros de los grupos administrativos de VoIP son apropiados según el título del trabajo						
4.4.1.2.3	Determinar si los usuarios o miembros de grupos asociados con las funciones de administrador ya no deberían tener acceso debido a la terminación, transferencia de trabajo o redefinición de trabajo						
4.4.2	**Gestión de certificados digitales** **Objetivo de auditoría de seguridad:** Los certificados digitales X.509 utilizados para impulsar la autenticación del servidor con SSL/TLS, se gestionan adecuadamente y protegen las claves privadas correspondientes						
4.4.2.1	**Los certificados digitales SSL/TLS se monitorean y administran adecuadamente** **Control:** Se mantiene y actualiza un registro electrónico o digital de todos los certificados digitales X.509 implementados (identidades digitales)	DS5.7 DS5.8	PC2.6 PC2.7				
4.4.2.1.1	Determine que se mantiene un registro o índice de seguimiento adecuado de todos los certificados digitales implementados, mostrando al menos la siguiente información: - ID de certificado, proveedor - Fecha de caducidad - Fecha de revocación (si corresponde) - Clave privada (una larga cadena de dígitos hexadecimales) - ID del servidor relevante Contraseña para desbloquear el certificado en el almacén de certificados del sistema operativo						

No.	4. CONFIGURACIÓN DE SERVIDORES Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
4.4.2.1.2	Determinar que el acceso al registro o índice anterior está restringido a una pequeña lista de confianza, personal superior						
4.4.3	**Acceso al servidor** **Objetivo de auditoría de seguridad:** El acceso al servidor es limitado según sea necesario para realizar la función de trabajo						
4.4.3.1	**Restricciones de acceso al servidor** **Control:** El acceso a los servidores VoIP está definido por la función del trabajo	DS5.4	PC2.5				
4.4.3.1.1	Determinar si el acceso al servidor VoIP está definido por la función de trabajo						
4.4.3.1.2	Para el conjunto de muestra de servidores VoIP, determinar quién puede acceder a los servidores revisando la documentación relevante						
4.4.3.1.3	Evaluar si estas configuraciones de acceso son apropiadas y coherentes con la política de seguridad empresarial						
4.4.4	**Limitar el acceso a los puertos a los servidores VoIP** **Objetivo de auditoría de seguridad:** La configuración de red está configurada para proporcionar la máxima seguridad						
4.4.4.1	**VoIP está configurado para acceso externo seguro** **Control:** El acceso a VoIP requiere un túnel VPN encriptado	DS5.7 DS5.8	PC2.6 PC2.7				
4.4.4.1.1	Utilizando la muestra de documentos del servidor VoIP, determinar lo siguiente: - Se requiere un túnel VPN encriptado o SSL/TLS para obtener acceso a cualquier servidor VoIP en uso - Solo se permite el cifrado estándar de la industria (AES o 3DES) Se requiere una autenticación fuerte para todos los usuarios externos						
4.5	**Configuración de mensajería VoIP**						

No.	4. CONFIGURACIÓN DE SERVIDORES Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
4.5.1	**El acceso a İnternet está altamente restringido** **Objetivo de auditoría de seguridad:** el acceso desde y hacia İnternet está restringido a los administradores						
4.5.1.1	**El acceso a internet desde cualquier dispositivo VoIP está prohibido** **Control:** No se permite que las estaciones de trabajo con acceso a internet se conecten a ninguna VLAN de voz	DS9	PC4				
4.5.1.1.1	Revisar la documentación de la arquitectura VoIP para determinar si alguna estación de trabajo (PC, computadora portátil, bloc de notas, netbook o tableta) puede acceder a la red de datos						
4.5.1.1.2	Desde una estación de trabajo interna, intentar la conexión a la dirección IP de uno o más servidores VoIP. (Esto no debería tener éxito en todos los casos)						
4.5.1.2	Determinar si se requiere antivirus y otro software de protección antimalware para proteger los servidores VoIP						
4.5.1.3	Para cada servidor, determinar que los paquetes de software requeridos por proveedor y nivel de versión/revisión están instalados, actualizados y monitoreados						
4.6	**Cumplimiento de mensajería** **Objetivo de auditoría de seguridad:** VoIP está configurado adecuadamente para cumplir con los requisitos internos relevantes de regulación, legales, industriales y empresariales						
4.6.1	**La retención de mensajes es apropiada para las necesidades de la empresa** **Control:** Los mensajes de texto (mensajería instantánea y chat) se conservan durante el período de tiempo adecuado para cumplir con el requisito más restrictivo	DS11.2	PC5.2				

No.	4. CONFIGURACIÓN DE SERVIDORES Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
4.6.1.1	Verificar que la política empresarial escrita defina específica y claramente el período de retención para todos los mensajes electrónicos y que este período de tiempo sea igual o superior al del requisito de cumplimiento relevante más restrictivo						
4.6.1.2	Verificar que la administración de operaciones del servidor VoIP tenga plena conciencia de las políticas de retención de mensajes y descubrimiento electrónico						
4.6.1.3	Considerar asesoramiento legal sobre si las políticas de retención también se aplican al contenido de video						
4.6.2	**Las políticas están en lugar para efectuar una retención legal** **Control:** Una política de retención legal está documentada, actualizada y transmitida a la administración de operaciones del servidor VoIP						
4.6.2.1	Obtener una copia de la política de retención legal y determinar si ha sido comunicada y entendida por la administración de operaciones del servidor VoIP						
4.6.2.2	Mediante consultas y observaciones, determinar si la administración de operaciones del servidor VoIP tiene las herramientas y la experiencia necesarias para realizar búsquedas de descubrimiento electrónico en varios buzones de texto						
4.7	**Auditoría y registro** **Objetivo de auditoría de seguridad:** El servidor VoIP está configurado para registrar el acceso a las funciones críticas del proceso						
4.7.1	**La auditoría está habilitada** **Control:** El registro del servidor VoIP se mantiene y revisa, ya sea registros del sistema operativo o registros del servidor VoIP o ambos	DS9	PC4				

No.	4. CONFIGURACIÓN DE SERVIDORES Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
4.7.1.1	Determinar si se ha establecido una política de auditoría para requerir el registro de los procesos administrativos						
4.7.1.2	Si existe una política, determine si se ha habilitado para todos los sitios del servidor VoIP						
4.7.1.3	Determinar si los informes sobre la revisión de registros son creados y revisados por un gerente						
4.7.1.4	Evaluar quién tiene acceso de edición a los registros de VoIP						
		Total (promedio porcentajes de cumplimiento)			**Total** Tiempo efectivo en minutos		

Guía de Auditoría GA-5 RED

Guía de Auditoría VoIPSAM		**Guía de Auditoría**
5. RED		
Objetivo:	Determinar el estado de la red utilizada por el entorno del servidor VoIP para verificar el nivel de protección contra el acceso no autorizado e intrusiones	**GA-5**
Papel de Trabajo:	**PT-GA-5**	

No.	**5. RED** **Procedimiento de control**	**Referencia Cobit**	**Referencia VoIPSAM**	**% Cumplimiento**	**Nombre Auditor**	**Fecha**	**Tiempo efectivo minutos**
5.1	**Diseño de red** **Objetivo de auditoría de seguridad:** La red utilizada por el entorno del servidor VoIP está protegida contra el acceso no autorizado y se minimizan las oportunidades de intrusión						
5.1.1	**Ubicación de la red del servidor** **Control:** Los servidores que alojan el servidor VoIP se encuentran en una subred y una VLAN adecuadamente protegidas	DS5.10	PC2.6				
5.1.1.1	Obtener un esquema de red para los servidores VoIP dentro del alcance de la auditoría						
5.1.1.2	Determinar si los segmentos de red del servidor VoIP están adecuadamente protegidos, es decir, no son accesibles directamente desde internet, detrás de los firewalls apropiados y dentro del alcance de los IDS / IPS implementados						
5.1.1.3	Determinar que los firewalls frente a las VLAN de VoIP son compatibles con VoIP (es decir, "entienden" los protocolos VoIP implementados [SIP o H.323]) y que los puertos apropiados están abiertos en el firewall, dependiendo del hardware VoIP específico						
5.2	**Protección de red** **Objetivo de auditoría de seguridad:** Las redes VoIP y VLAN se incluyen en el monitoreo de seguridad y la evaluación de vulnerabilidades						

No.	5. RED Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
5.2.1	**Inclusión en evaluaciones de red y pruebas de penetración** **Control:** Los servidores VoIP e IP PBX están incluidos en todas las evaluaciones de seguridad de la red y las pruebas de penetración	DS5.9	PC4				
5.2.1.1	Revisar la documentación relacionada con las evaluaciones recientes de vulnerabilidad y las pruebas de penetración (realizadas por evaluadores internos o externos) y determinar que todos los servidores VoIP y VLAN se incluyeron en el alcance de tales pruebas						
5.2.1.2	Determinar si todas las vulnerabilidades relacionadas con las redes VoIP y las VLAN se corrigieron adecuadamente de manera oportuna						
		Total (promedio porcentajes de cumplimiento)			**Total** Tiempo efectivo en minutos		

Guía de Auditoría GA-6 PLANIFICACIÓN DE CONTINGENCIAS

Guía de Auditoría VoIPSAM		**Guía de Auditoría**
6. PLANIFICACIÓN DE CONTINGENCIAS		
Objetivo:	Determinar si los servicios esenciales del servidor VoIP están incluidos en el Plan de Contingencia de TI / Plan de Continuidad del Negocio	**GA-6**
Papel de Trabajo:	**PT-GA-6**	

No.	**6. PLANIFICACIÓN DE CONTINGENCIAS Procedimiento de control**	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
6.1	**Planificación de contingencias** **Objetivo de auditoría de seguridad:** Los servicios esenciales del servidor VoIP están incluidos en el Plan de Contingencia de TI / Plan de Continuidad del Negocio						
6.1.1	**Análisis de impacto de negocio contingente (BIA)** **Control:** Las aplicaciones del servidor VoIP están incluidas en el BIA de la unidad de negocios	DS4	PC1				
6.1.1.1	Obtener el BIA para las unidades de negocios que operan servidores de VoIP.						
6.1.1.2	Determinar si el BIA considera los servidores VoIP en su análisis de continuidad						
6.1.2	**Plan de contingencia para aplicaciones de servidor VoIP** **Control:** Las aplicaciones del servidor VoIP se incluyen en el plan de contingencia en función de su perfil de alto riesgo	DS4	PC1				
6.1.2.1	Obtener el BIA (Análisis de Impacto del Negocio)						
6.1.2.2	Determinar si las aplicaciones del servidor VoIP están identificadas adecuadamente en el orden de restauración						

No.	6. PLANIFICACIÓN DE CONTINGENCIAS Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
6.1.2.3	Para aquellos servidores que tienen una calificación de alto impacto, determinar que el plan de continuidad incluye el procesamiento provisional y los planes de restauración						
6.2	**Copia de seguridad y recuperación** **Objetivo de auditoría de seguridad:** El programa de respaldo y recuperación del servidor VoIP es apropiado para proteger la inversión de la empresa en un servicio confiable de mensajería de voz, texto y video						
6.2.1	**Copia de seguridad y recuperación** **Control:** Se documenta una copia de seguridad y un proceso de recuperación que aborda las necesidades de contingencia	DS11.2 DS11.5	PC5.2 PC5.3				
6.2.1.1	Obtener y revisar una copia del plan de recuperación ante desastres de la empresa (DRP) y determinar si se han tenido en cuenta los niveles de servicio, es decir, todos los siguientes: - Acuerdos de nivel de servicio (SLA), que definen cuánto tiempo puede estar inactivo VoIP antes de que se restaure el servicio (probablemente muy corto) - Objetivos del punto de recuperación (RPO), que determinan la cantidad de datos que se pueden perder, medidos en minutos - Objetivos de tiempo de recuperación (RTO), que determinan el tiempo máximo permitido para recuperar cada servicio, medido en minutos						
6.2.1.2	Obtener y revisar una copia de la última prueba de recuperación y determinar si se probó todo lo anterior y si todas las deficiencias en el proceso de recuperación probado se han remediado por completo						

No.	6. PLANIFICACIÓN DE CONTINGENCIAS Procedimiento de control	Referencia Cobit	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
6.2.1.3	Determinar si las copias de respaldo de las bases de datos y el software del servidor VoIP son: - Mantenidas en una instalación segura fuera del sitio - Las cintas o discos de respaldo se cifran antes de salir de las instalaciones - El acceso a las operaciones de copia de seguridad fuera del sitio está restringido a un pequeño número de empleados de confianza - Las copias de respaldo se llevan al almacenamiento externo por un tercero de manera segura (por ejemplo, vehículos blindados, guardias armados). Mantenidas en un servicio de utilidad de bóveda						
		Total (promedio porcentajes de cumplimiento)			**Total** Tiempo efectivo en minutos		

Guía de Auditoría GA-7 CULTURA DE SEGURIDAD

Guía de Auditoría VoIPSAM		**Guía de Auditoría**
7. CULTURA DE SEGURIDAD		
Objetivo:	Determinar la existencia de un Plan de cultura de seguridad que permita combatir los ataques de ingeniería social y la mitigación de los riesgos asociados	**GA-7**
Papel de Trabajo:	**PT-GA-7**	

No.	7. CULTURA DE SEGURIDAD Procedimiento de control	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
7.1	**Plan de cultura de seguridad** **Objetivo de auditoría de seguridad:** Verificar la existencia de un Plan de Cultura de Seguridad para combatir los ataques de ingeniería social, los procesos se deben diseñar con la ingeniería social en mente; el control versa en aspectos relacionados a ataques de ingeniería social teniendo en cuenta que se deben satisfacer los beneficios, costos y riesgos asociados, lo cual se logra mediante un conjunto de pasos a seguir para desarrollar un plan de cultura de seguridad que permita a la organización mitigar los riesgos asociados	PA4 PD5				
7.1.1	**Control:** Obtener el documento del plan de cultura de seguridad	PA4 PD5				
7.2	**Concienciación y formación** **Objetivo de auditoría de seguridad:** La formación detallada sobre amenazas sociales y técnicas de ingeniería social es fundamental y puede incluir ejemplos basados en casos reales para mayor impacto. La simulación de ataques de ingeniería social es una excelente manera de evaluar la preparación del personal y su capacidad para identificar amenazas.	**PA4.1**				
7.2.1	**Sesiones de capacitación** Programa regular de entrenamiento sobre amenazas de seguridad, incluyendo amenazas sociales y técnicas específicas de ingeniería social en VoIP.					
7.2.1.1	**Control de programa de entrenamiento** **Control:** Obtener el calendario para sesiones regulares de capacitación sobre amenazas de seguridad en VoIP					

No.	7. CULTURA DE SEGURIDAD Procedimiento de control	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
7.2.1.2	**Evaluación posterior a la sesión** **Control:** Obtener los documentos de las pruebas de conocimiento después de cada sesión para medir la comprensión de las amenazas de seguridad y los protocolos de respuesta					
7.2.1.3	**Seguimiento de incidentes reportados** **Control:** Obtener los documentos del registro y análisis de los incidentes reportados relacionados con las amenazas tratadas en las sesiones para evaluar la efectividad de la formación					
7.2.2	**Simulacros de phishing y pruebas de concientización** Simulaciones de ataques de ingeniería social para evaluar la capacidad de los empleados para identificar y reportar diversos tipos de ataques					
7.2.2.1	**Seguimiento de Simulacros de Phishing** **Control:** Obtener los documentos del registro de los resultados de los simulacros de ataques de ingeniería social, incluyendo la identificación y respuestas de los empleados					
7.2.2.2	**Análisis de desempeño possimulacro** **Control:** Obtener los documentos de las revisiones de respuestas y tiempos de respuesta durante los simulacros para identificar áreas de mejora y necesidades de refuerzo en la capacitación.					
7.3	**Políticas y procedimientos** **Objetivo de auditoría de seguridad:** Las políticas claras y las cláusulas detalladas sobre prevención, detección y respuesta ante ataques de ingeniería social son cruciales. La implementación de controles de acceso estrictos y autenticación robusta puede ser fundamental para prevenir estos ataques	PA4.2				
7.3.1	**Políticas de seguridad** Documentos formales que establecen directrices para el uso seguro de sistemas VoIP, incluyendo medidas específicas contra amenazas de espionaje, interrupción intencionada y abuso de servicio					
7.3.1.1	**Control de actualización de políticas** **Control:** Obtener el registro de revisiones y actualizaciones en las políticas de seguridad VoIP, que incluya los cambios y las fechas de implementación	PC4.4				
7.3.1.2	**Auditorías de cumplimiento** **Control:** Obtener los documentos de auditorías periódicas realizadas que permitan verificar el cumplimiento de las políticas establecidas y especifique las áreas de no conformidad para su corrección					

No.	7. CULTURA DE SEGURIDAD Procedimiento de control	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
7.3.1.3	**Pruebas de vulnerabilidad** **Control:** Obtener los documentos que registren las pruebas de penetración regulares que se han realizado para verificar la efectividad de las políticas en la prevención de ataques.					
7.3.2	**Procedimientos de verificación de identidad** Métodos y procesos para verificar la identidad de los usuarios antes de acceder a sistemas VoIP, con enfoque en prevenir el robo de servicio y el espionaje					
7.3.2.1	**Verificación de identidad y acceso** **Control:** Verificar si se implementan controles de acceso, incluyendo autenticación multifactor (MFA) y registros de acceso a sistemas VoIP					
7.3.2.2	**Evaluación de controles de acceso** **Control:** Evaluar la efectividad de los controles de acceso y la identificación de posibles brechas de seguridad.					
7.4	**Fomento de una cultura de seguridad** **Objetivo de auditoría de seguridad:** El compromiso de la alta dirección y la comunicación constante son pilares importantes para una cultura de seguridad sólida. Los incentivos pueden ser efectivos para fomentar el comportamiento seguro y la denuncia de intentos de ingeniería social	PA4.3				
7.4.1	**Liderazgo comprometido** Compromiso visible de la alta dirección hacia la prevención de todos los tipos de ataques de ingeniería social en VoIP					
7.4.1.1	**Seguimiento del compromiso de la alta dirección** **Control**: Verificar la existencia de actividades y comunicaciones de liderazgo relacionadas con la seguridad en VoIP para evaluar el nivel de compromiso					
7.4.1.2	**Encuestas de satisfacción de empleados** **Control:** Verificar la realización de encuestas periódicas para medir la percepción de los empleados sobre el compromiso de la alta dirección con la seguridad					
7.4.2	**Comunicación constante** Mantenimiento de una comunicación activa sobre la importancia de la seguridad, resaltando casos reales y consejos para evitar cada tipo de ataque					
7.4.2.1	**Evaluación de Comunicaciones de Seguridad** **Control:** Verificar y revisar registros de comunicaciones internas sobre seguridad para garantizar la divulgación adecuada de medidas preventivas contra ataques de ingeniería social					
7.4.2.2	**Retroalimentación de Comunicación** **Control:** Recopilar comentarios de los empleados sobre la efectividad y relevancia de la comunicación sobre seguridad para realizar ajustes necesarios					

No.	7. CULTURA DE SEGURIDAD Procedimiento de control	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
7.4.3	**Incentivos y motivadores** Establecimiento de programas de incentivos para reforzar comportamientos seguros y la denuncia de intentos de ingeniería social					
7.4.3.1	**Evaluación de programas de incentivos** **Control:** Verificar la existencia de análisis periódicos para medir la efectividad de los programas de incentivos en la detección y denuncia de ataques de ingeniería social					
7.5	**Actualización y evaluación continua** **Objetivo de auditoría de seguridad:** La actualización continua de políticas y evaluación de riesgos es esencial para mantenerse al día con las últimas amenazas. La implementación de herramientas de seguridad como filtros antispam y sistemas de autenticación robustos puede fortalecer significativamente la defensa contra ataques de ingeniería social	PD5.1				
7.5.1	**Revisiones periódicas de políticas** Actualizaciones regulares de políticas de seguridad VoIP, incluyendo medidas actualizadas contra todas las variantes de ataques de ingeniería social	PC4.5				
7.5.1.1	**Registro de actualizaciones de seguridad** **Control:** Verificar el registro de las actualizaciones implementadas en las herramientas de seguridad, como filtros antispam y sistemas de autenticación					
7.5.1.2	**Programación de revisiones** **Control:** Obtener y verificar el calendario para revisiones regulares de políticas, con un equipo designado para identificar y abordar las lagunas en las políticas actuales relacionadas con ataques de ingeniería social					
7.5.1.3	**Evaluación de cambios** **Control:** Verificar la existencia de análisis posteriores a las revisiones para determinar la efectividad de las actualizaciones en la prevención y detección de nuevos métodos de ataques					
7.5.2	**Evaluación de riesgos** Evaluaciones continuas de los riesgos de ingeniería social en VoIP, identificando y abordando nuevos métodos de ataque					
7.5.2.1	**Análisis de riesgos y tendencias** **Control:** Verificar las evaluaciones periódicas de riesgos basadas en análisis de tendencias y patrones de ataques de ingeniería social identificados.					
7.5.2.2	**Análisis de tendencias de ataque** **Control:** Verificar la conformación de un equipo dedicado para el análisis continuo de tendencias y patrones de ataques, permitiendo ajustes inmediatos en las estrategias de seguridad en respuesta a nuevas amenazas identificadas					

No.	7. CULTURA DE SEGURIDAD Procedimiento de control	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
7.6	**Implementación de herramientas de seguridad** **Objetivo de auditoría de seguridad:** Implementar herramientas como filtros antispam y antimalware es esencial. También es importante revisar y ajustar estas herramientas según los cambios en las tendencias de ataques	PD5.2				
7.6.1	**Filtros antispam y antimalware** Uso de software para detectar y bloquear correos y llamadas no deseadas, incluyendo SPIT					
7.6.1.1	**Revisión y actualización de configuraciones** **Control:** Verificar la existencia de revisiones periódicas de las configuraciones de los filtros para asegurar que estén alineadas con las últimas técnicas de detección y bloqueo de SPIT					
7.6.2	**Seguridad en la autenticación** Implementación de sistemas de autenticación robustos para prevenir suplantaciones y accesos no autorizados					
7.6.2.1	**Auditorías de autenticación** **Control:** Verificar la realización de auditorías regulares para verificar la integridad y efectividad de los sistemas de autenticación, identificando y corrigiendo posibles vulnerabilidades					
7.7	**Responsabilidad y reporte** **Objetivo de auditoría de seguridad:** Establecer un canal seguro para reportar incidentes y la política de no represalias son cruciales para fomentar un entorno de denuncia seguro y confiable. La evaluación periódica de la efectividad de los programas de incentivos es una excelente manera de asegurarse de que sigan siendo efectivos	PD5.3				
7.7.1	**Canal de reporte de incidentes** Establecimiento de un canal seguro y confidencial para reportar incidentes de ingeniería social, incluyendo todos los tipos de ataques mencionados					
7.7.1.1	**Seguimiento de incidentes reportados** **Control:** Verificar la existencia de un registro detallado de incidentes de ingeniería social reportados, incluyendo acciones tomadas y resultados de la investigación					
7.7.1.2	**Monitoreo del canal de reporte** **Control:** Verificar la existencia de un equipo encargado de supervisar y responder rápidamente a los informes recibidos a través del canal de incidentes, garantizando una respuesta oportuna y adecuada					
7.7.2	**Política de no represalias** Garantizar que los empleados se sientan seguros al reportar incidentes y se eviten represalias por hacerlo.					

No.	7. CULTURA DE SEGURIDAD Procedimiento de control	Referencia VoIPSAM	% Cumplimiento	Nombre Auditor	Fecha	Tiempo efectivo minutos
7.7.2.1	**Encuestas de satisfacción** **Control:** Verificar la existencia de encuestas periódicas para evaluar la percepción de los empleados sobre la efectividad de la política de no represalias y hacer ajustes según la retroalimentación recibida					
7.7.3	**Evaluación de incentivos y motivadores** Revisión y evaluación de la efectividad de los programas de incentivos en la detección y reporte de intentos de ingeniería social					
7.7.3.1	**Evaluación de programas de incentivos** **Control:** Monitorear la efectividad de los programas de incentivos en la detección y reporte de intentos de ataques, ajustando según los resultados					
7.7.3.2	**Análisis de efectividad de incentivos** **Control:** Evaluar la eficacia de los programas de incentivos en relación con la detección y denuncia de intentos de ingeniería social, ajustando los programas según los resultados obtenidos					
	Total (promedio porcentajes de cumplimiento)			**Total** Tiempo efectivo en minutos		

Guía de Auditoría EVALUACIÓN DE MADUREZ

Guía de Auditoría VoIPSAM		**Guía de Auditoría**
8. EVALUACIÓN DE MADUREZ		
Objetivo:	Evaluar la madurez de los procesos revisados. Con base en los resultados de la revisión de la auditoría de seguridad y las observaciones del revisor, asigne un nivel de madurez a cada uno de los procedimientos de control	**GA-8**

No.	**8. EVALUACIÓN DE MADUREZ Procedimiento de Control**	**Referencia Cobit**	**Referencia VoIPSAM**	**Madurez evaluada**	**Madurez objetivo**	**Nombre Auditor**	**Fecha**	**Tiempo efectivo minutos**
8.1	**Definir la arquitectura de información** El establecimiento de un modelo de datos empresarial que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos	PO2	PA2					
8.1.1	**Modelo de arquitectura de información empresarial** Establecer y mantener un modelo de información empresarial para permitir el desarrollo de aplicaciones y actividades de soporte de decisiones, de acuerdo con los planes de TI	PO2.1	PA2.1					
8.1.2	**Esquema de clasificación de datos** Establecer un esquema de clasificación que se aplique en toda la empresa, en función de la criticidad y la sensibilidad (p. Ej., Pública, confidencial, secreta) de los datos de la empresa. Este esquema debe incluir detalles sobre la propiedad de los datos; definición de niveles de seguridad apropiados y controles de protección; y una breve descripción de los requisitos de retención y destrucción de datos, criticidad y sensibilidad. Debe usarse como base para aplicar controles como controles de acceso, archivo o encriptación.	PO2.3	PA2.2					
8.2	**Definir los procesos, organización y relaciones** El establecimiento de estructuras organizacionales de TI transparentes, flexibles y responsables, y en la de implementación de procesos de TI con dueños, y en la integración de roles y responsabilidades hacia los procesos de negocio y de decisión	PO4	PA3					
8.2.1	**Establecimiento de roles y responsabilidades** Establecer y comunicar los roles y responsabilidades para el personal de TI y los usuarios finales que delimiten entre el personal de TI y la autoridad, las	PO4.6	PA3.1					

No.	8. EVALUACIÓN DE MADUREZ Procedimiento de Control	Referencia Cobit	Referencia VoIPSAM	Madurez evaluada	Madurez objetivo	Nombre Auditor	Fecha	Tiempo efectivo minutos
	responsabilidades y la responsabilidad del usuario final para satisfacer las necesidades de la organización							
8.2.2	**Responsabilidad sobre el riesgo, la seguridad y el cumplimiento** Incrustar la propiedad y la responsabilidad de los riesgos relacionados con TI dentro de la empresa en un nivel superior apropiado. Definir y asignar roles críticos para gestionar los riesgos de TI, incluida la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento	PO4.8	PA3.2					
8.2.3	**Propiedad de datos y de sistema** Proporcionar a la empresa procedimientos y herramientas que le permitan abordar sus responsabilidades de propiedad de los sistemas de datos e información. Los propietarios deben tomar decisiones sobre la clasificación de la información y los sistemas y protegerlos de acuerdo con esta clasificación	PO4.9	PA3.3					
8.3	**Definición del plan de cultura de seguridad** Plan de Cultura de Seguridad para combatir los ataques de ingeniería social, los procesos se deben diseñar con la ingeniería social en mente; el control versa en aspectos relacionados a ataques de ingeniería social teniendo en cuenta que se deben satisfacer los beneficios, costos y riesgos asociados, lo cual se logra mediante un conjunto de pasos a seguir para desarrollar un plan de cultura de seguridad que permita a la organización mitigar los riesgos asociados		PA4					
8.3.1	**Concienciación y formación** La formación detallada sobre amenazas sociales y técnicas de ingeniería social es fundamental y podría incluir ejemplos basados en casos reales para mayor impacto. La simulación de ataques de ingeniería social es una excelente manera de evaluar la preparación del personal y su capacidad para identificar amenazas. Se incluyen sesiones de capacitación, simulacros de phishing y pruebas de concientización		PA4.1					
8.3.2	**Políticas y procedimientos** Las políticas claras y las cláusulas detalladas sobre prevención, detección y respuesta ante ataques de ingeniería social son cruciales. La implementación de controles de acceso estrictos y autenticación robusta puede ser fundamental para prevenir estos ataques. Se requiere la definición de políticas de seguridad claras y procedimientos de verificación de identidad		PA4.2					

No.	8. EVALUACIÓN DE MADUREZ Procedimiento de Control	Referencia Cobit	Referencia VoIPSAM	Madurez evaluada	Madurez objetivo	Nombre Auditor	Fecha	Tiempo efectivo minutos
8.3.3	**Fomento de una cultura de seguridad** El compromiso de la alta dirección y la comunicación constante son pilares importantes para una cultura de seguridad sólida. Los incentivos pueden ser efectivos para fomentar el comportamiento seguro y la denuncia de intentos de ingeniería social. Se requiere liderazgo comprometido de la alta dirección y comunicación constante		PA4.3					
8.4	**Identificar soluciones automatizadas** La administración del proceso de Identificar soluciones automatizadas que satisfaga el requerimiento de negocio de TI de traducir los requerimientos funcionales y de control del negocio a diseño efectivo y eficiente de soluciones automatizadas	AI1	PB1					
8.4.1	**Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio** Identificar, priorizar, especificar y acordar los requisitos funcionales y técnicos del negocio que cubren el alcance completo de todas las iniciativas requeridas para lograr los resultados esperados del programa de inversión habilitado por TI	AI1.1	PB1.1					
8.4.2	**Estudio de factibilidad y formulación de cursos de acción alternativos** Desarrollar un estudio de factibilidad que examine la posibilidad de implementar los requisitos. La gestión empresarial, respaldada por la función de TI, debe evaluar la viabilidad y los cursos de acción alternativos y hacer una recomendación al patrocinador comercial	AI1.3	PB1.2					
8.5	**Adquirir y mantener infraestructura tecnológica** Las organizaciones deben contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza la existencia de un soporte tecnológico continuo para las aplicaciones del negocio	AI3	PB2					
8.5.1	**Plan de adquisición de infraestructura tecnológica** Producir un plan para la adquisición, implementación y mantenimiento de la infraestructura tecnológica que cumpla con los requisitos comerciales, funcionales y técnicos establecidos y que esté de acuerdo con la dirección tecnológica de la organización	AI3.1	PB2.1					
8.6	**Instalar y acreditar soluciones y cambios**	AI7	PB3					

No.	8. EVALUACIÓN DE MADUREZ Procedimiento de Control	Referencia Cobit	Referencia VoIPSAM	Madurez evaluada	Madurez objetivo	Nombre Auditor	Fecha	Tiempo efectivo minutos
	Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación y la transición en sí al ambiente de producción, y revisar la posimplantación. Esto garantiza que los sistemas operativos estén en línea con las expectativas convenidas y con los resultados							
8.6.1	**Capacitación** Capacitar a los miembros del personal de los departamentos de usuarios afectados y al grupo de operaciones de la función de TI de acuerdo con el plan de capacitación e implementación definido y los materiales asociados, como parte de cada proyecto de desarrollo, implementación o modificación de sistemas de información	AI7.1	PB3.1					
8.6.2	**Plan de Prueba** Establecer un plan de prueba basado en estándares de toda la organización que definan roles, responsabilidades y criterios de entrada y salida. Asegurar que el plan sea aprobado por las partes relevantes	AI7.2	PB3.2					
8.6.3	**Plan de Implementación** Establecer un plan de implementación y respaldo	AI7.3	PB3.3					
8.6.4	**Ambiente de Prueba** Definir y establecer un entorno de prueba seguro representativo del entorno de operaciones planificadas en relación con la seguridad, los controles internos, las prácticas operativas, la calidad de los datos y los requisitos de privacidad y las cargas de trabajo	AI7.4	PB3.4					
8.6.5	**Entrenamiento y culturización: Plan de cultura de seguridad** Educar, capacitar y fortalecer la conciencia de los empleados respecto a los riesgos específicos asociados con los ataques de ingeniería social en el contexto de las comunicaciones VoIP		PB3.5					
8.7	**Garantizar la seguridad de los sistemas** La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas, así como realizar acciones correctivas sobre las debilidades o incidentes	DS5	PC2					

No.	8. EVALUACIÓN DE MADUREZ Procedimiento de Control	Referencia Cobit	Referencia VoIPSAM	Madurez evaluada	Madurez objetivo	Nombre Auditor	Fecha	Tiempo efectivo minutos
	de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad							
8.7.1	**Administración de la seguridad de TI** Administrar la seguridad de TI al más alto nivel organizacional apropiado, de modo que la administración de las acciones de seguridad esté en línea con los requisitos del negocio	DS5.1	PC2.1					
8.7.2	**Plan de seguridad de TI** Traducir los requisitos de negocio, riesgo y cumplimiento en un plan de seguridad de TI general, teniendo en cuenta la infraestructura de TI y la cultura de seguridad. Asegurar que el plan se implemente en políticas y procedimientos de seguridad junto con inversiones apropiadas en servicios, personal, software y hardware. Comunique las políticas y procedimientos de seguridad a las partes interesadas y los usuarios	DS5.2	PC2.2					
8.7.3	**Administrar el plan de cultura de seguridad** Gestión efectiva, supervisión y coordinación de todas las actividades y componentes del plan de seguridad VoIP, específicamente dirigido a contrarrestar los ataques de ingeniería social		PC2.3					
8.7.4	**Administración de Identidad** Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas de TI (aplicación empresarial, entorno de TI, operaciones del sistema, desarrollo y mantenimiento) sean identificables de forma única. Habilitar identidades de usuario a través de mecanismos de autenticación. Confirme que los derechos de acceso de los usuarios a los sistemas y los datos están en línea con las necesidades comerciales definidas y documentadas y que los requisitos del trabajo están vinculados a las identidades de los usuarios. Asegurar que los derechos de acceso del usuario sean solicitados por la administración del usuario, aprobados por los propietarios del sistema e implementados por la persona responsable de la seguridad. Mantener identidades de usuario y derechos de acceso en un repositorio central. Implemente medidas técnicas y de procedimiento rentables y manténgalas actualizadas para establecer la identificación del usuario, implementar la autenticación y hacer cumplir los derechos de acceso.	DS5.3	PC2.4					

No.	8. EVALUACIÓN DE MADUREZ Procedimiento de Control	Referencia Cobit	Referencia VoIPSAM	Madurez evaluada	Madurez objetivo	Nombre Auditor	Fecha	Tiempo efectivo minutos
8.7.5	**Administración de cuentas de usuario** Dirección de respuesta, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y privilegios de usuario relacionados con un conjunto de procedimientos de administración de cuentas de usuario. Incluya un procedimiento de aprobación que describa los datos o el propietario del sistema que otorga los privilegios de acceso. Estos procedimientos deberían aplicarse a todos los usuarios, incluidos los administradores (usuarios privilegiados) y los usuarios internos y externos, para casos normales y de emergencia. Los derechos y obligaciones relacionados con el acceso a los sistemas y la información de la empresa deben organizarse contractualmente para todo tipo de usuarios. Realizar una revisión periódica de la administración de todas las cuentas y privilegios relacionados	DS5.4	PC2.5					
8.7.6	**Seguridad de la red** Usar técnicas de seguridad y procedimientos de administración relacionados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de red, detección de intrusos) para autorizar el acceso y controlar los flujos de información desde y hacia las redes	DS5.10	PC2.8					
8.8	**Administrar la configuración** Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conforme se necesite. Una efectiva administración de la configuración facilita una mayor disponibilidad, minimiza los problemas de producción y resuelve los problemas más rápido	DS9	PC4					
8.8.1	**Repositorio y línea base de configuración** Establecer una herramienta de soporte y un repositorio central para contener toda la información relevante sobre los elementos de configuración. Monitorear y registrar todos los activos y cambios en los activos. Mantener una línea base de elementos de configuración para cada sistema y servicio como un punto de control al que regresar después de los cambios	DS9.1	PC4.1					
8.8.2	**Identificación y mantenimiento de elementos de configuración**	DS9.2	PC4.2					

No.	8. EVALUACIÓN DE MADUREZ Procedimiento de Control	Referencia Cobit	Referencia VoIPSAM	Madurez evaluada	Madurez objetivo	Nombre Auditor	Fecha	Tiempo efectivo minutos
	Establecer procedimientos de configuración para admitir la administración y el registro de todos los cambios en el repositorio de configuración. Integrar estos procedimientos con los procedimientos de gestión de cambios, gestión de incidentes y gestión de problemas							
8.8.3	**Revisión de integridad de la configuración** Revisar periódicamente los datos de configuración para verificar y confirmar la integridad de la configuración actual e histórica	DS9.3	PC4.3					
8.8.4	**Nuevas políticas del plan de cultura de seguridad** Desarrollo, revisión y actualización de políticas específicas diseñadas para mitigar los riesgos asociados con los ataques de ingeniería social en el ámbito de las comunicaciones VoIP		PC4.4					
8.8.5	Depuración del plan de cultura de seguridad Revisar, mejorar y optimizar los componentes clave del plan de seguridad VoIP para contrarrestar los ataques de ingeniería social		PC4.5					
8.9	**Gestionar datos** Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio	DS11	PC5					
8.9.1	**Acuerdos de Almacenamiento y Conservación** Definir e implementar procedimientos para el almacenamiento, retención y archivo de datos efectivos y eficientes para cumplir con los objetivos comerciales, la política de seguridad y los requisitos reglamentarios de la organización	DS11.2	PC5.2					
8.9.2	**Respaldo y restauración** Definir e implementar procedimientos para el respaldo y la restauración de sistemas, aplicaciones, datos y documentación de acuerdo con los requisitos de negocio y el plan de continuidad	DS11.5	PC5.3					
8.9.3	**Requerimientos de seguridad para la administración de datos** Definir e implementar políticas y procedimientos para identificar y aplicar los requisitos de seguridad aplicables a la recepción, procesamiento,	DS11.6	PC5.4					

No.	8. EVALUACIÓN DE MADUREZ Procedimiento de Control	Referencia Cobit	Referencia VoIPSAM	Madurez evaluada	Madurez objetivo	Nombre Auditor	Fecha	Tiempo efectivo minutos
	almacenamiento y salida de datos para cumplir con los objetivos de negocio, la política de seguridad de la organización y los requisitos reglamentarios							
8.10	**Monitorear y evaluar control interno** Establecer un programa de control interno efectivo para TI requiere un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las autoevaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables	ME2	PD2					
8.10.1	**Revisiones de auditoría** Monitorear y evaluar la eficiencia y efectividad de los controles internos de revisión gerencial de TI.	ME2.2	PD2.2					
8.10.2	**Excepciones de control** Identificar y analizar excepciones de control e identifique sus causas subyacentes. Escalar las excepciones de control e informe a las partes interesadas de manera adecuada. Instituir la acción correctiva necesaria	ME2.3	PD2.3					
8.10.3	**Control de auto evaluación** Evaluar la integridad y efectividad del control de la administración sobre los procesos, políticas y contratos de TI a través de un programa continuo de autoevaluación	ME2.4	PD2.4					
8.10.4	**Acciones Correctivas** Identificar, iniciar, rastrear e implementar acciones correctivas que surjan de las evaluaciones e informes de control.	ME2.7	PD2.5					
8.11	**Monitorear plan de cultura de seguridad** Supervisión y evaluación continua de todas las estrategias, políticas y procedimientos implementados para fortalecer la seguridad en VoIP contra ataques de ingeniería social. Esta etapa garantiza la efectividad y el cumplimiento constante de las medidas establecidas, además de proporcionar la oportunidad de realizar ajustes o mejoras según sea necesario		PD5					
8.11.1	**Actualización y evaluación continua** La actualización continua de políticas y evaluación de riesgos es esencial para mantenerse al día con las últimas amenazas. La implementación de herramientas de seguridad como filtros antispam y sistemas de autenticación		PD5.1					

No.	8. EVALUACIÓN DE MADUREZ Procedimiento de Control	Referencia Cobit	Referencia VoIPSAM	Madurez evaluada	Madurez objetivo	Nombre Auditor	Fecha	Tiempo efectivo minutos
	robustos puede fortalecer significativamente la defensa contra ataques de ingeniería social							
8.11.2	**Implementación de herramientas de seguridad** Implementar herramientas como filtros antispam y anti-malware es esencial. También es importante revisar y ajustar estas herramientas según los cambios en las tendencias de ataques		PD5.2					
8.11.3	**Responsabilidad y reporte** Establecer un canal seguro para reportar incidentes y la política de no represalias son cruciales para fomentar un entorno de denuncia seguro y confiable. La evaluación periódica de la efectividad de los programas de incentivos es una excelente manera de asegurarse de que sigan siendo efectivos		PD5.3					
8.12	**Garantizar el cumplimiento de los requisitos externos** Una supervisión efectiva del cumplimiento requiere el establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento, optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio	ME3	PD3					
8.12.1	**Identificar los requerimientos de las leyes, regulaciones y cumplimientos contractuales** Identificar de forma continua, las leyes, regulaciones y otros requisitos externos locales e internacionales que deben cumplirse para su incorporación a las políticas, estándares, procedimientos y metodologías de TI de la organización	ME3.1	PD3.1					
8.12.2	**Optimizar la respuesta a requerimientos externos** Revisar y ajustar las políticas, estándares, procedimientos y metodologías de TI para garantizar que los requisitos legales, reglamentarios y contractuales se aborden y comuniquen	ME3.2	PD3.2					
8.12.3	**Evaluación del cumplimiento con requerimientos externos** Confirmar el cumplimiento de las políticas, estándares, procedimientos y metodologías de TI con los requisitos legales y reglamentarios	ME3.3	PD3.3					
8.12.4	**Aseguramiento Positivo del Cumplimiento** Obtener e informar la garantía de cumplimiento y cumplimiento de todas las políticas internas derivadas de directivas internas o requisitos legales,	ME3.4	PD3.4					

No.	8. EVALUACIÓN DE MADUREZ Procedimiento de Control	Referencia Cobit	Referencia VoIPSAM	Madurez evaluada	Madurez objetivo	Nombre Auditor	Fecha	Tiempo efectivo minutos
	reglamentarios o contractuales externos, confirmando que el propietario responsable del proceso ha tomado las medidas correctivas de manera oportuna							

Anexo F. Solicitud y aprobación de aplicación del modelo VoIPSAM



Escuela Superior Politécnica de Chimborazo

Facultad de Informática y Electrónica

Oficio Nro. ESPOCH-FIE.DOC-2023-1511-O

Riobamba, 27 de marzo de 2023

Asunto: Solicitud autorización aplicación Modelo de Auditoria de Seguridad VoIP - VoIPSAM (tesis doctoral)

Señor Ingeniero
Byron Ernesto Vaca Barahona, PhD.
Rector
ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
En su Despacho

De mi consideración:

Reciba un atento y cordial saludo, a la vez el deseo de éxitos en el desarrollo de sus acertadas funciones.

Yo, **Oscar Danilo Gavilánez Alvarez**, Docente ocasional de la FIE-ESPOCH y estudiante del Programa de Doctorado en Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos – Perú, me dirijo a Usted de la manera más comedida solicitando autorice a quien corresponda me permita la **aplicación del Modelo de Auditoria de Seguridad VoIP - VoIPSAM** (planteado en mi tesis doctoral) a través de un caso práctico en la Dirección de Tecnologías de la Información y Comunicación DTIC-ESPOCH.

Por la favorable atención al presente anticipo mis agradecimientos, reiterando mis sentimientos de alta consideración y estima.

Con sentimientos de distinguida consideración.

Atentamente,
SABER PARA SER

Documento firmado electrónicamente

Ing. Oscar Danilo Gavilanez Alvarez
PROFESOR OCASIONAL

Anexos:
- Solicitud Oscar Gavilánez-signed.pdf

Escuela Superior Politécnica de Chimborazo
50 AÑOS

Facultad de Informática y Electrónica

Oficio Nro. ESPOCH-FIE.DOC-2023-1511-O

Riobamba, 27 de marzo de 2023

Copia:
Señor Ingeniero
Diego Bernardo Palacios Campana
Director Tecnologías de la Información y Comunicación

OSCAR DANILO CAVILANES ALVAREZ

Riobamba, 27 marzo 2023

Dr. Byron Vaca

RECTOR ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

Presente

De mi consideración

Reciba un atento y cordial saludo, a la vez el deseo de éxitos en el desarrollo de sus acertadas funciones.

Yo, **Oscar Danilo Gavilánez Alvarez**, Docente ocasional de la FIE-ESPOCH y estudiante del Programa de Doctorado en Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos – Perú, me dirijo a Usted de la manera más comedida solicitando autorice a quien corresponda me permita la **aplicación del Modelo de Auditoría de Seguridad VoIP - VoIPSAM** (planteado en mi tesis doctoral) a través de un caso práctico en la Dirección de Tecnologías de la Información y Comunicación DTIC-ESPOCH.

Por la favorable atención al presente anticipo mis agradecimientos, reiterando mis sentimientos de alta consideración y estima.

Atentamente,



Ing. Oscar Danilo Gavilánez Alvarez

0602764748
Estudiante del Programa de Doctorado en Ingeniería de Sistemas e Informática UNMSM
Celular: 0987353867
oscar.gavilanez@gmail.com

Escuela Superior Politécnica de Chimborazo
50 AÑOS

Rectorado

Oficio Nro. 1637.R.ESPOCH.SGD.2023

Riobamba, 28 de marzo de 2023

Asunto: Solicitud de informe previa autorización aplicación Modelo de Auditoría de Seguridad VoIP - VoIPSAM (tesis doctoral)

Señor Ingeniero
Diego Bernardo Palacios Campana
Director Tecnologías de la Información y Comunicación
ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
En su Despacho

De mi consideración:

Con atento saludo, me permito adjuntar el Oficio Nro. ESPOCH-FIE.DOC-2023-1511-O, firmado electrónicamente por el Ing. Oscar Danilo Gavilánez Alvarez; PROFESOR OCASIONAL de la Facultad de Informática y Electrónica; quien solicita la autorización para aplicar Modelo de Auditoría de Seguridad VoIP – VoIPSAM, agradeceré se analice el contenido y previo a la autorización presentar un informe de factibilidad y confidencialidad.

Con sentimientos de distinguida consideración.

Atentamente,
SABER PARA SER

Documento firmado electrónicamente

Ing. Byron Ernesto Vaca Barahona, PhD.
RECTOR

Referencias:
- ESPOCH-FIE.DOC-2023-1511-O

Anexos:
- Solicitud Oscar Gavilánez-signed.pdf
- ESPOCH-FIE.DOC-2023-1511-O.pdf

Copia:
Señor Ingeniero
Oscar Danilo Gavilanez Alvarez
Profesor Ocasional

Escuela Superior Politécnica de Chimborazo
50 AÑOS

Rectorado

Oficio Nro. 1637.R.ESPOCH.SGD.2023

Riobamba, 28 de marzo de 2023

Señora Magíster
Lola Fabiola Maldonado Leon
Gestora Pública

cecilia g
Señor Rector de acuerdo a la sumilla inserta de la señora Gestora Pública, una vez que se ha revisado la documentación, procedo a redactar el oficio, favor firmar para continuar con el trámite.

Escuela Superior Politécnica de Chimborazo
50 AÑOS

Dirección de Tecnologías de la Información y Comunicación

Oficio Nro. 1008-DTIC-ESPOCH-2023

Riobamba, 19 de abril de 2023

Asunto: Aplicación Modelo de Auditoría de Seguridad VoIP - VoIPSAM (tesis doctoral)

Señor Ingeniero
Byron Ernesto Vaca Barahona, PhD.
Rector
ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
En su Despacho

De mi consideración:

Con un respetuoso saludo, y en respuesta al Documento No. 1637.R.ESPOCH.SGD.2023 suscrito por su autoridad, me permito poner bajo vuestro conocimiento el Documento 037-DTIC.UGSI-ESPOCH-2023, elaborado por el Ing. Juan Carlos Díaz, Analista de Seguridad de Tecnologías de la Información 3, quien informa:

"... por medio de la presente me permito informar que, se mantuvo una reunión con el Ing. Oscar Danilo Gavilánez Álvarez; PROFESOR OCASIONAL de la Facultad de Informática y Electrónica, autor de la tesis doctoral "Modelo de Auditoría de Seguridad VoIP – VoIPSAM", y se dio a conocer que la ejecución de esta tesis se base en la aplicación de metodologías, por medio de auditorías (preguntas). Actividad que no involucra comprometimiento en la seguridad informática de la institución...".

En tal virtud es procedente el pedido del Ing. Óscar Gavilánez, profesor Ocasional de la Facultad de Informática y Electrónica.

Particular que comunico para los fines pertinentes.

Con sentimientos de distinguida consideración.

Atentamente,
SABER PARA SER

Documento firmado electrónicamente

Ing. Diego Bernardo Palacios Campana
DIRECTOR TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN

Referencias:
- 037-DTIC.UGSI-ESPOCH-2023

Escuela Superior Politécnica de Chimborazo
50 AÑOS

Dirección de Tecnologías de la Información y Comunicación

Oficio Nro. 1008-DTIC-ESPOCH-2023

Riobamba, 19 de abril de 2023

Anexos:
- Solicitud Oscar Gavilánez-signed.pdf
- ESPOCH-FIE.DOC-2023-1511-O.pdf

Copia:
Señor Ingeniero
Oscar Danilo Gavilanez Alvarez
Profesor Ocasional

ml
Sr. Director en base a su disposición, solicito proceda con la firma para continuar con el trámite correspondiente.

Anexo G. Encuesta B2CE. Auditoría de Seguridad VoIP (estudio de caso)

La presente encuesta tiene por objetivo recolectar información que permita determinar si los componentes presentados a continuación fueron considerados y valorados en forma relevante según la metodología del modelo de Auditoría que Usted ha utilizado. La encuesta le tomará pocos minutos y sus respuestas son totalmente confidenciales.

Solo puede responder la encuesta una vez; no obstante, puede editar las respuestas hasta el cierre de la encuesta el 03 de septiembre de 2024. Todas las preguntas requieren respuesta.

Si tiene alguna duda respecto a la encuesta, envíe un correo electrónico a: oscar.gavilanez@gmail.com

¡Valoro sus comentarios!

Nombre completo

Por favor registre sus nombres y apellidos completos

---

e-mail

Cargo

Por favor indique su cargo (Administrador TI, Administrador VoIP, Consultor de seguridad, Auditor de seguridad, Especialista en Soporte y Mantenimiento, perfiles relacionados)

Experiencia

Por favor indique su tiempo de experiencia relacionada a seguridades VoIP y Certificaciones (Cisco CCNA Collaboration, Cisco CCNA Voice, COBIT® 4.1, COBIT®5, Val IT, Risk IT, ITIL ® y normas internacionales ISO)

Institución a la que pertenece

Modelo de Auditoría utilizado

COBIT 4.1

VoIPSAM

A. Planificación y Organización

La sección requiere determinar si los componentes presentados a continuación fueron considerados y valorados en forma relevante según la metodología del modelo de Auditoría que Usted ha utilizado.

A1. Componente: Definición del plan estratégico de TI. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Administración del Valor de TI. Alineación de TI con el Negocio. Plan Estratégico de TI

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A2. Componente: Definición de la arquitectura de la información. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Modelo de Arquitectura de Información Empresarial. Esquema de Clasificación de Datos

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A3. Componente: Definición de procesos, organización y relaciones de TI. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Establecimiento de Roles y Responsabilidades. Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento. Propiedad de Datos y de Sistemas

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A4. Componente: Definición del Plan de Cultura de Seguridad. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Concienciación y Formación. Políticas y Procedimientos. Fomento de una Cultura de Seguridad

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A5. Componente: Comunicación de las aspiraciones y la dirección de la gerencia ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Implantación de Políticas de TI. Comunicación de los Objetivos y la Dirección de TI

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A6. Componente: Administración de Recursos Humanos de TI ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

- Muy en desacuerdo
- En desacuerdo

- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

A7. Componente: Administración de Proyectos ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B. Adquisición e Implementación

La sección requiere determinar si los componentes presentados a continuación fueron considerados y valorados en forma relevante según la metodología del modelo de Auditoría que Usted ha utilizado.

B1. Componente: Identificación de soluciones automatizadas. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del negocio. Estudio de Factibilidad y Formulación de Cursos de Acción Alternativos. Requerimientos, Decisión de Factibilidad y Aprobación

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B2. Componente: Adquisición y mantenimiento de la infraestructura tecnológica ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Plan de adquisición de infraestructura tecnológica

- Muy en desacuerdo

- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

B3. Componente: Instalación y acreditación de soluciones y cambios. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Entrenamiento. Plan de Prueba. Plan de Implantación. Ambiente de Prueba. Entrenamiento y culturización. Plan de Cultura de Seguridad

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

C. Entrega y Soporte

La sección requiere determinar si los componentes presentados a continuación fueron considerados y valorados en forma relevante según la metodología del modelo de Auditoría que Usted ha utilizado.

C1. Componente: Garantía de la continuidad del servicio. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

C2. Componente: Garantía de la seguridad de los sistemas. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Administración de la Seguridad de TI. Plan de Seguridad de TI. Administrar el Plan de Cultura de Seguridad. Administración de Identidad. Administración de Cuentas del Usuario. Protección de la Tecnología de Seguridad. Administración de Llaves Criptográficas. Seguridad de la Red

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

C3. Componente: Administración de la mesa de servicio y los incidentes. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Administración de la mesa de servicio y los incidentes

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

C4. Componente: Administración de la configuración. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Repositorio y Línea Base de Configuración. Identificación y Mantenimiento de Elementos de Configuración. Revisión de Integridad de la Configuración. Nuevas Políticas del Plan de Cultura de Seguridad. Depuración Plan de Cultura de Seguridad

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

C5. Componente: Administración de los datos. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Requerimientos del Negocio para Administración de Datos. Acuerdos de Almacenamiento y Conservación. Respaldo y Restauración. Requerimientos de Seguridad para la Administración de Datos

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

D. Monitoreo y Evaluación

La sección requiere determinar si los componentes presentados a continuación fueron considerados y valorados en forma relevante según la metodología del modelo de Auditoría que Usted ha utilizado.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

D1. Componente: Monitoreo y Evaluación del Desempeño de TI. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

D2. Componente: Monitoreo y evaluación del control interno. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Monitoreo del Marco de Trabajo de Control Interno. Revisiones de Auditoría. Excepciones de Control. Control de Auto Evaluación. Acciones Correctivas

- Muy en desacuerdo

- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

D3. Componente: Garantía del Cumplimiento de los requisitos externos. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales. Optimizar la Respuesta a Requerimientos Externos. Evaluación del Cumplimiento con Requerimientos Externos. Aseguramiento Positivo del Cumplimiento

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

D4. Componente: Proporcionar Gobierno de TI. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

D5. Componente: Monitoreo del Plan de Cultura de Seguridad. ¿El componente fue considerado en forma relevante por el modelo de Auditoría?

Actualización y evaluación continua. Implementación de herramientas de seguridad. Responsabilidad y Reporte.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo

- Muy de acuerdo

E. Confiabilidad respecto a la aplicación del modelo de Auditoría de seguridad

Se requiere determinar a través de los ítems si existe confiabilidad respecto a la aplicación del modelo de Auditoría que Usted ha utilizado.

E1. ¿Considera que existen mejoras en la seguridad del sistema VoIP con la aplicación del modelo utilizado?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

E2. ¿Considera que es fuerte (minimiza vulnerabilidades) el modelo de auditoría de seguridad VoIP utilizado?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

E3. ¿Considera que la aplicación del modelo utilizado previene exitosamente los ataques a la seguridad de VoIP?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

E4. ¿Considera que la aplicación del modelo utilizado previene exitosamente las técnicas de ataque de ingeniería social?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

E5. ¿Considera que existe una mejora de la confidencialidad luego de la aplicación del modelo utilizado?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

E6. ¿Considera que existe una mejora de la integridad luego de la aplicación del modelo utilizado?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

E7. ¿Considera que existe una mejora en la disponibilidad luego de la aplicación del modelo utilizado?

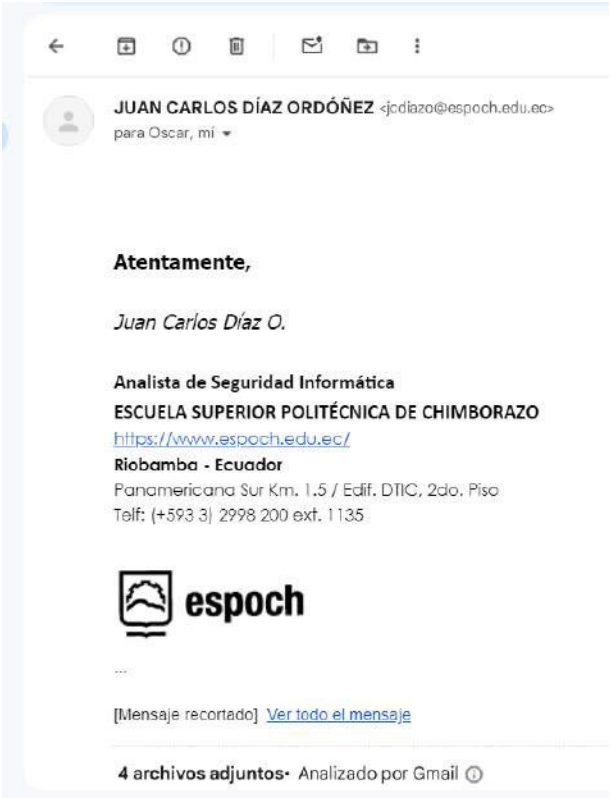
- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

F. Tiempo efectivo de la aplicación de la auditoría

Se requiere conocer el tiempo efectivo utilizado respecto a la aplicación del modelo de Auditoría que Usted ha utilizado.

¿Cuántas horas de trabajo efectivo dedicó usted a la aplicación del modelo de auditoría utilizado?

Anexo H. Resultados de auditorías aplicadas



JUAN CARLOS DÍAZ ORDÓÑEZ <jcdiazo@espoch.edu.ec>
para Oscar, mi

Atentamente,

Juan Carlos Díaz O.

Analista de Seguridad Informática
ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
https://www.espoch.edu.ec/
Riobamba - Ecuador
Panamericana Sur Km. 1.5 / Edif. DTIC, 2do. Piso
Telf: (+593 3) 2998 200 ext. 1135

espoch

...

[Mensaje recortado] Ver todo el mensaje

4 archivos adjuntos · Analizado por Gmail

PGA-1

Plan General de Auditoría VoIPSAM

Objetivo:	Evaluar el cumplimiento de las políticas corporativas en cuanto a la gestión de la seguridad VoIP
Naturaleza:	Procedimientos Internos
Alcance:	ESPOCH
Plazo:	6 semanas

No.	Procedimiento	Referencia Guía de Auditoría	Papel de Trabajo	Nombre del auditor	Fecha Inicio:	Tiempo efectivo minutos
1	PLANIFICACIÓN Y ALCANCE DE LA AUDITORÍA	GA-1		Juan Carlos Díaz Ordóñez Gustavo Xavier Hidalgo Solorzano	1/4/2024	1750
2	PASOS PREPARATORIOS	GA-2	PT-GA-2	Juan Carlos Díaz Ordóñez Gustavo Xavier Hidalgo Solorzano	30/4/2024	645
3	GOBERNANZA	GA-3	PT-GA-3	Juan Carlos Díaz Ordóñez Gustavo Xavier Hidalgo Solorzano	8/5/2024	1625
4	CONFIGURACIÓN DE SERVIDORES	GA-4	PT-GA-4	Juan Carlos Díaz Ordóñez Gustavo Xavier Hidalgo Solorzano	11/6/2024	1075
5	RED	GA-5	PT-GA-5	Juan Carlos Díaz Ordóñez Gustavo Xavier Hidalgo Solorzano	26/6/2024	125
6	PLANIFICACIÓN DE CONTINGENCIAS	GA-6	PT-GA-6	Juan Carlos Díaz Ordóñez Gustavo Xavier Hidalgo Solorzano	1/7/2024	80
7	CULTURA DE SEGURIDAD	GA-7	PT-GA-7	Juan Carlos Díaz Ordóñez Gustavo Xavier Hidalgo Solorzano	2/7/2024	280
8	EVALUACIÓN DE MADUREZ	GA-8		Juan Carlos Díaz Ordóñez Gustavo Xavier Hidalgo Solorzano	8/7/2024	830
					Total	**6410**

Juan Carlos Díaz Ordóñez
0801808270
Auditor

Gustavo Xavier Hidalgo Solorzano
0802116228
Auditor

CERTIFICACIÓN

Riobamba, 23 de agosto 2024

Los suscritos, Ing. Juan Carlos Díaz Ordóñez e Ing. Gustavo Xavier Hidalgo Solorzano, en calidad de Analista de Seguridad Informática y Analista de Automatización de Procesos 3 respectivamente, funcionarios de la Escuela Superior Politécnica de Chimborazo ESPOCH, por medio de la presente certificamos que se aplicó el Modelo de Auditoría de Seguridad VoIP - VoIPSAM en las instalaciones de la DTIC de la ESPOCH, conforme lo planteado en la Guía de Auditoría de Seguridad VoIP mediante VoIPSAM de la tesis doctoral del Ing. Oscar Danilo Gavilánez Álvarez, titulada Modelo de auditoría de seguridad VoIP.

El mencionado modelo fue implementado en el período comprendido entre abril – julio 2024, siguiendo las directrices y procedimientos descritos en la Guía de Auditoría de Seguridad VoIP mediante VoIPSAM, con el objetivo de evaluar y fortalecer la seguridad en los sistemas de comunicación VoIP de la DTIC-ESPOCH.

El proceso de auditoría incluyó la revisión exhaustiva de los sistemas de comunicación VoIP, la identificación de posibles vulnerabilidades y las recomendaciones respectivas para garantizar la seguridad y el correcto funcionamiento de dichos sistemas dentro de nuestra institución.

Finalmente, se deja constancia de que los resultados obtenidos han sido documentados y entregados al Ing. Oscar Danilo Gavilánez Álvarez.

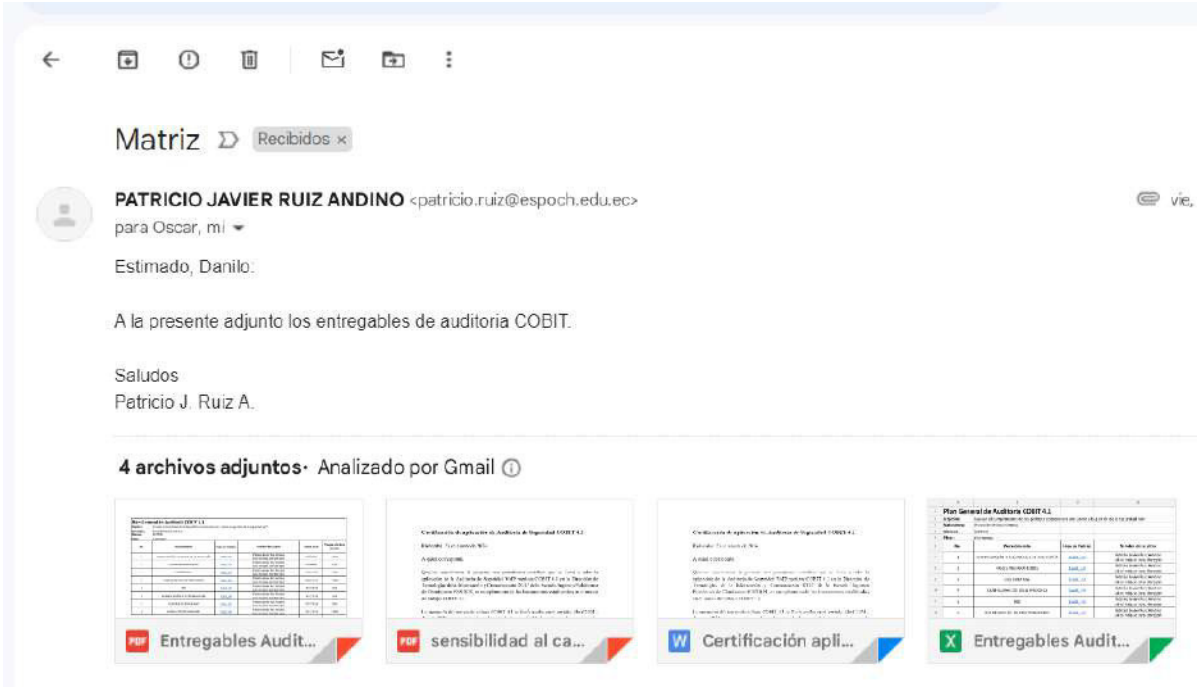
Suscribimos la presente certificación en Riobamba, a los 23 días del mes de agosto del año 2024.

Atentamente,

Ing. Juan Carlos Díaz Ordóñez
0801808270
Analista de Seguridad Informática

Ing. Gustavo Xavier Hidalgo Solorzano
0802116228
Analista de Automatización de Procesos 3

Dirección de Tecnologías de la Información y Comunicación DTIC
Dirección de Procesos y Mejora Continua.
Escuela Superior Politécnica de Chimborazo ESPOCH



Matriz Recibidos ×

PATRICIO JAVIER RUIZ ANDINO <patricio.ruiz@espoch.edu.ec> vie,
para Oscar, mi

Estimado, Danilo:

A la presente adjunto los entregables de auditoria COBIT.

Saludos
Patricio J. Ruiz A.

4 archivos adjuntos · Analizado por Gmail

Entregables Audit... | sensibilidad al ca... | Certificación apli... | Entregables Audit...

Plan General de Auditoría COBIT 4.1

Objetivo: Evaluar el cumplimiento de las políticas corporativas en cuanto a la gestión de la seguridad VoIP
Naturaleza: Procedimientos internos
Alcance: ESPOCH
Plazo: 6 semanas

No.	Procedimiento	Hoja de Trabajo	Nombre del auditor	Fecha Inicio	Tiempo efectivo minutos
1	PLANIFICACIÓN Y ALCANCE DE LA AUDITORÍA	Cobit_H1	Patricio Javier Ruiz Andino Julio Enrique Jara Obregón	1/4/2024	1870
2	PASOS PREPARATORIOS	Cobit_H2	Patricio Javier Ruiz Andino Julio Enrique Jara Obregón	6/5/2024	765
3	GOBERNANZA	Cobit_H3	Patricio Javier Ruiz Andino Julio Enrique Jara Obregón	15/5/2024	1745
4	CONFIGURACIÓN DE SERVIDORES	Cobit_H4	Patricio Javier Ruiz Andino Julio Enrique Jara Obregón	24/6/2024	1200
5	RED	Cobit_H5	Patricio Javier Ruiz Andino Julio Enrique Jara Obregón	10/7/2024	260
6	PLANIFICACIÓN DE CONTINGENCIAS	Cobit_H6	Patricio Javier Ruiz Andino Julio Enrique Jara Obregón	16/7/2024	240
7	CULTURA DE SEGURIDAD	Cobit_H7	Patricio Javier Ruiz Andino Julio Enrique Jara Obregón	22/7/2024	360
8	EVALUACIÓN DE MADUREZ	Cobit_H8	Patricio Javier Ruiz Andino Julio Enrique Jara Obregón	23/7/2024	1400
				Total	**7840**

Patricio Javier Ruiz Andino
0602934804
Auditor

Julio Enrique Jara Obregón
0603020561
Auditor

Certificación de aplicación de Auditoría de Seguridad COBIT 4.1

Riobamba, 23 de agosto de 2024.

A quien corresponda,

Quienes suscribimos la presente nos permitimos certificar que se llevó a cabo la aplicación de la Auditoría de Seguridad VoIP mediate COBIT 4.1 en la Dirección de Tecnologías de la Información y Comunicación DTIC de la Escuela Superior Politécnica de Chimborazo ESPOCH, en cumplimiento de los lineamientos establecidos en el marco de trabajo COBIT 4.1.

La ejecución del marco de trabajo COBIT 4.1 se llevó a cabo en el período Abril 2024 - Agosto 2024, y se centró en la evaluación de la seguridad de los sistemas de comunicación VoIP de la DTIC-ESPOCH. Durante la auditoría, se identificaron y analizaron diversos aspectos críticos de seguridad, proponiendo las mejoras necesarias para optimizar la protección de estos sistemas.

Los resultados y conclusiones de dicha auditoría han sido debidamente registrados y entregados al Ing. Oscar Danilo Gavilánez Alvarez como aporte para su tesis doctoral.

Atentamente,



Ing. Patricio Javier Ruiz Andino
Analista de infraestructura, de tecnologías de la información
y la comunicación DTIC- ESPOCH
Cédula: 0602934804



Ing. Julio Enrique Jara Obregón
Analista de soporte y mantenimiento DTIC- ESPOCH
Cédula: 0603020561

Anexo I. Alfa de Cronbach global y por sección obtenidos mediante SPSS

Alfa de Cronbach global. Fiabilidad

Notas

Salida creada		03-SEP-2024 23:05:01
Comentarios		
Entrada	Conjunto de datos activo	Conjunto_de_datos1
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	4
	Entrada de matriz	
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se tratan como perdidos.
	Casos utilizados	Las estadísticas se basan en todos los casos con datos válidos para todas las variables en el procedimiento.
Sintaxis		RELIABILITY /VARIABLES=P1 P2 P3 P4 P5 P6 P7 P8 P9 P10 P11 P12 P13 P14 P15 P16 P17 P18 P19 P20 P21 P22 P23 P24 P25 P26 P27 /SCALE('ALL VARIABLES') ALL /MODEL=ALPHA /STATISTICS=DESCRIPTIVE /SUMMARY=MEANS VARIANCE.
Recursos	Tiempo de procesador	00:00:00,00
	Tiempo transcurrido	00:00:00,00

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	4	100,0
	Excluido[a]	0	,0
	Total	4	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,978	,982	27

Estadísticas de elemento

	Media	Desviación estándar	N
P1	4,00	,816	4
P2	4,00	,816	4
P3	4,50	,577	4
P4	2,00	1,155	4
P5	4,00	,816	4
P6	4,00	,816	4
P7	4,00	,816	4
P8	3,25	,957	4
P9	4,25	,957	4

P10	3,75	1,500	4
P11	4,00	,816	4
P12	4,00	,816	4
P13	4,75	,500	4
P14	4,50	,577	4
P15	4,00	,816	4
P16	3,50	,577	4
P17	4,00	,816	4
P18	4,25	,500	4
P19	4,25	,957	4
P20	2,50	1,732	4
P21	4,00	,816	4
P22	4,00	,816	4
P23	4,75	,500	4
P24	4,75	,500	4
P25	4,00	,816	4
P26	4,25	,957	4
P27	3,25	,957	4

Estadísticas de elemento de resumen

	Media	Mínimo	Máximo	Rango	Máximo / Mínimo	Varianza
Medias de elemento	3,944	2,000	4,750	2,750	2,375	,386
Varianzas de elemento	,784	,250	3,000	2,750	12,000	,360

Estadísticas de elemento de resumen

	N de elementos
Medias de elemento	27
Varianzas de elemento	27

Alfa de Cronbach Sección A

Fiabilidad

Notas

Salida creada		03-SEP-2024 22:49:53
Comentarios		
Entrada	Conjunto de datos activo	Conjunto_de_datos1
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	4
	Entrada de matriz	
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se tratan como perdidos.
	Casos utilizados	Las estadísticas se basan en todos los casos con datos válidos para todas las variables en el procedimiento.

Sintaxis		RELIABILITY /VARIABLES=P1 P2 P3 P4 P5 P6 P7 /SCALE('ALL VARIABLES') ALL /MODEL=ALPHA /STATISTICS=DESCRIPTIVE /SUMMARY=MEANS VARIANCE.
Recursos	Tiempo de procesador	00:00:00,02
	Tiempo transcurrido	00:00:00,02

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	4	100,0
	Excluido[a]	0	,0
	Total	4	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,913	,920	7

Estadísticas de elemento

	Media	Desviación estándar	N
P1	4,00	,816	4
P2	4,00	,816	4
P3	4,50	,577	4
P4	2,00	1,155	4
P5	4,00	,816	4
P6	4,00	,816	4
P7	4,00	,816	4

Estadísticas de elemento de resumen

	Media	Mínimo	Máximo	Rango	Máximo / Mínimo	Varianza
Medias de elemento	3,786	2,000	4,500	2,500	2,250	,655
Varianzas de elemento	,714	,333	1,333	1,000	4,000	,090

Estadísticas de elemento de resumen

	N de elementos
Medias de elemento	7
Varianzas de elemento	7

Alfa de Cronbach Sección B

Fiabilidad

Notas

Salida creada	03-SEP-2024 23:00:24
Comentarios	

Entrada	Conjunto de datos activo	Conjunto_de_datos1
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	4
	Entrada de matriz	
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se tratan como perdidos.
	Casos utilizados	Las estadísticas se basan en todos los casos con datos válidos para todas las variables en el procedimiento.
Sintaxis		RELIABILITY /VARIABLES=P8 P9 P10 /SCALE('ALL VARIABLES') ALL /MODEL=ALPHA /STATISTICS=DESCRIPTIVE /SUMMARY=MEANS VARIANCE.
Recursos	Tiempo de procesador	00:00:00,00
	Tiempo transcurrido	00:00:00,00

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	4	100,0
	Excluido[a]	0	,0

Total	4	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,971	,997	3

Estadísticas de elemento

	Media	Desviación estándar	N
P8	3,25	,957	4
P9	4,25	,957	4
P10	3,75	1,500	4

Estadísticas de elemento de resumen

	Media	Mínimo	Máximo	Rango	Máximo / Mínimo	Varianza
Medias de elemento	3,750	3,250	4,250	1,000	1,308	,250
Varianzas de elemento	1,361	,917	2,250	1,333	2,455	,593

Estadísticas de elemento de resumen

	N de elementos
Medias de elemento	3
Varianzas de elemento	3

Alfa de Cronbach Sección C

Fiabilidad

Notas

Salida creada		03-SEP-2024 23:01:33
Comentarios		
Entrada	Conjunto de datos activo	Conjunto_de_datos1
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	4
	Entrada de matriz	
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se tratan como perdidos.
	Casos utilizados	Las estadísticas se basan en todos los casos con datos válidos para todas las variables en el procedimiento.
Sintaxis		RELIABILITY /VARIABLES=P11 P12 P13 P14 P15 /SCALE('ALL VARIABLES') ALL /MODEL=ALPHA /STATISTICS=DESCRIPTIVE /SUMMARY=MEANS VARIANCE.
Recursos	Tiempo de procesador	00:00:00,02
	Tiempo transcurrido	00:00:00,01

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	4	100,0
	Excluido[a]	0	,0
	Total	4	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,954	,957	5

Estadísticas de elemento

	Media	Desviación estándar	N
P11	4,00	,816	4
P12	4,00	,816	4
P13	4,75	,500	4
P14	4,50	,577	4
P15	4,00	,816	4

Estadísticas de elemento de resumen

	Media	Mínimo	Máximo	Rango	Máximo / Mínimo	Varianza
Medias de elemento	4,250	4,000	4,750	,750	1,188	,125

Varianzas de elemento	,517	,250	,667	,417	2,667	,043

Estadísticas de elemento de resumen

	N de elementos
Medias de elemento	5
Varianzas de elemento	5

Alfa de Cronbach Sección D

Fiabilidad

Notas

Salida creada		03-SEP-2024 23:02:48
Comentarios		
Entrada	Conjunto de datos activo	Conjunto_de_datos1
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	4
	Entrada de matriz	
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se tratan como perdidos.
	Casos utilizados	Las estadísticas se basan en todos los casos con datos válidos para todas las variables en el procedimiento.

Sintaxis		RELIABILITY /VARIABLES=P16 P17 P18 P19 P20 /SCALE('ALL VARIABLES') ALL /MODEL=ALPHA /STATISTICS=DESCRIPTIVE /SUMMARY=MEANS VARIANCE.
Recursos	Tiempo de procesador	00:00:00,02
	Tiempo transcurrido	00:00:00,01

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	4	100,0
	Excluido[a]	0	,0
	Total	4	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,870	,912	5

Estadísticas de elemento

	Media	Desviación estándar	N
P16	3,50	,577	4
P17	4,00	,816	4
P18	4,25	,500	4
P19	4,25	,957	4
P20	2,50	1,732	4

Estadísticas de elemento de resumen

	Media	Mínimo	Máximo	Rango	Máximo / Mínimo	Varianza
Medias de elemento	3,700	2,500	4,250	1,750	1,700	,544
Varianzas de elemento	1,033	,250	3,000	2,750	12,000	1,280

Estadísticas de elemento de resumen

	N de elementos
Medias de elemento	5
Varianzas de elemento	5

Alfa de Cronbach Sección E

Fiabilidad

Notas

Salida creada		03-SEP-2024 23:03:55
Comentarios		
Entrada	Conjunto de datos activo	Conjunto_de_datos1
	Filtro	<ninguno>

	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	4
	Entrada de matriz	
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se tratan como perdidos.
	Casos utilizados	Las estadísticas se basan en todos los casos con datos válidos para todas las variables en el procedimiento.
Sintaxis		RELIABILITY /VARIABLES=P21 P22 P23 P24 P25 P26 P27 /SCALE('ALL VARIABLES') ALL /MODEL=ALPHA /STATISTICS=DESCRIPTIVE /SUMMARY=MEANS VARIANCE.
Recursos	Tiempo de procesador	00:00:00,00
	Tiempo transcurrido	00:00:00,00

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	4	100,0
	Excluido[a]	0	,0
	Total	4	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,886	,900	7

Estadísticas de elemento

	Media	Desviación estándar	N
P21	4,00	,816	4
P22	4,00	,816	4
P23	4,75	,500	4
P24	4,75	,500	4
P25	4,00	,816	4
P26	4,25	,957	4
P27	3,25	,957	4

Estadísticas de elemento de resumen

	Media	Mínimo	Máximo	Rango	Máximo / Mínimo	Varianza
Medias de elemento	4,143	3,250	4,750	1,500	1,462	,268
Varianzas de elemento	,619	,250	,917	,667	3,667	,076

Estadísticas de elemento de resumen

	N de elementos
Medias de elemento	7
Varianzas de elemento	7

Anexo J. Prueba T Estudio de caso

Sección A. Prueba T

Prueba T

Notas

Salida creada		04-SEP-2024 01:49:07
Comentarios		
Entrada	Conjunto de datos activo	Conjunto_de_datos7
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	28
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se trata como valores perdidos.
	Casos utilizados	Las estadísticas para cada análisis se basan en los casos sin datos perdidos o fuera de rango para cualquier variable del análisis.
Sintaxis		T-TEST GROUPS=modelo('COB' 'SAM') /MISSING=ANALYSIS /VARIABLES=respuesta /CRITERIA=CI(.95).
Recursos	Tiempo de procesador	00:00:00,00
	Tiempo transcurrido	00:00:00,00

[Conjunto_de_datos7]

Estadísticas de grupo

	modelo	N	Media	Desviación estándar	Media de error estándar
respuesta	COB	14	3,214	1,0509	,2809
	SAM	14	4,357	,7449	,1991

Prueba de muestras independientes

		Prueba de Levene de calidad de varianzas		prueba t para la igualdad de medias	
		F	Sig.	t	gl
respuesta	Se asumen varianzas iguales	,520	,477	-3,320	26
	No se asumen varianzas iguales			-3,320	23,431

Prueba de muestras independientes

		prueba t para la igualdad de medias		
		Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar
respuesta	Se asumen varianzas iguales	,003	-1,1429	,3443
	No se asumen varianzas iguales	,003	-1,1429	,3443

Prueba de muestras independientes

		prueba t para la igualdad de medias	
		95% de intervalo de confianza de la diferencia	
		Inferior	Superior
respuesta	Se asumen varianzas iguales	-1,8505	-,4352
	No se asumen varianzas iguales	-1,8543	-,4314

Sección B. Prueba T

Prueba T

Notas

Salida creada		04-SEP-2024 02:22:47
Comentarios		
Entrada	Conjunto de datos activo	Conjunto_de_datos8
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	12
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se trata como valores perdidos.
	Casos utilizados	Las estadísticas para cada análisis se basan en los casos sin datos perdidos o fuera de rango para cualquier variable del análisis.
Sintaxis		T-TEST GROUPS=modelo('COB' 'SAM') /MISSING=ANALYSIS /VARIABLES=respuesta /CRITERIA=CI(.95).
Recursos	Tiempo de procesador	00:00:00,00
	Tiempo transcurrido	00:00:00,00

Estadísticas de grupo

modelo	N	Media	Desviación estándar	Media de error estándar

respuesta	COB	6	2,83	,753	,307
	SAM	6	4,67	,516	,211

Prueba de muestras independientes

		Prueba de Levene de calidad de varianzas		prueba t para la igualdad de medias	
		F	Sig.	t	gl
respuesta	Se asumen varianzas iguales	,328	,580	-4,919	10
	No se asumen varianzas iguales			-4,919	8,853

Prueba de muestras independientes

		prueba t para la igualdad de medias		
		Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar
respuesta	Se asumen varianzas iguales	,001	-1,833	,373
	No se asumen varianzas iguales	,001	-1,833	,373

Prueba de muestras independientes

		prueba t para la igualdad de medias	
		95% de intervalo de confianza de la diferencia	
		Inferior	Superior
respuesta	Se asumen varianzas iguales	-2,664	-1,003
	No se asumen varianzas iguales	-2,679	-,988

Sección C. Prueba T

Prueba T

Notas

Salida creada		04-SEP-2024 02:33:00
Comentarios		
Entrada	Conjunto de datos activo	Conjunto_de_datos10
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	20
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se trata como valores perdidos.
	Casos utilizados	Las estadísticas para cada análisis se basan en los casos sin datos perdidos o fuera de rango para cualquier variable del análisis.
Sintaxis		T-TEST GROUPS=modelo('COB' 'SAM') /MISSING=ANALYSIS /VARIABLES=respuesta /CRITERIA=CI(.95).
Recursos	Tiempo de procesador	00:00:00,00
	Tiempo transcurrido	00:00:00,09

Estadísticas de grupo

modelo	N	Media	Desviación estándar	Media de error estándar

respuesta	COB	10	3,80	,632	,200
	SAM	10	4,70	,483	,153

Prueba de muestras independientes

		Prueba de Levene de calidad de varianzas		prueba t para la igualdad de medias	
		F	Sig.	t	gl
respuesta	Se asumen varianzas iguales	,199	,661	-3,576	18
	No se asumen varianzas iguales			-3,576	16,834

Prueba de muestras independientes

		prueba t para la igualdad de medias		
		Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar
respuesta	Se asumen varianzas iguales	,002	-,900	,252
	No se asumen varianzas iguales	,002	-,900	,252

Prueba de muestras independientes

		prueba t para la igualdad de medias	
		95% de intervalo de confianza de la diferencia	
		Inferior	Superior
respuesta	Se asumen varianzas iguales	-1,429	-,371
	No se asumen varianzas iguales	-1,431	-,369

Sección D. Prueba T

Prueba T

Notas

Salida creada		04-SEP-2024 02:36:57
Comentarios		
Entrada	Conjunto de datos activo	Conjunto_de_datos12
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	20
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se trata como valores perdidos.
	Casos utilizados	Las estadísticas para cada análisis se basan en los casos sin datos perdidos o fuera de rango para cualquier variable del análisis.
Sintaxis		T-TEST GROUPS=modelo('COB' 'SAM') /MISSING=ANALYSIS /VARIABLES=respuesta /CRITERIA=CI(.95).
Recursos	Tiempo de procesador	00:00:00,00
	Tiempo transcurrido	00:00:00,00

Estadísticas de grupo

modelo	N	Media	Desviación estándar	Media de error estándar

respuesta	COB	10	3,00	1,155	,365
	SAM	10	4,40	,516	,163

Prueba de muestras independientes

		Prueba de Levene de calidad de varianzas		prueba t para la igualdad de medias	
		F	Sig.	t	gl
respuesta	Se asumen varianzas iguales	1,618	,220	-3,500	18
	No se asumen varianzas iguales			-3,500	12,462

Prueba de muestras independientes

		prueba t para la igualdad de medias		
		Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar
respuesta	Se asumen varianzas iguales	,003	-1,400	,400
	No se asumen varianzas iguales	,004	-1,400	,400

Prueba de muestras independientes

		prueba t para la igualdad de medias	
		95% de intervalo de confianza de la diferencia	
		Inferior	Superior
respuesta	Se asumen varianzas iguales	-2,240	-,560
	No se asumen varianzas iguales	-2,268	-,532

Sección E. Prueba T

Prueba T

Notas

Salida creada		04-SEP-2024 02:38:50
Comentarios		
Entrada	Conjunto de datos activo	Conjunto_de_datos13
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	28
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se trata como valores perdidos.
	Casos utilizados	Las estadísticas para cada análisis se basan en los casos sin datos perdidos o fuera de rango para cualquier variable del análisis.
Sintaxis		T-TEST GROUPS=modelo('COB' 'SAM') /MISSING=ANALYSIS /VARIABLES=respuesta /CRITERIA=CI(.95).
Recursos	Tiempo de procesador	00:00:00,02
	Tiempo transcurrido	00:00:00,02

Estadísticas de grupo

	modelo	N	Media	Desviación estándar	Media de error estándar

respuesta	COB	14	3,64	,842	,225
	SAM	14	4,64	,497	,133

Prueba de muestras independientes

		Prueba de Levene de calidad de varianzas		prueba t para la igualdad de medias	
		F	Sig.	t	gl
respuesta	Se asumen varianzas iguales	3,664	,067	-3,827	26
	No se asumen varianzas iguales			-3,827	21,086

Prueba de muestras independientes

		prueba t para la igualdad de medias		
		Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar
respuesta	Se asumen varianzas iguales	,001	-1,000	,261
	No se asumen varianzas iguales	,001	-1,000	,261

Prueba de muestras independientes

		prueba t para la igualdad de medias	
		95% de intervalo de confianza de la diferencia	
		Inferior	Superior
respuesta	Se asumen varianzas iguales	-1,537	-,463
	No se asumen varianzas iguales	-1,543	-,457

Anexo K. Prueba t - HS1

Prueba T

Notas

Salida creada		25-MAR-2025 23:58:40
Comentarios		
Entrada	Conjunto de datos activo	Conjunto_de_datos2
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	4
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se trata como valores perdidos.
	Casos utilizados	Las estadísticas para cada análisis se basan en los casos sin datos perdidos o fuera de rango para cualquier variable del análisis.
Sintaxis		T-TEST PAIRS=COBIT4.1 WITH VoIPSAM (PAIRED) /CRITERIA=CI(.9500) /MISSING=ANALYSIS.
Recursos	Tiempo de procesador	00:00:00,02
	Tiempo transcurrido	00:00:00,03

[Conjunto_de_datos2]

Estadísticas de muestras emparejadas

		Media	N	Desviación estándar	Media de error estándar
Par 1	COBIT 4.1	861,25	4	740,094	370,047
	VoIPSAM	726,25	4	754,656	377,328

Correlaciones de muestras emparejadas

		N	Correlación	Sig.
Par 1	COBIT 4.1 & VoIPSAM	4	1,000	,000

Prueba de muestras emparejadas

		Diferencias emparejadas			
					95% de intervalo de confianza de la diferencia
		Media	Desviación estándar	Media de error estándar	Inferior
Par 1	COBIT 4.1 - VoIPSAM	135,000	17,795	8,898	106,684

Prueba de muestras emparejadas

		Diferencias emparejadas			
		95% de intervalo de confianza de la diferencia			
		Superior	t	gl	Sig. (bilateral)
Par 1	COBIT 4.1 - VoIPSAM	163,316	15,173	3	,001

Anexo L. Prueba t – HS3

Prueba T

Notas

Salida creada		26-MAR-2025 01:15:25
Comentarios		
Entrada	Conjunto de datos activo	Conjunto_de_datos12
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	24
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se trata como valores perdidos.
	Casos utilizados	Las estadísticas para cada análisis se basan en los casos sin datos perdidos o fuera de rango para cualquier variable del análisis.
Sintaxis		T-TEST GROUPS=Grupo(1 2) /MISSING=ANALYSIS /VARIABLES=respuesta /CRITERIA=CI(.95).
Recursos	Tiempo de procesador	00:00:00,00
	Tiempo transcurrido	00:00:00,04

[Conjunto_de_datos12]

Estadísticas de grupo

	Grupo	N	Media	Desviación estándar	Media de error estándar
respuesta	1	12	2,75	1,485	,429
	2	12	4,42	,793	,229

Prueba de muestras independientes

		Prueba de Levene de calidad de varianzas		prueba t para la igualdad de medias	
		F	Sig.	t	gl
respuesta	Se asumen varianzas iguales	8,822	,007	-3,430	22
	No se asumen varianzas iguales			-3,430	16,803

Prueba de muestras independientes

		prueba t para la igualdad de medias		
		Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar
respuesta	Se asumen varianzas iguales	,002	-1,667	,486
	No se asumen varianzas iguales	,003	-1,667	,486

Prueba de muestras independientes

	prueba t para la igualdad de medias

		95% de intervalo de confianza de la diferencia	
		Inferior	Superior
respuesta	Se asumen varianzas iguales	-2,674	-,659
	No se asumen varianzas iguales	-2,693	-,641

Anexo M. Eficiencia Shapiro-Wilk - Prueba t

Explorar

Notas

Salida creada		03-SEP-2024 23:57:25
Comentarios		
Entrada	Datos	D:\PERU 2023\PROTOCOLO CASO DE ESTUDIO\ESTADISTICA Eficiencia\Datos_eficiencia.sav
	Conjunto de datos activo	Conjunto_de_datos1
	Filtro	<ninguno>
	Ponderación	<ninguno>
	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	8
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario para variables dependientes se tratan como perdidos.
	Casos utilizados	Los estadísticos se basan en casos sin valores perdidos para ninguna de la variable dependiente o factor utilizado.

Sintaxis		EXAMINE VARIABLES=COBIT4.1 VoIPSAM /PLOT BOXPLOT STEMLEAF NPPLOT /COMPARE GROUPS /STATISTICS DESCRIPTIVES /CINTERVAL 95 /MISSING LISTWISE /NOTOTAL.
Recursos	Tiempo de procesador	00:00:00,69
	Tiempo transcurrido	00:00:00,69

Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
COBIT 4.1	8	100,0%	0	0,0%	8	100,0%
VoIPSAM	8	100,0%	0	0,0%	8	100,0%

Descriptivos

			Estadístico	Error estándar
COBIT 4.1	Media		980,00	235,234
	95% de intervalo de confianza para la media	Límite inferior	423,76	
		Límite superior	1536,24	
	Media recortada al 5%		971,67	

	Mediana		982,50	
	Varianza		442678,571	
	Desviación estándar		665,341	
	Mínimo		240	
	Máximo		1870	
	Rango		1630	
	Rango intercuartil		1374	
	Asimetría		,136	,752
	Curtosis		-1,887	1,481
VoIPSAM	Media		801,25	228,664
	95% de intervalo de confianza para la media	Límite inferior	260,55	
		Límite superior	1341,95	
	Media recortada al 5%		788,61	
	Mediana		737,50	
	Varianza		418298,214	
	Desviación estándar		646,760	
	Mínimo		80	
	Máximo		1750	
	Rango		1670	
	Rango intercuartil		1324	
	Asimetría		,425	,752
	Curtosis		-1,313	1,481

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
COBIT 4.1	,199	8	,200*	,892	8	,245
VoIPSAM	,165	8	,200*	,912	8	,372

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

COBIT 4.1

COBIT 4.1 Stem-and-Leaf Plot

Frequency Stem & Leaf

3,00 0 . 223

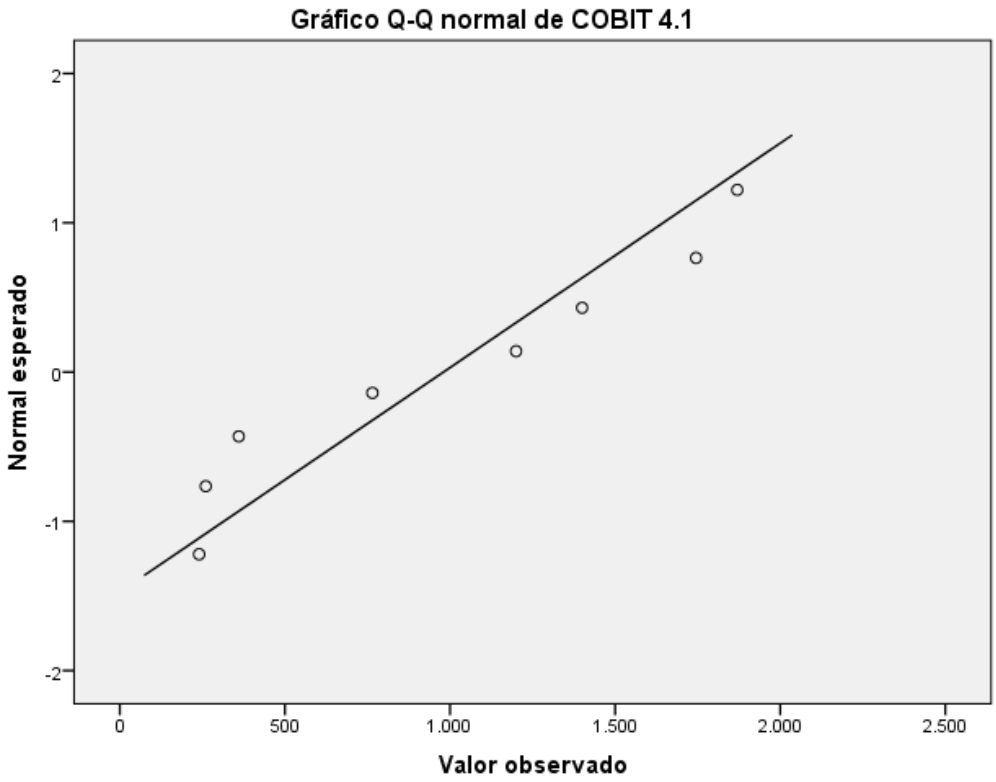
1,00 0 . 7

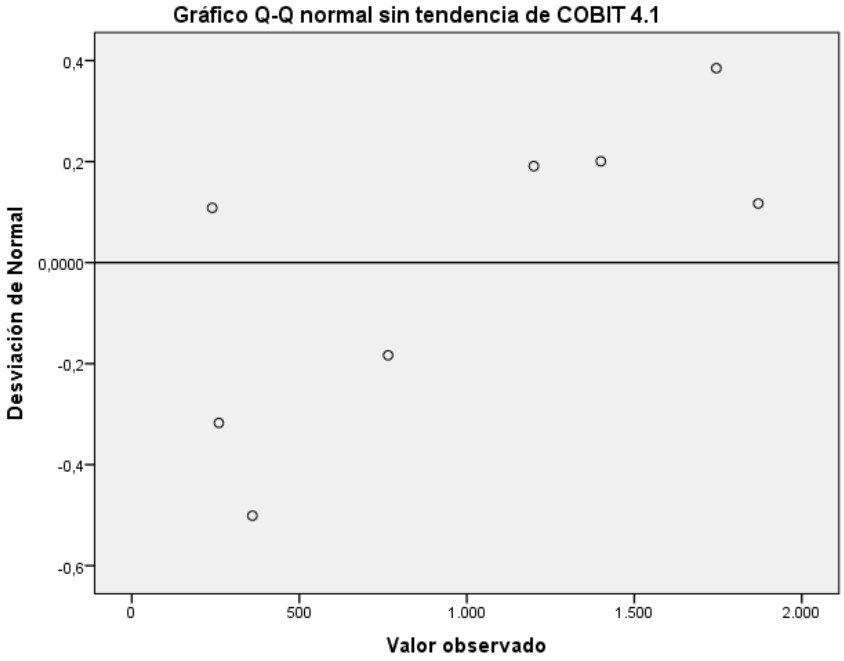
2,00 1 . 24

2,00 1 . 78

Stem width: 1000

Each leaf: 1 case(s)


Gráfico Q-Q normal de COBIT 4.1
Normal esperado
Valor observado
2
1
0
-1
-2
0
500
1.000
1.500
2.000
2.500


Gráfico Q-Q normal sin tendencia de COBIT 4.1
Desviación de Normal
Valor observado
0,4
0,2
0,0000
-0,2
-0,4
-0,6
0
500
1.000
1.500
2.000



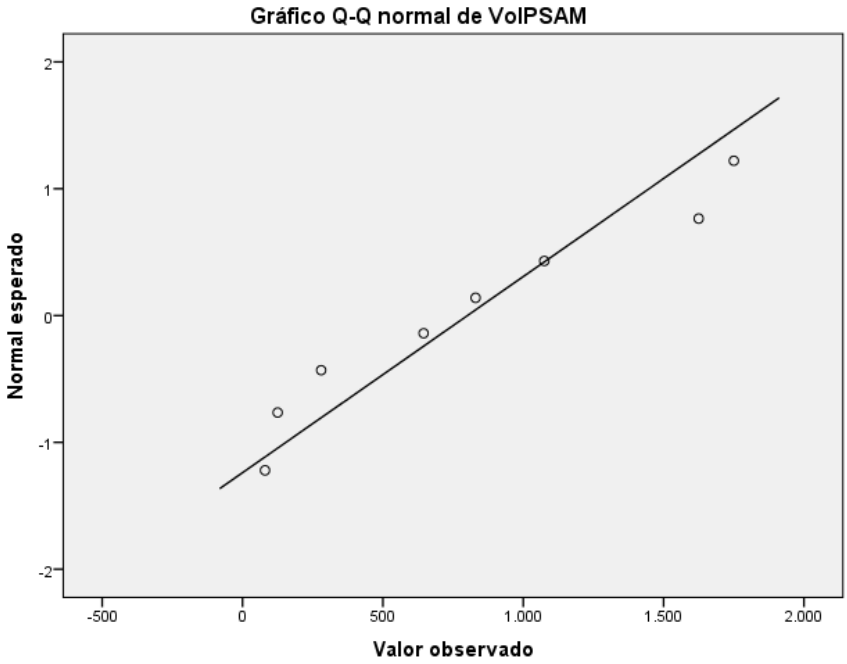
VoIPSAM

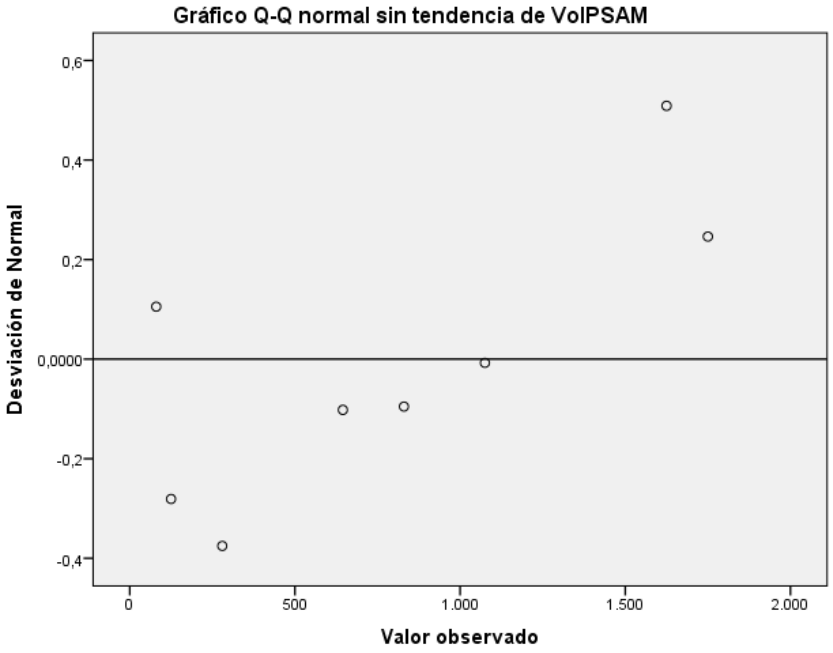
VoIPSAM Stem-and-Leaf Plot

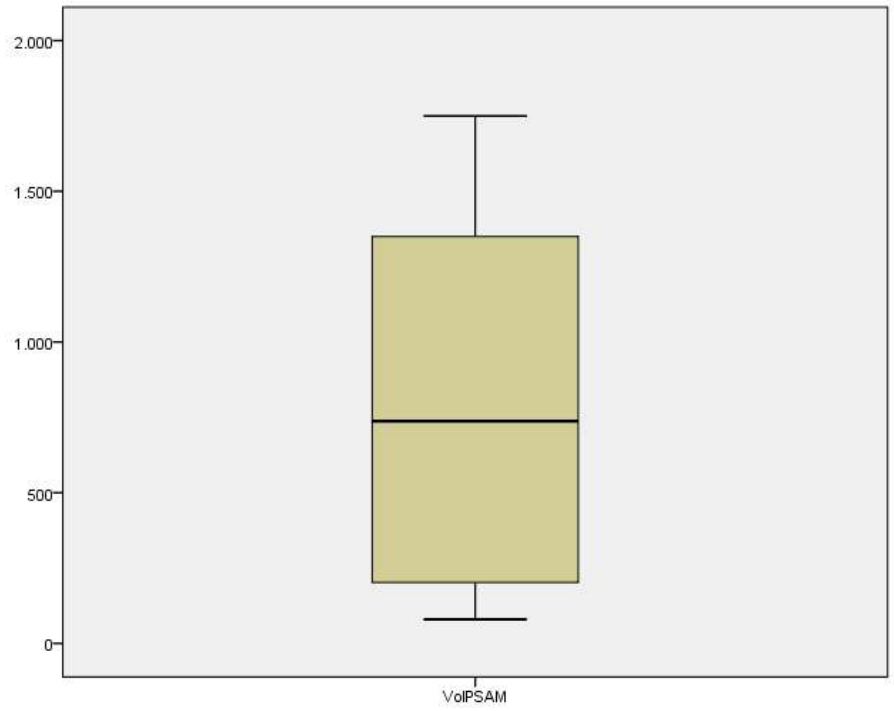
Frequency	Stem &	Leaf
3,00	0 .	012
2,00	0 .	68
1,00	1 .	0
2,00	1 .	67

Stem width: 1000

Each leaf: 1 case(s)


Gráfico Q-Q normal de VolPSAM
Normal esperado
2
1
0
-1
-2
-500
0
500
1.000
1.500
2.000
Valor observado


Gráfico Q-Q normal sin tendencia de VolPSAM
Desviación de Normal
0,6
0,4
0,2
0,0000
-0,2
-0,4
0
500
1.000
1.500
2.000
Valor observado




```
T-TEST PAIRS=COBIT4.1 WITH VoIPSAM (PAIRED)
  /CRITERIA=CI(.9500)
  /MISSING=ANALYSIS.
```

Prueba T

Notas

Salida creada		03-SEP-2024 23:57:46
Comentarios		
Entrada	Datos	D:\PERU 2023\PROTOCOLO CASO DE ESTUDIO\ESTADISTICA Eficiencia\Datos_eficiencia.sav
	Conjunto de datos activo	Conjunto_de_datos1
	Filtro	<ninguno>
	Ponderación	<ninguno>

	Segmentar archivo	<ninguno>
	N de filas en el archivo de datos de trabajo	8
Manejo de valor perdido	Definición de ausencia	Los valores perdidos definidos por el usuario se trata como valores perdidos.
	Casos utilizados	Las estadísticas para cada análisis se basan en los casos sin datos perdidos o fuera de rango para cualquier variable del análisis.
Sintaxis		T-TEST PAIRS=COBIT4.1 WITH VoIPSAM (PAIRED) /CRITERIA=CI(.9500) /MISSING=ANALYSIS.
Recursos	Tiempo de procesador	00:00:00,02
	Tiempo transcurrido	00:00:00,01

Estadísticas de muestras emparejadas

		Media	N	Desviación estándar	Media de error estándar
Par 1	COBIT 4.1	980,00	8	665,341	235,234
	VoIPSAM	801,25	8	646,760	228,664

Correlaciones de muestras emparejadas

		N	Correlación	Sig.
Par 1	COBIT 4.1 & VoIPSAM	8	,971	,000

Prueba de muestras emparejadas

		Diferencias emparejadas			
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia
					Inferior
Par 1	COBIT 4.1 - VoIPSAM	178,750	159,614	56,432	45,309

Prueba de muestras emparejadas

		Diferencias emparejadas			
		95% de intervalo de confianza de la diferencia	t	gl	Sig. (bilateral)
		Superior			
Par 1	COBIT 4.1 - VoIPSAM	312,191	3,168	7	,016

Anexo N. Artículos Publicados

Artículo: Audit Analysis Models, Security Frameworks and Their Relevance for VoIP.

Referencia:

Gavilanez, O., Rodriguez, G., & Gavilanez, F. (2017). *Audit Analysis Models, Security Frameworks and Their Relevance for VoIP*. https://doi.org/10.48550/arXiv.1704.02440

Título: Audit Analysis Models, Security Frameworks and Their Relevance for VoIP

Autores: Oscar Gavilanez, Glen Rodríguez, Franklin Gavilanez

Revista / Conferencia: 12th International Conference on Cyber Warfare and Security - ICCWS 2017, At Dayton, USA

Indexación: Scopus

DOI: https://doi.org/10.48550/arXiv.1704.02440

Estado: Publicado

Audit Analysis Models, Security Frameworks and Their Relevance for VoIP

Oscar Gavilanez[1,2], Glen Rodriguez[2] and Franklin Gavilanez[3]
[1]Systems Engineering, Escuela Superior Politécnica de Chimborazo ESPOCH, Ecuador
[2]Systems Engineering, Universidad Nacional Mayor de San Marcos UNMSM, Peru
[3]Mathematics, Montgomery College, USA
oscar.gavilanez@unmsm.edu.pe
glen.rodriguez@gmail.com
franklin.gavilanez@montgomerycollege.edu

Abstract: Voice over IP (VoIP) is the transmission of voice and multimedia content over Internet Protocol (IP) networks, this paper reviews models, frameworks and auditing standards proposed to this date to manage VoIP security through a literature review, with descriptions of both the historical and philosophical evolution reflecting an adequate knowledge of related research. Three research questions are raised here: RQ1. What are the requirements to be met by a model of security audit in VoIP systems to achieve their goals? RQ2. Today, are there additional attacks that previous works have not considered? RQ3. Which security requirements in the VoIP systems are covered (and which are not covered) by security frameworks? After some discussion about VoIP Protocols, Attacks on VoIP, Information Technology (IT) audit, IT security audits, Frameworks and auditing standards, we present a unified view of VoIP Security Requirements; as well as considering the contributions and disadvantages of frameworks and auditing standards toward achieving those requirements through a comparative evaluation. It was determined that there is no security framework which considers social engineering attacks in spite of being an important aspect to consider in security management VoIP; also there is no specific framework that covers all categories of security requirements for VoIP system, therefore, a more extensive model is needed.

Keywords: VoIP security, attacks on VoIP, IT security audit, IT security frameworks, social engineering attacks

1. Introduction

This article aims to analyse models, frameworks and auditing standards for relevance in VoIP systems; and to establish if previous jobs meet all safety requirements in VoIP systems. Three research questions are raised here: RQ1. What are the requirements to be met by a model of security audit in VoIP systems to achieve their goals? RQ2. Today, are there additional attacks that previous works have not considered? RQ3. Which security requirements in the VoIP systems are covered (and which are not covered) by security frameworks?

The paper is organized as follows. Section 2 shows the literature review regarding attacks on VoIP Security, IT security audits, framework and auditing standards, and VoIP Security Requirements. Section 3 deals with approaches and benchmarking of frameworks and standards, requirements and needs of the VoIP management systems. Finally, section 4 concludes with answers to the research questions.

2. Literature review

2.1 Introduction to VoIP

VoIP refers to communication protocols, technologies, methodologies and data transportation involved in the delivery of voice communications and multimedia sessions over the internet, rather than the public switched telephone network (PSTN). The communication voice uses the internet protocol (IP) which is low cost and is a major factor behind VoIP implementations, thus organizations can save thousands of dollars a year by opting for this technology, however, safety related problems should then be considered.

Ibrahim, Abdullah and Dehghantanha (2012) state that VoIP applications combine video and audio data along with the usual data packets traveling within a network system. Users make phone calls using softphones or IP phones (like Skype) and send instant messages through their computer. Geneiatakis, Lambrinoudakis and Kambourakis (2008) state that VoIP infrastructure inherits and uses various protocols of the stack architecture of the Internet, specifically in the network and transport use of Internet Protocol IP, and TCP, UDP or SCTP, respectively.

WRIGHT STATE UNIVERSITY
CHANGING LIVES

AFIT
AIR FORCE INSTITUTE OF TECHNOLOGY

Proceedings of the
12th International Conference on Cyber Warfare and Security

Wright State University with the
Air Force Institute of Technology
Dayton, USA
2-3 March 2017



Edited by
Dr. Adam R. Bryant
Wright State University
Dr. Juan R. Lopez, Jr and Dr. Robert F. Mills
Air Force Institute of Technology

acpi

A conference managed by ACPI, UK

Artículo: VoIP security auditing model based on COBIT 4.1

Referencia:

Gavilanez, O., & Rodriguez, G. (2022). VoIP security auditing model based on COBIT 4.1. *International Journal of Security and Networks*, *17*(2), 63-76. https://doi.org/10.1504/IJSN.2022.123293

Título: VoIP security auditing model based on COBIT 4.1.

Autores: Oscar Gavilanez, Glen Rodríguez

Revista / Conferencia: International Journal of Security and Networks

Indexación: Scopus

Cuartil: Q4

DOI: https://doi.org/10.1504/IJSN.2022.123293

Estado: Publicado

Int. J. Security and Networks, Vol. 17, No. 2, 2022 63

VoIP security auditing model based on COBIT 4.1

Oscar Danilo Gavilánez Alvarez and
Glen Dario Rodriguez Rafael*

Facultad de Ingeniería de Sistemas e Informática,
Universidad Nacional Mayor de San Marcos,
Lima, Peru
Email: oscar.gavilanez@unmsm.edu.pe
Email: grodriguezr@unmsm.edu.pe
*Corresponding author

Abstract: The article justifies the need for a specific model of VoIP security auditing that evaluates the incidence of security problems and addresses the challenges in terms of protecting IT resources. The current VoIP security problems are determined based on the analysis of auditing frameworks, and a model based on COBIT 4.1 is proposed to address these problems. As an innovation, the model includes the security culture plan and social engineering from the approach of the user as an IT service customer. In this work, we present the validation of the surveys using Cronbach's alpha and the results of the statistical average of the surveys applied to experts in social engineering and security auditing in VoIP. The proposed VoIP security auditing model, called VoIPSAM, considers four domains – plan and organise, acquire and implement, delivery and support. and monitor and evaluate – which consider specific security policies for its application.

Keywords: model of security auditing; social engineering; security culture plan; VoIP; COBIT.

Reference to this paper should be made as follows: Gavilánez Alvarez, O.D. and Rodriguez Rafael, G.D. (2022) 'VoIP security auditing model based on COBIT 4.1', *Int. J. Security and Networks*, Vol. 17, No. 2, pp.63–76.

Biographical notes: Oscar Danilo Gavilánez Alvarez received his System Engineer degree and Magister degree in Network Interconnectivity from ESPOCH. He is currently studying his PhD in Systems Engineering and Computer Science at the Universidad Nacional de San Marcos, Lima, Peru. His research interests include: telecommunications, network security, VoIP and SCADA.

Glen Dario Rodriguez Rafael received his Bachelors in 1994 from UNI, Peru, and MSc In 2001 and Dr.Eng. in 2004 by Toyohashi University of Technology , Japan. He is a Professor of Systems Engineering at UNMSM and UNI. His research interests include wireless communication, network security, software testing and evolutionary computing.

1 Introduction

The importance of voice over internet protocol (VoIP), the technology that allows phone calls using the internet, lies in its functionality, multiple features, advantages and cost savings. VoIP is exposed to various security threats that compromise the confidentiality, availability and integrity of the data.

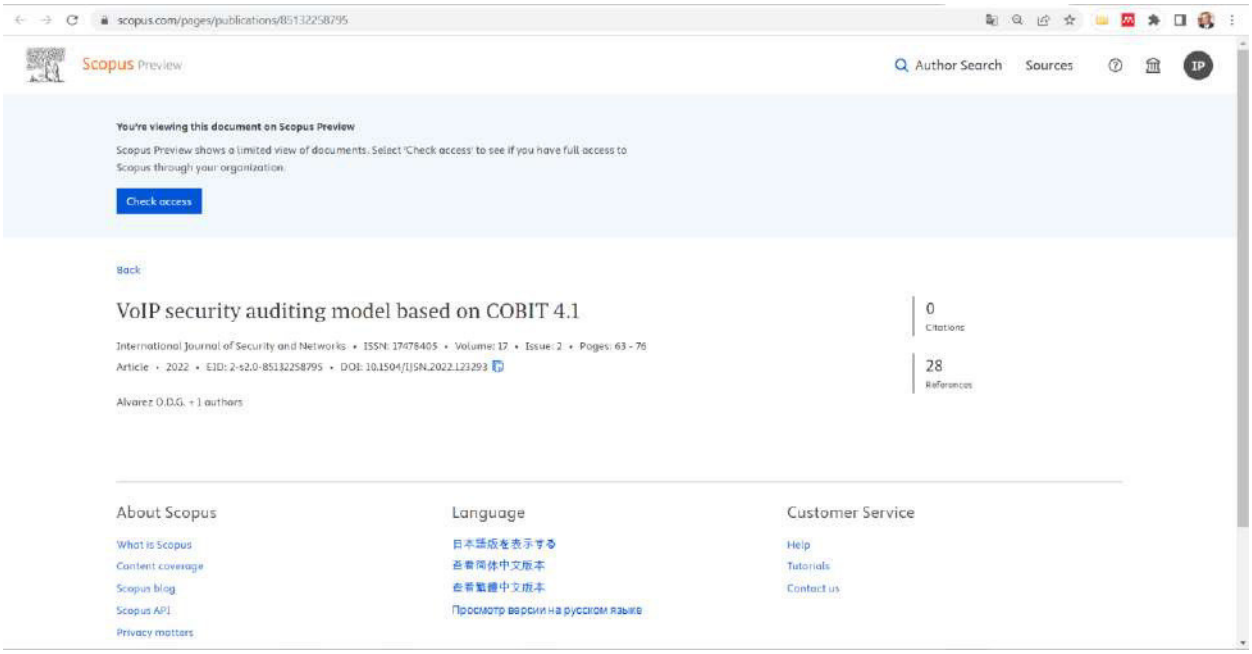
Systems auditing is an information systems (IS) and information technology (IT) review process that enables organisations to identify findings, mitigate risks and implement adequate controls to protect critical and valuable information.

There are multiple risks associated with equipment, information and communication systems that do not have current security controls, which add to the number of internal threats, therefore increasing the risk factor. New systems are developed every day that affect the information security of organisations, making it necessary to have a complete security strategy to prevent leaks and failures in the systems.

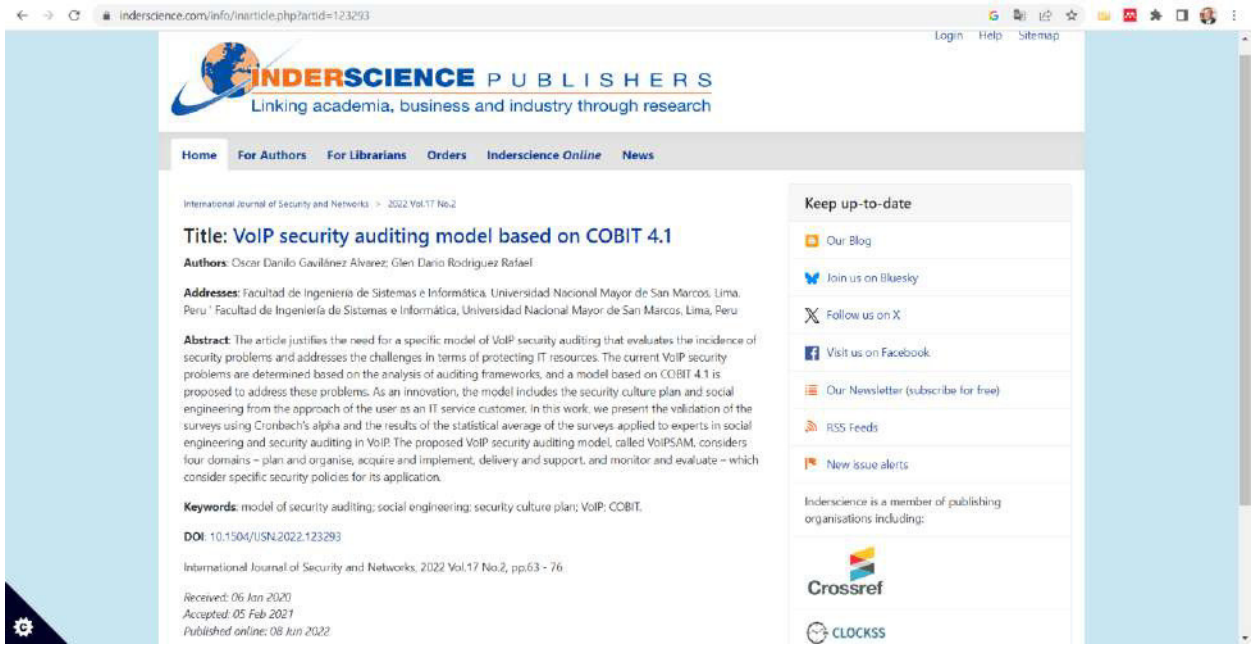
Companies must avoid numerous security risks, including identity theft, information leakage, and fraud, amongst others. Therefore, it is necessary to have in place a framework related to information security such as COBIT 4.1, a standard developed by IS Audit and Control Association (ISACA) that manages governance, control, assurance and auditing processes for ICT on a broad level.

VoIP is a unique system. Consequently, it requires a personalised model that adequately manages the specific communication security risks when using internet protocol (IP). One such risk is social engineering which as mentioned previously, stands in third place (27%) with respect to cyber-attacks according to the 2019 cybersecurity status report prepared by ISACA.

Copyright © 2022 Inderscience Enterprises Ltd.


scopus.com/pages/publications/85132258795
Scopus Preview
Author Search
Sources
You're viewing this document on Scopus Preview
Scopus Preview shows a limited view of documents. Select 'Check access' to see if you have full access to Scopus through your organization.
Check access
Back
VoIP security auditing model based on COBIT 4.1
International Journal of Security and Networks • ISSN: 17478405 • Volume: 17 • Issue: 2 • Pages: 63 - 76
Article • 2022 • EID: 2-s2.0-85132258795 • DOI: 10.1504/IJSN.2022.123293
Alvarez O.D.G. + 1 authors
0
Citations
28
References
About Scopus
What is Scopus
Content coverage
Scopus blog
Scopus API
Privacy matters
Language
日本語版を表示する
查看简体中文版本
查看繁體中文版本
Просмотр версии на русском языке
Customer Service
Help
Tutorials
Contact us


inderscience.com/info/inarticletoc.php?jcode=ijsn&year=2022&vol=17&issue=2
Login
Help
Sitemap
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research
Home
For Authors
For Librarians
Orders
Inderscience Online
News
International Journal of Security and Networks > Published issues > 2022 Vol.17 No.2
International Journal of Security and Networks
2022 Vol.17 No.2
Pages
Title and author(s)
63-76
VoIP security auditing model based on COBIT 4.1
Oscar Danilo Gavilánez Alvarez; Glen Dario Rodriguez Rafael
DOI: 10.1504/IJSN.2022.123293
77-91
Using blockchains to protect critical infrastructures: a comparison between Ethereum and Hyperledger Fabric
Wilson S. Melo Jr.; Lucas S. Dos Santos; Lucila M.S. Bento; Paulo R. Nascimento; Carlos A.R.
Sign up for new issue alerts
Subscribe/buy articles/issues
View sample articles
Copyright and author entitlement
Forthcoming articles
Journal information in easy print format (PDF)
Publishing with Inderscience: ethical statement
Recommend to a librarian (PDF)
Feedback to Editor
Get permission to reproduce content
Find related journals


inderscience.com/info/inarticle.php?artid=123293
Login Help Sitemap
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research
Home For Authors For Librarians Orders Inderscience Online News
International Journal of Security and Networks > 2022 Vol.17 No.2
Title: VoIP security auditing model based on COBIT 4.1
Authors: Oscar Danilo Gavilánez Alvarez; Glen Dario Rodriguez Rafael
Addresses: Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Peru ' Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Peru
Abstract: The article justifies the need for a specific model of VoIP security auditing that evaluates the incidence of security problems and addresses the challenges in terms of protecting IT resources. The current VoIP security problems are determined based on the analysis of auditing frameworks, and a model based on COBIT 4.1 is proposed to address these problems. As an innovation, the model includes the security culture plan and social engineering from the approach of the user as an IT service customer. In this work, we present the validation of the surveys using Cronbach's alpha and the results of the statistical average of the surveys applied to experts in social engineering and security auditing in VoIP. The proposed VoIP security auditing model, called VoIPSAM, considers four domains – plan and organise, acquire and implement, delivery and support, and monitor and evaluate – which consider specific security policies for its application.
Keywords: model of security auditing; social engineering; security culture plan; VoIP; COBIT.
DOI: 10.1504/IJSN.2022.123293
International Journal of Security and Networks, 2022 Vol.17 No.2, pp.63 - 76
Received: 06 Jan 2020
Accepted: 05 Feb 2021
Published online: 08 Jun 2022
Keep up-to-date
Our Blog
Join us on Bluesky
Follow us on X
Visit us on Facebook
Our Newsletter (subscribe for free)
RSS Feeds
New issue alerts
Inderscience is a member of publishing organisations including:
Crossref
CLOCKSS

Anexo O. Encuesta de validación externa EVE. Estudio de caso

Validación Externa de Resultados de Auditorías (COBIT 4.1 vs VoIPSAM)

Propósito: Validar externamente la coherencia metodológica y técnica de los resultados obtenidos en el estudio de caso, comparando un modelo tradicional (COBIT 4.1) y el modelo propuesto (VoIPSAM), desde la perspectiva de expertos externos independientes.

Instrucciones: Lea los archivos del estudio (Resultados completos del estudio de caso, tablas consolidadas de resultados, guías VoIPSAM y COBIT 4.1) y conteste los ítems según su criterio profesional.

Perfil del experto

Esta sección tiene como finalidad caracterizar el perfil académico y profesional de los participantes, así como garantizar su independencia respecto al estudio de caso y al autor.

P0.1. Nombre, Apellido y mail de contacto:

(Indique su nombre, apellido y mail de contacto)

P0.2. País y Universidad de formación doctoral y/o actividad profesional actual:

(Indique el país y la Universidad donde realizó su doctorado o el país donde ejerce actualmente su actividad académica o profesional)

P0.3. Rol principal que desempeña actualmente:

- o Investigador
- o Docente universitario
- o Consultor en seguridad de la información
- o Auditor de sistemas
- o Otro

P0.4. Años de experiencia en seguridad informática:

- 2–5 años
- 6–10 años
- Más de 10 años

P0.5. Experiencia específica en VoIP:

- Investigación
- Auditoría
- Implementación
- Gestión / administración
- No posee experiencia directa

P0.6. Certificaciones relevantes en seguridad de la información o TI (si aplica):

P0.6. Declaración de independencia:

Declaro que mi participación se realiza con criterio técnico y académico independiente, que he evaluado la información proporcionada de manera objetiva, y que no he tenido participación directa en la ejecución de las auditorías analizadas.

- Sí
- No

Eje 1. Coherencia método–resultado

Evalúa si existe correspondencia lógica y metodológica entre el diseño del estudio de caso, los procedimientos aplicados y los resultados obtenidos en las auditorías realizadas con COBIT 4.1 y VoIPSAM. Las preguntas buscan determinar si los resultados reflejan adecuadamente la metodología empleada y si el proceso seguido justifica los hallazgos reportados.

P1. El diseño comparativo (COBIT 4.1 vs. VoIPSAM) es adecuado para explicar las diferencias observadas en los resultados.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo

- De acuerdo
- Muy de acuerdo

P2. Los resultados presentados se derivan lógicamente del método aplicado.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

P3. La selección de técnicas estadísticas empleadas es consistente con el tipo de datos y el diseño del estudio.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

Eje 2. Consistencia interna de los resultados

Analiza la estabilidad y coherencia interna de los resultados obtenidos a lo largo de las diferentes fases de la auditoría. Se pretende verificar si los datos presentan uniformidad, ausencia de contradicciones y alineación entre mediciones parciales y resultados globales.

P4. No se observan contradicciones relevantes entre las distintas tablas y resultados reportados.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

P5. Los resultados por áreas/procesos son coherentes con los resultados globales del estudio.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

P6. La tendencia general de los resultados es estable y consistente a lo largo del análisis.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

Eje 3. Adecuación de los indicadores utilizados

Valora si los indicadores empleados para medir eficiencia temporal, relevancia de las evaluaciones y percepción de vulnerabilidad son pertinentes, claros y suficientes para representar los fenómenos que se desean evaluar en auditorías de seguridad VoIP

P7. El tiempo de ejecución es un indicador adecuado para medir la eficiencia temporal de las auditorías.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

P8. Los indicadores de percepción/relevancia utilizados son apropiados para evaluar los objetivos planteados.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo

- Muy de acuerdo

P9. Los indicadores seleccionados permiten interpretar de forma clara las diferencias entre ambos modelos.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

Eje 4. Correspondencia modelo–resultado (VoIPSAM vs. COBIT 4.1)

Evalúa si los resultados obtenidos guardan relación directa con los componentes del modelo VoIPSAM y con los elementos evaluados mediante COBIT 4.1. Las preguntas buscan verificar que los hallazgos pueden explicarse razonablemente a partir de las características y estructura de los modelos utilizados

P10. Las diferencias de resultados son coherentes con el carácter específico de VoIPSAM frente al carácter generalista de COBIT 4.1.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

P11. La mayor cobertura y focalización reportada es consistente con las características estructurales de VoIPSAM.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

P12. Los resultados reflejan adecuadamente las diferencias conceptuales entre ambos modelos.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

Eje 5. Transferibilidad de los resultados

Analiza si los resultados del estudio de caso pueden ser aplicables o adaptables a otras organizaciones con infraestructuras VoIP, considerando similitudes técnicas, organizacionales y operativas, así como las limitaciones propias del contexto estudiado

P13. Los resultados podrían replicarse en organizaciones con infraestructuras VoIP similares.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

P14. Los resultados son útiles como referencia para auditorías VoIP en otros contextos institucionales.

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo

P15. El comportamiento observado en los resultados no depende exclusivamente del contexto de la Institución.

- Muy en desacuerdo
- En desacuerdo

- Ni de acuerdo ni en desacuerdo
- De acuerdo
- Muy de acuerdo