Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería Industrial
Escuela Profesional de Ingeniería Industrial

Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI

TESIS

Para optar el Título Profesional de Ingeniero Industrial

Modalidad Ordinaria

AUTOR

Jaime Fernando VÁSQUEZ ESCALANTE

ASESOR

César CAMPOS CONTRERAS

Lima, Perú

2018

Referencia bibliográfica

Vásquez, J. (2018). *Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Industrial, Escuela Profesional de Ingeniería Industrial]. Repositorio institucional Cybertesis UNMSM.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMERICA)
FACULTAD DE INGENIERÍA INDUSTRIAL

ACTA N°022-VDAP-FII-2018

SUSTENTACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO INDUSTRIAL

El Jurado designado por la Facultad de Ingeniería Industrial, reunido en acto público en el Auditorio de la Facultad de Ingeniería Industrial, el día **lunes 06 de agosto de 2018,** a las 16:00 horas, dio inicio a la sustentación de la tesis:

"IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN ISO 27001:2013, PARA PROTEGER LA INFORMACIÓN EN LOS PROCESOS DE TI"

Que presenta el Bachiller:

VÁSQUEZ ESCALANTE, JAIME FERNANDO

Para optar el Título Profesional de Ingeniero Industrial en la Modalidad: **Ordinaria.**

Luego de la exposición, absueltas las preguntas del Jurado y siendo las 17:15 horas se procedió a la evaluación secreta, habiendo sido APROBADO por UNANIMIDAD con la calificación promedio de DIECISIETE, lo cual se comunicó públicamente.

Ciudad Universitaria, 06 de agosto del 2018

MG. SALAS BACALLA JULIO ALEJANDRO
Presidente

MG. CALSINA MIRAMIRA WILLY HUGO
Miembro

ING. MORALES DA COSTA OSCAR ABRAHAM
Miembro

MG. CAMPOS CONTRERAS CESAR
Asesor

DEDICATORIA

Dedico esta Tesis a mis padres Jaime y Vilma por haberme dado su apoyo emocional y económico para que pueda terminar.

A mis profesores que siempre compartieron sus conocimientos y experiencia para mi aprendizaje.

A mi esposa Yuliana por el apoyo incondicional que me ha brindado.

A mis compañeros de trabajo quienes con su experiencia y colaboración siempre logramos los objetivos trazados en el proyecto.

TABLA DE CONTENIDO

TABLA DE CONTENIDO 3

INTRODUCCIÓN 9

RESUMEN 11

CAPITULO I: PLANTEAMIENTO DEL PROBLEMA 12

1.1. SITUACIÓN PROBLEMÁTICA 12
1.2. FORMULACIÓN DEL PROBLEMA 13
1.2.1. PROBLEMA GENERAL 13
1.2.2. PROBLEMAS ESPECÍFICOS 14
1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN 14
1.4. OBJETIVOS DE LA INVESTIGACIÓN 16
1.5. OBJETIVO GENERAL 16
1.6. OBJETIVOS ESPECÍFICOS 17

CAPITULO II: MARCO TEÓRICO 18

2.1. ANTECEDENTES 18
2.2. BASES TEÓRICAS 21
2.2.1. DETALLE DE LA ORGANIZACIÓN 21
2.2.2. NORMA ISO 27001:2013 22
2.2.3. GESTIÓN DE PROYECTOS (PMBOK) 25
2.2.4. METODOLOGÍA DE MEJORA CONTINUA 26
2.2.5. DIAGRAMAS DE FLUJO 27
2.2.6. ANÁLISIS DE BRECHA (GAP) 28
2.3. GLOSARIO DE TERMINOS 30

CAPITULO III: HIPOTESIS Y VARIABLES 34

3.1. HIPÓTESIS GENERAL 34
3.2. HIPÓTESIS ESPECÍFICAS 34
3.3. IDENTIFICACIÓN DE VARIABLES 34
3.4. OPERACIONALIZACIÓN DE VARIABLES 35

CAPITULO IV: METODOLOGÍA 36

4.1. TIPO Y DISEÑO DE INVESTIGACIÓN 36

4.2. POBLACIÓN DE ESTUDIO **36**
4.3. TAMAÑO Y SELECCIÓN DE MUESTRA **36**
4.4. TÉCNICA DE RECOLECCIÓN DE DATOS **36**

CAPITULO V: DESARROLLO DEL PROYECTO **38**

5.1. INICIO DEL PROYECTO **38**
5.2. CRONOGRAMA DE TRABAJO **41**
5.3. ANALISIS COSTO / BENEFICIO **43**
5.4. RECURSOS **45**
5.5. ORGANIGRAMA DEL PROYECTO **46**
5.6. RIESGOS DEL PROYECTO **47**
5.7. DIAGNOSTICO **51**
5.8. PLANIFICAR **52**
5.8.1. COMPRENDER LA ORGANIZACIÓN Y SU CONTEXTO 52
5.8.2. IDENTIFICACIÓN DE LOS PROCESOS DEL NEGOCIO 54
5.8.3. COMPRENDER LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS 60
5.8.4. DETERMINAR EL ALCANCE DEL SGSI 60
5.8.5. LIDERAZGO Y COMPROMISO 63
5.8.6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 63
5.8.7. ROLES Y RESPONSABILIDADES DEL SGSI 64
5.8.8. ACCIONES PARA ABORDAR LOS RIESGOS Y OPORTUNIDADES .66
5.8.8.1. Inventario de los Activos de Información 66
5.8.8.2. Valorización del activo de información 67
5.8.8.3. Descripción del Riesgo 68
5.8.8.4. Probabilidad de Ocurrencia 68
5.8.8.5. Nivel de Impacto 68
5.8.8.6. Calculo del Riesgo 69
5.8.8.7. Tratamiento del Riesgo 70
5.8.8.8. Cálculo del Riesgo Residual 70
5.8.9. DECLARACIÓN DE APLICABILIDAD 71
5.8.10. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN 77
5.8.11. GESTIÓN DE CAMBIOS 77
5.8.12. INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 80
5.8.13. OBJETIVOS DE SI 84
5.8.14. COMPETENCIAS Y CONOCIMIENTO 86
5.8.15. COMUNICACIÓN 89

5.8.16. INFORMACIÓN DOCUMENTADA 92
5.9. HACER **98**
5.9.1. INVENTARIO DE ACTIVOS 98
5.9.2. EVALUACIÓN DEL RIESGO 124
5.9.3. PLAN DE TRATAMIENTO DE RIESGOS 139
5.10. MEDIR **160**
5.10.1. MEDICIÓN DEL SGSI 160
5.10.2. AUDITORIA INTERNA 168
5.10.3. REVISIÓN DE GESTIÓN 172
5.11. ACTUAR **172**
5.11.1. NO CONFORMIDADES Y ACCIONES CORRECTIVAS 172
5.11.2. MEJORA CONTINUA 174
5.12. AUDITORIA DE CERTIFICACIÓN **176**
5.13. CIERRE DEL PROYECTO **178**
6.1. ANALISIS DE BRECHAS **181**
6.2. ANALISIS DE LOS INDICADORES **185**
6.3. GRAFICO DE MEORA DE INDICADORES **186**
CAPITULO VII: RESULTADOS **190**
7.1. ANALISIS DE BRECHAS **190**
7.2. ANALISIS DE LOS INDICADORES **190**
CONCLUSIONES **193**
RECOMENDACIONES **194**
REFERENCIAS BIBLIOGRAFICAS **196**
ANEXOS **198**
ANEXO I: MATRIZ DE CONSISTENCIA **198**
ANEXO II: FORMATO GAP DE CLÁUSULA **199**
ANEXO III: FORMATO GAP DE CONTROLES **204**
ANEXO IV: CATALOGO DE SERVICIOS **211**
ANEXO V: SOLICITUD DE CAMBIO (RFC) **216**
ANEXO VI: SOLICITUD DE ACCIÓN CORRECTIVA **217**
ANEXO VII: ANALISIS DE CAUSA **218**

CUADRO DE TABLAS

CUADRO N° 2.1 ETAPAS DE LA MEJORA CONTINUA 27

CUADRO N° 2.2 DIAGRAMA DE FLUJO 28

CUADRO N° 2.3 PARAMETROS ANALISIS DE BRECHAS 29

CUADRO N° 3.1 OPERACIONALIZACIÓN DE LAS VARIABLES 35

CUADRO N° 5.1 PROJECT CHARTER 38

CUADRO N° 5.2 EQUIPO IMPLEMENTADOR 40

CUADRO N° 5.3 AHORRO DE IMPLEMENTAR EL SGSI 43

CUADRO N° 5.4 COSTO DE IMPLEMENTAR EL SGSI 44

CUADRO N° 5.5 ANÁLISIS COSTO/BENEFICIO 45

CUADRO N° 5.6 TIEMPO DE RECUPERACIÓN 45

CUADRO N° 5.7 RECURSOS DEL PROYECTO 45

CUADRO N° 5.8 RIESGOS DEL PROYECTO 47

CUADRO N° 5.9 DIAGNOSTICO INICIAL DE CLÁUSULAS 51

CUADRO N° 5.10 DIAGNOSTICO INICIAL DE CONTROLES 51

CUADRO N° 5.11 LINEAMIENTOS ESTRATEGICOS 53

CUADRO N° 5.12 FACTORES INTERNOS 53

CUADRO N° 5.13 FACTORES EXTERNOS 53

CUADRO N° 5.14 PARTES INTERESADAS Y REQUISITOS DE SI 60

CUADRO N° 5.15 ALCANCE DEL SGSI 61

CUADRO N° 5.16 TIPOS DE ACTIVOS 66

CUADRO N° 5.17 VALORIZACIÓN DE LOS ACTIVOS 67

CUADRO N° 5.18 PROBABILIDAD DE OCURRENCIA 68

CUADRO N° 5.19 CÁLCULO DEL IMPACTO 69

CUADRO N° 5.20 CÁLCULO DEL RIESGO 69

CUADRO N° 5.21 CRITERIO DE ACEPTACIÓN DEL RIESGO 70

CUADRO N° 5.22 CÁLCULO DEL RIESGO RESIDUAL 71

CUADRO N° 5.23 ENUNCIADO DE APLICABILIDAD 71

CUADRO N° 5.24 OBJETIVOS DE SEGURIDAD DE INFORMACIÓN 84

CUADRO N° 5.25 PLAN DE CAPACITACIÓN 86

CUADRO N° 5.26 PLAN DE CONCIENCIACIÓN 87

CUADRO N° 5.27 PLAN DE COMUNICACIÓN DEL SGSI 89

CUADRO N° 5.28 CLASIFICACIÓN DE LA INFORMACIÓN 93

CUADRO N° 5.29 CONTROL DE VERSIONES 93

CUADRO N° 5.30 CÓDIGO POR ÁREA 94

CUADRO N° 5.31 MATRIZ DE APROBACIONES 95

CUADRO N° 5.32 LISTA DE DOCUMENTOS DEL SGSI 95

CUADRO N° 5.33 INVENTARIO DE ACTIVOS 98

CUADRO N° 5.34 EVALUACIÓN DE RIESGOS 124

CUADRO N° 5.35 PLAN DE TRATAMIENTO DE RIESGOS 139

CUADRO N° 5.36 MONITOREO DE LOS PROCESOS DEL SGSI 160

CUADRO N° 5.37 MONITOREO DE LOS CONTROLES 165

CUADRO N° 5.38 ACTA DE CIERRE DEL PROYECTO 179

CUADRO N° 6.1 DIAGNOSTICO FINAL - CLAUSULAS 181

CUADRO N° 6.2 DIAGNOSTICO FINAL - CONTROLES 183

CUADRO N° 6.3: ANALISIS DE INDICADORES 185

CUADRO DE FIGURAS

FIGURA N° 5.1 CRONOGRAMA DE TRABAJO 41

FIGURA N° 5.2 ORGANIGRAMA 46

FIGURA N° 5.3 MAPA DE PROCESOS..... 54

FIGURA N° 5.6 PROCESO DE CAMBIOS..... 79

FIGURA N° 5.7 HERRAMIENTA DE MONITOREO..... 82

FIGURA N° 5.8 CATEGORIA DE INCIDENTES DE SI..... 82

FIGURA N° 5.9 GRUPO RESOLUTOR SGSI..... 83

FIGURA N° 5.10 PROCESO DOCUMENTAL..... 92

FIGURA N° 5.11 PLAN DE AUDITORIA..... 170

FIGURA N° 5.12 REUNION CIERRE AUDITORIA EXTERNA..... 177

FIGURA N° 5.13 CERTIFICADO ISO 27001:2013..... 178

FIGURA N° 6.1 COMPARATIVO CLAUSULAS (ANTES Y DESPUES)..... 181

FIGURA N° 6.2 COMPARATIVO DEGRADADO DE CLAUSULAS (ANTES Y DESPUES)..... 182

FIGURA N° 6.3 COMPARATIVO CONTROLES (ANTES Y DESPUES)..... 183

FIGURA N° 6.4 COMPARATIVO DEGRADADO DE CONTROLES (ANTES Y DESPUES)..... 184

FIGURA N° 6.5 GRAFICO DEL OBJETIVO 1..... 186

FIGURA N° 6.6 GRAFICO DEL OBJETIVO 2..... 186

FIGURA N° 6.7 GRAFICO DEL OBJETIVO 2..... 187

FIGURA N° 6.8 GRAFICO DEL OBJETIVO 3..... 187

FIGURA N° 6.9 GRAFICO DEL OBJETIVO 4..... 188

FIGURA N° 6.10 GRAFICO DEL OBJETIVO 5..... 188

FIGURA N° 6.11 GRAFICO DEL OBJETIVO 6..... 189

INTRODUCCIÓN

Se entiende por seguridad de la información al conjunto de medidas preventivas y correctivas implementados en las organizaciones que permiten proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

La importancia que tiene la seguridad de la información y el poder que implica manejar información es un tema muy delicado que no está en el conocimiento de muchos. Por ejemplo, el contexto de internet, muchos usuarios no le dan mayor importancia a su información que publican en la red y de qué forma lo hacen y más aún, muchos no diferencian lo privado de lo público. Por otro lado, están las empresas, quienes son las encargadas de manejar la información privada y/o pública que los usuarios les confían.

Asimismo, cada año la tecnología va en constante aumento y cambio, motivo por el cual aparecen nuevas amenazas que atentan contra la seguridad de la información (virus, ciberataques, hackers, etc.). Muchas empresas a nivel mundial enfrentan diversos problemas para proteger su información, por lo que corren un alto riesgo de perder información crítica para su negocio, su imagen y a la vez su ventaja competitiva en el mercado.

Debido a ello, el mercado actual obliga a las empresas u organizaciones que brindan servicios en tecnología de la información a establecer entandares, procedimientos, políticas y controles que garanticen la protección de su información y la de sus clientes y así obtener y mantener su ventaja competitiva en el mercado, y evitar pérdidas económicas que ello podría generar.

El presente trabajo referente a la implementación del sistema de gestión ISO 27001:2013 para proteger la información en los procesos de TI tiene como propósito establecer los lineamientos y/o controles para resguardar la información importante en una organización.

Para la aplicación del presente trabajo se tomará el caso de la empresa GMD® la cual brinda los servicios de administración de la plataforma tecnológica y mesa

de ayuda para uno de sus principales clientes del sector público: “La Oficina de Normalización Previsional (ONP)”.

El presente estudio ha considerado siete capítulos, en el capítulo I se define el planteamiento del problema formulando la formulación del problema y los objetivos de la presente tesis. El Capítulo II muestra el marco teórico con la pertinencia en la selección de los antecedentes, las bases teóricas y el glosario de términos. En el Capítulo III se presentan las hipótesis y variables con sus respectivos indicadores. En el Capítulo IV se aborda la metodología con el tipo, nivel, diseño, población y muestra y las técnicas e instrumentos seleccionados para el procesamiento, análisis e interpretación de la información. El Capítulo V se muestra el desarrollo del proyecto con el inicio, actividades y cierre del mismo. En el capítulo VI se presentan el análisis de los datos. En el Capítulo VII se detallan los resultados obtenidos. Posteriormente se presentan las conclusiones, recomendaciones y finalmente, las referencias bibliográficas seleccionadas en concordancia a las variables del estudio enriqueciendo la presente investigación.

RESUMEN

La implementación del sistema de gestión ISO 27001:2013 contribuye a la protección de la información de los procesos de TI (Tecnología de la Información), mediante la implementación de lineamientos y controles que la resguarde.

En este trabajo se detallan las actividades para una correcta implementación del sistema de gestión de seguridad de la información, asimismo recalca la importancia de concienciar al personal en la importancia de salvaguardar la información que manejan en sus actividades laborales.

El objetivo del presente trabajo es proteger la información en sus tres dimensiones: confidencialidad, integridad y disponibilidad mediante la implementación de una metodología de riesgos que permita identificar las amenazas que atenten contra la seguridad de la información en los procesos de TI de la organización GMD® que administra la plataforma tecnológica y mesa de ayuda de su cliente “ONP”.

El presente trabajo es **descriptiva aplicada** y su diseño corresponde al **experimental** la población fue conformada por 56 personas que son la totalidad de empleados que laboran en el proyecto, debido a su tamaño la muestra es la totalidad de personas, a saber 56 personas, las técnicas que se utilizaron fueron las siguientes: Encuestas, análisis documentario y auditorías

Como conclusión la hipótesis general nos muestra que el sistema de gestión de seguridad de la información ISO 27001:2013 permite salvaguardar la información de diversas amenazas mediante el cumplimiento de los objetivos de seguridad y el no contar con multas o penalidades por perdida de la información en los procesos de tecnología de la información (TI)

Palabras claves: (Confidencialidad, Integridad, Disponibilidad, Gestión de Riesgos)

CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. SITUACIÓN PROBLEMÁTICA

Todas las empresas del sector público y privado que están en el ámbito de las tecnologías de información afrontan diversos riesgos que atentan contra la información crítica para su negocio, la cual es soportada por hardware, software, personas, redes, etc. Proteger la información en sus (03) tres ámbitos: confidencialidad, integridad y disponibilidad, pueden ser importante para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial.

Durante los últimos años se han presentado sucesos de ciberseguridad que pusieron de manifiesto que ningún sector es inmune a los ataques y que es importante seguir los procedimientos de seguridad, entre los más destacados tenemos los siguientes:

- El robo de 81 millones de dólares al Banco Central de Bangladés, perpetrado por piratas informáticos que lograron acceder a los sistemas informáticos del Banco y transferir esa cantidad de dinero a varios casinos de Filipinas. Un error ortográfico en el nombre de uno de los destinatarios levantó las alarmas evitando así el mayor robo de la historia, puesto que en realidad se habían realizado 35 peticiones para obtener casi 1.000 millones de dólares.
- El robo de unos 64 millones de dólares en bitcoins a la plataforma de intercambio Bitfinex de Hong Kong, el mayor operador mundial de intercambio de bitcoin basado en dólares, lo que provocó una caída de la cotización de la moneda virtual superior al 23%.
- La publicación de datos de 154 millones de votantes de Estados Unidos. Los datos incluían información personal como dirección, correo electrónico, número de teléfono o enlaces a redes sociales.
- El robo de 1.000 millones de cuentas a Yahoo. Además de fechas de nacimiento, direcciones de correo electrónico, números de teléfono, contraseñas en MD5, la información robada también contenía preguntas y respuestas de seguridad sin cifrar.

En el Perú la Oficina de Normalización Previsional (ONP) tiene a su cargo la administración del Sistema Nacional de Pensiones a que se refiere el Decreto Ley N°19990 y de otros regímenes previsionales a cargo del Estado, que le sean encargados, siendo una de sus funciones el pago de los derechos pensionarios.

La Oficina de Tecnologías de Información (OTI) es el órgano de soporte responsable de brindar el apoyo tecnológico necesario en el procesamiento de información propio de los procesos institucionales, así como desarrollar los planes y proyectos que requiera la gestión de la ONP, por lo cual se decidió tercerizar los procesos de administración de la plataforma central y la mesa de servicios con el objetivo de mantener una infraestructura tecnológica a demanda, basada en estándares generalmente aceptados por la industria del sector, transparente para los servicios de aplicaciones y para los usuarios finales; evitando la obsolescencia tecnológica, no solo desde el punto de vista de equipos y tecnología, sino también desde el punto de vista de políticas, procedimientos y capacitación, así como el incremento o disminución de servicios y capacidades, que permita a la ONP asumir de forma óptima los encargos conferidos de acuerdo a ley.

La empresa GMD® fue adjudicado como proveedor de los servicios de administración de la plataforma central y mesa de servicios, encargado de administrar y resguardar la información de los pensionistas de la ONP.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. PROBLEMA GENERAL

¿De qué manera la implementación del sistema de gestión ISO 27001:2013 permite proteger la información en los procesos de TI?

1.2.2. PROBLEMAS ESPECÍFICOS

- ¿En qué medida la política de seguridad de la información influye en el sistema de gestión de seguridad de la información?
- ¿Cómo influye el cumplimiento de las regulaciones legales y contractuales en la seguridad de la información?
- ¿Cómo influye la mejora continua en la eficacia del SGSI?
- ¿Cómo se influye el mantener una cultura organizacional a que el personal asuma su responsabilidad por la seguridad de la información?
- ¿Cómo proteger la información y sus activos de información a través de un SGSI?
- ¿Cómo se deben atender los incidentes de seguridad de la información?

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

En las contrataciones con el estado peruano, se establece el artículo 223 del reglamento de contrataciones y adquisiciones del estado, el cual establece las multas por el incumplimiento en el contrato.

GMD®, en anteriores contrataciones que ha tenido con la Oficina de Normalización Previsional (ONP), en donde ha gestionado proyectos de administración de su plataforma tecnológica central, incurrió en multas (penalidades) por no cumplir los requisitos de seguridad para proteger la información que maneja, siendo los principales incidentes de seguridad ocurridos los que se listan a continuación:

- Incumplimiento de los entregables en la fecha requerida
- Por incumplimiento de los niveles de servicio (SLA)
- Incumplimiento de los planes y/o procedimientos
- Difundir información a terceros sin contar con autorización
- Acceder de forma remota a un computador sin la autorización respectiva
- Por ingresar o retirar equipos informáticos sin la autorización respectiva
- Por compartir información, música, videos a otros usuarios o terceros sin la autorización respectiva

- Por no contar con licencias para brindar el servicio
- Por no realizar pruebas de contingencia
- Por errores que afecten el pago de uno o varios pensionistas
- Por efectuar cambios en la plataforma y que afecten la operativa de los sistemas
- Por la indisponibilidad de la mesa de servicios
- Por realizar cambios de personal que no hayan sido autorizados

Dichos incidentes han traído como consecuencia un impacto económico (multas) que ascendieron a un total de **S/ 542,850.00**

La justificación económica se puede apreciar en la sección: **Análisis Costo/Beneficio**

En vista de lo citado anteriormente, GMD® en su visión de negocio y el reto de expandirse en el mercado, decidió implementar un mecanismo que le permita proteger la información, por lo cual se optó por implementar un sistema de gestión de seguridad de la información, el cual está bajo el estándar ISO 27001:2013 para los procesos de TI en los proyectos de administración de la plataforma tecnológica y mesa de servicios.

¿Cuáles serían los beneficios de contar con un sistema de gestión de seguridad de la información?

Los beneficios de contar con un sistema de gestión de seguridad de la información son los siguientes:

En la Organización: La certificación le permite obtener una ventaja comercial sobre sus competidores en el mercado por contar con controles que garanticen a los clientes mantener protegida su información, permite reducir el impacto de los riesgos asociados a los activos de información, garantiza la continuidad del negocio mediante la implementación de un plan de contingencias.

En lo legal: Cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología perfecta para cumplir con todos ellos.

En lo económico: La filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos la empresa va a ahorrar mucho dinero.

En lo tecnológico: Permite la revisión de las nuevas tecnologías.

En los empleados: Proporciona capacitación constante del personal lo que conlleva a mejoras salariales, garantiza la continuidad laboral al no cerrar el proyecto por perdidas económicas.

¿Qué tipo de empresas pueden implementar un sistema de gestión de seguridad de la información?

Todas las empresas sean de cualquier sector (público o privado) y de cualquier rubro (tecnológico, industrial, pesquero, etc.) sea grande o pequeña puede implementar un sistema de gestión de la seguridad de la información para el resguardo de su información.

1.4. OBJETIVOS DE LA INVESTIGACIÓN

Establecer los lineamientos para la correcta implementación de un sistema de gestión de seguridad de la información bajo el estándar internacional ISO 27001:2013 en los procesos de tecnología de información.

1.5. OBJETIVO GENERAL

Implementar el sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI.

1.6. OBJETIVOS ESPECÍFICOS

Los objetivos específicos que se plantean son los siguientes:

- Contar con una política de seguridad de la información que sea entendible y esté disponible a todo el personal
- Cumplir con todas las regulaciones aplicables en torno a la seguridad de la información
- Mejorar continuamente la eficacia del SGSI
- Mantener una cultura organizacional que aliente a todos los trabajadores a asumir una responsabilidad por la seguridad de la información
- Proteger la información y sus activos de información a través de un SGSI para garantizar su confidencialidad, integridad y disponibilidad.
- Dar respuesta inmediata a los incidentes que se presenten.

CAPITULO II: MARCO TEÓRICO

2.1. ANTECEDENTES

Barrantes Porras, Carlos Eduardo y Hugo Herrera, Javier Roberto (2012) en su tesis "Diseño e Implementación de un sistema de gestión de seguridad de información en procesos tecnológicos (Perú)

Concluyen que la implementación de un sistema de gestión de seguridad de la información permitió reducir y mitigar los riesgos relacionados a los activos de información de los procesos que se encuentran bajo la gerencia de tecnología de Card Perú S.A. que ponen en peligro los recursos, servicios y continuidad de los procesos tecnológicos.

Para ello se implementó una política de seguridad de información que fue desplegada a todo el personal y terceros involucrados en los procesos de TI, se gestionaron y monitorearon los incidentes y vulnerabilidades de seguridad de la información, se formó a la totalidad del personal en los procesos de TI en temas de seguridad de la información y se pudo controlar toda la documentación del SGSI.

Ampuero Chang, Carlos Enrique (2011) en su tesis: "Diseño de un Sistema de Gestión de Seguridad de Información para una Compañía de Seguros (Perú)"

Se concluye que la implementación del sistema de gestión de seguridad de la información permite la gestión en la implementación de controles y procedimientos para el cumplimiento de las normas relacionadas a la gestión de riesgos de operación, gestión de seguridad de información y gestión de continuidad de negocios (G-140), las cuales son reguladas por la Superintendencia de Banca, Seguros y AFP (SBS), ente regulatorio peruano para las entidades financieras, seguros y empresas privadas de sistemas de pensiones.

Villena Aguilar, Moisés Antonio (2006) en su tesis: "Sistema de gestión de seguridad de información para una institución financiera (Perú)"

El autor concluye en que la presente tesis permitió establecer los principales lineamientos para poder implementar de manera exitosa, un adecuado modelo de sistema de gestión de seguridad de información (SGSI) en una institución financiera en el Perú, el cual apunte a asegurar que la tecnología de información usada esté alineada con la estrategia de negocio y que los activos de información tengan el nivel de protección acorde con el valor y riesgo que represente para la organización.

De igual forma el autor de la presente tesis pudo observar que desafortunadamente, en ocasiones, se ve a un SGSI como una entidad complicada que dificulta la consecución de objetivos, imponiendo normas y procedimientos rígidos a los usuarios, a los sistemas y a los gestores. Sin embargo, al final se puedo verse no como un objetivo en sí mismo, sino como un medio de apoyo a la consecución de los objetivos.

Aguirre Mollehuanca, David (2014) en su tesis: "Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A."

El autor de la tesis concluye en que el diseño de un sistema de gestión de seguridad de información para la empresa SERPOST que el apoyo de la alta gerencia para el diseño del sistema de gestión que permitió concientizar a los jefes de área y dueños de los procesos para que entendieran que el SGSI no solo busca proteger la información digital, sino toda la información crítica del negocio independientemente del medio que la contenga.

Asimismo, destaca lo necesario que es mejorar la comunicación con el área de logística para acelerar los procesos de compra de aquellos activos que ayudaran en el tratamiento de riesgos detectados, especialmente, si estos riesgos son considerados altos o graves por la organización

Aguirre Cardno, Juan David y Aristizabal Betancourt, Catalina (2012) en su tesis: "Diseño del sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda (Colombia)"

La implementación del sistema de gestión de la seguridad de la información en el grupo empresarial La Ofrenda S.A (Organización dedicada a satisfacer integralmente las necesidades de la población en servicios funerarios, parques cementerios y cremación) con sede principal en la ciudad de Pereira (Colombia) permitió salvaguardar sus activos más importantes: la información junto con los procesos que la administran además de cada una de las personas que hacen parte de los mismos siendo estos el pilar fundamental para la compañía. Se cumplieron los objetivos de: determinar los riesgos que se presentan con la información que se maneja en la Empresa, clasificar el nivel de impacto de los riesgos, construir planes de mitigación de riesgos (disminuir los riesgos) y utilizar herramientas tecnológicas y de desarrollo que permitan la gestión de los procesos que avalen la seguridad de la información.

Buitrago Estrada Johanna, Bonilla Pineda Diego, Murillo Varón Carol (2012) en su tesis: "Diseño de una metodología para la implementación del sistema de gestión de seguridad de la información - SGSI, en el sector de laboratorios de análisis microbiológicos (Colombia), basado en ISO 27001".

Los autores de la tesis concluyen que el establecimiento de un SGSI en el sector de laboratorios es de gran utilidad al proporcionar una metodología adecuada para garantizar la confidencialidad, la integridad y la disponibilidad de los activos de su negocio que tengan que ver con la información.

Asimismo, destacan la importancia del diseño de un SGSI que sea dinámico y fácilmente adaptable a los cambios y las mejoras a introducir en la compañía, la aplicación del modelo PHVA (Planear, Hacer, Verificar, Actuar) basado en el concepto de mejora continua.

Mediante la implementación del sistema de gestión de seguridad de la información para empresas del sector de laboratorios de análisis microbiológicos

de control de calidad, basado en la ISO 27001, se pudieron obtener los siguientes beneficios:

- Se cuenta con una guía práctica para el lector en la que se expliquen los lineamientos de las normas que enmarcan la seguridad de la información, aclarando los requisitos y contextualizándolos en el sector de laboratorios de análisis microbiológico.
- Se cuenta con una metodología para la implementación y mantenimiento de la norma ISO27001 que involucre fase de planificación, implementación, revisión, mantenimiento y mejora.
- Se pueden proponer herramientas que faciliten la implementación de la norma IS0 27001 en cada una de sus etapas.

2.2. BASES TEÓRICAS

2.2.1. DETALLE DE LA ORGANIZACIÓN

GMD® es una empresa de Outsourcing de Procesos de Negocios, Tecnología de la Información (TI) y Transformación Digital con mayor confiabilidad y experiencia del Perú (según consultora internacional IDC). Cuenta con 33 años de experiencia, desarrollando e implementando exitosamente soluciones que generan valor a los procesos de negocios de sus clientes, un staff de 3000 profesionales y la mejor infraestructura como la fábrica de software más grande del país, 2 Data Center de Clase Mundial, 1 de los cuales está certificado en Tier III, en diseño y construcción y 2 call center en alta disponibilidad.

GMD cuenta con certificaciones de calidad como la ISO 9001, ISO 27001, OHSAS 18001, ISO 20000, ISO 22301, NTP 392-030 y metodologías de clase mundial como la CMMI-5, ITIL y PMI. Que respaldan nuestros procesos y operaciones, así como la satisfacción de nuestros clientes.

En junio 2013. GMD® y ONP firmaron los contratos para la administración de los servicios: “CP 0015-2013 Centro de datos y comunicaciones”; y “CP 0016-2013 Mesa de Servicios”.

A continuación, se detallan el alcance de cada uno de ellos:

SERVICIO DE CENTRO DE DATOS Y COMUNICACIONES

El objetivo del servicio es la administración del Centro de Datos y Comunicaciones en apoyo tecnológico de las actividades operativas de la ONP correspondientes a su objeto principal consistente en la administración del Sistema Nacional de Pensiones a que se refiere el Decreto Ley 19990, así como los otros Sistemas de Pensiones administrados por el Estado que le han sido encargados.

Los servicios comprendidos se listan a continuación:

1. Servicio de infraestructura y administración de centro de datos
2. Servicio de procesamiento central y servicios de almacenamiento.
3. Servicio de seguridad informática.
4. Servicio de administración de base de datos, servidores Unix/Linux, aplicaciones y servidores Windows
5. Servicio de Comunicaciones

MESA DE SERVICIOS

El objeto del servicio es abastecer de equipos tecnológicos, dar soporte a usuarios a nivel nacional, brindando atención telefónica o personal en el caso se requiera, ante cualquier consulta, incidente o requerimiento.

2.2.2. NORMA ISO 27001:2013

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento; aquí se puede ver la cantidad de certificados en los últimos años:

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo

amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, antivirus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

ISO/IEC 27001 se divide en 11 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

Sección 0 – Introducción – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.
Sección 1 – Alcance – explica que esta norma es aplicable a cualquier tipo de organización.
Sección 2 – Referencias normativas – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.
Sección 3 – Términos y definiciones – de nuevo, hace referencia a la norma ISO/IEC 27000.
Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.
Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.
Sección 6 – Planificación – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el

tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

Sección 7 – Apoyo – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

Sección 9 – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Annexo A – este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18).

2.2.3. GESTIÓN DE PROYECTOS (PMBOK)

La dirección de proyectos es la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto para cumplir con los requerimientos de este. Se logra mediante la aplicación e integración adecuadas de los 47 procesos de la dirección de proyectos, agrupados lógicamente, que conforman los 5 grupos de procesos. Estos 5 grupos de procesos son: Iniciación Planificación Ejecución Monitoreo y Control Cierre

Las áreas de conocimiento definidas en el PMBOK® son:

- **Gestión de Integración:** Procesos requeridos para integrar todas las actividades, documentos y recursos del proyecto.

- **Gestión de Alcance:** Procesos requeridos para identificar todo el trabajo requerido y sólo el trabajo requerido para obtener los entregables del proyecto y cumplir los objetivos.
- **Gestión de Tiempo:** Procesos requeridos para asegurar que el proyecto es finalizado a tiempo.
- **Gestión de Costos:** Procesos requeridos para asegurar que el proyecto es finalizado dentro de un presupuesto aprobado.
- **Gestión de Calidad:** Procesos requeridos para asegurar que el proyecto cumple los requerimientos y necesidades por los cuales fue emprendido.
- **Gestión de Comunicaciones:** Procesos requeridos para asegurar la generación, distribución, almacenamiento y disposición última de toda la información del proyecto, a tiempo y de forma adecuada.
- **Gestión de Recursos Humanos:** Procesos requeridos para administrar eficientemente la gente que participa en el proyecto.
- **Gestión de Riesgos:** Procesos requeridos para identificar, analizar y responder efectivamente a los riesgos del proyecto.
- **Gestión de Adquisiciones:** Procesos requeridos para adquirir bienes y servicios fuera de la organización del proyecto.

2.2.4. METODOLOGÍA DE MEJORA CONTINUA

La Metodología de Mejora Continua proporciona un modelo práctico para el mejoramiento. El modelo consiste en tres preguntas y el ciclo Planear – Ejecutar – Verificar – Actuar (Ciclo de Deming).

En la Metodología de la Mejora Continua, estas pruebas se llevan a cabo dentro del marco del ciclo PEVA: Planificar las acciones a tomar (definición de objetivos y su medida, definición de estrategias de solución), Implementar (Capacitación y puesta en marcha), Medir (los resultados, el grado de logros en los objetivos, los posibles efectos laterales) y Mejorar: (poner en marcha las mejoras obtenidas, redefinir los estándares). Este ciclo vuelve a empezar y no debe parar nunca: ése es el principio de la mejora continua. En el cuadro 2.1 se muestran las fases de la mejora continua.

CUADRO N° 2.1 ETAPAS DE LA MEJORA CONTINUA

Etapa	Descripción
Planificar (Establecer el SGSI)	Establecer la política. Objetivos, procesos y procedimientos del SGSI pertinentes a la gestión de riesgo y mejorar la seguridad de la información para obtener resultados de acuerdo con las políticas y objetivos generales de la organización
Implementar (Implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos del SGSI
Medir (Monitorear y revisar el SGSI)	Evaluar, y donde sea aplicable, medir el rendimiento del proceso contra la política del SGSI, sus objetivos y experiencia práctica, e informar los resultados para gestionar su revisión
Mejorar (Mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de auditorías internas del SGSI y de revisión de gestión u otra información relevante, para lograr mejora continua del SGSI

Fuente: Elaboración propia

2.2.5. DIAGRAMAS DE FLUJO

Un diagrama de flujo es una representación gráfica de un proceso. Cada paso del proceso es representado por un símbolo diferente que contiene una breve descripción de la etapa de proceso. Los símbolos gráficos del flujo del proceso están unidos entre sí con flechas que indican la dirección de flujo del proceso.

El diagrama de flujo ofrece una descripción visual de las actividades implicadas en un proceso mostrando la relación secuencial ente ellas, facilitando la rápida comprensión de cada actividad y su relación con las demás.

Los beneficios de los diagramas de procesos son los siguientes:

- Facilita la obtención de una visión transparente del proceso, mejorando su comprensión.
- Permiten definir los límites de un proceso.
- Proporciona un método de comunicación más eficaz, al introducir un lenguaje común

- Ayuda a establecer el valor agregado de cada una de las actividades que componen el proceso.
- Constituye una excelente referencia para establecer mecanismos de control y medición de los procesos, así como de los objetivos concretos para las distintas operaciones llevadas a cabo.
- Constituye el punto de comienzo indispensable para acciones de mejora, rediseño o reingeniería.

CUADRO N° 2.2 DIAGRAMA DE FLUJO

SIMBOLO	REPRESENTA
	**Inicio** / **Termino** Indica el inicio o la terminación del proceso
	**Decisión** Indica un punto en el flujo en que se produce una bifurcación del tipo “SI” – “NO”
	**Base de Datos** / **Aplicaciones** Empleado para representar la grabación de datos
	**Actividad** Representa una actividad llevada a cabo en un proceso
	**Documento** Se refiere a un documento utilizado en un proceso
	**Línea de flujo** Proporciona indicación sobre el sentido del flujo del proceso

Fuente: Elaboración propia

La herramienta de mayor uso para el diseño de diagrama de actividades es el Microsoft Visio y/o Bizagi.

2.2.6. ANÁLISIS DE BRECHA (GAP)

Es una herramienta que permite establecer una comparativa entre los procesos del negocio con los lineamientos o requisitos internacionales, estableciendo

cuales son las falencias y la brecha que separa a un esquema propio de un estándar.

Para el presente trabajo el análisis de brecha se debe realizar comparando los controles y documentación con la que cuente el proyecto en relación con los requisitos exigidos en la norma ISO/IEC 27001:2013.

Para el caso de reducir las brechas se toman las siguientes acciones:

- Asignar mayor cantidad de recursos
- Variar el alcance del sistema de gestión
- Variar el tiempo de implementación

Se ha elaborado el siguiente cuadro de nivel de cumplimiento:

CUADRO N° 2.3 PARAMETROS ANALISIS DE BRECHAS

Nivel	% Valor	Descripción
Implementado	100%	Proceso cumple con la norma y se encuentra documentado
Definido	75%	Proceso parcialmente implementado y documentado
Limitado	50%	Proceso cumple con la norma, pero no está documentado
Inicial	25%	Proceso implementado, pero no cumple con la norma
No implementado	0%	Proceso no implementado y no cumple con la norma
N.A.	No Aplica	No aplica al proceso

Fuente: Elaboración propia

El nivel y evidencias de cumplimiento se registran en el formato de análisis de brechas (GAP) correspondiente tanto de cláusulas (Anexo GAP Cláusulas) y controles del anexo A (Anexo GAP Controles)

2.3. GLOSARIO DE TERMINOS

- **Activo de Información:** Es todo proceso, tecnología o persona que interviene directa o indirectamente en el procesamiento, transmisión, almacenamiento o destrucción de la información, y por lo tanto tiene valor para la organización. Ej.: instalaciones, hardware, software, personas, soportes de información, servicios, datos e Información, equipamiento auxiliar, etc.
- **Área de Negocio:** Se refiere al área del Proyecto que forma parte del alcance del Sistema de Gestión de Seguridad de la Información.
- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Comité de Seguridad de la Información:** Reunión integrada por representantes de todas las áreas o procesos relevantes de la organización definida dentro del alcance, destinado a garantizar el apoyo manifiesto de los responsables a las iniciativas de seguridad.
- **Custodio de la Información:** Persona o entidad responsable de resguardar los activos de información que utiliza y/o custodia, independiente del soporte en la que se encuentre, aplicando controles de seguridad razonables con la finalidad de minimizar los riesgos de seguridad de la información.
- **Control o salvaguarda:** Medida que está modificando riesgo.
- **Data Center:** Es el área de servicios de operación de centro de cómputo.
- **Documento:** Información y su medio de soporte, el medio de soporte puede ser papel, medio magnético y electrónico, fotografía o una combinación de estos.
- **Evento:** Aparición o cambio de un conjunto particular de circunstancias. Por lo general, una amenaza representa un tipo de

circunstancia negativa, y una oportunidad representa un tipo de circunstancia positiva para el negocio.

- **Evaluación de riesgos:** Proceso de comparación de los resultados de análisis de riesgos con criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.
- **Incidente de Seguridad de la información:** Uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones y amenazan la seguridad de la información.
- **Identificación de riesgos:** Proceso de encontrar, reconocer y describir los riesgos.
- **Lista Maestra de documentos:** Es el registro utilizado para identificar y controlar la actualización e inventario de los documentos del Sistema de Gestión de Calidad.
- **MOF:** Manual de Organización y Funciones.
- Monitoreo: la comprobación continua, supervisar, observar críticamente o determinar la situación con el fin de identificar el cambio del nivel de rendimiento requerido o esperado.
- **Nivel de riesgo:** Magnitud de un riesgo, expresado en términos de la combinación de consecuencias y la probabilidad.
- **Propietario de activo de información:** Rol que identifica a un individuo o entidad que tiene responsabilidad aprobada por la Ata Dirección de controlar la producción, desarrollo, mantenimiento, uso y seguridad del activo de información.
- **PCA:** Parte de Control de Accesos
- **Propietario del Riesgo:** Identifica a la persona o entidad que tiene la responsabilidad gerencial de aceptar el riesgo (inherente y/o residual)

en relación con el activo de información; y aprobar el tratamiento de riesgo asociado.

- **Probabilidad:** posibilidad de que algo suceda.
- **Riesgo:** Es el efecto de la incertidumbre sobre los objetivos.
- **Requerimientos de seguridad de la información:** Son las dimensiones de seguridad de la información que requieren protección, los cuales son:
  - **Confidencialidad:** Propiedad que la información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.
  - **Integridad:** Propiedad de salvaguardar o mantener la exactitud de los activos.
  - **Disponibilidad:** Propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.
- **Riesgo residual:** riesgo restante después del tratamiento del riesgo.
- **Revisión:** actividad emprendida para determinar la conveniencia, adecuación y eficacia de la materia objeto de alcanzar los objetivos establecidos.
- **SGSI:** Sistema de Gestión de Seguridad de la Información, alineado con ISO/IEC 27001:2013.
- **Usuario del Activo:** Identifica a la persona o entidad autorizada que hace uso adecuado del activo.
- **Tratamiento de riesgos:** Proceso para modificar el riesgo.
- **Solicitud de cambio RFC (Request for Change):** Es un formulario, en forma impresa o digital, que se utiliza para registrar los detalles de una solicitud de un cambio en cualquier elemento de configuración perteneciente a un servicio, a un proyecto de software o a una infraestructura.

- **Comité de Cambio (CAB):** Es el comité responsable de la aprobación de un cambio.
- **Comité de Cambio de Emergencia (ECAB):** Es el comité responsable de la aprobación de un cambio de emergencia.
- **CMDB (Base de datos de la Gestión de Configuración):** Es una base de datos que contiene detalles relevantes de cada elemento de configuración y la relación entre ellos.
- **Elementos de configuración (EC):** Son documentos, registros, servicios, especificaciones técnicas, recursos o código de software que pueden consistir en múltiples productos de trabajo relacionados, los cuales forman la línea base.
- **Cambio Estándar:** Es un cambio que esta preautorizado por la Gestión de Cambios y tiene un procedimiento aceptado, representan bajo riesgo.
- **Cambio Normal:** Es un cambio que requiere una aprobación formal.
- **Cambio Emergencia:** Tiene como fin reparar un error en un servicio o que está afectando en gran medida al negocio negativamente. Un cambio de emergencia también se debe probar y documentar con el máximo detalle posible.
- **Capacitación:** La capacitación se refiere a los métodos que se usan para proporcionar a los empleados nuevos y actuales, las habilidades que requieren para desempeñar su trabajo" (Dessler, 2001).

CAPITULO III: HIPOTESIS Y VARIABLES

3.1. HIPÓTESIS GENERAL

Con la implementación del sistema de gestión ISO 27001:2013, se garantiza la protección de la información en los procesos de tecnología de la información.

3.2. HIPÓTESIS ESPECÍFICAS

- La política de seguridad de la información establece los lineamientos y el compromiso de la alta dirección en el cumplimiento del sistema de gestión de seguridad de la información
- Al cumplir con los requisitos regulatorios y/o las obligaciones contractuales referentes a la seguridad de la información permite evitar multas de incumplimiento legal
- La mejora continua contribuye a la mejora en la eficacia del SGSI mediante la revisión del cumplimiento de los estándares y la identificación de mejoras en los procesos de TI.
- La cultura organización alienta al personal a asumir una responsabilidad en relación con la seguridad de la información
- La protección de la información y sus activos de información se garantizan mediante la protección de la confidencialidad, integridad y disponibilidad de la información
- El atender los incidentes de seguridad permiten reducir el impacto negativo en la información

3.3. IDENTIFICACIÓN DE VARIABLES

VARIABLE INDEPENDIENTE: Implementación del sistema de gestión ISO 27001:2013 en los procesos de TI

VARIABLE DEPENDIENTE: Protección de la información en los procesos de tecnología de la información (TI).

3.4. OPERACIONALIZACIÓN DE VARIABLES

CUADRO N° 3.1 OPERACIONALIZACIÓN DE LAS VARIABLES

VARIABLE	INDICADOR
V1 Implementación de un sistema de gestión ISO 27001:2013	1.1. Certificación del sistema de gestión (Certificado internacional)
V2 Protección de la información en los procesos de tecnología de la información	2.1. Cantidad de personas que conocen la política de seguridad de la información
	2.2. Clientes satisfechos con el servicio
	2.3. SLA establecidos que se han cumplidos
	2.4. Penalidades por incumplimiento contractuales
	2.5. Cumplimiento de la norma ISO 27001:2013
	2.6. Cantidad de personas capacitadas en temas de seguridad de la información
	2.7. Cantidad de Personas que aprobaron el examen de las charlas de seguridad de la información
	2.8. Riesgos atendidos (confidencialidad, integridad y disponibilidad de la información)
	2.9. Pruebas de continuidad ejecutadas
	2.10. Incidentes reportados correctamente
	2.11. Incidentes atendidos correctamente

Fuente: Elaboración propia

CAPITULO IV: METODOLOGÍA

4.1. TIPO Y DISEÑO DE INVESTIGACIÓN

El presente trabajo de investigación está enmarcado dentro del tipo de investigación **descriptiva aplicada**, ya que describe, explica la influencia o relación entre las variables de investigación en la realidad concreta del universo.

Diseño de la investigación

El estudio responde a un Diseño **experimental** ya que se fundamenta en el Método Científico y utiliza como procesos lógicos la inducción y la deducción. Consiste en realizar actividades con la finalidad de comprobar, demostrar o reproducir ciertos fenómenos hechos o principios en forma natural o artificial, de tal forma que permita establecer experiencias para formular hipótesis que permitan a través del proceso científico conducir a generalizaciones científicas, que puedan verificarse en hechos concretos en la vida diaria.

4.2. POBLACIÓN DE ESTUDIO

La población de estudio es de 56 personas.

4.3. TAMAÑO Y SELECCIÓN DE MUESTRA

La muestra que se tomara para el presente trabajo es la cantidad total de la población (56 personas) debido a la cantidad es pequeña, en comparación a otras.

4.4. TÉCNICA DE RECOLECCIÓN DE DATOS

Las técnicas que se utilizaran para el análisis y verificación del proyecto son las siguientes:

- **Encuestas:** Son las preguntas en forma escrita u oral que aplica el investigador a una parte de la población denominada muestra poblacional, con la finalidad de obtener informaciones referentes a su objeto de investigación.

- **Análisis documentario:** Revisión de los procesos en comparación con la documentación elaborada del proyecto.
- **Auditorías:** Revisiones del cumplimiento del estándar internacional ISO/IEC 27001:2013 con las procedimientos y registros que el proyecto cuente.

CAPITULO V: DESARROLLO DEL PROYECTO

5.1. INICIO DEL PROYECTO

El **07 de agosto de 2014** se dio inicio al proyecto de implementación del SGSI para los procesos de TI para proteger la información crítica del proyecto, para lo cual se elaboró y aprobó el siguiente Project Charter.

CUADRO N° 5.1 PROJECT CHARTER

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN ISO 27001:2013	SGSI

DESCRIPCIÓN DEL PROYECTO

El proyecto: Implementación de un sistema de gestión de seguridad de la información bajo el estándar ISO/IEC 27001:2013 consiste en la adecuación de los requisitos exigidos en la norma como la implementación de controles aplicables del Anexo A de la norma en mención. La implementación consiste en las siguientes etapas:

Etapas:

- DIAGNOSTICO
- PLANIFICAR
  - Contexto de la organización
  - Liderazgo
  - Planeación
  - Soporte
- HACER
  - Operación
- MEDIR
  - Evaluación del desempeño
- ACTUAR
  - Mejora
- AUDITORÍA DE CERTIFICACIÓN

Equipo de Trabajo:

- Jaime Vásquez --> Líder del Proyecto / Oficial de Seguridad de la Información
- Demetrio Tantalean --> Sponsor del Proyecto
- Cesar Depaz --> Analista de Procesos

El proyecto será realizado desde el 11 de agosto de 2014 al 20 de mayo de 2015

DEFINICIÓN DEL PRODUCTO DEL PROYECTO

Implementación de un sistema de gestión de seguridad de la información bajo el estándar ISO/IEC 27001:2013 para los procesos de tecnología de la información de la administración de la plataforma central y mesa de servicios

DEFINICIÓN DE REQUISITOS DEL PROYECTO

- Se entregará un informe del avance mensual del proyecto
- Entregar un documento final con los resultados obtenidos post implementación

OBJETIVOS DEL PROJECTO		
CONCEPTO	OBJETIVOS	CRITERIO DE ÉXITO
1. ALCANCE	Cumplir con la elaboración de los siguientes entregables: alcance del SGSI, Metodología de riesgos, Política y objetivos de SI, y toda la documentación que evidencie el cumplimiento del SGSI	Aprobación de todos los documentos
2. TIEMPO	Cumplir el proyecto en los plazos establecidos	Seguimiento del cronograma del proyecto
3. COSTO	Cumplir con el presupuesto estimado del proyecto: S/ 137,666.00	No exceder del presupuesto

FINALIDAD DEL PROYECTO
Evitar multas o penalidades por no proteger la información del cliente

JUSTIFICACIÓN DEL PROYECTO		
JUSTIFICACIÓN CUALITATIVA	*JUSTIFICACIÓN CUANTITATIVA*	
Evitar multas o penalidades por no proteger la información del cliente	Multas	S/. 542,850.00

DESIGNACIÓN DEL PROJECT MANAGER DEL PROYECTO		
NOMBRE	Jaime Vásquez	*NIVELES DE AUTORIDAD*
REPORTA A	Demetrio Tantalean	Exigir el cumplimiento de los entregables del proyecto
SUPERVISA A	Cesar Depaz	

CRONOGRAMA DE HITOS DEL PROYECTO	
HITO O EVENTO SIGNIFICATIVO	*FECHA PROGRAMADA*
Inicio del Proyecto	11 de agosto de 2014
Diagnostico	11/08/14 – 04/09/14
Planificar	05/09/14 – 17/03/15
Hacer	18/03/15 – 02/04/15
Medir	03/04/15 – 30/04/15
Actuar	01/05/15 – 21/05/15
Auditoria de certificación	2da semana de mayo de 2015
Fin del Proyecto	20 de mayo de 2015

ORGANIZACIONES O GRUPOS ORGANIZACIONALES QUE INTERVIENEN EN EL PROYECTO	
ORGANIZACIÓN O GRUPO ORGANIZXACIONAL	*ROL QUE DESEMPEÑA*
GMD	Proveer el servicio de administración de la plataforma central y mesa de servicios de la ONP

PRINCIPALES AMENAZAS DEL PROYECTO
- Tiempo insuficiente para consolidar los controles y almacenar evidencias asociadas al SGSI que no permita superar con éxito la auditoría de certificación - El alcance del certificado vigente abarca ahora a 2 proyectos diferentes - Nueva versión de la norma - No aprobación de los documentos generados a raíz del proyecto - No cumplimiento en el tiempo establecido de actividades o documentos del cronograma del proyecto

PRINCIPALES OPORTUNIDADES DEL PROYECTO
La implementación del SGSI permite identificar la eficacia de los controles y tecnología utilizada en el presente proyecto

PRESUPUESTO PRELIMINAR DEL PROYECTO			
CONCEPTO			*MONTO (S/.)*
1. PERSONAL	Oficial de Seguridad de la Información y Analista de Procesos (MO Anual)		S/. 111,720.00
2. MATERIALES	Licencias de Office		S/. 7,256.00
3. MAQUINAS	Notebook, Desktop y Proyector		S/. 7,740.00
4. OTROS COSTOS	Capacitaciones (Auditor Interno, Líder y Riesgos)		S/. 10,950.00
TOTAL PRESUPUESTO			**S/. 137,666.00**
SPONSOR QUE AUTORIZA EL PROYECTO			
NOMBRE	*EMPRESA*	*CARGO*	*FECHA*
Demetrio Tantalean	GMD	Gerente del Proyecto	7/08/2014

Fuente: Elaboración propia

Asimismo, se definió el equipo implementador del sistema de gestión de seguridad de la información el cual se aprecia en el CUADRO N° 5.2

CUADRO N° 5.2 EQUIPO IMPLEMENTADOR

Cargo	**Nombre del responsable**	
Oficial de Seguridad de la Información	**Jaime Vásquez** (Líder del Proyecto)	
Analista de Procesos	Cesar Depaz	
Gerente del Proyecto	**Demetrio Tantalean** (Sponsor del Proyecto)	

Fuente: Elaboración propia

5.2. CRONOGRAMA DE TRABAJO

El equipo implementador elaboro el cronograma de trabajo con la descripción de las principales actividades a realizar para el proyecto de implementación del sistema de gestión de seguridad de la información el cual se detalla en la figura 5.1.

FIGURA N° 5.1 CRONOGRAMA DE TRABAJO

EDT	Nombre de tarea	Duración	Comienzo	Fin
1	**IMPLEMENTACIÓN SGSI - ISO 27001:2013**	**204 días?**	**lun 11/08/14**	**jue 21/05/15**
1.1	**DIAGNOSTICO**	**19 días**	**lun 11/08/14**	**jue 4/09/14**
1.1.1	Realización del diagnostico (GAP) respecto a la norma ISO/IEC 27001:2013	10 días	lun 11/08/14	vie 22/08/14
1.1.2	Elaboración del informe del diagnostico	5 días	lun 25/08/14	vie 29/08/14
1.1.3	Presentación del informe del diagnostico	1 día	lun 1/09/14	lun 1/09/14
1.1.4	Actualización del cronograma de trabajo	3 días	mar 2/09/14	jue 4/09/14
1.2	**PLANIFICAR**	**138 días?**	**vie 5/09/14**	**mar 17/03/15**
1.2.1	**Contexto de la Organización**	**26 días?**	**vie 5/09/14**	**vie 10/10/14**
1.2.1.1	**Comprender la organización y su contexto**	**10 días**	**vie 5/09/14**	**jue 18/09/14**
1.2.1.1.1	Estudio de la organización y su contexto	5 días	vie 5/09/14	jue 11/09/14
1.2.1.1.2	Identificación y estudio de los procesos de negocio / actividades	5 días	vie 12/09/14	jue 18/09/14
1.2.1.2	**Comprender las necesidades y expectativas de las partes interesadas**	**6 días?**	**vie 19/09/14**	**vie 26/09/14**
1.2.1.2.1	Identificación y estudio de las necesidades y expectativas de las partes interesadas	5 días	vie 19/09/14	jue 25/09/14
1.2.1.2.2	Identificación y aprobación de requisitos de seguridad	1 día?	vie 26/09/14	vie 26/09/14
1.2.1.3	**Determinar el alcance del SGSI**	**10 días**	**lun 29/09/14**	**vie 10/10/14**
1.2.1.3.1	Identificación de las instalaciones físicas	5 días	lun 29/09/14	vie 3/10/14
1.2.1.3.2	Definición y aprobación del alcance del SGSI	5 días	lun 6/10/14	vie 10/10/14
1.2.2	**Liderazgo**	**16 días?**	**lun 13/10/14**	**lun 3/11/14**
1.2.2.1	**Liderazgo y compromiso**	**1 día?**	**lun 13/10/14**	**lun 13/10/14**
1.2.2.1.1	Provisión de recursos	1 día?	lun 13/10/14	lun 13/10/14
1.2.2.2	**Politica**	**5 días?**	**mar 14/10/14**	**lun 20/10/14**
1.2.2.2.1	Definición y aprobación de la Política de Seguridad de la Información	5 días?	mar 14/10/14	lun 20/10/14
1.2.2.3	**Roles organizacionales, responsabilidades y autoridades**	**10 días?**	**mar 21/10/14**	**lun 3/11/14**
1.2.2.3.1	Definición y establecimiento del Comité del SGSI	5 días?	mar 21/10/14	lun 27/10/14
1.2.2.3.2	Definición y aprobación de roles, funciones, responsabilidades y autoridades dentro del SGSI	5 días	mar 28/10/14	lun 3/11/14

EDT	Nombre de tarea	Duración	Comienzo	Fin
1.2.3	**Planeación**	**40 días?**	**mar 4/11/14**	**lun 29/12/14**
1.2.3.1	**Acciones para abordar los riesgos y oportunidades**	**37 días?**	**mar 4/11/14**	**mié 24/12/14**
1.2.3.1.1	Adecuación de la metodología de evaluación de riesgos	5 días	mar 4/11/14	lun 10/11/14
1.2.3.1.2	Definición de los criterios de aceptación de riesgos	5 días	mar 11/11/14	lun 17/11/14
1.2.3.1.3	Plan de tratamiento de riesgos	5 días	mar 18/11/14	lun 24/11/14
1.2.3.1.4	Capacitación respecto a la metología de evaluación de riesgos	5 días	mar 25/11/14	lun 1/12/14
1.2.3.1.5	**Declaración de aplicabilidad (Controles)**	**17 días?**	**mar 2/12/14**	**mié 24/12/14**
1.2.3.1.5.1	A.5 - Políticas de seguridad de la información	5 días	mar 2/12/14	lun 8/12/14
1.2.3.1.5.2	A.6 - Organización de la seguridad de la información	1 día?	mar 9/12/14	mar 9/12/14
1.2.3.1.5.3	A.7 - Seguridad ligada a los recursos humanos	1 día?	mié 10/12/14	mié 10/12/14
1.2.3.1.5.4	A.8 - Administración de activos	1 día?	jue 11/12/14	jue 11/12/14
1.2.3.1.5.5	A.9 - Control de accesos	1 día?	vie 12/12/14	vie 12/12/14
1.2.3.1.5.6	A.11 - Seguridad física y del ambiente	1 día?	lun 15/12/14	lun 15/12/14
1.2.3.1.5.9	A.14 - Adquisición, desarrollo y mantenimiento del sistema	1 día?	jue 18/12/14	jue 18/12/14
1.2.3.1.5.1	A.15 - Relaciones con el proveedor	1 día?	vie 19/12/14	vie 19/12/14
1.2.3.1.5.1	A.16 - Gestión de incidentes de seguridad de la información	1 día?	lun 22/12/14	lun 22/12/14
1.2.3.1.5.1	A.17 - Aspectos de seguridad de la información en la GCN	1 día?	mar 23/12/14	mar 23/12/14
1.2.3.1.5.1	A.18 - Cumplimiento	1 día?	mié 24/12/14	mié 24/12/14
1.2.3.2	Objetivos de seguridad de la información	3 días	jue 25/12/14	lun 29/12/14
1.2.4	**Soporte**	**56 días**	**mar 30/12/14**	**mar 17/03/15**
1.2.4.1	Recursos	1 día	mar 30/12/14	mar 30/12/14
1.2.4.2	**Competencias**	**5 días**	**mié 31/12/14**	**mar 6/01/15**
1.2.4.2.1	Plan de capacitación	5 días	mié 31/12/14	mar 6/01/15
1.2.4.3	**Conocimiento**	**5 días**	**mié 7/01/15**	**mar 13/01/15**
1.2.4.3.1	Charla de concienciación	5 días	mié 7/01/15	mar 13/01/15
1.2.4.4	**Comunicación**	**5 días**	**mié 14/01/15**	**mar 20/01/15**
1.2.4.4.1	Plan de comunicación del SGSI	5 días	mié 14/01/15	mar 20/01/15
1.2.4.5	**Información documentada**	**40 días**	**mié 21/01/15**	**mar 17/03/15**
1.2.4.5.1	Procedimiento para la generación de documentos	2 días	mié 21/01/15	jue 22/01/15
1.2.4.5.2	Procedimiento para la gestión de registros	2 días	vie 23/01/15	lun 26/01/15
1.2.4.5.3	**Elaboración de documentos del SGSI**	**36 días**	**mar 27/01/15**	**mar 17/03/15**
1.2.4.5.3.1	Politica de SI	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.2	Politica de escritorio y pantalla limpio	12 días	lun 2/03/15	mar 17/03/15
1.2.4.5.3.3	Politica de accesos	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.4	Manual del SGSI	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.5	Respalado de información	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.6	Gestión de cambios	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.7	Auditoria interna	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.8	Control de documentos	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.9	Control de registros	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.1	No Conformidades y acciones correctivas	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.1	Ingreso del personal	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.1	Salida del personal	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.1	Proceso disciplinario	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.1	Incidentes de Seguridad de la Información	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.1	Gestión de riesgos	12 días	mar 27/01/15	mié 11/02/15
1.2.4.5.3.1	Documentos operativos	12 días	mar 27/01/15	mié 11/02/15

EDT	Nombre de tarea	Duración	Comienzo	Fin
1.3	**HACER**	**12 días**	**mié 18/03/15**	**jue 2/04/15**
1.3.1	**Operación**	**12 días**	**mié 18/03/15**	**jue 2/04/15**
1.3.1.1	**Control y planificación operacional**	**6 días**	**mié 18/03/15**	**mié 25/03/15**
1.3.1.1.1	Medición de los Objetivos de SI	1 día	mié 18/03/15	mié 18/03/15
1.3.1.1.2	Gestión de cambios	5 días	jue 19/03/15	mié 25/03/15
1.3.1.2	Evaluación de riesgos	3 días	jue 26/03/15	lun 30/03/15
1.3.1.3	Plan de tratamiento de riesgos	3 días	mar 31/03/15	jue 2/04/15
1.4	**MEDIR**	**20 días**	**vie 3/04/15**	**jue 30/04/15**
1.4.1	**Evaluación del desempeño**	**20 días**	**vie 3/04/15**	**jue 30/04/15**
1.4.1.1	Plan de medición del SGSI	5 días	vie 3/04/15	jue 9/04/15
1.4.1.2	Medición del SGSI	1 día	vie 10/04/15	vie 10/04/15
1.4.1.3	**Auditoria Interna**	**11 días**	**vie 10/04/15**	**vie 24/04/15**
1.4.1.3.1	Programa de auditoria	2 días	vie 10/04/15	lun 13/04/15
1.4.1.3.2	Plan de auditoria	2 días	mar 14/04/15	mié 15/04/15
1.4.1.3.3	Ejecución de la auditoria interna	2 días	mié 22/04/15	jue 23/04/15
1.4.1.3.4	Informe de auditoría Interna	1 día	vie 24/04/15	vie 24/04/15
1.4.1.4	Revisión de gestión	1 día	jue 30/04/15	jue 30/04/15
1.5	**ACTUAR**	**15 días?**	**vie 1/05/15**	**jue 21/05/15**
1.5.1	**Mejora**	**15 días?**	**vie 1/05/15**	**jue 21/05/15**
1.5.1.1	**No Conformidades y acciones correctivas**	**15 días**	**vie 1/05/15**	**jue 21/05/15**
1.5.1.1.1	**Analisis de causas**	**15 días**	**vie 1/05/15**	**jue 21/05/15**
1.5.1.1.1.1	Generar SAC	2 días	vie 1/05/15	lun 4/05/15
1.5.1.1.1.2	Seguimiento y cierre	10 días	vie 8/05/15	jue 21/05/15
1.5.1.2	**Mejora Continua**	**5 días?**	**vie 1/05/15**	**vie 8/05/15**
1.5.1.2.1	Identificar oportunidad de mejora	5 días?	vie 1/05/15	jue 7/05/15
1.5.1.2.2	Plan de acción	0 días	vie 8/05/15	vie 8/05/15
1.5.1.2.3	Implementar mejora	0 días	vie 8/05/15	vie 8/05/15
2	**AUDITORIA DE CERTIFICACIÓN**	**21 días?**	**lun 20/04/15**	**lun 18/05/15**
2.1	Plan de auditoria	1 día?	lun 20/04/15	lun 20/04/15
2.2	Ejecución de la auditoria externa	5 días	lun 11/05/15	vie 15/05/15
2.3	Informe de auditoria	1 día?	lun 18/05/15	lun 18/05/15
3	Cierre del Proyecto	1 día	mar 19/05/15	mar 19/05/15

Fuente: Elaboración propia

5.3. ANALISIS COSTO / BENEFICIO

A continuación, se presenta el detalle económico para la viabilidad del proyecto (análisis costo/beneficio) según el cuadro N° 5.3 al cuadro N° 5.6.

CUADRO N° 5.3 AHORRO DE IMPLEMENTAR EL SGSI

Ahorro de Implementar el SGSI	Costo Anual (s/.)
Incumplimiento de los entregables en la fecha requerida	S/. 30,800.00
Por incumplimiento de los niveles de servicio (SLA)	S/. 115,500.00
Incumplimiento de los planes y/o procedimientos	S/. 34,650.00

Ahorro de Implementar el SGSI	Costo Anual (s/.)
Difundir información a terceros sin contar con autorización	S/. 92,400.00
Acceder de forma remota a un computador sin la autorización respectiva	S/. 3,850.00
Por ingresar o retirar equipos informáticos sin la autorización respectiva	S/. 9,625.00
Por compartir información, música, videos a otros usuarios o terceros sin la autorización respectiva	S/. 5,775.00
Por no contar con licencias para brindar el servicio	S/. 38,500.00
Por no realizar pruebas de contingencia	S/. 19,250.00
Por errores que afecten el pago de uno o varios pensionistas	S/. 38,500.00
Por efectuar cambios en la plataforma y que afecten la operativa de los sistemas	S/. 115,500.00
Por la indisponibilidad de la mesa de servicios	S/. 7,700.00
Por realizar cambios de personal que no hayan sido autorizados	S/. 30,800.00
TOTAL DE PENALIDADES EFECTUADAS	**S/. 542,850.00**

Fuente: Elaboración propia

CUADRO N° 5.4 COSTO DE IMPLEMENTAR EL SGSI

Costo Implementación del SGSI	Costo Anual (s/.)
Oficial de Seguridad	S/. 60,600.00
Analista de Procesos	S/. 51,120.00
Curso Interpretación y Auditor Interno SGSI	S/. 1,950.00
Curso Auditor Líder ISO/IEC 27001:2013	S/. 5,500.00
Curso de gestión de riesgos ISO 31000	S/. 3,500.00
Microsoft Office Estándar (2 licencias)	S/. 860.00
Microsoft Visio (2 licencias)	S/. 2,198.00
Microsoft Project (2 licencias)	S/. 4,198.00
Notebook i7 - 320 GB, 8GB RAM (Oficial de Seguridad)	S/. 3,200.00
Desktop + Monitor + Mouse (Analista de Procesos)	S/. 2,500.00
Proyector Home Cinema 2030 para las charlas de seguridad	S/. 2,040.00
COSTO TOTAL	**S/. 137,666.00**

Fuente: Elaboración propia

CUADRO N° 5.5 ANÁLISIS COSTO/BENEFICIO

Beneficio (B)	S/ 542,850.00
Costo (C)	S/ 137,666.00
B/C	3.94

Fuente: Elaboración propia

Del cuadro 5.5, como B/C > 1 → **EL PROYECTO ES RENTABLE**

CUADRO N° 5.6 TIEMPO DE RECUPERACIÓN

Meses	12
Meses/(B/C)	3.0432
Tiempo Recuperación	3 meses

Fuente: Elaboración propia

El tiempo de recuperación de la inversión del proyecto de implantación del SGSI es de 3 meses.

5.4. RECURSOS

Los recursos o insumos que se requieren para el proyecto de implementación son los que figuran en la tabla 5.7

CUADRO N° 5.7 RECURSOS DEL PROYECTO

Nro.	TIPO	RECURSO	PROVEEDOR
1	Humano	Oficial de Seguridad de la Información	GMD
2	Humano	Analista de Procesos	GMD
3	Capacitación	Curso Interpretación y Auditor Interno SGSI	SGS DEL PERÚ
4	Capacitación	Curso Auditor Líder ISO/IEC 27001:2013	TUV RHEINLAND

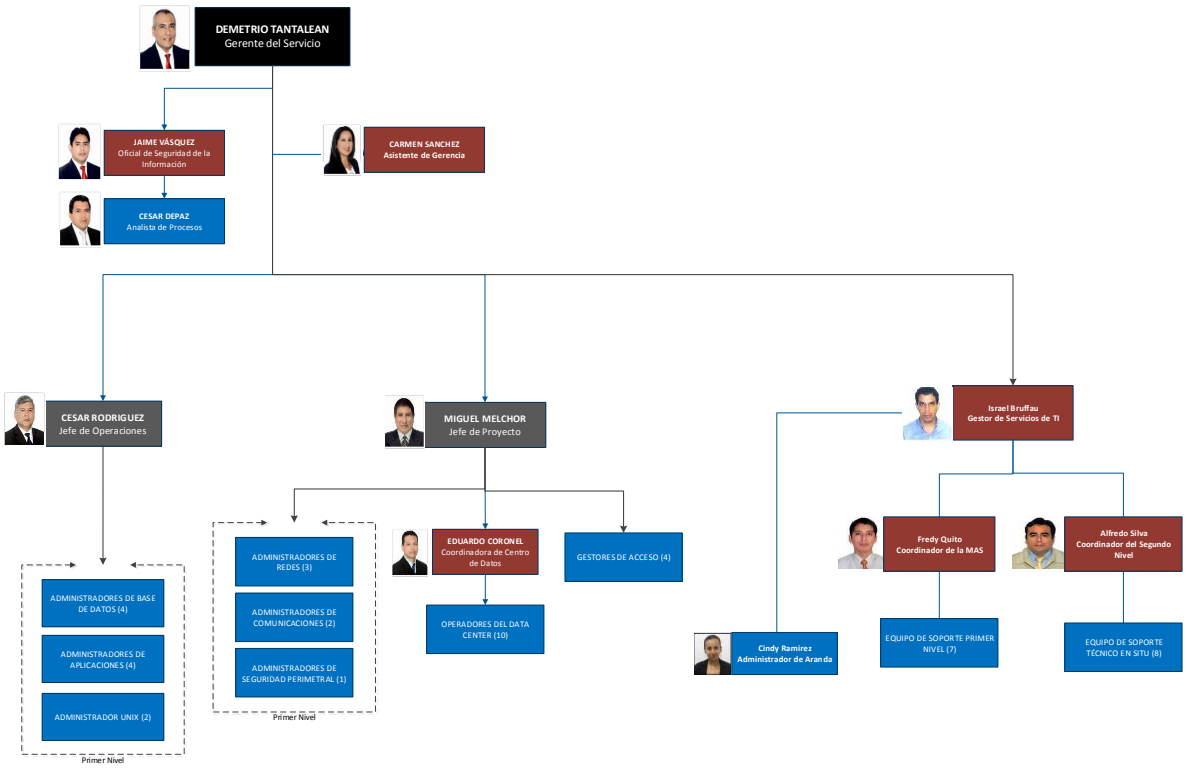
Nro.	TIPO	RECURSO	PROVEEDOR
5	Capacitación	Curso de gestión de riesgos ISO 31000	PRIME PROFESIONAL
6	Software	Microsoft Office Standard / Visio / Project	MICROSOFT
7	Hardware	Notebook i7 - 320 GB, 8GB RAM	LENOVO
8	Hardware	Desktop + Monitor + Mouse	LENOVO
9	Hardware	Proyector Home Cinema 2030	EPSON

Fuente: Elaboración propia

5.5. ORGANIGRAMA DEL PROYECTO

Se presenta el organigrama del personal asignado al proyecto.

FIGURA N° 5.2 ORGANIGRAMA



Fuente: Elaboración propia

5.6. RIESGOS DEL PROYECTO

CUADRO N° 5.8 RIESGOS DEL PROYECTO

Probabilidad	Valor	Impacto	Valor	Nivel del Riesgo	Valor
Muy Frecuente	5	Muy Alto	5	Muy Alto	> 49
Frecuente	4	Alto	4	Alto	30 - 49
Probable	3	Medio	3	Medio	20 -29
Poco Probable	2	Bajo	2	Bajo	10 -19
Raramente	1	Muy Bajo	1	Muy Bajo	Menor a 10

CÓDIGO	DESCRIPCIÓN DEL RIESGO	CAUSA RAÍZ	CONSECUENCIA	PROBABILIDAD	OBJETIVO AFECTADO	ESTIMACIÓN DE IMPACTO	PROB X IMPACTO	TIPO DE RIESGO	PROPIETARIO DEL RIESGO
RI001	Poca disponibilidad o ausencia del personal asignado al proyecto	Recarga de actividades Personal insuficiente	Incumplimiento de los plazos y/o actividades indicadas en el cronograma	4	Alcance	1	4	Alto	Gerente del Proyecto
					Tiempo	5	20		
					Costo	1	4		
					Calidad	3	12		
					Total Probabilidad x Impacto		40		
RI002	Trabajo no programado	Actividades solicitadas por la alta gerencia del proyecto	Incumplimiento de los plazos y/o actividades indicadas en el cronograma	4	Alcance	1	4	Alto	Gerente del Proyecto
					Tiempo	5	20		
					Costo	1	4		
					Calidad	4	16		
					Total Probabilidad x Impacto		44		

CÓDIGO	DESCRIPCIÓN DEL RIESGO	CAUSA RAÍZ	CONSECUENCIA	PROBABILIDAD	OBJETIVO AFECTADO	ESTIMACIÓN DE IMPACTO	PROB X IMPACTO	TIPO DE RIESGO	PROPIETARIO DEL RIESGO
RI003	Cambio en el alcance del proyecto	Cambios en el contexto de la organización. Nuevos requisitos legales.	Incumplimiento de los plazos y/o actividades indicadas en el cronograma	2	Alcance	5	10	Medio	Gerente del Proyecto
					Tiempo	3	6		
					Costo	3	6		
					Calidad	3	6		
					Total Probabilidad x Impacto		28		
RI004	Modificación del cronograma de trabajo	Cambios en el contexto de la organización. Nuevos requisitos legales.	Incumplimiento de los plazos y/o actividades indicadas en el cronograma	3	Alcance	1	3	Alto	Gerente del Proyecto
					Tiempo	5	15		
					Costo	3	9		
					Calidad	3	9		
					Total Probabilidad x Impacto		36		
RI005	No se identifique correctamente los activos de información	Error Humano Poco conocimiento técnico	No conformidad del SGSI	3	Alcance	1	3	Medio	Gerente del Proyecto
					Tiempo	1	3		
					Costo	1	3		
					Calidad	5	15		
					Total Probabilidad x Impacto		24		
RI006	Controles implementados no son los correctos	Error Humano Poco conocimiento técnico	No conformidad del SGSI	3	Alcance	1	3	Alto	Gerente del Proyecto
					Tiempo	1	3		
					Costo	3	9		
					Calidad	5	15		
					Total Probabilidad x Impacto		30		
RI007	No hay compromiso del personal del proyecto	desinterés del personal No hay conocimiento referente al SGSI	No conformidad del SGSI	3	Alcance	1	3	Medio	Gerente del Proyecto
					Tiempo	1	3		
					Costo	1	3		
					Calidad	5	15		

CÓDIGO	DESCRIPCIÓN DEL RIESGO	CAUSA RAÍZ	CONSECUENCIA	PROBABILIDAD	OBJETIVO AFECTADO	ESTIMACIÓN DE IMPACTO	PROB X IMPACTO	TIPO DE RIESGO	PROPIETARIO DEL RIESGO
					Total Probabilidad x Impacto		24		
RI008	Demora en la aprobación de los documentos generados por el proyecto	desinterés del personal No hay conocimiento referente al SGSI	No conformidad del SGSI	3	Alcance	1	3	Alto	Gerente del Proyecto
					Tiempo	5	15		
					Costo	1	3		
					Calidad	5	15		
					Total Probabilidad x Impacto		36		
RI009	Incumplimiento en los programas y planes de auditorías internas	Demora en el cumplimiento del plan de trabajo	No conformidad del SGSI	3	Alcance	1	3	Alto	Gerente del Proyecto
					Tiempo	5	15		
					Costo	1	3		
					Calidad	5	15		
					Total Probabilidad x Impacto		36		

CÓDIGO	DESCRIPCIÓN DEL RIESGO	PLAN DE RESPUESTAS	TIPO DE RESPUESTA	RESPONSABLE DE LA RESPUESTA
RI001	Poca disponibilidad o ausencia del personal asignado al proyecto	Aprobación del cronograma de trabajo Recursos asignados solo a las actividades descritas en el proyecto	Mitigar	Comité del SGSI
RI002	Trabajo no programado	Aprobación del cronograma de trabajo Recursos asignados solo a las actividades descritas en el proyecto	Mitigar	Comité del SGSI
RI003	Cambio en el alcance del proyecto	Aprobación del alcance del proyecto	Mitigar	Comité del SGSI

CÓDIGO	DESCRIPCIÓN DEL RIESGO	PLAN DE RESPUESTAS	TIPO DE RESPUESTA	RESPONSABLE DE LA RESPUESTA
RI004	Modificación del cronograma de trabajo	Aprobación del cronograma de trabajo Recursos asignados solo a las actividades descritas en el proyecto	Mitigar	Comité del SGSI
RI005	No se identifique correctamente los activos de información	Participar en las reuniones de identificación del riesgo con el propietario del activo de información	Mitigar	Oficial de Seguridad de la Información
RI006	Controles implementados no son los correctos	Participar en las reuniones de identificación del riesgo con el propietario del activo de información	Mitigar	Oficial de Seguridad de la Información
RI007	No hay compromiso del personal del proyecto	Realizar charlas para generar conciencia del personal en la importancia del cumplimiento del sistema de gestión	Mitigar	Oficial de Seguridad de la Información
RI008	Demora en la aprobación de los documentos generados por el proyecto	Seguimiento del plan de trabajo (cronograma) para la identificación de desfaces en el proyecto Definir tiempos de holgura para la aprobación de documentos	Mitigar	Oficial de Seguridad de la Información
RI009	Incumplimiento en los programas y planes de auditorías internas	Seguimiento del plan de trabajo (cronograma) para la identificación de desfaces en el proyecto Definir tiempos de holgura para la aprobación de documentos	Mitigar	Oficial de Seguridad de la Información

Fuente: Elaboración propia

5.7. DIAGNOSTICO

El objetivo de esta fase es medir el nivel actual de cumplimiento de la ISO 27001:2013 en los procesos de TI.

Para medir el nivel de cumplimiento inicial se realiza un análisis de diagnóstico (análisis GAP) según los formatos indicados en el Anexo II: Formato GAP de Clausulas y Anexo III: Formato GAP de Controles el cual dio como resultado lo mostrado a continuación en las tablas 5.9 y 5.10.

CUADRO N° 5.9 DIAGNOSTICO INICIAL DE CLÁUSULAS

Descripción de la Clausula	% Cumplimiento Inicial - Cláusulas
4. CONTEXTO DE LA ORGANIZACIÓN	31%
5. LIDERAZGO	50%
6. PLANIFICACIÓN	56%
7. APOYO	38%
8. OPERACIÓN	33%
9. EVALUACIÓN DE DESEMPEÑO	52%
10. MEJORA	25%
% CUMPLIMIENTO TOTAL	**41%**

Fuente: Elaboración propia

CUADRO N° 5.10 DIAGNOSTICO INICIAL DE CONTROLES

Descripción de Dominio	% Cumplimiento Inicial – Anexo A
A.5 - Políticas de seguridad de la información	0%
A.6 - Organización de la seguridad de la información	50%
A.7 - Seguridad ligada a los recursos humanos	70%
A.8 - Administración de activos	60%
A.9 - Control de accesos	60%
A.10 – Criptografía	N.A
A.11 - Seguridad física y del ambiente	75%
A.12 - Seguridad de las operaciones	60%
A.13 - Seguridad de las comunicaciones	60%

Descripción de Dominio	% Cumplimiento Inicial – Anexo A
A.14 - Adquisición, desarrollo y mantenimiento del sistema	50%
A.15 - Relaciones con el proveedor	50%
A.16 - Gestión de incidentes de seguridad de la información	40%
A.17 - Aspectos de seguridad de la información en la GCN	50%
A.18 – Cumplimiento	50%
% CUMPLIMIENTO	**52%**

Fuente: Elaboración propia

Se observa un cumplimiento del 41% en las cláusulas y un 52% de cumplimiento en los controles del Anexo A de la norma ISO 27001:2013

Nota (*): en el proyecto no se consideran controles criptográficos.

5.8. PLANIFICAR

5.8.1. COMPRENDER LA ORGANIZACIÓN Y SU CONTEXTO

La organización es el proyecto que la empresa GMD® brinda a su cliente en la ONP en la administración de la plataforma central y mesa de servicios, cuyos procesos fueron graficados según el punto 5.8.2 Identificación de los procesos de negocio.

El SGSI busca identificar aquellos factores internos y externos relacionados a la seguridad de la información, los cuales se muestran a continuación:

CUADRO N° 5.11 LINEAMIENTOS ESTRATEGICOS

LINEAMIENTOS ESTRATEGICOS	OBJETIVOS
VALOR	Incrementar Actividad Asegurar rentabilidad
ESTABILIDAD	Mayor eficiencia
PRESTIGIO	Orientar cultura de servicio al cliente Desarrollar y retener talento

Fuente: Elaboración propia

CUADRO N° 5.12 FACTORES INTERNOS

FACTORES INTERNOS	RELACIÓN CON LA SEGURIDAD
PRODUCTOS Y SERVICIOS	Mayor demanda de seguridad en los servicios de tecnología
ORGANIZACIÓN - PERSONAL	La seguridad de la información requiere la participación de todas las áreas del negocio
FINANZAS - CONTABILIDAD	Se requiere mantener confidencialidad, integridad y disponibilidad de la información financiera-contable

Fuente: Elaboración propia

CUADRO N° 5.13 FACTORES EXTERNOS

FACTORES EXTERNOS	RELACIÓN CON EL SGSI
POLÍTICO – LEGAL	Cumplir con las leyes y regulaciones relacionadas con la seguridad de la información
ECONÓMICO - FINANCIERO	Incremento del Cibercrimen en el Perú está afectando la economía y financieramente a las organizaciones en general
SOCIAL - CULTURAL	Se inicia el desarrollo en una cultura basada en la seguridad.

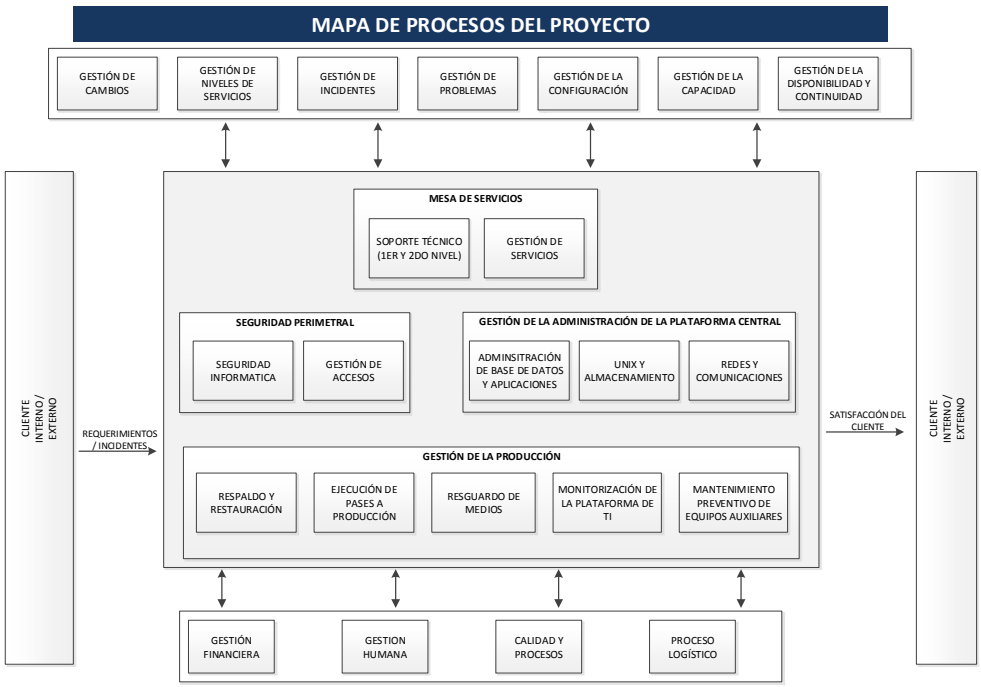
FACTORES EXTERNOS	RELACIÓN CON EL SGSI
TECNOLÓGICO	Uso de soluciones tecnológicas para proteger la información del negocio
MERCADO OBJETIVO	Mayor demanda de servicios de gestión de seguridad de la información en los sectores financiero, gobierno, etc.
COMPETENCIA	Mayor atención en la seguridad de la información

Fuente: Elaboración propia

5.8.2. IDENTIFICACIÓN DE LOS PROCESOS DEL NEGOCIO

Un proceso es un conjunto de tareas lógicamente relacionadas que existen para conseguir un resultado bien definido dentro de un negocio; por lo tanto, toman una entrada y le agregan valor para producir una salida. A continuación, se muestra el diagrama de procesos del proyecto.

FIGURA N° 5.3 MAPA DE PROCESOS



Fuente: Elaboración propia

PROCESOS CORE

Los procesos core son aquellos procesos que dan valor al cliente, es decir, que son la parte principal del negocio, para el presente trabajo tenemos los siguientes:

Gestión de Incidentes: El objetivo es describir las actividades a realizar para restaurar la operación normal del servicio tan pronto como sea posible y minimizar el impacto adverso en las operaciones del negocio, lo que garantiza que los niveles acordados de calidad del servicio se mantengan.

Gestión de Problemas: El objetivo es describir las actividades a realizar para lograr estabilidad en la infraestructura de TI minimizando el impacto que puedan tener los incidentes y problemas en el negocio y prevenir la recurrencia de incidentes y problemas encontrando las causas raíces e iniciando las acciones para mejorar y corregir la situación.

Gestión de Cambio: Asegurar que los cambios que afectan al servicio sean controlados, para ello se deberá analizar los criterios de aceptación, elaborar planes de implementación (responsabilidades, tiempos, recursos, etc.), evaluar el impacto a los demás servicios o al negocio y controlar los riesgos logrando mantener los niveles aceptables de disponibilidad y continuidad del servicio.

Gestión de Configuración: El proceso establece los procedimientos y herramientas para la identificación registro, control y recuperación de elementos de configuración relacionados con los servicios de la organización. De igual forma asegura que todos los elementos de configuración están registrados, proteger y asegurar la integridad de todos los elementos de configuración, monitoriza el estado de todos los elementos de configuración y controla las interrelaciones entre los elementos de configuración.

Gestión de Niveles de Servicio: El objetivo del presente proceso es asegurar que todos los servicios vigentes, se proveen bajo el marco de objetivos y niveles de provisión acordados, alcanzables y medibles; mediante evaluación y revisión constante del cumplimiento de estos objetivos contra los valores logrados en la

provisión, para lograr mantener un nivel de calidad permanente en la provisión de los servicios.

Gestión de Capacidad: El objetivo del proceso es asegurar la garantía del servicio a través del cumplimiento de los requisitos de capacidad y rendimiento de manera eficiente en cuanto al tiempo y al costo para que el negocio experimente el valor que se le prometió.

Gestión de Disponibilidad y Continuidad: El principal objetivo es planificar, ejecutar y controlar la disponibilidad del servicio para el cumplimiento de los acuerdos de niveles de servicio (ANS / OLA); así mismo definir las acciones y procedimientos necesarios para garantizar la rápida y oportuna recuperación y puesta en marcha de los sistemas que soportan las operaciones.

PROCESOS OPERATIVOS

Entre los procesos operativos identificados, se encuentra el proceso de cobranzas, el proceso de ventas y el proceso de emisión, pero los dos últimos van de la mano con el proceso de Riesgos, por lo que han sido mencionados anteriormente.

Mesa de Servicios: El alcance del servicio consta de los siguientes puntos:

- Proporcionar equipamiento tecnológico a los usuarios ONP y/o los que ONP demande en materia de dispositivos conocidos como equipamiento tecnológico. El servicio de equipamiento tecnológico consta de: alquiler de equipamiento, soporte técnico, así como el mantenimiento preventivo y correctivo. (Desktop, Laptops, Equipos All in One, Lectora de Código de Barras, Estación de trabajo de equipo de diseño, Equipo portátil de diseño).
- Atender las solicitudes e incidentes a nivel nacional de los usuarios de acuerdo con el Catálogo de Servicios.
- Brindar el soporte en sitio sobre el equipamiento tecnológico brindado por el contratista para el servicio (instalación de hardware y software en sitio, traslados, incidentes microinformáticos, reparaciones, etc.).

Administración de la Plataforma Central

Base de Datos:

- Administración, monitoreo, configuración y gestión de accesos de la base de datos
- Monitoreo proactivo de las bases de datos en base
- Mantenimientos preventivos y correctivos de las bases de datos
- Afinamiento de la Base de datos
- Auditorías a las bases de datos

Servidores Unix y Linux:

- Gestión de los ambientes (Creación / Modificación / Eliminación de ambientes)
- Monitoreo proactivo y automatizado de los servidores
- Mantenimientos preventivos y correctivos.

Aplicaciones:

- Creación / Modificación / Eliminación de las aplicaciones
- Monitoreo y afinamiento proactivo de los Servidores de Aplicaciones, Procesos y Servidores de Gestión documental.
- Mantenimientos preventivos y correctivos de los Servidores de Aplicaciones, Procesos y Servidores de Gestión documental.
- Modificaciones en las aplicaciones y configuración de las mismas (incluye accesos)

Redes y Comunicaciones

- Administración de servidores físicos / virtuales Windows, VMWare, otros.
- Mantenimiento de Licencias y Soporte Técnico

- Implementar un servidor de archivos para disponer de la información necesaria de cada área de manera centralizada.
- Realizar mantenimiento periódico físico y lógico a los equipos (hardware) que soportan el servicio.
- Mantener actualizado todo el hardware que soporta los servicios con las últimas versiones estables de BIOS y/o Firmware
- Mantener actualizado todo el software que soporta los servicios con las últimas versiones, hotfix, support packages, service pack y parches, para garantizar la disponibilidad y estabilidad del servicio.
- Monitorear los componentes de todos los servicios (hardware, software)
- Monitorear permanentemente la atención a incidentes y requerimientos.
- Mantener un inventario actualizado de todo el hardware y software que administre (switches, teléfonos IP, Access Point, equipos de videoconferencia, Rack de comunicaciones).

Seguridad Perimetral

- Atender los requerimientos de creación, modificación y eliminación de cuentas de accesos.
- Atender en el momento adecuado las vulnerabilidades detectadas.
- Realizar el mantenimiento preventivo del equipamiento que soporta los servicios de Seguridad Perimetral, Acceso a Internet y acceso remoto.
- Mantener actualizados los equipos con las últimas actualizaciones liberadas y estables.
- Distribuir la actualización de antivirus a los servidores y estaciones de trabajo de la ONP y de las empresas que le brindan servicios.

Gestión de las Operaciones

- Gestión de acceso físico al data center
- Pases a QA y producción

- Ejecución de scripts
- Respaldo de información
- Restauración de información
- Traslado, almacenamiento y custodia de medios magnéticos
- Mantenimiento de los equipos de apoyo (UPS, aire acondicionado, extintores, cámara de vigilancia, panel eléctrico, etc.)
- Monitoreo de los elementos del servicio

PROCESOS DE SOPORTE

Procesos que brindan soporte o apoyo a los procesos operativos, entre los cuales podemos mencionar:

Gestión Financiera: Evaluar y controlar los costos asociados a los servicios de forma que se ofrezca un servicio de calidad a los clientes con un uso eficiente de los recursos de TI necesarios; además el proceso indicará el establecimiento del presupuesto del servicio.

Gestión Humana: Gestiona las contrataciones del personal, asimismo evalúa las competencias de las personas que laboran en el proyecto.

Calidad y Procesos: Realiza el seguimiento del proyecto, identifica oportunidades de mejora y evalúa la eficacia del sistema de gestión implementado.

Proceso Logística: Gestionar las relaciones con los suministradores durante todo su ciclo de vida desde la elección hasta el término de las relaciones contractuales de manera que éstas satisfagan los acuerdos de niveles de servicios establecidos con nuestros clientes actuales y futuros.

5.8.3. COMPRENDER LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

Se debe determinar quiénes son las partes interesadas y requisitos de las partes interesadas que sean pertinentes a la seguridad de la información. En tal sentido, se muestra a continuación las partes interesadas y los requisitos de estas:

CUADRO N° 5.14 PARTES INTERESADAS Y REQUISITOS DE SI

PARTES INTERESADAS		REQUISITOS DEL SGSI
INTERNAS	ACCIONISTAS	Maximizar la rentabilidad del negocio.
	GERENTES	Maximizar la rentabilidad del negocio. Garantizar la disponibilidad de los servicios entregados al cliente.
	COLABORADORES	Laborar en una empresa sólida y de prestigio. Proteger su información personal.
EXTERNAS	CLIENTE	Asegurar la confidencialidad, integridad y disponibilidad de su información
	PROVEEDORES	Alianzas estratégicas Proteger la continuidad de las operaciones Cumplimiento de los compromisos pactados
	GOBIERNO	Cumplir con las leyes Responsabilidad Social

Fuente: Elaboración propia

5.8.4. DETERMINAR EL ALCANCE DEL SGSI

Se ha definido el siguiente alcance para el sistema de gestión de seguridad de la información:

CUADRO N° 5.15 ALCANCE DEL SGSI

DESCRIPCIÓN DEL ALCANCE	
El alcance del sistema de gestión es el siguiente: ***"Gestión de las Operaciones y la Plataforma de TI del Centro de Datos, Gestión de la Mesa de Servicio; y Gestión de la Seguridad y Accesos Informáticos"*** Las instalaciones donde se desarrollan los procesos y servicios dentro del alcance del SGSI son: • Centro de Datos Principal, ubicado en Jr. Chota 998, esquina con Jr. Ilo; propiedad de GMD. • Centro de Datos de Enlace, ubicada en Jirón Bolivia 109 Sótano 01 Centro Cívico y Comercial de Lima; propiedad de ONP. • Centro de Datos de Contingencia, ubicada en Av. Paseo de la republica 4675 Surquillo Lima; propiedad de GMD. • Oficinas administrativas ubicada en Jirón Bolivia 109 Centro Cívico y Comercial de Lima, Piso 12	
REQUISITOS	***CARACTERISTICAS***
Lograr la adecuación de los procesos al estándar ISO 27001:2013	Cumplimiento de la norma
Obtener la certificación internacional ISO 27001:2013	Auditoria externa de certificación
CRITERIO DE ACEPTACIÓN DEL PRODUCTO	
CONCEPTOS	***CRITERIOS DE ACEPTACIÓN***
1. TÉCNICOS	Se debe cumplir el 100% del cronograma de trabajo
2. DE CALIDAD	Se debe obtener la certificación del sistema de gestión
3. ADMINISTRATIVOS	Todos los entregables deben ser aprobados por el cliente
ENTREGABLES DEL PROYECTO	
FASE DEL PROYECTO	***PRODUCTO ENTREGADO***
DIAGNOSTICO	- Informe de Diagnostico (Análisis de brecha)
CONTEXTO DE LA ORGANIZACIÓN	- Identificación de las partes interesadas - Requisitos de seguridad de la información - Alcance del SGSI
LIDERAZGO	- Política de SI - Roles y responsabilidades del SGSI
PLANEACIÓN	- Metodología de gestión de riesgos - Declaración de aplicabilidad
SOPORTE	- Plan de capacitación - Plan de concienciación - Plan de comunicaciones del SGSI - Documentos del SGSI
OPERACIÓN	- Medición del SGSI - Gestión de cambios - Matriz de evaluación de riesgos - Plan de tratamiento de riesgos
EVALUACIÓN DEL DESEMPEÑO	- Programa de auditoria - Plan de auditoria interna - Informe de auditoría interna - Revisión de gestión
MEJORA	- Solicitud de acción correctiva
AUDITORIA DE CERTIFICACIÓN	- Certificado del SGSI

EXCLUSIÓNES DEL PROYECTO
Para el proyecto no se consideran los siguientes controles del anexo A de la norma ISO/IEC 27001:2013 • A.6.2.1 / A.6.2.2 Política de dispositivos móviles / Trabajo remoto. Dentro del alcance del SGSI no se contempla el uso de dispositivos móviles ni teletrabajo o trabajo remoto. • 10.1.1 Política sobre el uso de controles criptográficos / 10.1.2 Gestión de claves. Dentro del alcance del SGSI no se contempla el uso de controles criptograficos • A.11.2.6 Dentro del alcance del SGSI no se contempla el uso de equipos fuera de las instalaciones • A.13.2.2 Acuerdos sobre mensajería de información. Dentro del alcance del SGSI no se contempla transferencia de información a terceros. • A.13.2.3 • A.14.1.1 Dentro del alcance del SGSI no se contempla desarrollo de producto de software • A.14.2.1 hasta A.14.2.9 Dentro del alcance del SGSI no se contempla desarrollo de producto de software • A.14.3.1 Dentro del alcance del SGSI no se contempla desarrollo de producto de software • A.18.1.5 No hay regulación de controles criptográficos

RESTRICCIONES DEL PROYECTO	
INTERNOS A LA ORGANIZACIÓN	***EXTERNOS A LA ORGANIZACIÓN***
Los entregables deberán presentarse en la fecha propuesta en el cronograma	El cliente definirá los requisitos de seguridad aplicables al sistema de gestión
El presupuesto del proyecto no debe exceder lo presentado en la propuesta	
Se presentará un informe mensual sobre el avance del presente proyecto	

SUPUESTOS DEL PROYECTO	
INTERNOS A LA ORGANIZACIÓN	***EXTERNOS A LA ORGANIZACIÓN***
Los entregables se elaborarán y presentarán con anticipación (antes del plazo de compromiso)	El cliente respetara el cronograma de trabajo presentado
El servicio cuenta con el equipamiento tecnológico necesario (servidores, comunicaciones, etc.)	Implementados y operativos
El cronograma de trabajo no sufrirá cambio alguno	Los informes de avance serán revisados y aprobados por el cliente.

Fuente: Elaboración propia

5.8.5. LIDERAZGO Y COMPROMISO

La alta dirección demuestra su compromiso al definir los roles y responsabilidades, los recursos necesarios, al definir la política y los objetivos de seguridad de la información.

5.8.6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El servicio de administración de la plataforma central y mesa de administración de servicios responsable de administrar la plataforma central y de atender los requerimientos e incidentes reportados por los usuarios finales (cliente) administrados por la empresa GMD, consciente de la importancia de proteger la información importante para el negocio, decidió implementar un sistema de gestión de seguridad de la información (SGSI), para lo cual suscribe la presente política:

La alta dirección ha adoptado una Política de Seguridad de la Información, para asegurar la protección de la información en la prestación de los servicios del Centro de Datos y Comunicaciones; y Mesa de Administración de Servicios, por ello se compromete en:

- ✓ *Cumplir con las regulaciones aplicables en torno a la seguridad de la información.*
- ✓ *Mejorar continuamente la eficacia del SGSI*
- ✓ *Mantener una cultura organizacional que aliente a todos los trabajadores a asumir una responsabilidad por la seguridad de la información*
- ✓ *Mejorar continuamente el SGSI*
- ✓ *Proteger la información y sus activos de información a través de un SGSI para garantizar su confidencialidad, integridad y disponibilidad.*
- ✓ *Dar respuesta inmediata a los incidentes que se presenten*

5.8.7. ROLES Y RESPONSABILIDADES DEL SGSI

Comité del SGSI

Comité Conformado por: Gerente del Proyecto, Jefe de Proyecto y el Oficial de Seguridad de la Información; cuyas principales responsabilidades son las siguientes:

- Establecer, revisar, aprobar y comunicar la política y los objetivos de seguridad de la información y la importancia de su cumplimiento, asegurando que estos sean compatibles con el plan estratégico de la organización, y la importancia de su cumplimiento.
- Asegurar que los requisitos del sistema de gestión de la seguridad de la información están integrados a los procesos de la organización definiéndolos en los procedimientos y políticas del SGSI.
- Asegurar que los recursos necesarios para el sistema de gestión de la seguridad de la información están disponibles.
- Dirigir y apoyar a las personas para que contribuyan a la eficacia del sistema de gestión de la seguridad de la información.
- Promover la mejora continua.
- Revisar el SGSI de manera periódica (mínimo 1 vez al año), para la toma de decisiones para la mejora del sistema.
- Asignar roles específicos y responsabilidades para la seguridad de información en la organización.
- Revisar los resultados de las evaluaciones de riesgo y aprobar el tratamiento de los riesgos identificados, justificando aquellos que no serán tratados (aceptados).
- Revisar los hallazgos de auditoria del SGSI y definir las acciones necesarias al respecto.

Oficial de Seguridad de la Información

- Informar a la Alta Dirección sobre el desempeño del SGSI.
- Controlar los documentos del SGSI.

- Consolidar los resultados de la gestión del SGSI y comunicar esta información a las partes interesadas.
- Organizar la realización de las auditorías internas y externas del SGSI.
- Promover la capacitación y concientización del personal acerca de la gestión de la seguridad de la información.
- Liderar los proyectos de mejora del SGSI.
- Gestión de los acuerdos de niveles de servicio.

Propietario del Activo de Información

- Controlar el uso y seguridad de los activos que le son asignados para la creación, procesamiento, transmisión y almacenamiento de información relacionadas al proceso o área que le compete.
- Autorizar el uso del activo de información del cual es propietario, bajo responsabilidad, de manera que se preserve la seguridad de la información.
- Entender y abordar los riesgos/oportunidades relacionados a la seguridad de la información de los activos del proceso o área de su responsabilidad.
- Asegurar que el activo de información se utiliza únicamente para los propósitos de la organización.

Custodio del Activo de Información

- Cumplir las políticas, procedimientos y controles de seguridad de la información establecidos para el uso aceptable de los activos de información que le compete.
- Hacer uso correcto y seguro del activo de información que le compete.
- Comunicar al propietario del activo de información las amenazas y vulnerabilidades que identifique durante el desarrollo de sus actividades.
- Facilitar las actividades de implementación de controles de seguridad de la información sobre los activos de su competencia.

Propietario del Riesgo

- Asegurar que se implementen los controles de seguridad definidos para reducir a un nivel aceptable el riesgo que le fue asignado.

5.8.8. ACCIONES PARA ABORDAR LOS RIESGOS Y OPORTUNIDADES

A continuación, se detalla la metodología diseñada por el autor del presente trabajo para la gestión de riesgos de seguridad de la información el cual comprende las siguientes etapas:

- Identificar los activos y/ grupos de activos de información relevantes para el negocio.
- Identificar los eventos potenciales que pueden tener un efecto positivo o negativo sobre los activos de información
- Determinar la probabilidad de ocurrencia del evento.
- Estimar el nivel de impacto en función de la confidencialidad, integridad o disponibilidad.
- Estimar el nivel del riesgo
- Evaluar la prioridad para la atención del riesgo
- Identificar las acciones necesarias (Tratamiento de los riesgos)
- Calcular el riesgo residual

5.8.8.1. Inventario de los Activos de Información

Cada activo es clasificado según su tipo para lo cual se han identificado los siguientes tipos de activos de información:

CUADRO N° 5.16 TIPOS DE ACTIVOS

TIPO ACTIVO	DESCRIPCION
Servicios	Servicios que implican el acceso a datos o información, recibidos de terceros.

TIPO ACTIVO	DESCRIPCION
Datos e Información	Bases de datos, Archivos electrónicos, Documentos y registros en papel.
Software	Software base, Aplicaciones, Sistemas Operativos y utilitarios
Hardware	Servidores, Desktop, Laptops, Storage, Librería de Cintas, etc.
Redes de Comunicación	Switches, Routers, Firewalls, Access point, Sistemas de telefonía, etc.
Soportes de Información	Cintas de backups, DVD (Microformas)
Equipamiento Auxiliar	Aire acondicionado, UPS, Grupo electrógeno, Alarmas, Detectores de humo, Extintores de fuego, Medidores de temperatura, etc.
Instalaciones	Datacenters, Bóvedas, Sedes, Oficinas, Salas, Almacenes, Cintotecas, etc.
Personas	Personal interno, Personal externo, Proveedores, Clientes

Fuente: Elaboración propia

5.8.8.2. Valorización del activo de información

El valor del activo de información estará en función del impacto que podría tener en las siguientes dimensiones: Confidencialidad, Integridad y Disponibilidad, según se detalla en el cuadro 2.4

CUADRO N° 5.17 VALORIZACIÓN DE LOS ACTIVOS

CRITERIOS PARA LA VALORACION DE ACTIVOS DE INFORMACION			
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
Nivel	La falla o pérdida de un activo origina la divulgación o revelamiento no autorizado de información; produciendo un impacto que afecta los intereses de la organización (prestigio, económico, legal, competencia, etc.)	La falla o pérdida de un activo origina la alteración de la información (dejando de ser exacta y completa); produciendo un impacto que afecta los intereses de la organización (prestigio, económico, legal, competencia, etc.)	La falla o pérdida de un activo origina la interrupción del acceso y disponibilidad de la información; produciéndose un impacto que afecta los intereses de la organización (prestigio, económico, legal, competencia, etc.)
Muy Alto (5)	Impacto irreversible	Impacto irreversible	Impacto irreversible
Alto (4)	Impacto severo	Impacto severo	Impacto severo
Medio (3)	Impacto moderado	Impacto moderado	Impacto moderado
Bajo (2)	Impacto parcial	Impacto parcial	Impacto parcial
Muy Bajo (1)	Sin impacto	Sin impacto	Sin impacto

Fuente: Elaboración propia

El valor del activo será el promedio de los 3 valores registrados por cada dimensión citada anteriormente, aquellos activos con un valor del riesgo mayor o igual a 3 pasaran al análisis del riesgo.

5.8.8.3. Descripción del Riesgo

Se deben detallar los eventos o escenarios que podrían ocurrir y que podrían tener un impacto positivo o negativo en los activos de información.

Existen los siguientes tipos de eventos: naturales (Terremoto, inundaciones, etc.), Humanos (Falta de conocimiento, error humano, vandalismo), Tecnológico (Error de fábrica, falta de mantenimiento, etc.), Software (Infección de virus, falla del sistema operativo, etc.), entre otros.

5.8.8.4. Probabilidad de Ocurrencia

La probabilidad de ocurrencia del evento se establece de acuerdo con el siguiente cuadro de referencia:

CUADRO N° 5.18 PROBABILIDAD DE OCURRENCIA

PROBABILIDAD DE OCURRENCIA	
VALOR	FRECUENCIA
5	Muy Frecuente
4	Frecuente
3	Normal
2	Poco Frecuente
1	Raramente

Fuente: Elaboración propia

5.8.8.5. Nivel de Impacto

El nivel de impacto (positivo o negativo) es calculado teniendo en cuenta impacto que tendría el riesgo de materializarse en función de la confidencialidad, integridad y disponibilidad de la información, el valor del

impacto es el máximo valor obtenido de las 3 dimensiones citadas anteriormente

CUADRO N° 5.19 CÁLCULO DEL IMPACTO

IMPACTO			
CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR DEL IMPACTO

Fuente: Elaboración propia

5.8.8.6. Calculo del Riesgo

El valor del riesgo es calculado en función de la probabilidad y el impacto, a saber: Riesgo = Probabilidad x Impacto

CUADRO N° 5.20 CÁLCULO DEL RIESGO

IMPACTO						
Extremo	5	5	10	15	20	25
Mayor	4	4	8	12	16	20
Moderado	3	3	6	9	12	15
Menor	2	2	4	6	8	10
Insignificante	1	1	2	3	4	5
		1	2	3	4	5
		Raramente	Poco Frecuente	Normal	Frecuente	Muy Frecuente
		PROBABILIDAD				

Fuente: Elaboración propia

CUADRO N° 5.21 CRITERIO DE ACEPTACIÓN DEL RIESGO

CRITERIO DE ACEPTACIÓN DEL RIESGO		
NIVEL	RANGO	DESCRIPCIÓN
ALTO	[15 – 25]	Riesgo no aceptable
MEDIO	[9 – 12]	Riesgo no aceptable
BAJO	[1 – 8]	Riesgo aceptable

Fuente: Elaboración propia

5.8.8.7. Tratamiento del Riesgo

Para los riesgos se han establecidos las siguientes opciones de tratamiento:

- **Evitar:** Esta estrategia consiste en no iniciar o no continuar con la actividad que motiva el riesgo, por ejemplo, aislar los objetivos del proyecto, cambiar el objetivo que se encuentra amenazado, reducir el alcance del proyecto, entre otros.
- **Mitigar:** Esta estrategia consiste en actuar para reducir la probabilidad de ocurrencia o el impacto de un riesgo.
- **Compartir:** Consiste en trasladar el impacto o consecuencia de un riesgo a un tercero, junto con la responsabilidad de la respuesta.
- **Aceptar:** Consiste en reconocer y asumir las consecuencias del riesgo sin tomar medida alguna, a menos que el riesgo se materialice.

Para cada evento se realiza la descripción de las acciones a realizar con el propósito de realizar el tratamiento en base a la estrategia elegida (opción de tratamiento). La selección de un control debe ir acompañado de los plazos y responsables de atender cada riesgo.

5.8.8.8. Cálculo del Riesgo Residual

Es el valor del riesgo que resulta luego de aplicar los controles respectivos para atender el riesgo, el nivel de riesgo residual es calculado mediante la siguiente formula:

CUADRO N° 5.22 CÁLCULO DEL RIESGO RESIDUAL

Riesgo Residual = Riesgo – Riesgo x (Efectividad del control)

Fuente: Elaboración propia

5.8.9. DECLARACIÓN DE APLICABILIDAD

Se definen que controles del anexo A de la norma ISO 27001:2013 que son aplicables al sistema de gestión, para el presenta trabajo se han considerado los que se presentan a continuación:

CUADRO N° 5.23 ENUNCIADO DE APLICABILIDAD

OBJETIVO DE CONTROL	CONTROL	¿APLICA?	JUSTIFICACIÓN
5.1 Política de seguridad de la información	5.1.1 Política de seguridad de la información	SI	POL.GER.001 Política de Seguridad de la Información
	5.1.2 Revisión de las políticas de seguridad de la información	SI	POL.GER.001 Política de Seguridad de la Información
6.1 Organización Interna	6.1.1 Roles y responsabilidades de la seguridad de la información	SI	MAN.GER.001 Manual de Organización y Funciones del SGSI
	6.1.2 Segregación de funciones	SI	MAN.GER.001 Manual de Organización y Funciones del SGSI
	6.1.3 Contacto con autoridades	SI	FOR.GER.012 Lista de Contactos
	6.1.4 Contacto con grupos especiales de interés	SI	FOR.GER.012 Lista de Contactos
	6.1.5 Seguridad de la información en la gestión de proyectos	SI	PRO.MAS.053 Gestión de Cambios
6.2 Dispositivos móviles y trabajo remoto	6.2.1 Política de dispositivos móviles	NO	Dentro del alcance del SGSI no se contempla el uso de dispositivos móviles.
	6.2.2 Trabajo remoto	NO	Dentro del alcance del SGSI no se contempla el trabajo remoto
7.1 Previo al empleo	7.1.1 Proceso de selección	SI	PRO.GER.001 Ingreso de Personal
	7.1.2 Términos y condiciones de la relación laboral	SI	Contratos de Trabajo / Acuerdos de confidencialidad
7.2 Durante el empleo	7.2.1 Responsabilidad de la Dirección	SI	MAN.GER.001 Manual de Organización y Funciones del SGSI

OBJETIVO DE CONTROL	CONTROL	¿APLICA?	JUSTIFICACIÓN
	7.2.2 Concientización, educación y formación en seguridad de la información	SI	Plan de Capacitación
	7.2.3 Proceso disciplinario	SI	PRO.GER.002 Proceso Disciplinario
7.3 Desvinculación y cambio de empleo	7.3.1 Responsabilidades en la desvinculación o cambio de empleo	SI	PRO.GER.003 Terminación de Relación Laboral
8.1 Responsabilidad por los activos	8.1.1 Inventario de activos	SI	FOR.GER.016 Inventario de Activos
	8.1.2 Propiedad de los activos	SI	FOR.GER.016 Inventario de Activos
	8.1.3 Uso aceptable de los activos	SI	POL.GER.004 Política de Gestión de activos
	8.1.4 Devolución de los activos	SI	PRO.GER.003 Terminación de Relación Laboral
8.2 Clasificación de la información	8.2.1 Clasificación de la información	SI	POL.GER.004 Política de Gestión de activos
	8.2.2 Etiquetado de la información	SI	POL.GER.004 Política de Gestión de activos
	8.2.3 Manejo de activos	SI	POL.GER.004 Política de Gestión de activos
8.3 Manejo de medios de soporte	8.3.1 Gestión de los medios removibles	SI	POL.GER.004 Política de Gestión de activos
	8.3.2 Eliminación de los medios	SI	POL.GER.004 Política de Gestión de activos
	8.3.3 Transferencia física de los medios	SI	POL.GER.004 Política de Gestión de activos
9.1 Requisito de negocio para el control de acceso	9.1.1 Política de control de acceso	SI	PRO.SIN.001 Control de Accesos
	9.1.2 Acceso a las redes y a los servicios de la red	SI	PRO.SIN.001 Control de Accesos
9.2 Gestión de acceso de los usuarios	9.2.1 Registro y cancelación de registros de usuarios	SI	PRO.SIN.001 Control de Accesos
	9.2.2 Asignación de acceso de usuario	SI	PRO.SIN.001 Control de Accesos
	9.2.3 Gestión de derechos de acceso privilegiados	SI	PRO.SIN.001 Control de Accesos
	9.2.4 Gestión de información secreta de autenticación de usuarios	SI	PRO.SIN.001 Control de Accesos
	9.2.5 Revisión de los derechos de acceso de usuarios	SI	Informe Mensual de Servicio
	9.2.6 Eliminación o ajuste de los derechos de acceso	SI	Informe Mensual de Servicio
9.3 Responsabilidades del usuario	9.3.1 Uso de información de autenticación secreta	SI	Acuerdos de confidencialidad
9.4 Control de acceso al sistema y aplicaciones	9.4.1 Restricción de acceso a la información	SI	Controles de acceso físico (seguridad física) Controles de acceso a los sistemas de información

OBJETIVO DE CONTROL	CONTROL	¿APLICA?	JUSTIFICACIÓN
	9.4.2 Procedimiento de inicio de sesión seguro	SI	Control de acceso a los sistemas (Usuario y contraseña)
	9.4.3 Sistema de gestión de contraseñas	SI	PRO.SIN.001 Control de Accesos
	9.4.4 Uso de programas utilitarios privilegiados	SI	Declaración de cuentas privilegiadas
	9.4.5 Control de acceso al código fuente de los programas	SI	Herramienta Harvest para protección de código fuente de los programas que pasan a producción
10.1 Controles criptográficos	10.1.1 Política sobre el uso de controles criptográficos	NO	Dentro del alcance del SGSI no se contempla el uso de controles criptográficos
	10.1.2 Gestión de claves	NO	Dentro del alcance del SGSI no se contempla el uso de controles criptográficos
11.1 Áreas seguras	11.1.1 Perímetro de seguridad física	SI	Centros de Datos / Instalaciones / Perímetros de seguridad física
	11.1.2 Controles de acceso físico	SI	Personal de vigilancia Control de acceso con tarjeta de proximidad a las oficinas
	11.1.3 Seguridad de oficinas, salas e instalaciones	SI	Control de acceso físico a las instalaciones ONP / GMD
	11.1.4 Protección contra amenazas externas y del ambiente	SI	Centros de Datos / Instalaciones / Controles de seguridad contra amenazas externas y del ambiente
	11.1.5 Trabajo en áreas seguras	SI	Centros de Datos / Instalaciones / Perímetros de seguridad física
	11.1.6 Áreas de entrega y carga	SI	Centros de Datos / Instalaciones / Perímetros de seguridad física / control de acceso físico a las instalaciones ONP / GMD
11.2 Equipamiento	11.2.1 Ubicación y protección del equipamiento	SI	Equipos ubicados en instalaciones protegidas Centro de Datos Principal / Enlace / Contingencia
	11.2.2 Elementos de soporte	SI	Equipos de soporte a la infraestructura tecnológica Centro de Datos Principal / Enlace / Contingencia
	11.2.3 Seguridad en el cableado	SI	Cableado estructurado, equipos ubicados en racks, canaletas, otros
	11.2.4 Mantenimiento del equipamiento	SI	Plan de Mantenimiento Preventivo
	11.2.5 Retiro de activos	SI	Control físico de ingreso y salida de equipos
	11.2.6 Seguridad de equipamiento y los activos fuera de las instalaciones	NO	Dentro del alcance del SGSI no se contempla el uso de equipos fuera de las instalaciones.
	11.2.7 Seguridad en la reutilización o descarte de equipos	SI	PRO.MAS.060.Borrado.de.Información.de.Medios PRO.MAS.061.Respaldo.de.Información

OBJETIVO DE CONTROL	CONTROL	¿APLICA?	JUSTIFICACIÓN
	11.2.8 Equipo de usuario desatendido	SI	POL.GER.002 Política de Escritorio y Pantalla Limpios
	11.2.9 Política de escritorio y pantalla limpios	SI	POL.GER.002 Política de Escritorio y Pantalla Limpios
12.1 Procedimientos operacionales y responsabilidades	12.1.1 Procedimiento de operación documentados	SI	Políticas y procedimientos de seguridad de la información / Repositorio de documentos
	12.1.2 Gestión de cambios	SI	PRO.MAS.053 Gestión de Cambios
	12.1.3 Gestión de la capacidad	SI	Sistema de Monitoreo de Servicio Informe de capacidad Informe Mensual de Servicio
	12.1.4 Separación de los ambientes de desarrollo, prueba y operaciones	SI	Ambientes de desarrollo, pruebas y producción
12.2 Protección contra código malicioso	12.2.1 Controles contra código malicioso	SI	Seguridad perimetral (IPS, Firewall, Anti spam, Proxy directo y reverso, Antivirus, Antispyware)
12.3 Respaldo	12.3.1 Respaldo de la información	SI	PRO.CCE.001 Ejecución de Backup
12.4 Registro y monitoreo	12.4.1 Registro de evento	SI	Auditoria de Eventos
	12.4.2 Protección de la información de registros	SI	PRO.CCE.001 Ejecución de Backup
	12.4.3 Registros del administrador y operador	SI	Auditoria de Eventos
	12.4.4 Sincronización de relojes	SI	Control de sincronización de servidores NTP
12.5 Control de software de operación	12.5.1 Instalación del software en sistemas operacionales	SI	PRO.MAS.053 Gestión de Cambios
12.6 Gestión de la vulnerabilidad técnica	12.6.1 Gestión de las vulnerabilidades técnicas	SI	Informe de fixes y actualización de software base
	12.6.2 Restricciones sobre la instalación de software	SI	Lista de software base
12.7 Consideraciones de la auditoría de los sistemas de información	12.7.1 Controles de auditoría de sistemas de información	SI	Auditoria de Eventos
13.1 Gestión de la seguridad de red	13.1.1 Controles de red	SI	Seguridad perimetral (IPS, Firewall, Anti spam, Proxy directo y reverso, Antivirus, Antispyware)
	13.1.2 Seguridad de los servicios de red	SI	PRO.SIN.001 Control de Accesos
	13.1.3 Separación en las redes	SI	Seguridad perimetral / Segregación de redes VLANs
13.2 Transferencia de información	13.2.1 Políticas y procedimientos de transferencia de información	SI	Seguridad perimetral (IPS, Firewall, Anti spam, Proxy directo y reverso, Antivirus, Antispyware)
	13.2.2 Acuerdos sobre transferencia de información	NO	Dentro del alcance del SGSI no se contempla transferencia de información a terceros.

OBJETIVO DE CONTROL	CONTROL	¿APLICA?	JUSTIFICACIÓN
	13.2.3 Mensajería electrónica	NO	Dentro del alcance del SGSI no se contempla el uso de controles criptográficos
	13.2.4 Acuerdos de confidencialidad o no divulgación	SI	Acuerdos de confidencialidad
14.1 Requisitos de seguridad de los sistemas de información	14.1.1 Análisis y especificación de requisitos de seguridad de la información	NO	Dentro del alcance del SGSI no se contempla desarrollo de productos software
	14.1.2 Aseguramiento de servicios de aplicación en redes públicas	SI	Seguridad perimetral (IPS, Firewall, Anti spam, Proxy directo y reverso, Antivirus, Antispyware)
	14.1.3 Protección de las transacciones de servicios de aplicación	SI	Seguridad perimetral (IPS, Firewall, Anti spam, Proxy directo y reverso, Antivirus, Antispyware)
14.2 Seguridad en procesos de desarrollo y soporte	14.2.1 Política de desarrollo seguro	NO	Dentro del alcance del SGSI no se contempla desarrollo de productos software
	14.2.2 Procedimientos de control de cambios del sistema	NO	
	14.2.3 Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación	NO	
	14.2.4 Restricciones en los cambios a los paquetes de software	NO	
	14.2.5 Principios de ingeniería de sistema seguro	NO	
	14.2.6 Entorno de desarrollo seguro	NO	
	14.2.7 Desarrollo tercerizado	NO	
	14.2.8 Prueba de seguridad del sistema	NO	
	14.2.9 Prueba de aprobación del sistema	NO	
14.3 Datos de prueba	14.3.1 Protección de datos de prueba	NO	Dentro del alcance del SGSI no se contempla desarrollo de productos software
15.1 Seguridad de la información en las relaciones con el proveedor	15.1.1 Política de seguridad de la información para las relaciones con el proveedor	SI	Bases del servicio Contratos
	15.1.2 Abordar la seguridad dentro de los acuerdos del proveedor	SI	Cláusulas de seguridad de la información en contratos con los proveedores
	15.1.3 Cadena de suministro de tecnologías de la información y comunicaciones	SI	Contrato de servicio / ONP-GMD / Servicio de administración del centro de datos y comunicaciones Servicio de equipamiento tecnológico del personal y mesa de administración de servicios
15.2 Gestión de entrega del servicio del proveedor	15.2.1 Supervisión y revisión de los servicios del proveedor	SI	Informe Mensual de Servicio
	15.2.2 Gestión de cambios a los servicios del proveedor	SI	PRO.MAS.053 Gestión de Cambios

OBJETIVO DE CONTROL	CONTROL	¿APLICA?	JUSTIFICACIÓN
16.1 Gestión de incidentes de seguridad de la información y mejoras	16.1.1 Responsabilidades y procedimientos	SI	PRO.GER.008 Gestión de Incidentes de Seguridad
	16.1.2 Informe de eventos de seguridad de la información	SI	PRO.GER.008 Gestión de Incidentes de Seguridad
	16.1.3 Informe de debilidades de seguridad de la información	SI	Informe de fixes y actualización de software base
	16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información	SI	PRO.GER.008 Gestión de Incidentes de Seguridad
	16.1.5 Respuesta ante incidentes de seguridad de la información	SI	PRO.GER.008 Gestión de Incidentes de Seguridad
	16.1.6 Aprendizaje de los incidentes de seguridad de la información	SI	PRO.GER.008 Gestión de Incidentes de Seguridad
	16.1.7 Recolección de evidencia	SI	PRO.GER.008 Gestión de Incidentes de Seguridad
17.1 Continuidad de la seguridad de la información	17.1.1 Planificación de la continuidad de la seguridad de la información	SI	Plan de Contingencia
	17.1.2 Implementación de la continuidad de la seguridad de la información	SI	Plan de Contingencia
	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	Informe técnico de pruebas de contingencia
17.2 Redundancias	17.2.1 Disponibilidad de las instalaciones de procesamiento de la información	SI	Centro de Datos Principal / Centro de Datos Alterno
18.1 Cumplimiento con los requisitos legales y contractuales	18.1.1 Identificación de la legislación vigente y los requisitos contractuales	SI	FOR.GER.024 Identificación de Requisitos de Seguridad de la Información
	18.1.2 Derechos de propiedad intelectual	SI	POL.GER.005 Política de Administración de Software
	18.1.3 Protección de los registros	SI	PRO.GER.004 Control de Documentos / PRO.GER.005 Control de Registros
	18.1.4 Privacidad y protección de la información de carácter personal	SI	Controles de seguridad aplicables a las bases de datos de carácter personal
	18.1.5 Regulación de los controles criptográficos	NO	Dentro del alcance del SGSI no se contempla el uso de controles criptográficos
18.2 Revisiones de seguridad de la información	18.2.1 Revisión independiente de la seguridad de la información	SI	Auditorías Internas / Externas del SGSI
	18.2.2 Cumplimiento con las normas y políticas de seguridad de la información	SI	FOR.GER.023 Medición de Procesos y Controles del SGSI
	18.2.3 Verificación del cumplimiento técnico	SI	Informe Mensual de Servicio

Fuente: Elaboración propia

5.8.10. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

Planificación de la continuidad de la Seguridad de la Información: La continuidad de la seguridad de la información es planificada para ello se elaboran Planes de Continuidad y Disponibilidad con la finalidad de establecer los requisitos para asegurar la continuidad y disponibilidad de la operación, incluida la seguridad de la información.

Implementación de la continuidad de la seguridad de la información: Se establece, documenta, implementa y mantiene procesos, procedimientos y controles para asegurar el nivel necesario de continuidad; para la seguridad de la información durante una situación adversa.

Verificación, revisión y evaluación de la continuidad de la seguridad de la información: Los planes de continuidad y disponibilidad son probados, revisados y actualizados de manera anual. Posteriormente, el personal a cargo elabora un informe acerca del resultado obtenido y lo presenta al responsable del Área o Proyecto para la toma de decisiones correspondiente.

Cuando se encuentren resultados no favorables de dichas pruebas, el responsable del Área o proyecto se encargará de gestionar la corrección de dichos resultados.

Disponibilidad de las instalaciones de procesamiento de la Información: GMD cuenta con dos Data center: Surquillo y Chota (TIER III) los cuales tienen redundancia debido a que cada site cuenta con dos sistemas eléctricos independientes, lo que permite cumplir con los requisitos de disponibilidad de los servicios que brinda.

5.8.11. GESTIÓN DE CAMBIOS

A continuación, se establece el proceso para gestionar los cambios a fin de garantizar la integridad del Sistema de Gestión de Seguridad de la Información.

Identificar Requerimientos, necesidades, oportunidades de cambio

Se identifican los cambios que puedan afectar el Sistema de Gestión de Calidad a través de:

- Las revisiones por la dirección,
- Auditorías internas
- Auditorías externas
- Medición de la Satisfacción
- Revisión documentaria

Los cambios se clasifican en menores o mayores:

- Los cambios menores pueden ser sencillos: agregar una ayuda visual, aclarar un párrafo en un procedimiento documentado, etc.
- Los cambios mayores pueden implicar cambios en el alcance del sistema, la política, los objetivos, nuevos métodos o procedimientos de trabajo, integración con otros sistemas de gestión.

Registrar los cambios identificados

La mesa de servicios recibe las solicitudes de cambios y los registra asignándoles un código (número del ticket)

Todas las solicitudes de cambio son registradas en el formato de gestión de cambios (RFC)

Evaluar las Solicitudes de cambio

Todas las solicitudes de cambio deben ser evaluadas, para ello se debe de contar con la información necesaria, y quien hace la solicitud de cambio debe de estar disponible para proporcionar la información adicional que le sea requerida.

El Comité de Cambios debe reunirse para evaluar el cambio solicitado; se puede integrar un experto técnico que pueda aportar su opinión y conocimiento.

Para evaluar un cambio se tiene que contar como mínimo con la siguiente información:

- Descripción clara del cambio, incluyendo su alcance.

- La finalidad del cambio.
- Sus posibles consecuencias tanto positivas como negativas.
- Cómo se controlará la implementación del cambio.
- Cuáles serán los recursos necesarios y cómo se dispondrán.
- Cuáles son las responsabilidades y autoridades.

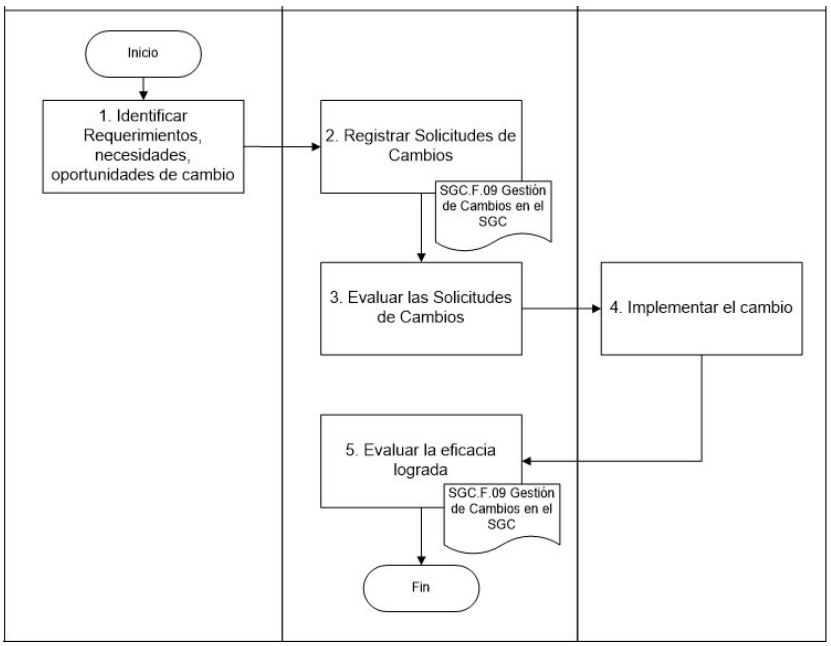
Implementar el cambio

La implementación de un cambio debe de hacerse sin afectar la integridad del sistema de gestión.

Seguimiento del Cambio

Se realizará el seguimiento a la implementación del cambio hasta que este se haya realizado, el líder de la implementación debe de informar a la mesa de servicios para que este ponga el cambio en el estatus de implementado en el (RFC)

FIGURA N° 5.6 PROCESO DE CAMBIOS



Fuente: Elaboración propia

5.8.12. INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La respuesta rápida, eficaz y metódica de los eventos e incidentes de seguridad de la información se lleva a cabo a través de la comunicación, atención, tratamiento y solución de estos, siguiendo los procedimientos de gestión de incidentes de cada área o proyecto.

El seguimiento y control es canalizado a través de los Comités del SGSI, para la toma de decisiones correspondiente.

Responsabilidades

El responsable del área o proyecto es responsable de:

- Asegurar que los incidentes de seguridad de la información tengan una respuesta rápida, efectiva y ordenada.
- Aplicar el Proceso Disciplinario en el SGSI (llamada de atención. Suspensión o despido) cuando la gravedad del incidente lo amerite.
- Asegurar que se recopilen, conserven y se presente un informe conteniendo las evidencias pertinentes y acciones preventivas y correctivas cuando el caso lo amerite.
- Supervisar el cumplimiento del presente procedimiento.
- El personal del proyecto es responsable de:
- Comunicar (reportar) los eventos y debilidades de seguridad de la información al responsable del área de negocio.

El Oficial de Seguridad de la Información es responsable de:

- Analizar los reportes de incidentes de seguridad con las áreas del alcance, con el propósito de identificar problemas relacionados con la seguridad de la información y gestionar su tratamiento de manera sistemática en coordinación con las áreas involucradas.
- Informar los resultados de la gestión de incidentes a los Comités de Operación y de Gestión en los niveles que corresponde.

A continuación, se definen algunos ejemplos para identificar los eventos e incidentes de seguridad de la información:

Eventos de seguridad de la información

Los eventos podrían darse en los siguientes escenarios, pero no se limitan a:

- Un mensaje de error en una aplicación
- Un usuario que se conecta a un sistema.
- Un intento fallido de un usuario para ingresar a una aplicación.
- Un firewall que permite o bloquea un acceso.
- Una notificación de cambio de contraseña de un usuario privilegiado, etc.
- Una puerta abierta.
- Un control de huella dactilar averiado
- La pérdida de un fotocheck y/o tarjeta de apertura de puertas
- La publicación de información sensible
- Etc.

Incidentes de Seguridad De La Información

Los incidentes podrían darse en los siguientes escenarios, pero no se limitan a:

- Acceso no autorizado a información reservada.
- Modificaciones no autorizadas.
- Revelación de información no autorizada.
- Infección de los sistemas de información con malware
- Fallas o interrupciones en los sistemas de información.
- Perdida de equipos.
- Cortes de suministro eléctrico.
- Ataque informático
- Ataque físico
- Etc.

Informe de eventos de Seguridad de la Información

Los eventos de seguridad de la información se informan lo antes posible, a través de los siguientes canales:

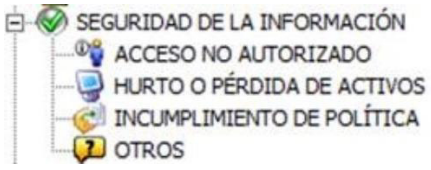
Para sistemas de Información: Los sistemas de procesamiento de información son monitoreados por el área de operaciones del Datacenter a través del uso de la herramienta de monitoreo "**Foglight".**

FIGURA N° 5.7 HERRAMIENTA DE MONITOREO

Fuente: Elaboración propia

Los eventos detectados por las herramientas de monitoreo (en modo de "Alertas del Sistema") son registrados en la herramienta Service Desk en donde el operador le asigna la categoría de evento o incidente teniendo en cuenta los criterios establecidos:

FIGURA N° 5.8 CATEGORIA DE INCIDENTES DE SI



Fuente: Elaboración propia

Inmediatamente, tanto los eventos o incidentes son escalados a los especialistas para realizar las acciones correctivas necesarias.

FIGURA N° 5.9 GRUPO RESOLUTOR SGSI

Fuente: Elaboración propia

Para los procesos del SGSI: Los eventos de seguridad de la información que involucran a personas o procesos son identificados por cualquier colaborador y comunicados al área que corresponda –de manera presencial, vía telefónica o por correo electrónico– para su tratamiento oportuno.

Los eventos detectados por las herramientas de monitoreo (alertas) son registrados en la herramienta Service Desk en donde el operador le asigna la categoría de evento o incidente correspondiente. (FIGURA 5.7)

Inmediatamente, tanto los eventos o incidentes son escalados a los especialistas para realizar las acciones correctivas necesarias. (FIGURA 5.8)

Aprendizaje de los incidentes de seguridad en la información

Las acciones o mejores prácticas que dieron solución a los eventos e incidentes de seguridad de la información que tuvieron un mayor impacto en la organización, son compartidas por el personal de las áreas involucradas (lecciones aprendidas) asimismo, en la herramienta Service Desk se registra la base de datos de conocimiento.

5.8.13. OBJETIVOS DE SI

Los objetivos de seguridad de la información se basan en los lineamientos de la política de seguridad de la información y ser medibles.

Tomando en cuenta lo citado, se definieron los siguientes objetivos de Seguridad de la Información:

CUADRO N° 5.24 OBJETIVOS DE SEGURIDAD DE INFORMACIÓN

POLITICA / OBJETIVOS DEL SGSI	LINEAMIENTOS ESTRATÉGICOS	INDICADOR	FORMULA	META
Contar con una política de seguridad de la información que sea entendible y esté disponible a todo el personal	PRESTIGIO	Conocimiento de la política de seguridad de la información	Cantidad de personas que conocen la política / cantidad total de personas	100%
Cumplir con las regulaciones aplicables en torno a la seguridad de la información.		Clientes satisfechos con el servicio	% Satisfacción del Cliente Interno	>=90%
		SLA establecidos que se han cumplidos	∑ SLAs cumplidos/ ∑ SLAs totales	100%
		Penalidades por incumplimiento contractuales	Monto de penalidades (S/.)	S/. 0
Mejorar continuamente el SGSI		Análisis de Brechas / GAP	Análisis GAP / Brechas Promedio (cláusulas y controles)	>=80%
Mantener una cultura organizacional que aliente a todos los trabajadores a asumir una responsabilidad por la seguridad de la información		Cantidad de personas capacitadas en temas de seguridad de la información	Personas capacitadas / Total personas en el proyecto	>=90%
		Cantidad de Personas que aprobaron el examen de las charlas de seguridad de la información	Personas que aprobaron el examen / Personas que dieron el examen)	>=90%

POLITICA / OBJETIVOS DEL SGSI	LINEAMIENTOS ESTRATÉGICOS	INDICADOR	FORMULA	META
Proteger la información y sus activos de información a través de un SGSI para garantizar su confidencialidad, integridad y disponibilidad	**VALOR**	Riesgos atendidos	Riesgos registrados / Riesgos atendidos	>=85%
		Pruebas de continuidad ejecutadas	Pruebas ejecutadas / Total de Pruebas planificadas	100%
Dar respuesta inmediata a los incidentes que se presenten	**ESTABILIDAD**	Incidentes reportados correctamente	Número de incidentes reportados / Total de incidentes ocurridos	>=90%
		Incidentes atendidos correctamente	Número de incidentes reportados / Total de incidentes atendidos	>=90%

Fuente: Elaboración propia

5.8.14. COMPETENCIAS Y CONOCIMIENTO

Se debe formar y capacitar al personal en temas de seguridad de la información y formación técnica especializada para lo cual se desarrolló el siguiente plan de capacitación y concienciación.

CUADRO N° 5.25 PLAN DE CAPACITACIÓN

Nombre de la Capacitación	Sustento	Público objetivo	Tipo
Formación de Auditor Líder de la norma ISO 27001:2013	Desarrollar habilidades y destrezas para planificar, ejecutar y evaluar una auditoría interna/externa	Oficial de Seguridad de la Información	Externa
ITIL FOUNDATION	Desarrollar conciencia general de los elementos, conceptos y terminología utilizados en el ciclo de vida del servicio de ITIL, incluyendo las relaciones entre las fases del ciclo de vida, los procesos utilizados y su contribución a las prácticas de gestión de servicio	Analista de Atención Usuarios/Técnicos de Soporte en Sitio/Administradores	Externa
ITIL INTERMEDIO: · Estrategia del Servicio · Diseño del Servicio · Transición del Servicio · Operación del Servicio · Mejora Continua	Desarrollar habilidades en coordinar y ejecutar actividades que permiten la gestión y operación constantes de los productos y servicios desarrollados o implementados durante las fases del ciclo de vida del servicio.	Gestores de Servicio TI	Externa
ITIL EXPERT: · Gestión del Ciclo de Vida del Servicio	Desarrollar habilidades superiores en cuanto a ITIL.	Gestores de Servicio TI	Externa
Cobit 5 Foundation	Optimizar el valor generado por las TI, manteniendo un equilibrio entre la obtención de beneficios y optimización de los niveles de riesgos y el uso de los recursos.	Jefes / Supervisores / Analistas de Calidad	Externa

Nombre de la Capacitación	Sustento	Público objetivo	Tipo
Administración de WebSphere Application Server	Adquirir los conocimientos para la plataforma IBM BPM	Administradores de Base de Datos / Aplicaciones	Interna
Administration de IBM Integration BUS	Adquirir los conocimientos para la plataforma IBM BPM	Administradores de Base de Datos / Aplicaciones	Interna
Administración de Base de Datos ORACLE	Adquirir los conocimientos para la plataforma IBM BPM	Operadores	Externa

Fuente: Elaboración propia

CUADRO N° 5.26 PLAN DE CONCIENCIACIÓN

TEMAS	Set-Nov 2014	Dic-Feb 2015	Mar-May 2015
Inducción a las políticas de seguridad de la información	X	X	X
Respaldo de la información	X		
lineamientos generales de la política de SGSI		X	X
Gestión de acceso físico	X		
Borrado y respaldo de información (DVD / CD / USB)		X	
Uso correcto de medios de almacenamiento			X
Eliminación de información			X
Gestión de incidentes de seguridad			X

Fuente: Elaboración propia

Inducción en las políticas de seguridad de la información

Se realizará cuando un personal nuevo ingrese a laborar al proyecto, en dicha capacitación se abordará los siguientes aspectos:

- Política de Seguridad de la Información.

- Objetivos de Seguridad de la Información.
- Contribución y beneficios al sistema de gestión.
- Consecuencias de incumplimiento de los requisitos del sistema de gestión de la seguridad de la información.

Una vez culminada la charla de inducción se tomará un examen para analizar cuanto conocimiento ha captado el personal.

Asimismo, se le hará firmar un compromiso de confidencialidad cual tendrá un plazo de la obligación de confidencialidad durante la vigencia del presente servicio y de cinco (05) años posterior retiro / renuncia del presente proyecto.

5.8.15. COMUNICACIÓN

Se establecen las comunicaciones del sistema de gestión el cual contempla: Que comunicar, Cuando comunicar, Quien debe comunicar, a quien se debe comunicar y los procesos que se ven afectados por la comunicación. Para el presente trabajo se ha establecido el siguiente plan de comunicaciones:

CUADRO N° 5.27 PLAN DE COMUNICACIÓN DEL SGSI

TITULO	ASUNTO (SUBJECT)	DIRIGIDO POR	DIRIGIDO A / O (ROLES)	FECHA DE INICIO	USO DEL CANAL	SETIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMRE			
QUE COMUNICAR	QUE COMUNICAR	QUIEN DEBE COMUNICAR	A QUIEN COMUNICAR	CUANDO COMUNICAR	CANAL DE COMUNICACIÓN	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
5.2 Política 6.2 Objetivos de seguridad de la información	Política y Objetivos del SGSI	Gerente del Servicio	Personal (Servicio)	Anual	email																
5.2 Política 6.2 Objetivos de seguridad de la información	Política de gestión del servicio y la importancia de su cumplimiento.	Oficial de Seguridad de la Información (Servicio)	Personal (Servicio)	Por Evento	Charla de inducción / File Server																
5.3 Roles organizacionales, responsabilidades y autoridades	Funciones y responsabilidades	Coordinador del área (Servicio)	Personal nuevo (Servicio)	Al inicio de la relación laboral y/o cuando se actualice la descripción de puestos.	Documento																

TITULO	ASUNTO (SUBJECT)	DIRIGIDO POR	DIRIGIDO A / O (ROLES)	FECHA DE INICIO	USO DEL CANAL	SETIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMRE			
QUE COMUNICAR	QUE COMUNICAR	QUIEN DEBE COMUNICAR	A QUIEN COMUNICAR	CUANDO COMUNICAR	CANAL DE COMUNICACIÓN	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
A.16 Gestión de Incidentes de seguridad de la información	Eventos o incidentes de seguridad de la información	Personal ONP / Personal del Servicio / Proveedores / Visitas	Mesa de Administración de Servicios	Por Evento	Informe																
9.1 Monitoreo, medición, análisis y evaluación	Servicio de Monitoreo	Responsable del Proceso (GMD)	Responsable del Proceso (ONP)	Mensual	Informe																
6.1 Acciones para abordar los riesgos y oportunidades	Resultados del análisis y evaluación de riesgos / Plan de tratamiento de riesgos	Oficial de Seguridad de la Información (Servicio)	Gestor de Seguridad de la Información (ONP)	Anual	Informe																
9.2 Auditoría Interna	Resultados de informes de auditoría	Oficial de Seguridad de la Información (Servicio)	Gestor de Seguridad de la Información (ONP)	Anual	Informe																
9.3 Revisión de gestión	Resultados de la revisión por la Dirección	Oficial de Seguridad de la Información (Servicio)	Comité del SGSI	Mensual	Acta de reunión																
10.1 No Conformidades y acciones correctivas	Resultado de las acciones correctivas y preventivas	Oficial de Seguridad de la Información (Servicio)	Gestor de Seguridad de la Información (ONP)	Permanente	Informe																
A.12.6.1 Gestión de las vulnerabilidades técnicas	Resultados del análisis de vulnerabilidades técnicas	Jefe de Producción	Supervisor de Administración de Plataformas y Redes	Anual	Informe																

TITULO	ASUNTO (SUBJECT)	DIRIGIDO POR	DIRIGIDO A / O (ROLES)	FECHA DE INICIO	USO DEL CANAL	SETIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMRE			
QUE COMUNICAR	QUE COMUNICAR	QUIEN DEBE COMUNICAR	A QUIEN COMUNICAR	CUANDO COMUNICAR	CANAL DE COMUNICACIÓN	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
A.17.1 Continuidad de la seguridad de la información	Resultados de las Pruebas de Continuidad de Servicio	Jefe de Producción	Supervisor de Administración de Plataformas y Redes	Anual	Informe																
A.18.1 Cumplimiento de los requisitos legales y contractuales	Requisitos legales aplicables al SGSI	Gestor de Seguridad de la Información (ONP)	Comité de SGSI	Por Evento	Correo electrónico																
7.5 Información documentada	Procedimientos y otros documentos del SGSI	Responsable del Proceso (GMD)	Responsable del Proceso (ONP)	Por Evento	Correo electrónico																

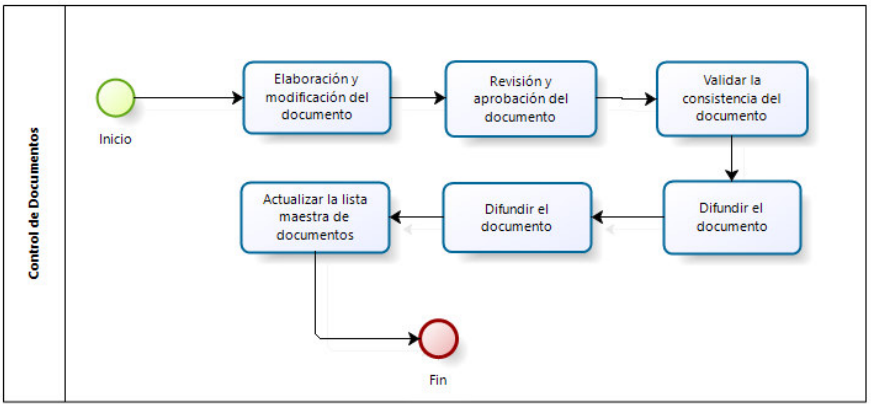
Fuente: Elaboración propia

5.8.16. INFORMACIÓN DOCUMENTADA

En esta fase se establecen los lineamientos para la elaboración, revisión, aprobación, distribución y control de los documentos del Sistema de Gestión de Seguridad de la Información para la elaboración de los documentos te considera los siguientes ítems:

- Software: Microsoft Word; los diagramas pueden elaborarse en Bizagi o Microsoft Visio.
- Configuración de página: Tamaño A4; orientación vertical; los márgenes: de 2.5 cm
- Fuente: Arial 11 puntos en encabezado, títulos, subtítulos y contenido general. 8 puntos en pie de página. Interlineado de 1.15 cm.

FIGURA N° 5.10 PROCESO DOCUMENTAL



Fuente: Elaboración propia

Los documentos se pueden clasificar en 3 tipos: Confidencial, restringido y publico los cuales se detallan a continuación:

CUADRO N° 5.28 CLASIFICACIÓN DE LA INFORMACIÓN

CLASIFICACIÓN	DEFINICIÓN	EJEMPLOS
CONFIDENCIAL	Es la información que debe mantenerse en la más estricta reserva. Está sujeta al cumplimiento de requisitos legales y/o contractuales. Tiene mucho valor para su propietario, es crítica para el desarrollo estratégico del negocio y su divulgación no autorizada podría ocasionar impactos severos a la organización en términos económicos y de prestigio, principalmente. Su divulgación a terceros podría darse sólo bajo la autorización formal del representante legal, mediante la firma de un acuerdo de confidencialidad.	Información de Clientes, Información Comercial, Información del personal, Información Económica-financiera, etc.
RESTRINGIDO	Es aquella información inherente a las operaciones de un proceso o área de negocio específica. Podría estar sujeto a cumplimiento legal y/o contractual, es crítica para las operaciones del proceso o área de negocio, su pérdida o divulgación no autorizada podría ocasionar perjuicios a la organización en términos económicos, de servicio al cliente y ventaja competitiva. Su divulgación a terceros podría darse sólo bajo la autorización formal de su propietario mediante la firma de un acuerdo de confidencialidad.	Procesos operativos, Políticas específicas, Procedimientos, Instructivos, Manuales técnicos y de usuario, Formatos y Registros, y otros similares
PÚBLICO	Información destinada al conocimiento de la comunidad.	Publicaciones en Página Web

Fuente: Elaboración propia

Para el control de versión se debe registrar los principales cambios realizados en el documento (Ver Cuadro N° 5.19) el siguiente recuadro que deberá registrar los principales cambios en los documentos, a continuación, se muestra un ejemplo:

CUADRO N° 5.29 CONTROL DE VERSIONES

Versión	Fecha de aprobación	Cambios del documento
1.0	12/02/2017	Elaboración del documento
2.0	21/12/2017	Cambio en la nomenclatura de los documentos.

Fuente: Elaboración propia

Los documentos internos del SGSI deberán ser codificados cuando sea aplicable y se hará siguiendo la siguiente abreviatura, por ejemplo:

- Políticas (POL)
- Manuales (MAN)
- Procedimiento (PRO)
- Instructivo (INS)
- Formato (FOR)

Asimismo, se debe especificar el área al que pertenece el documento, a saber:

CUADRO N° 5.30 CÓDIGO POR ÁREA

ÁREA	CÓDIGO
Gerencia del Servicio	GER
Centro de Cómputo	CCE
Emisión de Pagos	EMI
Mesa de Administración de Servicios	MAS
Seguridad Informática	SIN
Gestión de accesos	PCA
Base de Datos	BDD
Aplicaciones	APP
Unix y almacenamiento	UNI
Redes y Comunicaciones	RED

Fuente: Elaboración propia

A continuación, se muestra el flujo de revisión y aprobación de los documentos:

CUADRO N° 5.31 MATRIZ DE APROBACIONES

DOCUMENTOS DE LA ORGANIZACIÓN	DOCUMENTO		
	Elaboración o Modificación	Revisión	Publicado y Distribuido por
Documentos del Sistema de Gestión: Política y Objetivos	Oficial de Seguridad de la Información	Gerente del Proyecto	Gerente del Proyecto
Documentos del Sistema de Gestión: Manual, procedimientos, formatos, etc.	Oficial de Seguridad de la Información	Gerente del Proyecto	Oficial de Seguridad de la Información
Documentos de Operación	Personal dentro del alcance del SGSI	Dueño del proceso o área	Dueño del proceso o área

Fuente: Elaboración propia

A continuación, se detalla la lista de documentos del SGSI, según la norma ISO/IEC 27001:2013:

CUADRO N° 5.32 LISTA DE DOCUMENTOS DEL SGSI

DOCUMENTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
POLITICAS
POL.GER.001 Política de Seguridad de la Información
POL.GER.002 Política de Escritorio y Pantalla Limpios
POL.GER.003 Política de Gestión de Accesos
POL.GER.004 Política de Gestión de activos
POL.GER.005 Política de Administración de Software
MANUALES
MAN.GER.001 Manual de Organización y Funciones del SGSI
MAN.GER.002 Manual de Manual SGSI
MAN.GER.003 Manual de Gestión de Riesgos
MAN.GER.005 Manual de Alcance del SGSI
PROCEDIMIENTOS
PRO.GER.001 Ingreso de Personal
PRO.GER.002 Proceso Disciplinario

DOCUMENTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
PRO.GER.003 Terminación de Relación Laboral
PRO.GER.004 Control de Documentos
PRO.GER.005 Control de Registros
PRO.GER.006 Auditoria Interna SGSI
PRO.GER.007 Acciones Correctivas y Preventivas
PRO.GER.008 Gestión de Incidentes de Seguridad
PRO.GER.009 Medición efectividad de controles
PRO.GER.010 Comunicaciones del SGSI
PRO.GER.011 Cumplimiento y requisitos legales
PRO.GER.012 Gestión de activos de información
PRO.GER.013 Compresion y Encriptacion de Archivos con el Winzip
PRO.GER.014 Seguridad Física y del ambiente
PRO.GER.015 Relaciones con el proveedor
PRO.GER.016 Gestión de la continuidad
PRO.SIN.001 Control de Accesos
PRO.MAS.025 Gestión de Incidencias
PRO.MAS.053 Gestión de Cambios
FORMATOS
FOR.GER.001 Compromiso de confidencialidad
FOR.GER.002 Declaración Jurada
FOR.GER.003 Lista de personal
FOR.GER.004 Entrega de cargo
FOR.GER.005 Plan de capacitación del personal
FOR.GER.006 Plan de Contingencia
FOR.GER.007 Lista de asistencia
FOR.GER.008 Lista maestra de documentos
FOR.GER.009 Lista maestra de registros
FOR.GER.010 Solicitud de cambio
FOR.GER.011 Revisión post implementación
FOR.GER.012 Lista de Contactos
FOR.GER.013 Identificación de Partes Interesadas del SGSI
FOR.GER.014 Declaración de Responsabilidad de Uso de Cuentas Privilegiadas
FOR.GER.015 Examen
FOR.GER.016 Inventario de Activos

DOCUMENTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
FOR.GER.017 Gestión de riesgos y oportunidades
FOR.GER.018 Enunciado de Aplicabilidad
FOR.GER.019 Plan De Tratamiento de Riesgos
FOR.GER.020 Programa Anual de Auditoria
FOR.GER.021 Plan de Auditoria Interna
FOR.GER.022 SAC
FOR.GER.023 Medición de Procesos y Controles del SGSI
FOR.GER.024 Identificación de Requisitos de Seguridad de la Información
FOR.GER.025 Objetivos del SGSI

Fuente: Elaboración propia

5.9. HACER

Se identifican los activos de información del proyecto, asimismo se identifican los riesgos y oportunidades que atenten contra los activos correspondientes. A continuación, se detallan los mismos.

5.9.1. INVENTARIO DE ACTIVOS

CUADRO N° 5.33 INVENTARIO DE ACTIVOS

INVENTARIO DE ACTIVOS DE INFORMACIÓN													
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
1	**SOFTWARE**	Aplicaciones Core de ONP	Servicios y aplicaciones CORE de ONP que soporta en Centro de Datos.	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma de Central (ONP)	Administrador de Aplicaciones (GMD)	**4**	**5**	**5**	4.7	ALTO
2	**SOFTWARE**	Aplicaciones de ONP	Servicios y aplicaciones No Core de ONP que soporta en Centro de Datos	**RESTRINGIDO**	Centro de datos principal	Gestor de Plataforma Central (ONP)	Administrador de Aplicaciones (GMD)	**4**	**4**	**4**	4.0	ALTO
3	**SOFTWARE**	Sistemas Operativos / Tecnología Microsoft	Sistemas operativos de tecnología propietaria microsoft que soporta aplicaciones virtualizadas, versión: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2, Seven, XP, entre otros	**RESTRINGIDO**	Inventario de Servidores	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**4**	**4**	**5**	4.3	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
4	**SOFTWARE**	Sistemas Operativos / Tecnología Linux	Sistemas operativos de código abierto que soporta aplicaciones virtualizadas, distribuciones: Oracle Linux, Ubuntu, Red Hat Enterprise Linux, Centos, entre otros	**RESTRINGIDO**	Inventario de Servidores	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**4**	**4**	**5**	4.3	ALTO
5	**SOFTWARE**	Plataforma de Servidores Virtuales / Tecnología Vmware	Sistemas operativos que soportan servidores virtuales donde se ejecutan las aplicaciones, plataforma: Websphere, Vmware ESXi	**RESTRINGIDO**	Inventario de Servidores	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**4**	**4**	**5**	4.3	ALTO
6	**SOPORTE DE INFORMACIÓN**	Cintas LTO4, LTO5	Cintas donde se almacena el respaldo de información	**RESTRINGIDO**	Centro de Datos Principal	Analista de centro de datos (ONP)	Operador del Centro de Datos (GMD)	**5**	**5**	**4**	4.7	ALTO
7	**DATOS E INFORMACIÓN**	BDPRD11G	Base de Datos BD App C/S - Web Oracle 11.2.0.3.0, almacena datos relacionados a los módulos de seguridad, gestión de requerimientos, planillas, administración de caja chica, información personal de afiliados, empleadores y asegurados, activos fijos, plantillas, marcaciones, documentación, reclamos, control de pagos y gestión administrativa de ONP.	**CONFIDENCIAL**	ONPPRD03	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN													
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
8	**DATOS E INFORMACIÓN**	BDPR11G2	Base de Datos BD App C/S - Web Oracle 11.2.0.3.0, almacena datos relacionados a las cuentas de los aportantes, información inmobiliarias, contratos públicos o privados, usuarios, claves, información de acceso de las aplicaciones WAS y OAS, expediente del aportante, base de datos del pensionista de ONP	**CONFIDENCIAL**	ONPPRD03	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
9	**DATOS E INFORMACIÓN**	BDPR11G3	Base de Datos BD App C/S - Web Oracle 11.2.0.3.0, almacena datos relacionados a las boletas de pago de los pensionistas, gestión de archivos, procesos judiciales, carga de datos de empleadores y trámite documentario de ONP.	**CONFIDENCIAL**	ONPPRD03	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
10	**DATOS E INFORMACIÓN**	BDPR11G4	Base de Datos BD App C/S - Web Oracle 11.2.0.3.0, almacena datos relacionados a los trámites pendientes, datos de los empleadores, documentación y quejas realizadas de ONP.	**CONFIDENCIAL**	ONPPRD04	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN													
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
11	**DATOS E INFORMACIÓN**	BDPRD10G	Base de Datos BD App C/S - Web Oracle 11.2.0.3.0, almacena datos relacionados a la inscripción facultativa, trámites de pensión y jubilación adelantada, extracto de pagos de ONP.	**CONFIDENCIAL**	ONPPRD03	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
12	**DATOS E INFORMACIÓN**	BDWWW	Base de Datos BD App C/S - Web Oracle 11.2.0.3.0, almacena datos relacionados a la atención de procesos judiciales de la ONP.	**CONFIDENCIAL**	ONPPRD03	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
13	**DATOS E INFORMACIÓN**	HARVEST	Base de Datos BD App C/S - Web Oracle 11.2.0.3.0, almacena datos relacionados a las versiones de las fuentes de los sistemas de la ONP.	**CONFIDENCIAL**	ONPPRD04	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
14	**DATOS E INFORMACIÓN**	SBR2	Base de Datos BD App C/S - Oracle 11.2.0.3.0, almacena datos relacionados a los bonos de reconocimiento de los trabajadores.	**CONFIDENCIAL**	ONPPRD01	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
15	**DATOS E INFORMACIÓN**	PRODNSTD	Base de Datos BD App C/S - Web Oracle 11.2.0.3.0, almacena datos relacionados a las plantillas, trámite documentario, módulo derivación, inventario de expedientes de ONP.	**CONFIDENCIAL**	ONPPRD05	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
16	**DATOS E INFORMACIÓN**	NSP18PRD	Base de Datos BD App C/S - Web Oracle 11.2.0.3.0, almacena datos relacionados a las pensiones, trámites, calificaciones de ONP.	**CONFIDENCIAL**	ONPPRD05	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
17	**DATOS E INFORMACIÓN**	NSP19PRD	Base de Datos BD App C/S - Web Oracle 11.2.0.3.0, almacena datos relacionados a las pensiones, trámites, calificaciones de ONP.	**CONFIDENCIAL**	ONPPRD05	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
18	**DATOS E INFORMACIÓN**	NSP20PRD	Base de Datos BD App C/S - Web Oracle 11.2.0.3.0, almacena datos relacionados a las pensiones, trámites, calificaciones de ONP.	**CONFIDENCIAL**	ONPPRD05	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
19	**DATOS E INFORMACIÓN**	ONPPROD	Base de Datos BD App C/S Oracle 9.2.0.8.0, almacena datos relacionados a las declaraciones juradas de trabajadores, información legal, normas legales de ONP.	**CONFIDENCIAL**	ONPPRD02	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
20	**DATOS E INFORMACIÓN**	PLN4	Base de Datos BD App C/S - Oracle 11.2.0.3.0, almacena datos relacionados al control de plantillas, información para el pago a empresas verificadoras de la ONP.	**CONFIDENCIAL**	ONPPRD01	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
21	**DATOS E INFORMACIÓN**	SPR4	Base de Datos BD App C/S - Oracle 9.2.0.8.0, almacena datos relacionados a los presupuestos, reportes para	**CONFIDENCIAL**	ONPPRD02	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN													
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
			MEF, proyecciones, etc. de la ONP.									
22	**DATOS E INFORMACIÓN**	SAB2	Base de Datos BD App C/S - Oracle 11.2.0.3.0, almacena datos relacionados al archivo de solicitudes, plantillas, resoluciones, notificaciones de los bonos de reconocimiento de la ONP.	**CONFIDENCIAL**	ONPPRD01	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
23	**DATOS E INFORMACIÓN**	BDPRDCIA	Base de Datos BD App C/S - Oracle 11.2.0.3.0, almacena datos relacionados al cálculo de las reservas actuariales, flujos de cajas, gestión de aportes de la ONP.	**CONFIDENCIAL**	ONPPRD06	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
24	**DATOS E INFORMACIÓN**	BDPRGEST	Base de Datos BD App C/S - Web - Oracle 11.2.0.3.0, almacena datos relacionados la inversión, titularización, gestión de fondos de inversion, etc. de la ONP.	**CONFIDENCIAL**	ONPSRVLNX03	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
25	**DATOS E INFORMACIÓN**	DTSTAGE	Base de Datos BD App C/S - Oracle 11.2.0.3.0, almacena datos relacionados al repositorio de la herramienta DataStage de la ONP.	**CONFIDENCIAL**	ONPPRD04	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
26	**DATOS E INFORMACIÓN**	BDPRFNT	Base de Datos BD App Web - Oracle 11.2.0.3.0, almacena datos relacionados al Object Store del FileNet, imágenes, pdfs de usuarios del aplicativo de la ONP.	**CONFIDENCIAL**	ONPPRD04	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
27	**DATOS E INFORMACIÓN**	BDPRGCD	Base de Datos BD App Web - Oracle 11.2.0.3.0, almacena datos relacionados al FileNet GCD de la ONP.	**CONFIDENCIAL**	ONPPRD04	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
28	**DATOS E INFORMACIÓN**	EMI18PRD	Base de Datos BD App C/S - Oracle 11.2.0.3.0, almacena datos relacionados a los pagos de prestaciones de la ley 18	**CONFIDENCIAL**	ONPPRD06	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
29	**DATOS E INFORMACIÓN**	EMI19PRD	Base de Datos BD App C/S - Oracle 11.2.0.3.0, almacena datos relacionados a a los pagos de prestaciones de la ley 19	**CONFIDENCIAL**	ONPPRD06	Gestor de Plataforma Central (ONP)	Administrador de la Base de Datos (Servicio)	**5**	**5**	**5**	5.0	MUY ALTO
30	**HARDWARE**	Servidores Físicos Wintel Xeon G01	S.O.:Vmware ESXi 5.1.0 - Vsphere Enterprise Plus Funcionalidad: Hosting Vmware Virtual Servers Marca: HP, Modelo: ProLiant BL 465c G8 Cantidad: 14	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO
31	**HARDWARE**	Servidores Físicos Wintel Xeon G02	S.O.:Windows Server 2008 R2 (64bit) - Standard Edition Funcionalidad: Vcenter Server 5.1 Marca: HP, Modelo: ProLiant BL 460c G6 Cantidad: 01	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
32	**HARDWARE**	Servidores Físicos Wintel Xeon G03	S.O.:Windows Server 2008 R2 (64bit) - Standard Edition Funcionalidad: Suite PCSISTEL 6.0 Marca: HP, Modelo: ProLiant DL 180 G6 Cantidad: 01	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO
33	**HARDWARE**	Servidores Físicos Wintel Xeon G04	S.O.:Windows Server 2008 R2 (64bit) - Standard Edition Funcionalidad: HP DataProtector Marca: HP, Modelo: ProLiant DL320 G6 Cantidad: 01	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO
34	**HARDWARE**	Servidor Físico ONPHPVM1	HP Integrity BL860c i4 con 16 CPU (Intel(R) Itanium(R) Processor 9560 @ 2.53 GHz, 32 MB) y 288 GB RAM con sistema operativo HP-UX 11.31, en donde se ejecutan las máquinas virtuales ONPPRD01, ONPPRD04, ONPPRD05, ONPAPPQA, ONPWLSQA	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
35	**HARDWARE**	Servidor Físico ONPHPVM2	HP Integrity BL860c i4 con 16 CPU (Intel(R) Itanium(R) Processor 9560 @ 2.53 GHz, 32 MB) y 288 GB RAM con sistema operativo HP-UX 11.31, en donde se ejecutan las máquinas virtuales ONPPRD02, ONPPRD03, ONPPRD06, ONPAPPRD, ONPWLSPR	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO
36	**HARDWARE**	Servidor Físico ONPHPVM3	HP Integrity BL860c i4 con 16 CPU (Intel(R) Itanium(R) Processor 9560 @ 2.53 GHz, 32 MB) y 176 GB RAM con sistema operativo HP-UX 11.31, en donde se ejecutan las máquinas virtuales de contingencia	**RESTRINGIDO**	Centro de Datos Contingencia	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO
37	**HARDWARE**	Servidor Físico ONPQA01	HP Integrity rx3600 con 2 CPU (Itanium 2 9100 series Processor @ 1.67 GHz, 18 MB) y 16 GB RAM con sistema operativo HP-UX 11.23, en donde se ejecutan las bases de datos ADMQA y SPR4QA	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
38	**HARDWARE**	Servidor Físico ONPQA02	HP Integrity rx3600 con 2 CPU (Itanium 2 9100 series Processor @ 1.67 GHz, 18 MB) y 16 GB RAM con sistema operativo HP-UX 11.31, en donde se ejecutan las bases de datos BDQA11G, BDQAFNT BDQA11G2, BDQAGCD, BDQA11G3, FNTQAPED, BDQA11G4	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO
39	**HARDWARE**	Servidor Físico ONPQA03	HP Integrity rx3600 con 2 CPU (Itanium 2 9100 series Processor @ 1.67 GHz, 18 MB) y 16 GB RAM con sistema operativo HP-UX 11.31, en donde se ejecutan las bases de datos BDQACIA y FOGLIGHT	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO
40	**HARDWARE**	Servidor Físico ONPQA05	HP Integrity rx3600 con 2 CPU (Itanium 2 9340 series Processor @ 1.6 GHz, 20 MB) y 16 GB RAM con sistema operativo HP-UX 11.31, en donde se ejecutan las bases de datos NSTDQA PLN4QA, NSP18QA, SAB2QA, NSP19QA, SBR2QA, NSP20QA, EMI18QA, DTSTGQA, EMI19QA, BDQAFNPE	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
41	**HARDWARE**	Servidor Físico AIXHOST1	IBM Power 750 Type: 8233-E8B con 32 CPU (IBM Power 7 3612 MHZ) y 288 GB RAM en donde se ejcutan las LPARs ONPBMONDBP01, ONPWPSP01, ONPBMONDBD01, ONPWPSDBP01, ONPWPSD01, ONPBMONP01, ONPWASP01, ONPWASD01, ONPIHSP01, ONPFNETD01, ONPLBP02, ONPBMOND01, ,ONPWPSDBD01, ONPFNETP01, ONPIPC01, ONPWAS8P01, ONPWAS8P02, ONPWAS8DM, ONPVIOS01, ONPVIOS02	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO
42	**HARDWARE**	Servidor Físico AIXHOST2	IBM Power 750 Type: 8233-E8B con 32 CPU (IBM Power 7 3612 MHZ) y 288 GB RAM en donde se ejcutan las LPARs ONPBMONDBP02, ONPBMONP02, ONPIHSP02, ONPWPSP02, ONPWASP02, ONPWPSDBP02, ONPLBP01, ONPFNETP02, ONPPORTALP01, ONPPORTALD01,	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN													
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
			ONPVIOS03, ONPVIOS04, ONPNIM01									
43	**HARDWARE**	Servidor Físico AIXHOST3	IBM Power 750+ Type: 8408-E8D con 24 CPU (IBM Power 7 4060 MHZ) y 192 GB RAM en donde se ejcutan las LPARs ONPBDIP01, ONPBDIP02, ONPETLP01, ONPVIOS05, ONPVIOS06	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO
44	**HARDWARE**	Servidor Físico ONPHMC01	IBM System x3550 M3 Type: 7042-CR6 con 4 CPU (Intel(R) Xeon(R) CPU E5630 @ 2.53GHz) y 4 GB RAM. Equipo para la gestión de los servidores AIXHOST1, AIXHOST2 y AIXHOST3	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO
45	**HARDWARE**	Servidores Appliance G01	Equipos de gestión de operaciones del centro de datos: Call Manager, IP Contac Center, Firewalls, Proxy, Antispam, IPS/IDS, Balanceadores, entre otros	**RESTRINGIDO**	Centro de Datos Principal	Gestor de Plataforma Central (ONP)	Administrador UNIX (Servicio)	**4**	**4**	**5**	4.3	ALTO
46	**HARDWARE**	Desktop	Cantidad: 40 i5 320 GB	**RESTRINGIDO**	Edificio principal ONP	Gerente del Servicio	Personal del Servicio	**4**	**4**	**5**	4.3	ALTO
47	**HARDWARE**	Notebook	Cantidad: 8 i5 320 GB	**RESTRINGIDO**	Edificio principal ONP	Gerente del Servicio	Personal del Servicio	**4**	**4**	**5**	4.3	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
48	**RED DE COMUNICACIONES**	Switch de red acceso	Equipos de red que conectan mediante el cableado estructurado los equipos terminales (PC, impresoras, otros) con la red de datos principal	**RESTRINGIDO**	Edificio Principal ONP Sedes de ONP en provincia	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO
49	**RED DE COMUNICACIONES**	Switch de red distribucion	Equipos de red que conectan mediante el cableado estructurado los equipos terminales (PC, impresoras, otros) con la red de datos principal	**RESTRINGIDO**	Edificio Principal ONP Sedes de ONP en provincia	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO
50	**RED DE COMUNICACIONES**	Switch de red CORE	Equipos de red que conectan mediante el cableado estructurado los equipos terminales (PC, impresoras, otros) con la red de datos principal	**RESTRINGIDO**	Edificio Principal ONP Sedes de ONP en provincia	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO
51	**RED DE COMUNICACIONES**	Acces Point	Equipos de red inalambricos que conectan los equipos terminales (Laptops, otros) con la red de datos principal Cantidad: 50	**RESTRINGIDO**	Edificio Principal ONP Sedes de ONP en provincia	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO
52	**RED DE COMUNICACIONES**	Telefonos IP	Equipos de comunicación telefónica, marca general utilizada CISCO Cantidad: 40	**RESTRINGIDO**	Centro de Datos de Enlace Edificio Principal ONP Sedes de ONP en provincia	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
53	**RED DE COMUNICACIONES**	Cisco 2500 Series Wireless LAN Controller	Equipo de administración de los recursos de comunicación telefónica CISCO	**RESTRINGIDO**	Centro de Computo de Enlace	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO
54	**RED DE COMUNICACIONES**	Aceleradores de aplicaciones	Equipos de optimización de los recursos de comunicaciones telefónicas CISCO	**RESTRINGIDO**	Centro de Datos de Enlace Edificio Principal ONP Sedes de ONP en provincia	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO
55	**RED DE COMUNICACIONES**	Equipo de videoconferencia	Equipos de comunicación visual IP Polycom V500 IP (10) Televisores LG (10) 32´´	**RESTRINGIDO**	Centro de Datos de Enlace Edificio Principal ONP Sedes de ONP en provincia	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO
56	**RED DE COMUNICACIONES**	Call Manager	UCMPUB / UCMSUB Call Manager 10.5	**RESTRINGIDO**	Centro de Datos de Enlace Sótano 01	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO
57	**RED DE COMUNICACIONES**	Cisco Unity	Cisco Unity Version 10.5.1.10000-7 ONPSRVUNITY	**RESTRINGIDO**	Centro de Datos de Enlace Sótano 01	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO
58	**RED DE COMUNICACIONES**	IP Contac Center	IP Contac Center - UCCX_A - Contac Center / UCCX_AB-Contac Center	**RESTRINGIDO**	Centro de Datos de Enlace Sótano 01	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
59	**RED DE COMUNICACIONES**	CUEAC	Consola de operadora telefonica	**RESTRINGIDO**	Centro de Datos de Enlace Sótano 01	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO
60	**RED DE COMUNICACIONES**	PCSistel	Tarificador de llamadas telefonicas	**RESTRINGIDO**	Centro de Datos de Enlace Sótano 01	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO
61	**RED DE COMUNICACIONES**	UCS01 / UCS02 / UCS03	Servidor fisico donde se ejecutan los servidores virtuales de la plataforma de telefonia IP	**RESTRINGIDO**	Centro de Datos de Enlace Sótano 01	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO
62	**RED DE COMUNICACIONES**	ASA01	Firewall Cisco ASA para VPN de telefonia IP	**RESTRINGIDO**	Centro de Datos de Enlace Sótano 01	Gestor de Infraestructura, Redes y Comunicaciones (ONP)	Administrador de Comunicaciones (GMD)	**4**	**4**	**5**	4.3	ALTO
63	**PERSONAL**	Gerente de Servicio	Cantidad: 01 Responsable de la adecuada gestión y control del servicio de manera integral.	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**4**	**4**	**4**	4.0	ALTO
64	**PERSONAL**	Jefe de Producción	Cantidad: 01 Responsable de la adecuada gestión del centro de datos y la gestión de accesos (PCA)	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**4**	**4**	**4**	4.0	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
65	**PERSONAL**	Jefe de Soporte Técnico y Mesa de Ayuda	Cantidad: 01 Responsable de la adecuada gestión en la administración de la plataforma de TI, equipos de comunicaciones, equipos de seguridad perimetral y supervisar la gestión de la mesa de ayuda	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**4**	**4**	**4**	4.0	ALTO
66	**PERSONAL**	Jefe de Emisión y Aplicaciones de Negocio	Cantidad: 01 Responsable de la adecuada gestión en la administración de base de datos, aplicaciones y el proceso de emisión de las boletas de pago	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**4**	**4**	**4**	4.0	ALTO
67	**PERSONAL**	Coordinador de Base de Datos y Aplicaciones	Cantidad: 01 Supervisar y gestionar al equipo de administradores de base de datos y aplicaciones	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
68	**PERSONAL**	Administrador de Base de Datos	Cantidad: 03 Encargado de la administración, operación y mantenimiento de las base de datos (Oracle y SQL) en los ambientes de desarrollo, QA y producción.	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
69	**PERSONAL**	Administrador de Aplicaciones	Cantidad: 03 Encargado de la administración, operación y mantenimiento de los servidores de aplicaciones	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
			críticas y no críticas de la ONP, en ambiente Unix, Linux y Windows									
70	**PERSONAL**	Administrador UNIX	Cantidad: 01 Administración, operación y mantenimiento de los servidores UNIX/LINUX y Unidades de Almacenamiento.	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
71	**PERSONAL**	Coordinador de Redes y Comunicaciones	Cantidad: 01 Supervisar las labores operativas de los administradores de redes, comunicaciones y Seguridad Perimetral	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
72	**PERSONAL**	Administrador de Seguridad Perimetral	Cantidad: 01 Encargado de la gestión de la seguridad informática acorde a la solución implementada.	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
73	**PERSONAL**	Administrador de Redes	Cantidad: 03 Identificación, diagnóstico y solución de problemas en las redes de cómputo.	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
74	**PERSONAL**	Administrador de Comunicaciones	Cantidad: 01 Responsable de garantizar la operatividad de los equipos de comunicaciones instalados en la ONP	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
75	**PERSONAL**	Coordinador de PCA	Cantidad: 01 Supervisa las labores de los gestores de PCA, brinda los acceso a los sistemas según el procedimiento de gestión de accesos	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
76	**PERSONAL**	Gestor de Accesos (PCA)	Cantidad: 03 Encargado de gestionar el otorgamiento de accesos a los sistemas de la institución siguiendo el procedimiento de control de accesos.	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
77	**PERSONAL**	Coordinador del Centro de Datos	Cantidad: 02 Encargado de administrar las actividades relacionadas con el centro de cómputo y supervisa las actividades de los operadores	**RESTRINGIDO**	Centro de Datos de Enlace Centro de Datos Principal	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
78	**PERSONAL**	Operadores de Centro de Datos	Canitdad: 10 Encargado de ejecutar los pases a QA y Producción y monitorea la operatividad de los equipos ubicados en el centro de datos	**RESTRINGIDO**	Centro de Datos de Enlace Centro de Datos Principal	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
79	**PERSONAL**	Oficial de Seguridad de la Información	Cantidad: 01 Supervisar el cumplimiento de estándares y procedimientos relacionados con los sistemas de gestión (Calidad, Seguridad de la información y Salud Ocupacional).	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
80	**PERSONAL**	Analistas de Procesos	Cantidad: 02 Asegurar el cumplimiento de estándares y procedimientos relacionados con los sistemas de gestión (calidad, Seguridad de la información y salud ocupacional	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
81	**PERSONAL**	Coordinador del Centro de Servicios a Usuario	Cantidad: 01 Coordinar de manera eficaz con los recursos involucrados la atención de las diversas solicitudes e incidentes en los servicios que se encuentran dentro del catálogo de servicios	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
82	**PERSONAL**	Analista de Servicio al Usuario	Cantidad: 07 Ser la primera línea de soporte al usuario, recibir y registrar las llamadas, registrar y escalar los incidentes, problemas, y solicitudes de servicio; y mantener al cliente informado sobre el estado y progreso del ticket.	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
83	**PERSONAL**	Técnico de soporte en sitio	Cantidad: 08 Brindar el soporte general de todo el hardware, software y periféricos de todo el equipamiento tecnológico e impresoras de la	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN													
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
			organización (tanto alquilado como de propiedad de ONP).									
84	**PERSONAL**	Administrador de la solución de Gestión de Servicios de TI y Gestión de Activos de TI	Cantidad: 01 Administración, configuración y troubleshooting de la solución integrada de Gestión de Servicios de TI y Gestión de Activos de TI	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**5**	4.7	ALTO
85	**PERSONAL**	Gestor de Servicios de TI	Cantidad: 01 Gestionar las necesidades de la ONP relacionadas a los procesos de ITIL hacia los gestores a su cargo, canalizando y controlando las capacidades, recursos y los tiempos implicados	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**4**	4.3	ALTO
86	**PERSONAL**	Analista de Servicios de TI	Cantidad: 01 Proveer información adecuada de los servicios disponibles, obtener servicios más eficientes y de mayor calidad.	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**5**	**4**	**4**	4.3	ALTO
87	**INSTALACIONES**	Centro de Datos de Enlace	Instalaciones del centro de datos de ONP ubicado en el zótano 01 del edificio, donde se ubican los equipos de los servicio brindados por proveedores externos.	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Sótano 1	Jefe de la OTI	Gerente del Servicio	**5**	**5**	**5**	5.0	MUY ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN													
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
88	**INSTALACIONES**	Centro de Datos Principal	Instalaciones del centro de datos de GMD, ubicado en el centro de Lima, donde se ubican los equipos servidores de las aplicaciones core de ONP y que son administrador por GMD.	**RESTRINGIDO**	Jr. Chota 998, esquina con Jr. Ilo	GMD	Gerente de Servicios Data Center (GMD)	**5**	**5**	**5**	5.0	MUY ALTO
89	**INSTALACIONES**	Centro de Datos Contingencia	Instalaciones del centro de datos de GMD, ubicado en la zona sur del centro de datos principal, donde se ubican los equipos servidores de contingencia para las aplicaciones core de ONP y que son administrador por GMD.	**RESTRINGIDO**	Av. Paseo de la Republica 4675 Surquillo	GMD	Gerente de Servicios Data Center (GMD)	**5**	**5**	**5**	5.0	MUY ALTO
90	**INSTALACIONES**	Oficinas Administrativas PISO 12	Instalaciones dentro del edificio de ONP, piso 12, donde se ubica la Oficina del proveedor del servicio (GMD) para gestionar y asegurar la operatividad de los servicios brindados por contrato	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la ONP	Gerente del Servicio	**5**	**5**	**5**	5.0	MUY ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN													
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
91	**EQUIPOS AUXILIARES**	Aire acondicionado de precisión	Total: 6 Cantidad: 02, Marca; Emerson-Liebert CRV Equipo de aire acondicionado de precisión Cantidad: 02, Marca; HIREF Equipo de aire acondicionado de precisión Cantidad: 01, marca: SPLIP Cantidad: 01, marca: York	**RESTRINGIDO**	Centro de datos de enlace, Sótano 1	Analista de centro de datos (ONP)	Coordinador del centro de datos (GMD S.A.)	**4**	**4**	**5**	4.3	ALTO
92	**EQUIPOS AUXILIARES**	UPS	Total: 5 Cantidad: 04 de 20KVA (c/u), Marca: ABB Cantidad: 01marca: ETON Equipo UPS de 40KVA (UPS03)	**RESTRINGIDO**	Centro de datos de enlace, Sótano 1	Analista de centro de datos (ONP)	Coordinador del centro de datos (GMD S.A.)	**4**	**4**	**5**	4.3	ALTO
93	**EQUIPOS AUXILIARES**	Panel de sistema contra incendios	Cantidad: 01, marca: Fike Panel de control central del sistema contra incendios	**RESTRINGIDO**	Centro de datos de enlace, Sótano 1	Analista de centro de datos (ONP)	Coordinador del centro de datos (GMD S.A.)	**4**	**4**	**5**	4.3	ALTO
94	**EQUIPOS AUXILIARES**	Tanque de Gas	Cantidad: 02, marca: Fike Agente limpio de tipo de aplicación de inundación total, ubicado en la sala de servidores y sala de energía	**RESTRINGIDO**	Centro de datos de enlace, Sótano 1	Analista de centro de datos (ONP)	Coordinador del centro de datos (GMD S.A.)	**4**	**4**	**5**	4.3	ALTO
95	**EQUIPOS AUXILIARES**	NETBOTZ Cámara de sensor de temperatura, humedad y aniego	Cantidad; 04, marca; Netbotz Camara con sensor de temperatuta, humedad y aniego	**RESTRINGIDO**	Centro de datos de enlace, Sótano 1	Analista de centro de datos (ONP)	Coordinador del centro de datos (GMD S.A.)	**4**	**4**	**5**	4.3	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN													
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
96	**EQUIPOS AUXILIARES**	Termohigrometro	Cantidad: 02, Marca; Radioshack Equipo sensor de temperatura y medad	**RESTRINGIDO**	Centro de datos de enlace, Sótano 1, sla de servidores y sala de cintoteca	Analista de centro de datos (ONP)	Coordinador del centro de datos (GMD S.A.)	**4**	**4**	**5**	4.3	ALTO
97	**EQUIPOS AUXILIARES**	Digital Video Recorder	Cantidad: 09 marca: Hikvision Sistema de camaras de vigilancia - CCTV	**RESTRINGIDO**	Centro de datos de enlace, Sótano 1	Analista de centro de datos (ONP)	Coordinador del centro de datos (GMD S.A.)	**4**	**4**	**5**	4.3	ALTO
98	**EQUIPOS AUXILIARES**	Intercomunicador	Cantidad: 01, marca: Belcon Sistema de control de accesos - intercomunicador con pantalla a color de 7 pulgadas	**RESTRINGIDO**	Centro de datos de enlace, Sótano 1	Analista de centro de datos (ONP)	Coordinador del centro de datos (GMD S.A.)	**4**	**4**	**5**	4.3	ALTO
99	**EQUIPOS AUXILIARES**	Lectora de tarjeta proximidad	Cantidad: 01, marca: Rosslare Sistema de control de accesos - lector de proximidad restringido a personal autorizado	**RESTRINGIDO**	Centro de datos de enlace, Sótano 1	Analista de centro de datos (ONP)	Coordinador del centro de datos (GMD S.A.)	**4**	**4**	**5**	4.3	ALTO
100	**EQUIPOS AUXILIARES**	Tablero de transferencia automática	Cantidad: 01, marca: Deep SEA electronics Tablero de transferencia automática para energía comercial y grupo electrógeno	**RESTRINGIDO**	Centro de datos de enlace, Sótano 1	Analista de centro de datos (ONP)	Coordinador del centro de datos (GMD S.A.)	**4**	**4**	**5**	4.3	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
101	**EQUIPOS AUXILIARES**	Unidad condensadora	Total: 04 Cantidad: 02, Marca; Emerson Equipo condensador de aire acondicionado de precisión en la sala de servidores Soporta: Aire acondicionado Precisión (Emersón-Liebert CRV) Cantidad: 02, Marca; HIREF Equipo condensador de aire acondicionado de precisión en la sala de servidores Soporta: Aire acondicionado Precisión (HIREF) Cantidad: 01, Marca; MIDEA Soporta: Aire acondicionado Precisión (SPLIP) Cantidad: 01, Marca; York Soporta: Aire acondicionado Precisión (York)	**RESTRINGIDO**	Centro de datos de enlace, Sótano 1	Analista de centro de datos (ONP)	Coordinador del centro de datos (GMD S.A.)	**4**	**4**	**5**	4.3	ALTO
102	**EQUIPOS AUXILIARES**	Baterías	Total: 132 Marca; Orima, 12V 77W Soporta; UPS ABB de 20 KVA 100 baterías almacenadoras de energía para asegurar autonomía Marca; Orima, 12V 100W Soporta; UPS E Series 32baterias almacenadoras de energía para asegurar autonomía	**RESTRINGIDO**	Centro de datos de enlace, Sótano 1	Analista de centro de datos (ONP)	Coordinador del centro de datos (GMD S.A.)	**4**	**4**	**5**	4.3	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN												
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
103	**SERVICIOS**	Servicio de Administración de Centro de Datos y Comunicaciones (GMD)	Servicio de administración del centro de datos y comunicaciones sobre la base de mantener una infraestructura tecnológica a demanda, basada en estándares generalmente aceptados por la industria del sector, transparente para los servicios de aplicaciones y para los usuarios finales, que permita a la ONP asumir de forma óptima los encargos conferidos de acuerdo a ley	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**4**	**4**	**5**	4.3	ALTO
104	**SERVICIOS**	Servicio de Equipamiento Tecnológico del Personal y Mesa de Administración de Servicio (Consorcio GMD-PMC)	Servicio de abastecimiento de equipos tecnológicos, dar soporte a usuarios a nivel nacional, brindando atención telefónica o personal en el caso se requiera, ante cualquier consulta, incidente o requerimiento; todo ello sobre la base de mantener un equipamiento tecnológico basado en estándares, transparente para los servicios de aplicaciones y para los usuarios finales; evitando la obsolescencia tecnológica.	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**4**	**4**	**5**	4.3	ALTO

INVENTARIO DE ACTIVOS DE INFORMACIÓN													
ÍTEM	TIPO DE ACTIVO DE INFORMACION	NOMBRE DEL ACTIVO DE INFORMACION	DESCRIPCIÓN DEL ACTIVO DE INFORMACION	CLASIFICACIÓN DE LA INFORMACION	UBICACIÓN	PROPIETARIO DEL ACTIVO	ADMINISTRADOR DEL ACTIVO	VALOR DEL ACTIVO DE INFORMACION				
								[C]	[I]	[D]	VALOR	NIVEL
105	**DATOS E INFORMACIÓN**	Documentación del proyecto	Documentación elaborada del SGSI y la operativa del proyecto (Políticas, Manuales, Procedimientos, instructivos, etc.)	**RESTRINGIDO**	Centro Cívico y Comercial de Lima - Torre 1 - Piso 12	Jefe de la OTI	Gerente del Servicio	**4**	**4**	**4**	4.0	ALTO

Fuente: Elaboración propia

5.9.2. EVALUACIÓN DEL RIESGO

CUADRO N° 5.34 EVALUACIÓN DE RIESGOS

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
Base de Datos BDPRD11G, BDPRD11G2, BDPRD11G3, BDPRD11G4, etc	DATOS E INFORMACIÓN	AME001	ACCESO LOGICO NO AUTORIZADO	Incumplimiento de permisos, privilegios y control de acceso / No se tiene sistema de bloqueo de ataques	3	5	4	5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	4	3	3	14
	DATOS E INFORMACIÓN	AME002	ALTERACIÓN ACCIDENTAL DE LA INFORMACIÓN	SQL Injection	3		5		5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	4	3	3	14
	DATOS E INFORMACIÓN	AME003	DIVULGACION DE INFORMACION	El personal no tiene claro la función de la gestión de la seguridad de la información	3	5			5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	3	4	14
	DATOS E INFORMACIÓN	AME004	ERRORES DEL ADMINISTRADOR DEL EQUIPO O SISTEMA	Procedimientos de operación no documentados	4	4	4	5	5	20	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	3	2	7
	DATOS E INFORMACIÓN	AME005	MODIFICACIÓN DELIBERADA DE LA INFORMACIÓN	Políticas de Seguridad	3		5		5	15	ALTO	Jefe de la Oficina de	NO	2	3	3	3	22

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
				deficientes o inexistentes								Tecnología de la Información						
	DATOS E INFORMACIÓN	AME006	SUPLANTACION DE LA IDENTIDAD DEL USUARIO	Credenciales compartidas entre usuarios	4	4	4	5	5	20	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	3	2	7
Documentación del Proyecto	DATOS E INFORMACIÓN	AME007	ERRORES DEL ADMINISTRADOR DEL EQUIPO O SISTEMA	Procedimientos de operación no documentados	4	4	4	4	4	16	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	3	2	26
	DATOS E INFORMACIÓN	AME008	FUGA DE INFORMACION	Políticas de Seguridad deficientes o inexistentes	3	4			4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	4	4	3	29
	DATOS E INFORMACIÓN	AME009	MODIFICACIÓN DELIBERADA DE LA INFORMACIÓN	Políticas de Seguridad deficientes o inexistentes	3		4		4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	3	2	46
UPS, Baterías, Aire acondicionado, Termohigrometro, etc.	EQUIPOS AUXILIARES	AME010	VIBRACIONES, POLVO, SUCIEDAD,…	Falta de Mantenimiento Preventivo / No se tienen mecanismos para evitar los efectos de la contaminación	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	2	2	46

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
	EQUIPOS AUXILIARES	AME011	ACCESO FISICO NO AUTORIZADO	Acceso Físico no controlado / No se tienen controles para la seguridad física	3	4	3		4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	2	2	71
	EQUIPOS AUXILIARES	AME012	CORTE DEL SUMINISTRO ELÉCTRICO	No tener mecanismos alternos para el suministro eléctrico	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	2	2	46
	EQUIPOS AUXILIARES	AME013	ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE EQUIPOS (HARDWARE)	Temperatura y Humedad no controlados	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	37
	EQUIPOS AUXILIARES	AME014	FALLA DEL FUNCIONAMIENTO DEL SISTEMA DE CLIMATIZACIÓN	No se cuenta con mecanismos para controlar la temperatura y humedad en niveles apropiados	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	3	2	30
	EQUIPOS AUXILIARES	AME015	FALLA DEL FUNCIONAMIENTO DEL HARDWARE	Antigüedad del Equipo / Mantenimientos No Son Planificados	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	37
	EQUIPOS AUXILIARES	AME016	MANIPULACIÓN DE LOS EQUIPOS	Procedimientos de operación no documentados	3	4		4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	3	2	46

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
Servidores físicos y Appliance	HARDWARE	AME017	FALLA DEL FUNCIONAMIENTO DEL HARDWARE	Antigüedad del Equipo / Mantenimientos No Son Planificados	3			4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	3	2	46
	HARDWARE	AME018	ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE EQUIPOS (HARDWARE)	Temperatura y Humedad no controlados	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	1	2	3	2	46
	HARDWARE	AME019	ACCESO FISICO NO AUTORIZADO	Acceso Físico no controlado / No se tienen controles para la seguridad física	3	4	3		4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	61
	HARDWARE	AME020	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS (SATURACIÓN)	Errores de gestión de recursos	4			5	5	20	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	3	7
	HARDWARE	AME021	ABUSO DE PRIVILEGIOS DE ACCESO	Incumplimiento de permisos, privilegios y control de acceso	3	4	3	5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	37
	HARDWARE	AME022	VIBRACIONES, POLVO, SUCIEDAD,…	Falta de Mantenimiento Preventivo / No se tienen mecanismos para evitar los	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	2	2	46

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
				efectos de la contaminación														
	HARDWARE	AME023	ERRORES DEL ADMINISTRADOR DEL EQUIPO O SISTEMA	Falta capacitación en Seguridad Insuficiente / Procedimientos de operación no documentados / Falta de Técnicas de Programación de Software Seguro	4	4	4	5	5	20	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	14
Desktop / notebook	HARDWARE	AME024	ROBO	No se tienen mecanismos para la seguridad física de activos	3	4		4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	5	4	4	14
	HARDWARE	AME025	FALLA DEL FUNCIONAMIENTO DEL HARDWARE	Antigüedad del Equipo / Mantenimientos No Son Planificados	3			3	3	9	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	76
	HARDWARE	AME026	PÉRDIDA DE EQUIPOS	No se tienen mecanismos para la seguridad física de activos	3	4		4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	4	4	33
	HARDWARE	AME027	VIBRACIONES, POLVO, SUCIEDAD,…	Falta de Mantenimiento Preventivo / No se tienen mecanismos para evitar los	3			4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	61

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
				efectos de la contaminación														
Instalaciones / Data Center	INSTALACIONES	AME028	TERREMOTO (SISMOS)	Sede ubicada en zona sísmica / Fallas estructurales de las instalaciones	2			5	5	10	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	5	5	5	5	7
	INSTALACIONES	AME029	ATAQUE DESTRUCTIVO (VANDALISMO, TERRORISMO, ACCIÓN MILITAR,…)	Inseguridad en el contexto social	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	5	5	5	5	1
	INSTALACIONES	AME030	INCENDIO	No se tienen extintores ni sistema contra incendio / Tomas eléctricas en mal estado	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	5	5	5	4	3
	INSTALACIONES	AME031	INUNDACIÓN	Conexiones de agua dentro del área de procesamiento de datos	3			4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	5	5	4	12
	INSTALACIONES	AME032	ACCESO FISICO NO AUTORIZADO	Acceso Físico no controlado / No se tienen controles para la seguridad física	3	4	3		4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	61

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
Oficinas Administrativas PISO 12	INSTALACIONES	AME033	ACCESO FISICO NO AUTORIZADO	Acceso Físico no controlado / No se tienen controles para la seguridad física	4	4	3		4	16	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	33
	INSTALACIONES	AME034	ATAQUE DESTRUCTIVO (VANDALISMO, TERRORISMO, ACCIÓN MILITAR…)	Inseguridad en el contexto social	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	5	5	5	5	1
	INSTALACIONES	AME035	INUNDACIÓN	Conexiones de agua dentro del área de procesamiento de datos	3			4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	5	5	4	12
	INSTALACIONES	AME036	INCENDIO	No se tienen extintores ni sistema contra incendio / Tomas eléctricas en mal estado	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	5	5	5	4	3
	INSTALACIONES	AME037	TERREMOTO (SISMOS)	Sede ubicada en zona sísmica / Fallas estructurales de las instalaciones	2			5	5	10	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	5	5	5	5	7

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
Personal del Servicio (Gerente / jefes / Analistas / Administradores / Asistentes / etc.)	PERSONAL	AME038	INDISPONIBILIDAD DEL PERSONAL (HUELGAS, ABSENTISMO LABORAL, BAJAS NO JUSTIFICADAS, BLOQUEO DE LOS ACCESOS, ...)	No hay formación de Personal Alterno / Funciones no segregadas	4			4	4	16	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	4	3	20
	PERSONAL	AME039	FUGA DE INFORMACION	Dispositivos de Entrada y Salida de datos no controlados / Políticas de Seguridad deficientes o inexistentes	4	4			4	16	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	4	4	6
Switch Core, Switch de distribución, Teléfonos IP, Call Manager, etc.	RED DE COMUNICACIONES	AME040	ACCESO FISICO NO AUTORIZADO	Acceso Físico no controlado / No se tienen controles para la seguridad física	4	4	3		4	16	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	2	2	45
	RED DE COMUNICACIONES	AME041	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS (SATURACIÓN)	Errores de gestión de recursos	4			4	4	16	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	3	26
	RED DE COMUNICACIONES	AME042	CORTE DEL SUMINISTRO ELÉCTRICO	No tener mecanismos	3			5	5	15	ALTO	Jefe de la Oficina de	NO	2	2	3	2	37

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
				alternos para el suministro eléctrico								Tecnología de la Información						
	RED DE COMUNICACIONES	AME043	ERRORES DEL ADMINISTRADOR DEL EQUIPO O SISTEMA	Falta capacitación en Seguridad Insuficiente / Procedimientos de operación no documentados / Falta de Técnicas de Programación de Software Seguro	4	4	4	4	4	16	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	33
	RED DE COMUNICACIONES	AME044	CORTE DEL SUMINISTRO ELÉCTRICO	No tener mecanismos alternos para el suministro eléctrico	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	2	2	46
Servicio de Centro de Datos y Comunicaciones	SERVICIO	AME045	FALTA PLANIFICAR LA CONTINGENCIA	No se tiene un Site Alterno en caso de contingencia / No se tienen Planes de Continuidad	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	4	5	4	5
	SERVICIO	AME046	INCUMPLIMIENTO DE LOS ACUERDOS DE NIVELES DE SERVICIOS	No se cuenta con herramientas de monitoreo	3			5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	4	3	22

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
	SERVICIO	OPO001	INCREMENTO DEL COSTO DEL SOFTWARE (LICENCIAMIENTO) PARA LAS EMPRESAS CLIENTES	Alta demanda del cliente por nuevos servicios / equipamiento tecnológico	3			3	3	9	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	1	5	3	69
	SERVICIO	OPO002	INCREMENTO DE LA DEMANDA POR EL USO DE LA PLATAFORMA COMO SERVICIO (PAAS)	Alta demanda del cliente por nuevos servicios / equipamiento tecnológico	3	3	3	3	3	9	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	1	5	3	69
Aplicaciones Core de ONP	SOFTWARE	AME047	ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	Falta de Capacitación Técnica	3		5	5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	37
	SOFTWARE	AME048	DIFUSIÓN DE SOFTWARE DAÑINO (MALWARE)	Injección de Código / Injecciones de Comandos de Sistema Operativo	3	4	4	5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	4	3	22
	SOFTWARE	AME049	ACCESO LOGICO NO AUTORIZADO	Incumplimiento de permisos, privilegios y control de acceso / No se tiene sistema de bloqueo de ataques	3	4	4	5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	37

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
	SOFTWARE	AME050	ERRORES DE CONFIGURACION	Falta de Capacitación Técnica	3	4	5	5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	4	3	2	22
	SOFTWARE	AME051	SUPLANTACION DE LA IDENTIDAD DEL USUARIO	Credenciales compartidas entre usuarios	4	3	3	4	4	16	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	2	3	26
	SOFTWARE	AME052	VENCIMIENTO DE LICENCIA DE USO (SOFTWARE)	No se realiza seguimiento a la renovación de las licencias	3			4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	3	2	46
	SOFTWARE	AME053	VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	Error de Diseño / Problemas de Cifrado o Encriptado / Validación de entrada	3	4	4	5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	3	2	30
	SOFTWARE	AME054	ABUSO DE PRIVILEGIOS DE ACCESO	Incumplimiento de permisos, privilegios y control de acceso	3	4	4	5	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	37
Aplicaciones de ONP	SOFTWARE	AME055	ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	Falta de Capacitación Técnica	3		4	4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	3	46

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
	SOFTWARE	AME056	DIFUSIÓN DE SOFTWARE DAÑINO (MALWARE)	Injección de Código / Injecciones de Comandos de Sistema Operativo	3	4	4	4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	3	46
	SOFTWARE	AME057	ACCESO LOGICO NO AUTORIZADO	Incumplimiento de permisos, privilegios y control de acceso / No se tiene sistema de bloqueo de ataques	3	4	4	4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	3	46
	SOFTWARE	AME058	ERRORES DE CONFIGURACION	Falta de Capacitación Técnica	3	4	4	4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	61
	SOFTWARE	AME059	SUPLANTACION DE LA IDENTIDAD DEL USUARIO	Credenciales compartidas entre usuarios	4	3	3	3	3	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	2	3	61
	SOFTWARE	AME060	VENCIMIENTO DE LICENCIA DE USO (SOFTWARE)	No se realiza seguimiento a la renovación de las licencias	3			4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	2	2	71
	SOFTWARE	AME061	VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	Error de Diseño / Problemas de Cifrado o Encriptado / Validación de entrada	3	4	4	4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	2	2	71

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
	SOFTWARE	AME062	ABUSO DE PRIVILEGIOS DE ACCESO	Incumplimiento de permisos, privilegios y control de acceso	3	4	4	4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	2	3	46
Software / Sistema Operativo	SOFTWARE	AME063	INSTALACIÓN DE SOFTWARE NO LICENCIADO	No hay lineamientos para el uso de software licenciado	3			4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	2	3	46
	SOFTWARE	AME064	VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	Error de Diseño / Problemas de Cifrado o Encriptado / Validación de entrada	3	4	4	4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	2	3	61
	SOFTWARE	AME065	ABUSO DE PRIVILEGIOS DE ACCESO	Incumplimiento de permisos, privilegios y control de acceso	3	4	4	4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	2	3	46
	SOFTWARE	AME066	ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)	Falta de Capacitación Técnica	3		4	4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	2	2	71
	SOFTWARE	AME067	VENCIMIENTO DE LICENCIA DE USO (SOFTWARE)	No se realiza seguimiento a la renovación de las licencias	3			4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	2	2	71

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
	SOFTWARE	AME068	ACCESO LOGICO NO AUTORIZADO	Incumplimiento de permisos, privilegios y control de acceso / No se tiene sistema de bloqueo de ataques	3	4	4	4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	2	61
	SOFTWARE	AME069	DIFUSIÓN DE SOFTWARE DAÑINO (MALWARE)	Injección de Código / Injecciones de Comandos de Sistema Operativo	3	4	5	4	5	15	ALTO	Jefe de la Oficina de Tecnología de la Información	NO	2	2	3	3	30
Cintas LTO4, LTO5	SOPORE DE INFORMACIÓN	AME070	ROBO	No se tienen mecanismos para la seguridad física de activos	3	4		4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	5	4	4	14
	SOPORE DE INFORMACIÓN	AME071	FALTA DE SOPORTES DE INFORMACIÓN (CINTAS, DISCOS EXTERNOS, CD/DVD,…)	No se tiene contratado un proveedor de medios de soporte	3			4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	5	3	2	33
	SOPORE DE INFORMACIÓN	AME072	AVERÍA DE LOS MEDIOS DE ALMACENAMIENTO DE INFORMACIÓN (CINTAS, CD/DVD, HARD DISK, ETC.)	Mal uso de las personas	3			4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	5	2	2	44

IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO													EVALUACIÓN DEL RIESGO				
ACTIVO / GRUPO DE ACTIVOS	TIPO DE ACTIVO DE INFORMACIÓN	ID RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	PROBABILIDAD	IMPACTO				RIESGO	NIVEL DEL RIESGO	PROPIETARIO DEL RIESGO	¿RIESGO ACEPTABLE?	CRITERIOS DE EVALUACIÓN				PRIORIDAD
						[C]	[I]	[D]	VALOR DEL IMPACTO					FINANCIERO	OPERATIVO	LEGAL	IMAGEN	
	SOPORE DE INFORMACIÓN	AME073	DIVULGACION DE INFORMACION	El personal no tiene claro la función de la gestión de la seguridad de la información	3	4			4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	3	2	2	61
	SOPORE DE INFORMACIÓN	AME074	MANIPULACIÓN DE LOS EQUIPOS	Procedimientos de operación no documentados	3	4		4	4	12	MEDIO	Jefe de la Oficina de Tecnología de la Información	NO	2	5	4	3	21

Fuente: Elaboración Propia

5.9.3. PLAN DE TRATAMIENTO DE RIESGOS

CUADRO N° 5.35 PLAN DE TRATAMIENTO DE RIESGOS

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME001	Mitigar	Se elaborará una Política de control de accesos Se gestionará con el personal del proyecto la firma de los acuerdos de confidencialidad de no divulgar la información que accedan. Se emplearan controles de acceso lógico: - Uso de clave alfanumérica generada de 8 dígitos. - Bloqueo de cuenta por intentos fallidos (3 veces consecutivamente) - Se revisará de manera trimestral el control de acceso a las bases de datos. - Se conservarán y revisaran los registros LOG de autenticación y acceso a los bases de datos. - Se realizará la instalación de parches de seguridad según la recomendación del fabricante - Se monitoreará el acceso a la red (IDS/IPS)	9.1.1 Política de control de acceso	Pe	Pv	Sa	95%	Gestor de accesos	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME002	Mitigar	Se realizan pruebas de ethical hacking de manera anual. Se realizan cambios en la plataforma según la recomendación del fabricante ante cualquier vulnerabilidad detectada	12.6.1 Gestión de las vulnerabilidades técnicas	Pd	Pv	At	65%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME003	Mitigar	Se realizarán charlas de concienciación en temas de seguridad al ingreso al proyecto, así como de manera programada en el año	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME004	Mitigar	Revisión y/o actualización de los procedimientos e instructivos operativos del área o proceso	12.1.1 Procedimiento de operación documentados	Pe	Pv	Ma	90%	Analista de Procesos	Abr-15	Ago-15	BAJO	SI	CERRADO
AME005	Mitigar	Se elaborará la Política de seguridad de la información y será difundida al personal por diversos medios (Correo, capacitaciones, murales, etc.)	5.1.1 Política de seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME006	Mitigar	Se realizarán charlas de concienciación en temas de seguridad al ingreso al proyecto, así como de manera programada en el año	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME007	Mitigar	Revisión y/o actualización de los procedimientos e instructivos operativos del área o proceso	12.1.1 Procedimiento de operación documentados	Pe	Pv	Ma	90%	Analista de Procesos	Abr-15	Ago-15	BAJO	SI	CERRADO
AME008	Mitigar	Se elaborará la Política de seguridad de la información y será difundida al personal por diversos medios (Correo, capacitaciones, murales, etc.)	5.1.1 Política de seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME009	Mitigar	Se elaborará la Política de seguridad de la información y será difundida al personal por diversos medios (Correo, capacitaciones, murales, etc.)	5.1.1 Política de seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME010	Mitigar	Programar y ejecutar los mantenimientos preventivos (anual)	A.11.2.4 Mantenimiento del equipamiento	Pd	Pv	Sa	65%	Coordinador de Centro de Datos	Abr-15	Ago-15	BAJO	SI	CERRADO
AME011	Mitigar	Se llevará un control de ingreso a las instalaciones del data center. Los operadores acompañaran a las visitantes durante su permanencia en las instalaciones El ingreso será con anticipación al data center mínimo de 4 días. El acceso al data center cuenta con los siguientes controles: 1. Puerta eléctrica con tarjetas de proximidad. 2. Cámaras de videovigilancias.	A.11.1.2 Controles de acceso físico	Pe	Dt	Sa	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
		El Personal de seguridad verificara los objetos de entrada y salida de las personas.											
AME012	Mitigar	Se realizarán mantenimientos preventivos a los equipos de apoyo (UPS, etc..) Se realizarán mantenimientos y pruebas anuales al grupo electrógeno	17.1.1 Planificación de la continuidad de la seguridad de la información	Pe	Pv	Sa	95%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME013	Mitigar	Revisar los controles de medición de humedad y temperatura en el data center Los operadores monitorean el servicio mediante la herramienta de monitoreo Foglight, el cual permite monitorear la disponibilidad de la plataforma central a nivel nacional	12.1.3 Gestión de la capacidad	Pe	Dt	At	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME014	Mitigar	Revisar los controles de medición de humedad y temperatura en el data center Los operadores monitorean el servicio mediante la herramienta de monitoreo Foglight, el cual permite monitorear la disponibilidad de la plataforma central a nivel nacional	12.1.3 Gestión de la capacidad	Pe	Dt	At	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME015	Mitigar	Programar y ejecutar los mantenimientos preventivos (anual)	A.11.2.4 Mantenimiento del equipamiento	Pd	Pv	Sa	65%	Coordinador de Centro de Datos	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME016	Mitigar	Revisión y/o actualización de los procedimientos e instructivos operativos del área o proceso	12.1.1 Procedimiento de operación documentados	Pe	Pv	Ma	90%	Analista de Procesos	Abr-15	Ago-15	BAJO	SI	CERRADO
AME017	Mitigar	Programar y ejecutar los mantenimientos preventivos (anual)	A.11.2.4 Mantenimiento del equipamiento	Pd	Pv	Sa	65%	Administrador Unix	Abr-15	Ago-15	BAJO	SI	CERRADO
AME018	Mitigar	Revisar los controles de medición de humedad y temperatura en el data center Los operadores monitorean el servicio mediante la herramienta de monitoreo Foglight, el cual permite monitorear la disponibilidad de la plataforma central a nivel nacional	12.1.3 Gestión de la capacidad	Pe	Dt	At	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME019	Mitigar	Se llevará un control de ingreso a las instalaciones del data center. Los operadores acompañaran a las visitantes durante su permanencia en las instalaciones El ingreso será con anticipación al data center mínimo de 4 días. El acceso al data center cuenta con los siguientes controles: 1. Puerta eléctrica con tarjetas de proximidad. 2. Cámaras de videovigilancias. El Personal de seguridad verificara	A.11.1.2 Controles de acceso físico	Pe	Dt	Sa	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
		los objetos de entrada y salida de las personas.											
AME020	Mitigar	Se monitoreará la plataforma tecnológica mediante el uso de la herramienta Foglight, los administradores tendran 2 monitores uno para sus labores operativas y otra de monitoreo.	12.1.3 Gestión de la capacidad	Pe	Dt	At	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME021	Mitigar	Se elaborará una Política de control de accesos Se gestionará con el personal del proyecto la firma de los acuerdos de confidencialidad de no divulgar la información que accedan. Se emplearan controles de acceso lógico: - Uso de clave alfanumérica generada de 8 dígitos. - Bloqueo de cuenta por intentos fallidos (3 veces consecutivamente) - Se revisará de manera trimestral el e control de acceso a las bases de datos. - Se conservaran y revisaran los registros LOG de autenticación y acceso a los bases de datos. - Se realizara la instalación de parches de seguridad según la recomendación del fabricante	9.1.1 Política de control de acceso	Pe	Pv	Ma	90%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
		- Se monitoreará el acceso a la red (IDS/IPS)											
AME022	Mitigar	Programar y ejecutar los mantenimientos preventivos (anual)	A.11.2.4 Mantenimiento del equipamiento	Pd	Pv	Sa	65%	Administrador Unix	Abr-15	Ago-15	BAJO	SI	CERRADO
AME023	Mitigar	Revisión y/o actualización de los procedimientos e instructivos operativos del área o proceso	12.1.1 Procedimiento de operación documentados	Pe	Pv	Ma	90%	Analista de Procesos	Abr-15	Ago-15	BAJO	SI	CERRADO
AME024	Mitigar	El acceso a las oficinas será previa coordinación y autorización con el jefe o responsable del área. Los equipos (notebook) tendrá su cadena de seguridad. Se cuenta con cámara de vigilancia y personal de seguridad física de la sede	A.11.1.2 Controles de acceso físico	Pe	Dt	Sa	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME025	Mitigar	Programar y ejecutar los mantenimientos preventivos (anual)	A.11.2.4 Mantenimiento del equipamiento	Pd	Pv	Sa	65%	Coordinador de la Mesa de Servicios	Abr-15	Ago-15	BAJO	SI	CERRADO
AME026	Mitigar	El acceso a las oficinas será previa coordinación y autorización con el jefe o responsable del área. Los equipos (notebook) tendrá su cadena de seguridad. Se cuenta con cámara de vigilancia y personal de seguridad física de la sede	A.11.1.2 Controles de acceso físico	Pe	Dt	Sa	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME027	Mitigar	Programar y ejecutar los mantenimientos preventivos (anual)	A.11.2.4 Mantenimiento del equipamiento	Pd	Pv	Sa	65%	Coordinador de la Mesa de Servicios	Abr-15	Ago-15	BAJO	SI	CERRADO
AME028	Mitigar	Elaborar planes de respuesta ante emergencia (continuidad) Realizar simulacros periódicos, contar con brigadas de emergencia	A.17.1.1 Planificación de la continuidad de la seguridad de la información	Pe	Pv	Sa	95%	Jefe de Producción / Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME029	Mitigar	Elaborar planes de respuesta ante emergencia (continuidad) Realizar simulacros periódicos, contar con brigadas de emergencia	A.17.1.1 Planificación de la continuidad de la seguridad de la información	Pe	Pv	Sa	95%	Jefe de Producción / Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME030	Mitigar	Se realizarán las revisiones y cambio de extintores Se formarán brigadistas y se revisarán las señales de evacuación en caso de emergencia	A.11.1.2 Controles de acceso físico	Pe	Dt	Sa	75%		Abr-15	Ago-15	BAJO	SI	CERRADO
AME031	Mitigar	Elaborar planes de respuesta ante emergencia (continuidad) Realizar simulacros periódicos, contar con brigadas de emergencia	A.17.1.1 Planificación de la continuidad de la seguridad de la información	Pe	Pv	Sa	95%	Jefe de Producción / Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME032	Mitigar	Se llevará un control de ingreso a las instalaciones del data center. Los operadores acompañaran a las	A.11.1.2 Controles de acceso físico	Pe	Dt	Sa	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
		visitantes durante su permanencia en las instalaciones El ingreso será con anticipación al data center mínimo de 4 días. El acceso al data center cuenta con los siguientes controles: 1. Puerta eléctrica con tarjetas de proximidad. 2. Cámaras de videovigilancias. El Personal de seguridad verificara los objetos de entrada y salida de las personas.											
AME033	Mitigar	El acceso a la oficina será mediante correo de autorización del jefe de área. El acceso a las oficinas cuenta con los siguientes controles: 1. Puerta eléctrica con tarjetas de proximidad. 2. Cámaras de videovigilancias. 3. Compromiso de confidencialidad del personal / proveedor que acceda a la información 7. Personal de seguridad (Verificación de objetos de entrada y salida).	A.11.1.2 Controles de acceso físico	Pe	Dt	Sa	75%	Gerente del Proyecto	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME034	Mitigar	Elaborar planes de respuesta ante emergencia (continuidad) Realizar simulacros periódicos, contar con brigadas de emergencia	A.17.1.1 Planificación de la continuidad de la seguridad de la información	Pe	Pv	Sa	95%	Jefe de Producción / Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME035	Mitigar	Elaborar planes de respuesta ante emergencia (continuidad) Realizar simulacros periódicos, contar con brigadas de emergencia	A.17.1.1 Planificación de la continuidad de la seguridad de la información	Pe	Pv	Sa	95%	Jefe de Producción / Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME036	Mitigar	Se realizarán las revisiones y cambio de extintores Se formarán brigadistas y se revisaran las señales de evacuación en caso de emergencia	A.11.1.2 Controles de acceso físico	Pe	Dt	Sa	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME037	Mitigar	Elaborar planes de respuesta ante emergencia (continuidad) Realizar simulacros periódicos, contar con brigadas de emergencia	A.17.1.1 Planificación de la continuidad de la seguridad de la información	Pe	Pv	Sa	95%	Jefe de Producción / Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME038	Mitigar	Elaborar esquema o plan de reemplazo o sucesión en caso de ausencia de personal del proyecto	A.6.1.2 Segregación de funciones	Pe	Pv	Ma	90%	Jefaturas del Proyecto	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME039	Mitigar	Se realizarán charlas de concienciación en temas de seguridad al ingreso al proyecto así como de manera programada en el año	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME040	Mitigar	Se llevará un control de ingreso a las instalaciones del data center. Los operadores acompañaran a las visitantes durante su permanencia en las instalaciones El ingreso será con anticipación al data center mínimo de 4 días. El acceso al data center cuenta con los siguientes controles: 1. Puerta eléctrica con tarjetas de proximidad. 2. Cámaras de videovigilancias. El Personal de seguridad verificara los objetos de entrada y salida de las personas.	A.11.1.2 Controles de acceso físico	Pe	Dt	Sa	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME041	Mitigar	Se monitoreará la plataforma tecnológica mediante el uso de la herramienta Foglight, los administradores tendrán 2 monitores uno para sus labores operativas y otra de monitoreo.	12.1.3 Gestión de la capacidad	Pe	Dt	At	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME042	Mitigar	Se realizarán mantenimientos preventivos a los equipos de apoyo (UPS, etc..) Se realizarán mantenimientos y pruebas anuales al grupo electrógeno	17.1.1 Planificación de la continuidad de la seguridad de la información	Pe	Pv	Sa	95%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME043	Mitigar	Revisión y/o actualización de los procedimientos e instructivos operativos del área o proceso	12.1.1 Procedimiento de operación documentados	Pe	Pv	Ma	90%	Analista de Procesos	Abr-15	Ago-15	BAJO	SI	CERRADO
AME044	Mitigar	Se realizarán mantenimientos preventivos a los equipos de apoyo (UPS, etc..) Se realizarán mantenimientos y pruebas anuales al grupo electrógeno	17.1.1 Planificación de la continuidad de la seguridad de la información	Pe	Pv	Sa	95%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME045	Mitigar	Elaborar planes de respuesta ante emergencia (continuidad)	A.17.1.1 Planificación de la continuidad de la seguridad de la información	Pe	Pv	Sa	95%	Jefe de Producción / Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME046	Mitigar	Se monitoreará la plataforma tecnológica mediante el uso de la herramienta Foglight, los administradores tendrán 2 monitores uno para sus labores operativas y otra de monitoreo.	12.1.3 Gestión de la capacidad	Pe	Dt	At	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
OPO001	Mitigar	Revisión y/o actualización del proceso de gestión de cambios para la	12.1.2 Gestión de cambios	Oc	Pv	Sa	35%	Gestor de Servicios de TI	Abr-15	Ago-15	ALTO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
		plataforma central (riesgos, activos involucrados, plan de acción, plan de respuesta en caso de algún incidente, etc.)						Oficial de Seguridad de la Información					
OPO002	Mitigar	Revisión y/o actualización del proceso de gestión de cambios para la plataforma central (riesgos, activos involucrados, plan de acción, plan de respuesta en caso de algún incidente, etc.)	12.1.2 Gestión de cambios	Oc	Pv	Sa	35%	Gestor de Servicios de TI Oficial de Seguridad de la Información	Abr-15	Ago-15	ALTO	SI	CERRADO
AME047	Mitigar	Se realizarán charlas de concienciación en temas de seguridad al ingreso al proyecto así como de manera programada en el año	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME048	Mitigar	Elaboración y/o actualización del procedimiento de Gestión de Cambios. Se elaborará un programa de instalación de parches de seguridad y fixes a nivel de base de datos y aplicaciones.	12.2.1 Controles contra código malicioso	Pe	Cr	Sa	85%	Gestor de Servicios de TI Administrador de Seguridad Perimetral	Abr-15	Ago-15	BAJO	SI	CERRADO
AME049	Mitigar	1. Uso de clave alfanumérica generada de 8 dígitos. 2. Bloqueo de cuenta por intentos fallidos (3 veces consecutivamente) 3. Se cuenta con una matriz trimestral de control de acceso directo a las bases de datos.	9.1.1 Política de control de acceso	Pe	Pv	Sa	95%	Gestor de accesos	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
		4. Registros LOG de autenticación y acceso a los bases de datos. 5. Programa de instalación de parches de seguridad y fixes a nivel de base de datos y aplicaciones. 6. Monitoreo de acceso a la red (IDS/IPS)											
AME050	Mitigar	Se elaborará un plan de capacitación técnica anualmente según las necesidades de las actividades del personal /nuevas tecnologías, etc.)	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME051	Mitigar	Se realizarán charlas de concienciación en temas de seguridad al ingreso al proyecto así como de manera programada en el año	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME052	Mitigar	Se realizará la renovación anual del mantenimiento de licencias	18.1.2 Derechos de propiedad intelectual	Pd	Pv	Sa	65%	Gerente del Proyecto	Abr-15	Ago-15	BAJO	SI	CERRADO
AME053	Mitigar	Se realizan pruebas de ethical hacking de manera anual. Se realizan cambios en la plataforma según la recomendación del fabricante ante cualquier vulnerabilidad detectada	12.6.1 Gestión de las vulnerabilidades técnicas	Pd	Pv	At	65%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME054	Mitigar	Se elaborará una Política de control de accesos Se gestionará con el personal del proyecto la firma de los acuerdos de confidencialidad de no divulgar la información que accedan. Se emplearan controles de acceso lógico: - Uso de clave alfanumérica generada de 8 dígitos. - Bloqueo de cuenta por intentos fallidos (3 veces consecutivamente) - Se revisará de manera trimestral el e control de acceso a las bases de datos. - Se conservaran y revisaran los registros LOG de autenticación y acceso a los bases de datos. - Se realizara la instalación de parches de seguridad según la recomendación del fabricante - Se monitoreará el acceso a la red (IDS/IPS)	9.1.1 Política de control de acceso	Pe	Pv	Ma	90%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME055	Mitigar	Se elaborará un plan de capacitación técnica anualmente según las necesidades de las actividades del personal /nuevas tecnologías, etc.)	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME056	Mitigar	Elaboración y/o actualización del procedimiento de Gestión de Cambios. Se elaborará un programa de instalación de parches de seguridad y fixes a nivel de base de datos y aplicaciones.	12.2.1 Controles contra código malicioso	Pe	Cr	Sa	85%	Gestor de Servicios de TI Administrador de Seguridad Perimetral	Abr-15	Ago-15	BAJO	SI	CERRADO
AME057	Mitigar	Se elaborará una Política de control de accesos Se gestionará con el personal del proyecto la firma de los acuerdos de confidencialidad de no divulgar la información que accedan. Se emplearan controles de acceso lógico: - Uso de clave alfanumérica generada de 8 dígitos. - Bloqueo de cuenta por intentos fallidos (3 veces consecutivamente) - Se revisará de manera trimestral el e control de acceso a las bases de datos. - Se conservaran y revisaran los registros LOG de autenticación y acceso a los bases de datos. - Se realizara la instalación de parches de seguridad según la recomendación del fabricante - Se monitoreará el acceso a la red (IDS/IPS)	9.1.1 Política de control de acceso	Pe	Pv	Sa	95%	Gestor de accesos	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME058	Mitigar	Se elaborará un plan de capacitación técnica anualmente según las necesidades de las actividades del personal /nuevas tecnologías, etc.)	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME059	Mitigar	Se realizarán charlas de concienciación en temas de seguridad al ingreso al proyecto así como de manera programada en el año	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME060	Mitigar	Se realizará la renovación anual del mantenimiento de licencias	18.1.2 Derechos de propiedad intelectual	Pd	Pv	Sa	65%	Gerente del Proyecto	Abr-15	Ago-15	BAJO	SI	CERRADO
AME061	Mitigar	Se realizan pruebas de ethical hacking de manera anual. Se realizan cambios en la plataforma según la recomendación del fabricante ante cualquier vulnerabilidad detectada	12.6.1 Gestión de las vulnerabilidades técnicas	Pd	Pv	At	65%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME062	Mitigar	Se elaborará una Política de control de accesos Se gestionará con el personal del proyecto la firma de los acuerdos de confidencialidad de no divulgar la información que accedan. Se emplearan controles de acceso lógico: - Uso de clave alfanumérica	9.1.1 Política de control de acceso	Pe	Pv	Ma	90%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
		generada de 8 dígitos. - Bloqueo de cuenta por intentos fallidos (3 veces consecutivamente) - Se revisará de manera trimestral el e control de acceso a las bases de datos. - Se conservaran y revisaran los registros LOG de autenticación y acceso a los bases de datos. - Se realizara la instalación de parches de seguridad según la recomendación del fabricante - Se monitoreará el acceso a la red (IDS/IPS)											
AME063	Mitigar	Se implementará control de acceso a internet para restringir la instalación de programas sin autorización	A.12.6.2 Restricciones sobre la instalación de software	Pe	Pv	Ma	90%	Gestor de Servicios de TI Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME064	Mitigar	Se realizan pruebas de ethical hacking de manera anual. Se realizan cambios en la plataforma según la recomendación del fabricante ante cualquier vulnerabilidad detectada	12.6.1 Gestión de las vulnerabilidades técnicas	Pd	Pv	At	65%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME065	Mitigar	Se elaborará una Política de control de accesos Se gestionará con el personal del proyecto la firma de los acuerdos de confidencialidad de no divulgar la	9.1.1 Política de control de acceso	Pe	Pv	Ma	90%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
		información que accedan. Se emplearan controles de acceso lógico: - Uso de clave alfanumérica generada de 8 dígitos. - Bloqueo de cuenta por intentos fallidos (3 veces consecutivamente) - Se revisará de manera trimestral el e control de acceso a las bases de datos. - Se conservaran y revisaran los registros LOG de autenticación y acceso a los bases de datos. - Se realizara la instalación de parches de seguridad según la recomendación del fabricante - Se monitoreará el acceso a la red (IDS/IPS)											
AME066	Mitigar	Se elaborará un plan de capacitación técnica anualmente según las necesidades de las actividades del personal /nuevas tecnologías, etc.)	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME067	Mitigar	Se realizará la renovación anual del mantenimiento de licencias	18.1.2 Derechos de propiedad intelectual	Pd	Pv	Sa	65%	Gerente del Proyecto	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME068	Mitigar	Se elaborará una Política de control de accesos Se gestionará con el personal del proyecto la firma de los acuerdos de confidencialidad de no divulgar la información que accedan. Se emplearan controles de acceso lógico: - Uso de clave alfanumérica generada de 8 dígitos. - Bloqueo de cuenta por intentos fallidos (3 veces consecutivamente) - Se revisará de manera trimestral el e control de acceso a las bases de datos. - Se conservaran y revisaran los registros LOG de autenticación y acceso a los bases de datos. - Se realizara la instalación de parches de seguridad según la recomendación del fabricante - Se monitoreará el acceso a la red (IDS/IPS)	9.1.1 Política de control de acceso	Pe	Pv	Sa	95%	Gestor de accesos	Abr-15	Ago-15	BAJO	SI	CERRADO
AME069	Mitigar	Elaboración y/o actualización del procedimiento de Gestión de Cambios. Se elaborará un programa de instalación de parches de seguridad y fixes a nivel de base de datos y aplicaciones.	12.2.1 Controles contra código malicioso	Pe	Cr	Sa	85%	Gestor de Servicios de TI Administardor de Seguridad Perimetral	Abr-15	Ago-15	BAJO	SI	CERRADO

PLAN DE TRATAMIENTO DEL RIESGO													
ID RIESGO	OPCIÓN DE TRATAMIENTO	DESCRIPCIÓN DEL PLAN DE ACCIÓN	ANEXO A RELACIONADO	EFECTIVIDAD DEL CONTROL				RESPONSABLE DE IMPLEMENTACIÓN	FECHA		NIVEL DEL RIESGO RESIDUAL	¿RIESGO ACEPTABLE?	ESTADO DEL RIESGO
				[P]	[T]	[A]	[NE]		INICIO	FIN			
AME070	Mitigar	El acceso al data center será previa coordinación y autorización con el jefe o responsable del área. Se cuentan con cámaras de vigilancia y puerta de acceso vía tarjeta de proximidad Personal operador labora 24*7	A.11.1.2 Controles de acceso físico	Pe	Dt	Sa	75%	Jefe de Producción	Abr-15	Ago-15	BAJO	SI	CERRADO
AME071	Compartir	Se contarán con más de un proveedor de medios de respaldos (Cintas LTO4, LTO5) por ejemplo J&S Suministros y Backup SA	15.1.2 Abordar la seguridad dentro de los acuerdos del proveedor	Pe	Pv	Ma	90%	Gerente del Proyecto	Abr-15	Ago-15	BAJO	SI	CERRADO
AME072	Mitigar	Se realizarán charlas de concienciación en temas de seguridad al ingreso al proyecto asi como de manera programada en el año	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME073	Mitigar	Se realizarán charlas de concienciación en temas de seguridad al ingreso al proyecto así como de manera programada en el año	7.2.2 Concientización, educación y formación en seguridad de la información	Pd	Pv	Ma	60%	Oficial de Seguridad de la Información	Abr-15	Ago-15	BAJO	SI	CERRADO
AME074	Mitigar	Revisión y/o actualización de los procedimientos e instructivos operativos del área o proceso	12.1.1 Procedimiento de operación documentados	Pe	Pv	Ma	90%	Analista de Procesos	Abr-15	Ago-15	BAJO	SI	CERRADO

Fuente: Elaboración Propia

5.10. MEDIR

5.10.1. MEDICIÓN DEL SGSI

Se deben medir los procesos y los controles del SGSI.

CUADRO N° 5.36 MONITOREO DE LOS PROCESOS DEL SGSI

Dominio	Objetivo del Control	Evidencia de cumplimiento	Ubicación	Quien va a medir	Que se va a medir	Resultados (mayo 2015)
4. CONTEXTO DE LA ORGANIZACIÓN	4.1 Comprender la organización y su contexto	MAN.GER.005 Manual de Alcance del SGSI	File Server	Gestión de Calidad	Cumplimiento con los Requisitos de la ISO 27001	100%
	4.2 Comprender las necesidades y expectativas de las partes interesadas	FOR.GER.013 Identificación de Partes Interesadas del SGSI	File Server	Gestión de Calidad	Cumplimiento con los Requisitos de la ISO 27001	100%
		FOR.GER.024 Identificación de Requisitos de Seguridad de la Información				
	4.3 Determinar el alcance del sistema de gestión de seguridad de la información	MAN.GER.005 Manual de Alcance del SGSI	File Server	Gestión de Calidad	Cumplimiento con los Requisitos de la ISO 27001	100%
	4.4 Sistema de gestión de la seguridad de la información	Certificación ISO 27001:2013	File Server	Gestión de Calidad	Cumplimiento con los Requisitos de la ISO 27001	100%
		FOR.GER.008 Lista maestra de documentos				

Dominio	Objetivo del Control	Evidencia de cumplimiento	Ubicación	Quien va a medir	Que se va a medir	Resultados (mayo 2015)
5. LIDERAZGO	5.1 Liderazgo y compromiso	POL.GER.001 Política de Seguridad de la Información	File Server	Gestión de Calidad	Sensibilización en SGSI Cumplimiento de Objetivos Ver control A.5.1.1. y A.5.1.2	100%
		MAN.GER.002 Manual del SGSI				
		Comités del SGSI				
		Plan de Capacitación				
		FOR.GER.023 Medición de Procesos y Controles del SGSI				
		MAN.GER.001 Manual de Organización y Funciones del SGSI				
	5.2 Política	POL.GER.001 Política de Seguridad de la Información	File Server	Gestión de Calidad	Ver control A.5.1.1. y A.5.1.2	100%
		POL.GER.001 Política de Seguridad de la Información				
		FOR.GER.025 Objetivos del SGSI				
	5.3 Roles organizacionales, responsabilidades y autoridades	MAN.GER.001 Manual de Organización y Funciones del SGSI	File Server	Gestión de Calidad	Validar que considere todas las areas del alcance	100%

Dominio	Objetivo del Control	Evidencia de cumplimiento	Ubicación	Quien va a medir	Que se va a medir	Resultados (mayo 2015)
6. PLANIFICACIÓN	6.1 Acciones para abordar los riesgos y las oportunidades	FOR.GER.025 Objetivos del SGSI	File Server	Gestión de Calidad	Validar el avance del cronograma de los riesgos y oportunidades de las áreas del alcance	100%
	6.1.1 General	MAN.GER.003 Manual de Gestión de Riesgos				
		Comités del SGSI				
		FOR.GER.017 Gestión de riesgos y oportunidades				
	6.1.2 Evaluación de riesgo de la seguridad de la información	MAN.GER.003 Manual de Gestión de Riesgos	File Server	Gestión de Calidad	Análisis y Evaluación de riesgos y oportunidades de las áreas del alcance	100%
		FOR.GER.017 Gestión de riesgos y oportunidades				
	6.1.3 Tratamiento de riesgo de la seguridad de la información	MAN.GER.003 Manual de Gestión de Riesgos	File Server	Gestión de Calidad	Riesgos aceptados formalmente	100%
		FOR.GER.018 Enunciado de Aplicabilidad				
	6.2 Objetivos de seguridad de la información y planificación para lograrlos	FOR.GER.025 Objetivos del SGSI	File Server	Gestión de Calidad	Objetivos alineados a la política de seguridad y a los objetivos estratégicos	100%
		Comités del SGSI				
7. APOYO	7.1 Recursos	Comités del SGSI	File Server	Gestión de Calidad	Ejecución de Comités del SGSI	100%
	7.2 Competencias	MAN.GER.001 Manual de Organización y Funciones del SGSI	File Server	Gestión de Calidad	Validar con gestión Humana	100%

Dominio	Objetivo del Control	Evidencia de cumplimiento	Ubicación	Quien va a medir	Que se va a medir	Resultados (mayo 2015)
		Plan de Capacitación				
	7.3 Conocimiento	Charlas de concienciación	File Server	Gestión de Calidad	Ver control A.7.2.2. y A.7.2.3	100%
		POL.GER.001 Política de Seguridad de la Información				
		PRO.GER.002 Proceso Disciplinario				
	7.4 Comunicación	PRO.GER.010 Comunicaciones del SGSI	File Server	Gestión de Calidad	Ver control A.7.2.2.	100%
	7.5 Información documentada	FOR.GER.008 Lista maestra de documentos	File Server	Gestión de Calidad	Ver control	100%
	7.5.1 General					
	7.5.2 Creación y actualización	PRO.GER.004 Control de Documentos	File Server	Gestión de Calidad	Documentos validados el cumplimiento del estandar	100%
	7.5.3 Control de la información documentada	FOR.GER.008 Lista maestra de documentos	File Server	Gestión de Calidad	Ver control A.12.1.1 Procedimientos de operación documentados	100%
		PRO.GER.005 Control de Registros				
		PRO.GER.004 Control de Documentos				

Dominio	Objetivo del Control	Evidencia de cumplimiento	Ubicación	Quien va a medir	Que se va a medir	Resultados (mayo 2015)
8. OPERACIÓN	8.1 Control y planificación operacional	FOR.GER.023 Medición de Procesos y Controles del SGSI PRO.MAS.053 Gestión de Cambios	File Server	Gestión de Calidad	Cumplimiento	100%
	8.2 Evaluación de riesgo de la seguridad de la información	MAN.GER.003 Manual de Gestión de Riesgos FOR.GER.017 Gestión de riesgos y oportunidades	File Server	Gestión de Calidad	Cronograma y registro de Evaluación de riesgos	100%
	8.3 Tratamiento de riesgo de la seguridad de la información	FOR.GER.019 Plan De Tratamiento de Riesgos	File Server	Gestión de Calidad	Cronograma y registro de Evaluación de riesgos	100%
9. EVALUACIÓN DEL DESEMPEÑO	9.1 Monitoreo, medición, análisis y evaluación	FOR.GER.023 Medición de Procesos y Controles del SGSI	File Server	Gestión de Calidad	Revisión del Monitoreo del SGSI	100%
	9.2 Auditoría Interna	PRO.GER.006 Auditoria Interna SGSI	File Server	Gestión de Calidad	Ejecución de Auditorías internas en las áreas del alcance	100%
	9.3 Revisión de gestión	Comités del SGSI	File Server	Gestión de Calidad	Validar que se traten todos los puntos indicados en la Norma	100%
10 MEJORA	10.1 No Conformidades y acciones correctivas	PRO.GER.007 Acciones Correctivas y Preventivas	File Server	Gestión de Calidad	Avance del tratamiento de No Conformidades	100%
	10.2 Mejora continua	Comités del SGSI	File Server	Gestión de Calidad	Implementación de proyectos de mejora	100%

Fuente: Elaboración Propia

CUADRO N° 5.37 MONITOREO DE LOS CONTROLES

Objetivo de Control	Control	Método de Medición	Formula de Medición	Meta	Responsable de la Medición	Frecuencia de Medición	may-15
Políticas de seguridad							
Revisión de las políticas para la seguridad de la información	Políticas y procedimientos del SGSI	Verificación de las políticas y procedimientos del SGSI se mantengan como máximo 02 años vigentes luego de su aprobación.	N° de documentos del SGSI que se mantienen vigentes (02 años). / N° Total de documentos evaluados	[>= 80%]	Oficial de Seguridad de la Información	Anual	100%
Durante el empleo							
Concientización, educación y formación en seguridad de la información	Plan de Capacitación	Verificación del número de participantes en las capacitaciónes / charlas de seguridad de la información.	N° de personas capacitadas / N° de personas programadas para capacitación.	[>= 70%]	Oficial de Seguridad de la Información	Anual	100%
Clasificación de la información							
Etiquetado de la información	Medios de soporte / Cintas de backups	Verificación de los medios de soportes que cuenten con el etiquetado y protección adecuada según su clasificación en las cintotecas.	N° de medios de soporte etiquetados y conforme / N° de medios de soporte evaluados.	[>= 90%]	Oficial de Seguridad de la Información	Anual	100%
Responsabilidades del usuario							
Uso de información de autenticación secreta	Uso de clave y contraseña de manera adecuada	Verificación del número de incidentes de seguridad relacionados a uso compartido de clave y contraseña de acceso	N° de incidentes de seguridad relacionados a uso de contraseña y clave de acceso	[= 0]	Oficial de Seguridad de la Información	Anual	0
Areas seguras							
Controles de acceso físico	Controles de acceso físico a los Centro de Datos	Verificación del número de incidentes de seguridad relacionados a accesos físicos no autorizados	N° de incidentes de seguridad relacionados a acceso no autorizado a instalaciones físicas	[= 0]	Oficial de Seguridad de la Información	Anual	0
Equipamiento							

Objetivo de Control	Control	Método de Medición	Formula de Medición	Meta	Responsable de la Medición	Frecuencia de Medición	may-15
Mantenimiento del equipamiento	Plan de mantenimiento de equipos de apoyo del centro de datos (sótano 1)	Verificación del mantenimiento de los equipos de cómputo según lo establecido en el Plan de mantenimiento de equipos	N° de equipos con mantenimiento conforme / N° de equipos programados para mantenimiento.	[>= 90%]	Oficial de Seguridad de la Información	Anual	100%
Protección contra código malicioso							
Controles contra código malicioso	Controles contra código malicioso	Verificación del total de equipos cuenten con antivirus instalado y actualizado	N° de equipos cuente con antivirus instalado y actualizado conforme / N° de equipos evaluados.	[>= 80%]	Oficial de Seguridad de la Información	Anual	87%
Respaldo							
Respaldo de la información	Copias de seguridad Backups	Verificación de un muestreo de cintas tape backups se mantengan conformes al programa de backups establecido.	N° de cintas tape backups conforme / N° de cintas taba backups programados a realizarse.	[>= 90%]	Oficial de Seguridad de la Información	Anual	100%
Gestión de la seguridad de red							
Controles de red	Seguridad perimetral (IPS, Firewall, Antispam, Proxy directo y reverso, Antivirus, Antispyware)	Verificación del número de incidentes de seguridad relacionados a accesos a la red no autorizados	N° de incidentes de seguridad relacionados a acceso no autorizado a la red interna de la ONP	[= 0]	Oficial de Seguridad de la Información	Anual	0
Gestion de entrega del servicio del proveedor							
Supervisión y revisión de los servicios del proveedor	Informes / Reportes de cumplimiento del Proveedor	Cumplimiento de la lista de entregables	Matriz de entregable aprobado por OTI.ONP	[>= 90%]	Oficial de Seguridad de la Información	Anual	100%
Gestión de incidentes de seguridad de la información							
Respuesta a los incidentes de seguridad de la información	Registro de incidentes de seguridad de la información	Verificación de los registros de incidentes de seguridad de la información cerrados y abiertos al momento de la medición	N° de incidentes de seguridad resueltos / N° de incidentes de seguridad registrados (Reporte Aranda)	[>= 80%]	Oficial de Seguridad de la Información	Anual	96%

Objetivo de Control	Control	Método de Medición	Formula de Medición	Meta	Responsable de la Medición	Frecuencia de Medición	may-15
Continuidad de las operaciones							
Evaluación de la continuidad de las operaciones	Pruebas de continuidad y contingencia	Verificación del cumplimiento del programa anual de continuidad y contingencia del servicio	N° de pruebas de contingencia realizadas y conforme / N° de pruebas de contingencia programadas en el año.	[= 100%]	Oficial de Seguridad de la Información	Anual	100%
Revisiones de seguridad de la información							
Revisión independiente de la seguridad de la información	Auditorías del SGSI	Verificación del cumplimiento del programa anual de auditorías del SGSI	A= N° de auditorías del SGSI realizadas y conforme / N° de auditorías del SGSI programadas en el año.	[= 100%]	Oficial de Seguridad de la Información	Anual	100%

Fuente: Elaboración Propia

5.10.2. AUDITORIA INTERNA

Proceso que permite verificar en forma objetiva el cumplimiento y efectividad de todos los procesos que conforman el sistema de gestión de seguridad de la información.

Los lineamientos para la realización de la auditoria interna son los siguientes;

- La auditoría interna podrá ser ejecutada por un auditor y/o equipo auditor externo de acuerdo con los requisitos que establezca la organización y debe contar con los siguientes perfiles:
    - Debe ser liderada por un Líder Auditor y el equipo auditor que deben de ser Auditores Internos certificados en el Sistema de Gestión que se auditará.
    - Demostrar habilidades y conocimientos suficientes, relacionados con la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos del sistema de gestión a examinar, permitiéndole generar hallazgos y conclusiones apropiados. (Lo cual se evidenciará a través de certificados de cursos especializados correspondientes al Sistema de Gestión que será Auditado).
    - Tener experiencia del auditor en auditorías internas de procesos (evidencia en horas).

- Toda la información generada en el proceso deberá almacenarse en el repositorio correspondiente
- Los hallazgos que figuran en los informes deben cumplir con lo siguiente:
    - Deben redactarse de tal forma que sean entendidos fácilmente por el auditado y que posteriormente el área responsable del tratamiento pueda analizar y plantear soluciones acertadas al problema.
    - Las notas deben de ser: objetivas, claras, concretas, concisas, precisas y útiles para el auditado.
    - Deben de contar con la evidencia objetiva específica según sea el caso (código y nombre de documento, ubicación, fecha, etc.)

- Los informes finales deberán enviarse al área como máximo 7 días después de finalizada la auditoria.
- La Gerencia o Área responsable auditada debe asegurarse de que se establece el tratamiento para los hallazgos, es decir: se designa un responsable, se realizan las correcciones y se establecen las acciones correctivas necesarias para eliminar las no conformidades y sus causas.

A continuación, se muestra el proceso de auditoría interna implementado:

Programar Auditorías Internas

El Oficial de Seguridad de la Información determina el número de auditorías internas que se realizarán a lo largo del año.

Elaborar Programa de Auditorías

El oficial de seguridad de la información elabora el programa de auditorías en función a la naturaleza e importancia de la actividad sometida a auditoría.

Existen tres tipos de enfoque de auditoría:

A. Por áreas: Evalúa el grado de conformidad de un área con respecto a todos los procedimientos en los que participe.
B. Por procesos: Evalúa el grado de efectividad de las actividades de un servicio brindado de acuerdo con los procedimientos especificados.
C. Por requisitos de la norma: Evalúa el grado de conformidad que muestre el área auditada con respecto a un requisito específico de la norma.

El comité del SGSI aprueba la realización del programa de auditorías.

Coordinar participación del equipo auditor y Elaborar Plan

EL auditor Líder coordina la participación del equipo auditor, asimismo, se encarga de elaborar el Plan de Auditorías, el cual considera lo siguiente:

1. Tipo de Auditoría y número de la misma.
2. Mes y año de realización
3. Enfoque de la auditoría
4. Objetivo de la auditoría
5. Fechas y horas aproximadas de realización.
6. Integrantes del equipo auditor (independientes y sin responsabilidad directa al área auditada)
7. Área o departamento a ser auditados.
8. Procesos afectados (según enfoque)
9. Requisito de la norma a ser evaluado (según enfoque)
10. Representantes del auditado
11. Observaciones (si fuera necesario)

FIGURA N° 5.11 PLAN DE AUDITORIA

Sistema de Gestión :
Tipo de Auditoria :
Mes/Año :
Jefe Auditor :
Enfoque :
Objetivos :

Día	Auditores	Hora	Proceso Área / Departamento	Procedimientos, Instrucciones a Auditar	Requisitos del Sistema	Responsable de Área/Proc. Auditado

Observaciones :

Fuente: Elaboración Propia

Coordinar fecha y hora

El auditor líder coordina con el auditado la fecha y hora exacta en que se realizarán las auditorías, para asegurar que el representante esté presente durante la ejecución de la auditoría. Si existiera algún cambio durante el proceso se actualiza el Plan de Auditorías y se comunica a los involucrados.

Enviar Plan de Auditoría

Una vez coordinados la fecha y hora para la realización de las auditorías, el auditor líder envía el Plan de Auditoría a los auditores, auditados y demás involucrados o interesados.

Realizar la auditoría

Según las fechas establecidas, el equipo auditor procede a la realización de la auditoría y a la recopilación de las evidencias objetivas que permitan identificar no-conformidades, las situaciones destacables, verificar el estado de las notas abiertas y revisar la eficacia de las acciones cerradas.

Al término de la auditoria el auditor interno comentará de manera general con el auditado los hallazgos y registra los hallazgos en el Informe de Auditorias, y lo envía al Jefe Auditor.

Centralizar la información del equipo

El auditor líder centraliza, revisa y verifica que los hallazgos de su equipo no se repitan, se entiendan y estén bien redactados. Además, simplifica las notas si es factible, valida que existan las evidencias y valida la categoría de nota asignada.

Desplegar hallazgos con auditados

El auditor líder envía el informe de auditoría vía correo electrónico al auditado para que éste revise y dé su conformidad. El informe se enviará al auditado a más tardar 5 días hábiles luego de realizada la auditoría.

5.10.3. REVISIÓN DE GESTIÓN

La Alta Dirección revisa el SGSI de manera periódica para asegurar su conveniencia, suficiencia y efectividad continua:

Para lo cual debe considerar los siguientes puntos:

a) Estado de las acciones con relación a las revisiones anteriores.
b) Cambios en los asuntos internos y externos que son relevantes para el SGSI.
c) Retroalimentación sobre el desempeño del SGSI, incluyendo:
    1) Estado de las no conformidades y acciones correctivas.
    2) Resultados del monitoreo y medición.
    3) Resultados de las auditorias.
    4) Cumplimiento de los objetivos del SGSI.
d) Retroalimentación de las partes interesadas.
e) Resultados de la evaluación de riesgo y estado del plan de tratamiento de riesgos.
f) Oportunidades para la mejora continua.

5.11. ACTUAR

5.11.1. NO CONFORMIDADES Y ACCIONES CORRECTIVAS

Se han definido los siguientes escenarios como “No Conformidad”:

- **Incumplimiento de algún requisito legal y/o contractual:** Situación donde se evidencia un incumplimiento de algún requisito legal o contractual aplicado al servicio o al Sistema de Gestión de Seguridad de la Información.
- **Incumplimiento de las Políticas y/o normas de seguridad:** Situación donde se evidencia un incumplimiento de las políticas, normas, procedimientos, planes, controles, y similares, definidos dentro del Sistema de Gestión de Seguridad de la Información.

- **Incumplimiento de los objetivos de seguridad:** Situación donde se evidencia que los resultados de medición de los objetivos de seguridad no fueron satisfactorios conforme a las metas establecidas.
- **Resultados de auditorías internas / externas:** No conformidades detectadas por el equipo auditor o auditores en la realización de auditorías internos o externas.
- **Resultados de investigación de incidentes:** Situación donde como resultado de la investigación de incidentes se determine no conformidades en los procesos o actividades definidas dentro del Sistema de Gestión de Seguridad de la Información.
- **Resultados de monitoreo y seguimiento:** Situación donde como resultado del monitoreo se evidencie eventos de seguridad de manera sistemática y con potencialidad de vulnerar las políticas de seguridad de la información.
- **Resultados de la revisión por la Dirección:** Situación donde se determina que existe algún incumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información.
- **Incumplimiento de acciones establecidas en las solicitudes de acciones correctivas:** Situación donde se evidencie incumplimiento en los plazos o acciones no tomadas, sin justificación, que se definieron en las solicitudes de acciones correctivas / preventivas.

Para el tratamiento de una no conformidad, se debe elaborar una solicitud de acción correctiva (SAC) la misma que se describe en el ANEXO VI SOLICITUD DE ACCIÓN CORRECTIVA así mismo se debe identificar la causa raíz para la elaboración de los planes de acción, para el presente trabajo se ha considerado la herramienta de los 5 porque (ANEXO VII ANALISIS DE CAUSA)

se ha elaborado la siguiente solicitud de acción correctiva, la cual debe ser correctamente llenada. Asimismo, se debe identificar la cusa raíz de la no conformidad para lo cual se emplea el método de los 5 por qué.

5.11.2. MEJORA CONTINUA

El objetivo de este proceso es mejorar continuamente la eficacia del sistema de gestión de seguridad de la información, considerando principalmente los siguientes términos:

- Los procesos para el aumento del desempeño de la organización, de esta forma beneficiar a las partes interesadas.
- Los procesos para el aumento de la seguridad de la información.

El proceso de mejora continua es el siguiente:

Identificar Oportunidades de Mejora

En esta etapa, se definen claramente la oportunidad de mejora y reconocen la importancia de este. Se pueden utilizar principalmente Tormentas de Ideas, Encuestas y Entrevistas, se seleccionan las oportunidades de mejora según las siguientes fuentes:

- Elevación de los Objetivos.
- Auditorías Internas / Externas.
- Encuestas a Clientes.
- Reclamos e Incidentes.
- Sugerencias del Personal.

Adicionalmente, los criterios que se toman en cuenta son:

- La complejidad de la oportunidad de mejora.
- El impacto que la oportunidad de mejora tiene en los clientes, cómo los afecta, a cuántos y a qué nivel.
- El tiempo que tomaría solucionarlo.

Se elabora una lista de oportunidades de mejora y se asigna a un responsable o un grupo de responsables y el líder quien propondrá la fecha límite de solución de la oportunidad de mejora y los recursos necesarios para la ejecución de este.

Proponer Plan de Acción:

Se discuten las acciones que deberán ser tomadas. También es importante analizar los posibles efectos colaterales de las acciones propuestas y las actividades adicionales que se tomarán para contrarrestar los mismos si fuese ésta la solución que se adoptase.

Las acciones propuestas pueden ser analizadas también a partir del costo/beneficio y el tiempo de implementación y la eficacia de la misma, es decir, si logra el resultado para la cual fue aplicada, eliminando la causa raíz de la oportunidad de mejora.

Teniendo en cuenta estos aspectos, se procede a elaborar el plan de acción a través del Cronograma de Actividades, que incluye actividades detalladas de lo que se debe hacer, las fechas propuestas o duración estimada de cada actividad, responsable de la ejecución de cada una, de ser posible la forma en que deberá realizarse esta actividad, el costo de cada actividad, la meta a ser alcanzada y los mecanismos de control y verificación para determinar si la acción fue efectiva.

Aprobar Plan de Acción Propuesto:

El comité del SGSI deberá aprobar el plan de trabajo para la implementación de la mejora.

Ejecutar Plan de Acción Aprobado

En esta fase se implanta el Plan de Acción Aprobado. Para ello debe asegurarse de que todos los que se vean afectados entiendan la razón por la cual está siendo

implantada. El equipo de mejora hace un seguimiento a la implantación del plan asegurándose de que las soluciones sean implantadas de acuerdo con el plan.

Cuando al hacer el seguimiento, se encuentra que no se están logrando los objetivos deseados, se hacen los ajustes al Plan.

Verificar Mejora Efectiva

El Equipo de Mejora compara los resultados utilizando los datos recogidos antes y después de la acción tomada para verificar la efectividad de la acción y la reducción de los resultados indeseables. Si el resultado de la acción fue tan satisfactorio como se esperaba se envía el Informe al Comité del SGSI con el detalle correspondiente.

5.12. AUDITORIA DE CERTIFICACIÓN

Se realizó la auditoria externa de certificación del 10 al 14 de agosto 2015, el cual estuvo a cargo de la empresa TUV Rheinland, la misma que en su informe final declaro lo siguiente:

"La eficacia del sistema de gestión se verificó in situ, por medio de un muestreo aleatorio, por el equipo auditor. En este proceso, se evaluaron las secuencias de trabajo para saber si cumplen con los requisitos de la/s norma/s y con las descripciones de la documentación del sistema de gestión. Se han tenido en cuenta las características propias en las actividades de la empresa, así como los requisitos legales y reglamentarios aplicables y otros documentos principales. Esto se hizo mediante un método de muestreo, mediante la realización de entrevistas y la revisión de la documentación pertinente. El equipo de auditoría recomienda, por tanto: La emisión de nuevos certificado"

Posteriormente a la emisión del informe de auditoría se emitieron los certificados digitales/físicos los cuales se muestran a continuación:

FIGURA N° 5.12 REUNION CIERRE AUDITORIA EXTERNA

Fuente: Elaboración propia

FIGURA N° 5.13 CERTIFICADO ISO 27001:2013

Certificado

Normativa de aplicación ISO / IEC 27001:2013

N° registro certificado 01 153 04012

Titular del certificado: ONP Oficina de Normalización Previsional

Oficina de Normalización Previsional
Jr. Bolivia 109. Centro cívico y comercial de Lima
01 Lima, Peru

Ámbito de aplicación: Gestión de las Operaciones y la Plataforma de TI del Centro de Datos, Gestión de la Mesa de Servicio y Gestión de la Seguridad y Accesos Informáticos en concordancia con el ISO/IEC 27001:2013

Mediante una auditoría se verificó el cumplimiento de los requisitos recogidos en la norma ISO / IEC 27001:2013 - Information security management systems.

Validez: Este certificado es válido desde 2015-05-28 hasta 2018-05-27.

2015-09-17

TÜV Rheinland Cert GmbH
Am Grauen Stein - D-51105 Köln

www.tuv.com DAkkS Deutsche Akkreditierungsstelle D-ZM-16031-01-00 TÜVRheinland® Precisely Right.

Fuente: Elaboración propia

5.13. CIERRE DEL PROYECTO

El día 14-05-15 se procede al cierre del proyecto de “Implementación de un sistema de gestión de seguridad de la información para proteger la información en los procesos de tecnología de la información de la ONP”, según consta en el acta siguiente:

CUADRO N° 5.38 ACTA DE CIERRE DEL PROYECTO

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN BAJO EL ESTANDAR ISO/IEC 27001:2013	**SGSI**
NOMBRE DEL CLIENTE	
OFICINA DE NORMALIZACIÓN PREVISIONAL (ONP)	
DECLARACIÓN DE LA ACEPTACIÓN FORMAL	
Por la presente se deja constancia que el "Proyecto Implementación del sistema de gestión de seguridad de la información" a cargo de la empresa GMD, ha sido aceptado y aprobado por la Oficina de Tecnologías de la Información de la ONP., damos constancia por la presente que el proyecto ha sido culminado exitosamente.	

DIAGNOSTICO
- Informe de Diagnostico (Análisis de brecha)

CONTEXTO DE LA ORGANIZACIÓN
- Identificación de las partes interesadas
- Requisitos de seguridad de la información
- Alcance del SGSI

LIDERAZGO
- Política de SI
- Roles y responsabilidades del SGSI

PLANEACIÓN
- Metodología de gestión de riesgos
- Declaración de aplicabilidad

SOPORTE
- Plan de capacitación
- Plan de concienciación
- Plan de comunicaciones del SGSI
- Documentos del SGSI

OPERACIÓN
- Medición del SGSI
- Gestión de cambios
- Matriz de evaluación de riesgos
- Plan de tratamiento de riesgos

EVALUACIÓN DEL DESEMPEÑO
- Programa de auditoria
- Plan de auditoria interna
- Informe de auditoría interna
- Revisión de gestión

MEJORA
- Solicitud de acción correctiva

AUDITORIA DE CERTIFICACIÓN
- Certificado del SGSI

ACEPTADO POR	
NOMBRE DEL SPONSOR U OTRO FUNCIONARIO	**FECHA**
Demetrio Tantalean del Águila	14/05/2015
FINALIDAD DEL PROYECTO	
NOMBRE DEL STAKEHOLDER	**FECHA**
Alfredo Torres Calderón Huertas	14/05/2015
José Samame Quiñones	14/05/2015
Jennifer Ayllon Bulnes	14/05/2015

Fuente: Elaboración propia

CAPITULO VI: ANÁLISIS E INTERPRETACIÓN DE DATOS

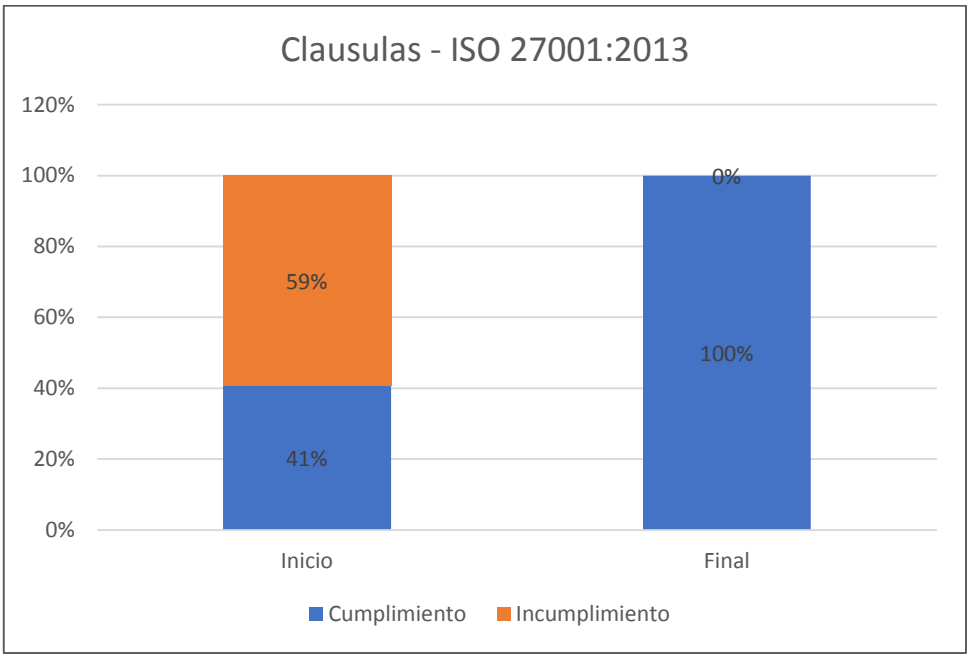
6.1. ANALISIS DE BRECHAS

CUADRO N° 6.1 DIAGNOSTICO FINAL - CLAUSULAS

Clausula	Inicio	Final
4. Contexto de la Organización	31%	100%
5. Liderazgo	50%	100%
6. Planificación	56%	100%
7. Apoyo	38%	100%
8. Operación	33%	100%
9. Evaluación del desempeño	52%	100%
10. Mejora	25%	100%
Cumplimiento	**41%**	**100%**

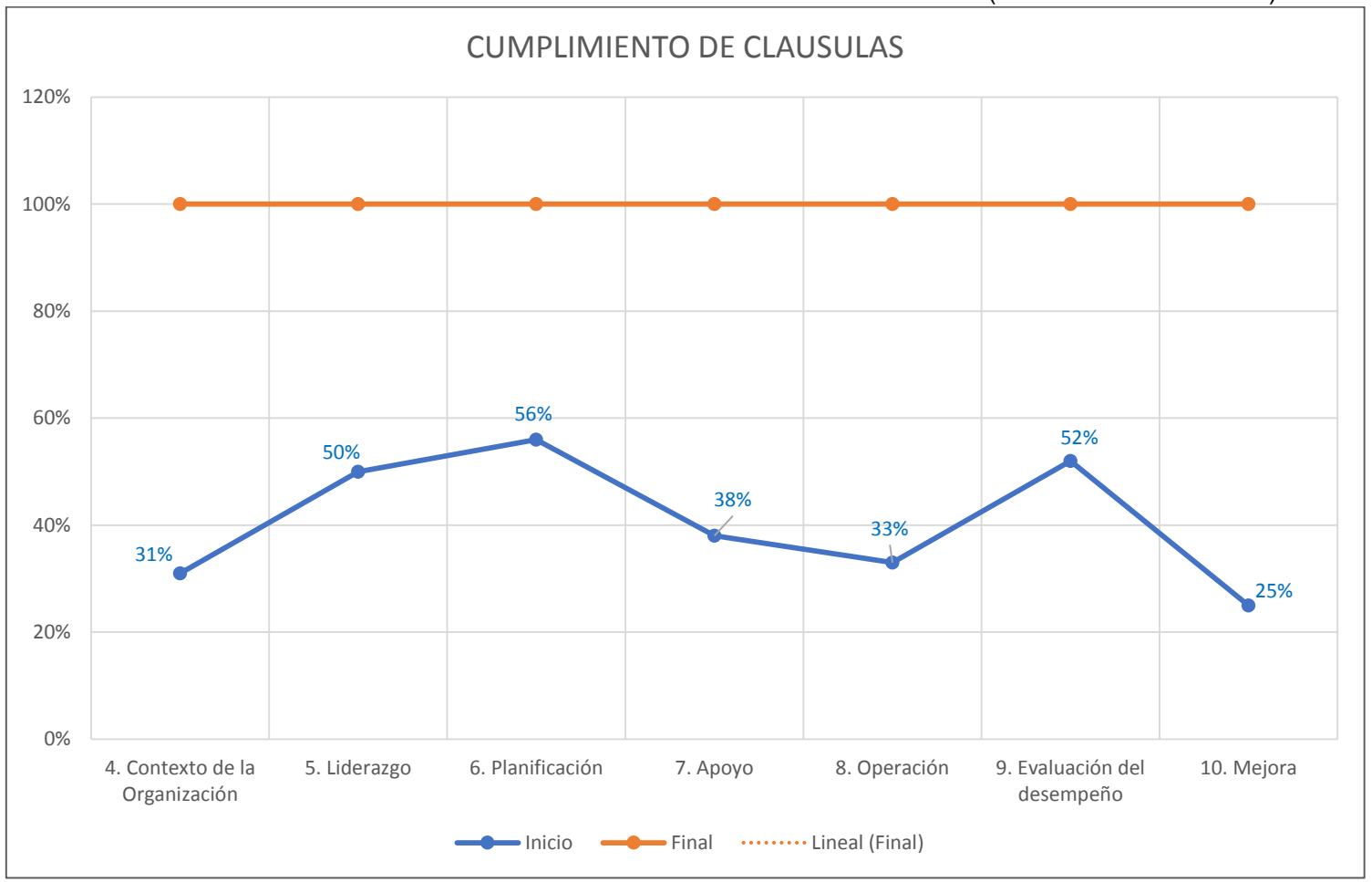
Fuente: Elaboración propia

FIGURA N° 6.1 COMPARATIVO CLAUSULAS (ANTES Y DESPUES)



Fuente: Elaboración propia

FIGURA N° 6.2 COMPARATIVO DEGRADADO DE CLAUSULAS (ANTES Y DESPUES)



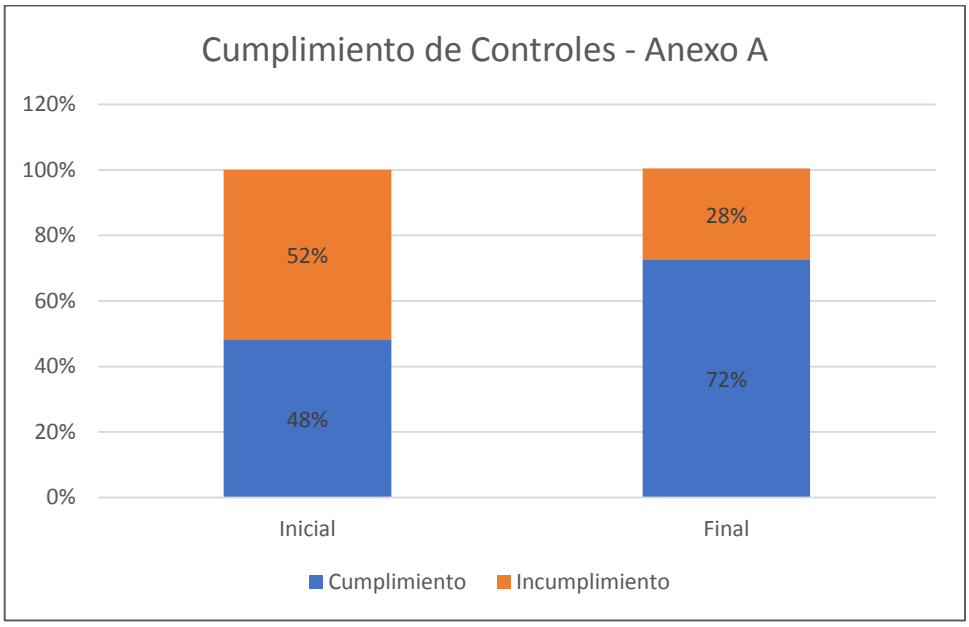
Fuente: Elaboración propia

CUADRO N° 6.2 DIAGNOSTICO FINAL - CONTROLES

Descripción de Controles	Inicial	Final
A.5 - Políticas de SI	0%	75%
A.6 - Organización de la SI	50%	75%
A.7 - Seguridad ligada a los RH	70%	83%
A.8 - Administración de activos	60%	79%
A.9 - Control de accesos	60%	79%
A.11 - Seguridad física y del ambiente	75%	85%
A.12 - Seguridad de las operaciones	60%	75%
A.13 - Seguridad de las comunicaciones	60%	80%
A.14 - Adquisición, desarrollo y mantenimiento del sistema	0%	0%
A.15 - Relaciones con el proveedor	50%	80%
A.16 - Gestión de incidentes de SI	40%	71%
A.17 - Aspectos de SI en la GCN	50%	80%
A.18 - Cumplimiento	50%	80%
Cumplimiento	**48%**	**72%**

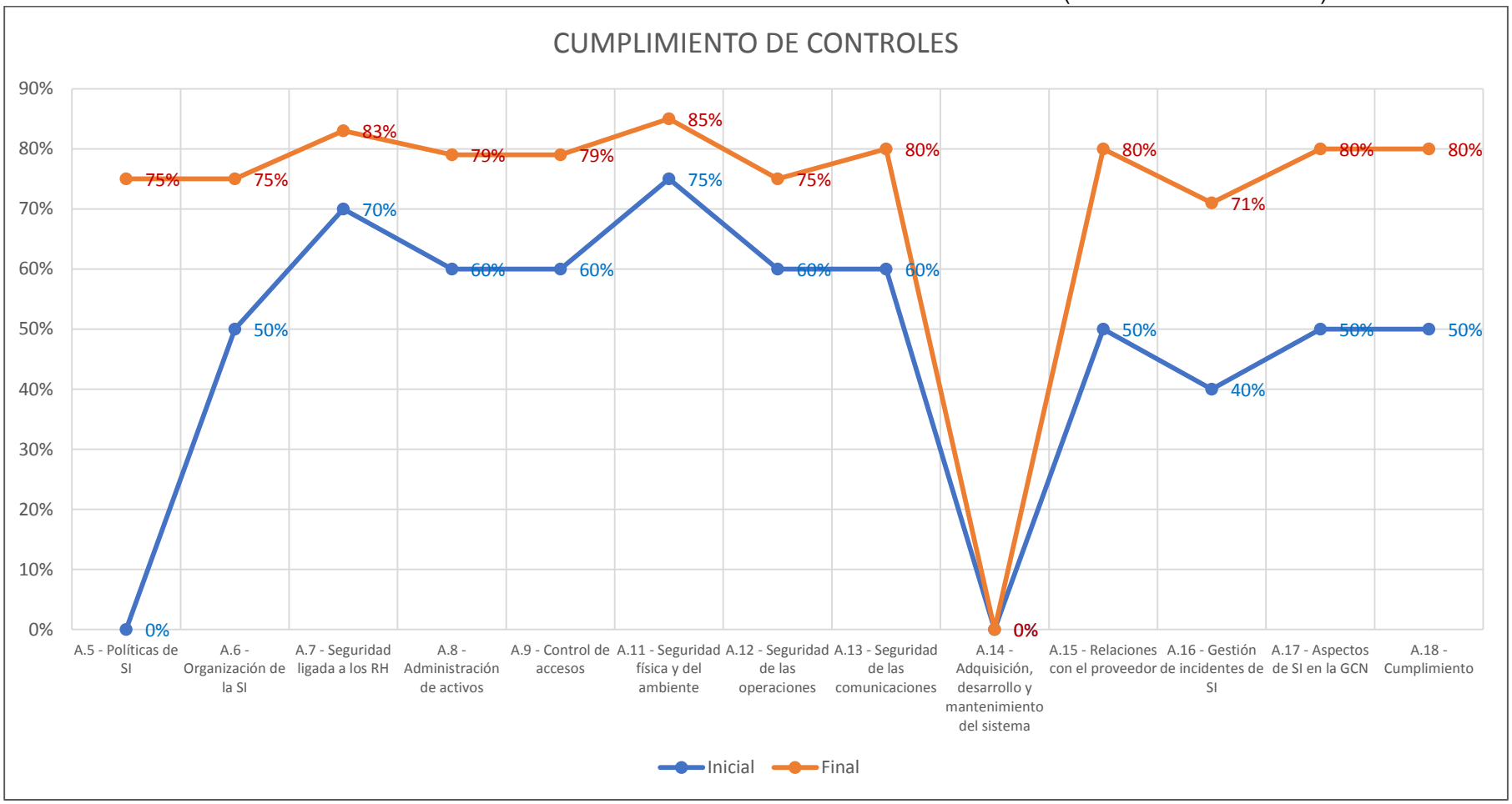
Fuente: Elaboración propia

FIGURA N° 6.3 COMPARATIVO CONTROLES (ANTES Y DESPUES)



Fuente: Elaboración propia

FIGURA N° 6.4 COMPARATIVO DEGRADADO DE CONTROLES (ANTES Y DESPUES)



Fuente: Elaboración propia

6.2. ANALISIS DE LOS INDICADORES

CUADRO N° 6.3: ANALISIS DE INDICADORES

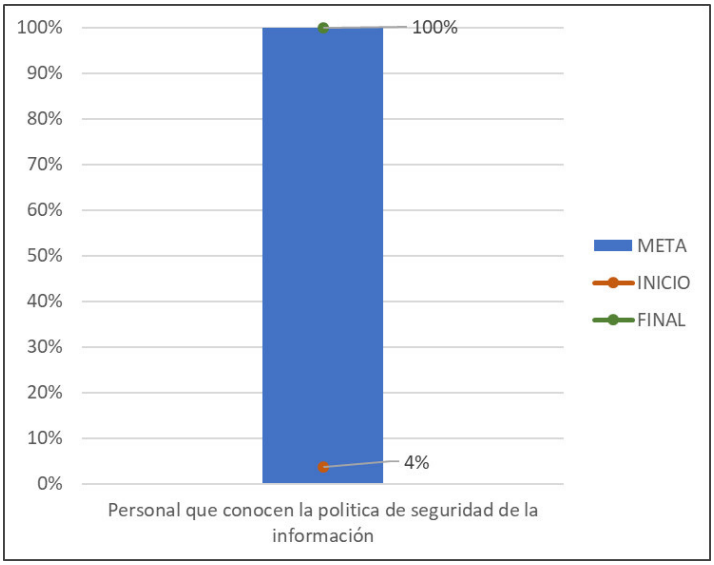
POLITICA / OBJETIVOS DEL SGSI	INDICADOR	FORMULA	META	ANTES		DESPUÉS	
Contar con una política de seguridad de la información que sea entendible y esté disponible a todo el personal	Personal que conocen la política de seguridad de la información	Cantidad de personas que conocen la política / cantidad total de personas	100%	2/56	4%	56/56	100%
Cumplir con las regulaciones aplicables en torno a la seguridad de la información.	Clientes satisfechos con el servicio	% Satisfacción del Cliente Interno	>=90%	Encuesta de satisfacción	78%	Encuesta de satisfacción	96%
	SLA establecidos que se han cumplidos	∑ SLAs cumplidos/ ∑ SLAs totales	100%	17/26	65%	26/26	100%
	No contar con penalidades por incumplimiento contractuales	Monto de penalidades (S/.)	S/. 0	Penalidades	S/ 542,850	Penalidades	S/ 0
Mantener una cultura organizacional que aliente a todos los trabajadores a asumir una responsabilidad por la seguridad de la información	Capacitar al personal en temas de seguridad de la información	Personas capacitadas / Total personas en el proyecto	>=90%	2/56	4%	56/56	100%
	Cantidad de Personas que aprobaron el examen de las charlas de seguridad de la información	Personas que aprobaron el examen / Personas que dieron el examen)	>=90%	2/56	4%	56/56	100%
Mejorar continuamente el SGSI	Cumplimiento de la norma ISO/IEC 27001:2013	Análisis GAP / Brechas Promedio (cláusulas y controles)	>=80%	Análisis GAP	46%	Análisis GAP	86%
Proteger la información y sus activos de información a través de un SGSI para garantizar su confidencialidad, integridad y disponibilidad	Riesgos atendidos	Riesgos registrados / Riesgos atendidos	>=85%	29/50	58%	76/76	100%
	Pruebas de continuidad ejecutadas	Pruebas ejecutadas / Total de Pruebas planificadas	100%	0/1	0%	1/1	100%
Dar respuesta inmediata a los incidentes que se presenten	Incidentes reportados correctamente	Número de incidentes reportados / Total de incidentes ocurridos	>=90%	148/325	46%	392/420	93%
	Incidentes atendidos correctamente	Número de incidentes reportados / Total de incidentes atendidos	>=90%	255/320	80%	405/420	96%

Fuente: Elaboración propia

6.3. GRAFICO DE MEORA DE INDICADORES

OBJETIVO 1: Contar con una política de seguridad de la información que sea entendible y esté disponible a todo el personal

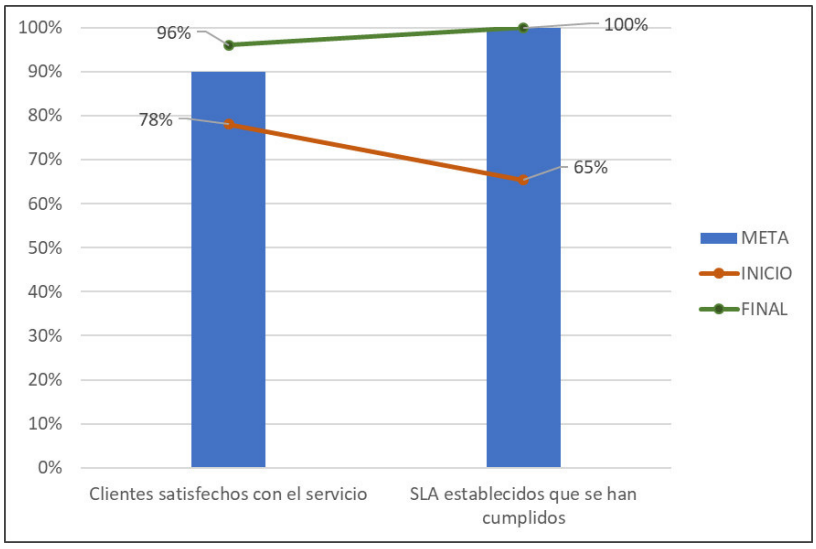
FIGURA N° 6.5 GRAFICO DEL OBJETIVO 1



Fuente: Elaboración propia

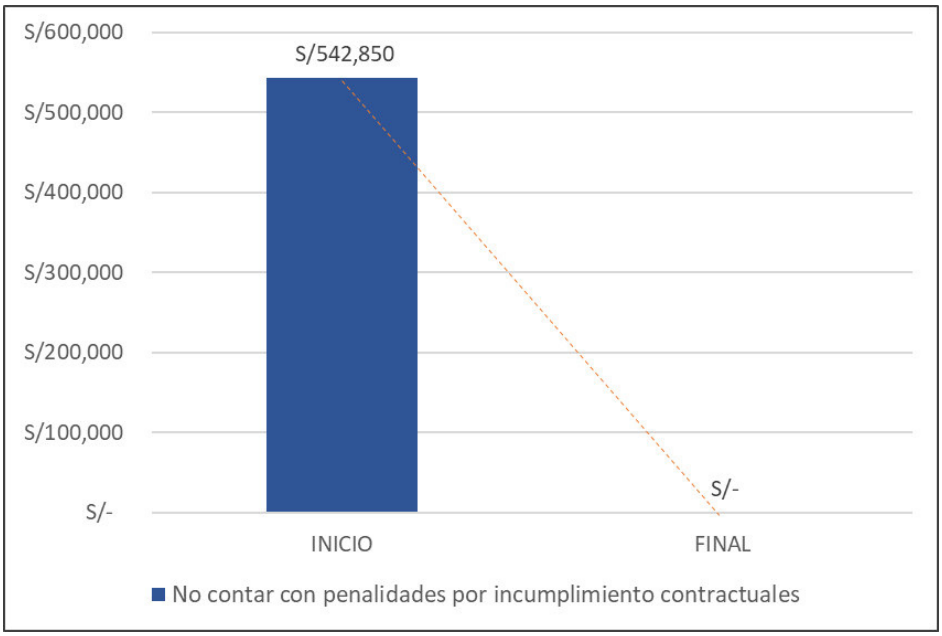
OBJETIVO 2: Cumplir con las regulaciones aplicables en torno a la seguridad de la información.

FIGURA N° 6.6 GRAFICO DEL OBJETIVO 2



Fuente: Elaboración propia

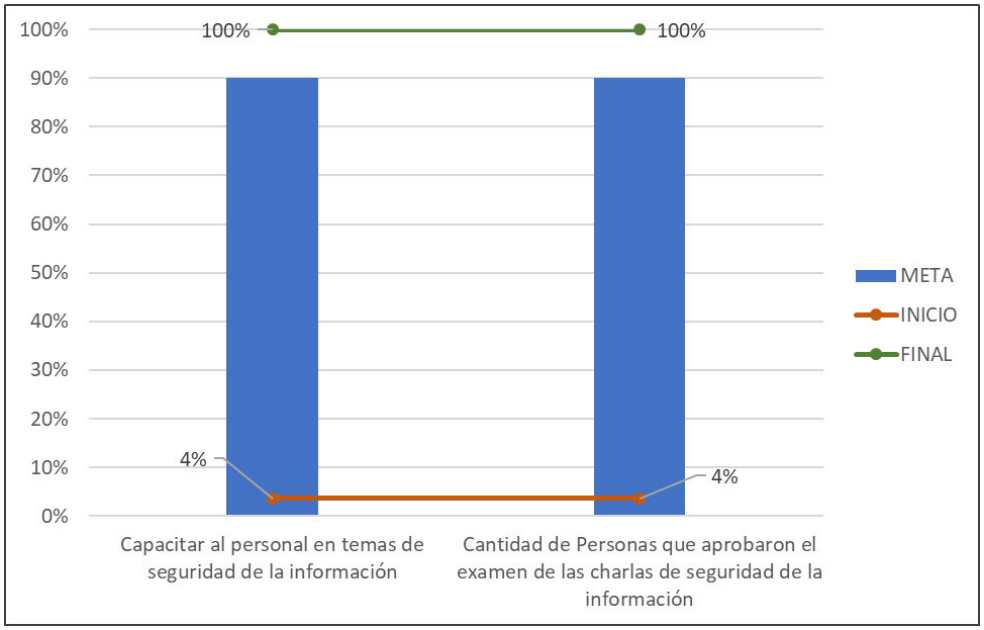
FIGURA N° 6.7 GRAFICO DEL OBJETIVO 2



Fuente: Elaboración propia

OBJETIVO 3: Mantener una cultura organizacional que aliente a todos los trabajadores a asumir una responsabilidad por la seguridad de la información

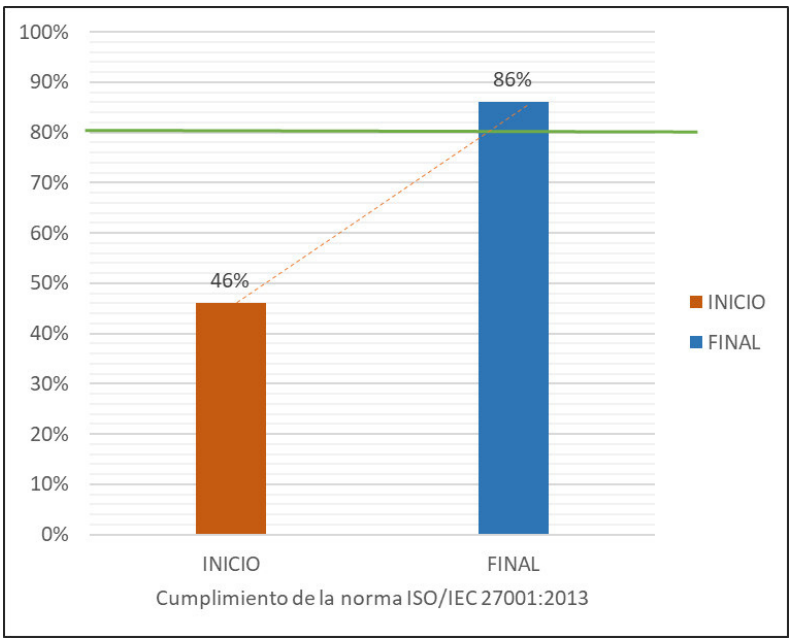
FIGURA N° 6.8 GRAFICO DEL OBJETIVO 3



Fuente: Elaboración propia

OBJETIVO 4: Mejorar continuamente el SGSI

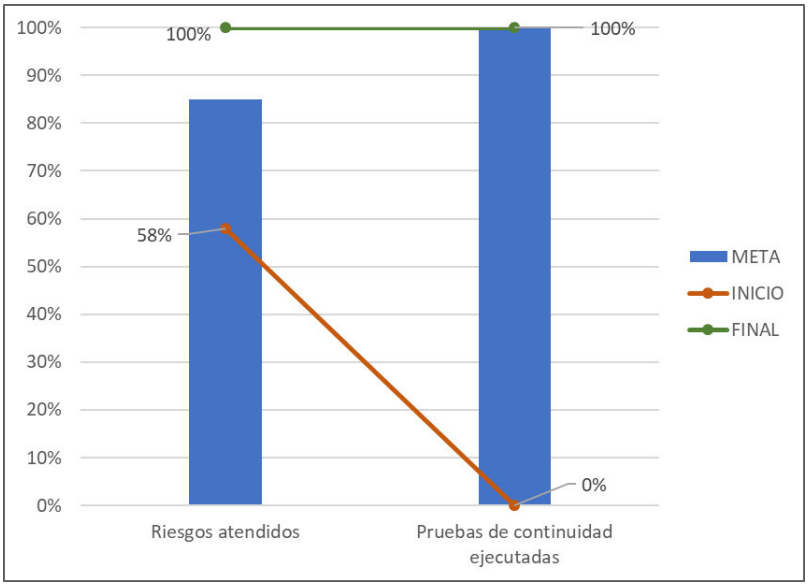
FIGURA N° 6.9 GRAFICO DEL OBJETIVO 4



Fuente: Elaboración propia

OBJETIVO 5: Proteger la información y sus activos de información a través de un SGSI para garantizar su confidencialidad, integridad y disponibilidad

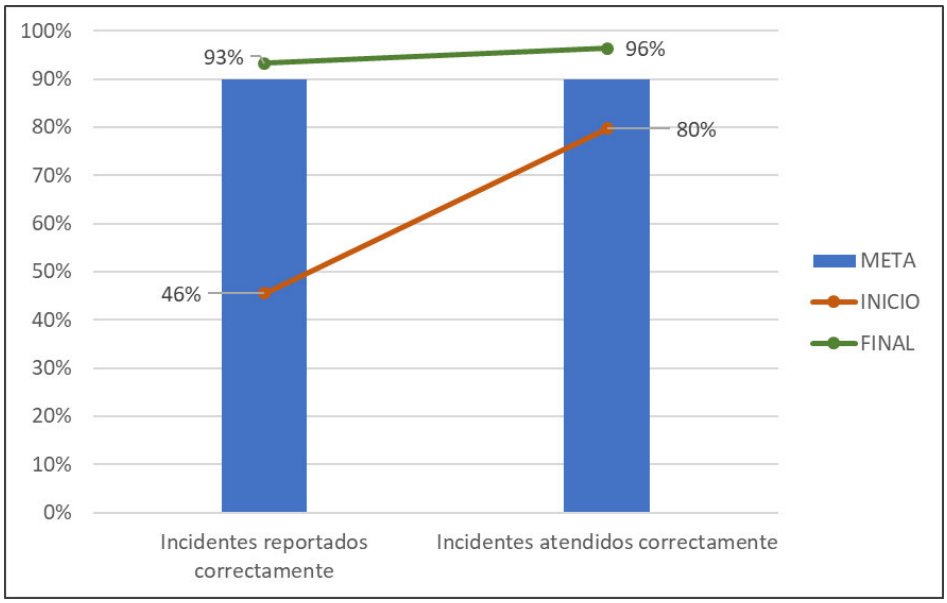
FIGURA N° 6.10 GRAFICO DEL OBJETIVO 5



Fuente: Elaboración propia

OBJETIVO 6: Dar respuesta inmediata a los incidentes que se presenten

FIGURA N° 6.11 GRAFICO DEL OBJETIVO 6



Fuente: Elaboración propia

CAPITULO VII: RESULTADOS

7.1. ANALISIS DE BRECHAS

Según los indicado en los capítulos anteriores, antes de la implementación del sistema de gestión de seguridad de la información (ISO 27001:2013), el análisis de brechas inicial dio como resultado un cumplimiento del 41% para las cláusulas y un 52% de cumplimiento de los controles del anexo A, dando como resultado un alto grado de incumplimiento.

Después de la identificación, análisis, evaluación y tratamiento del riesgo, se identificaron e implementaron los controles preventivos, correctivos y detectivos necesarios para minimizar la brecha, lo que trajo como resultado una mejora significativa en el cumplimiento de las cláusulas a un 81% y un cumplimiento del 91% de controles del anexo A.

Se evidencio el compromiso de la alta dirección a mejorar continuamente el Sistema de gestión de Seguridad de la Información (SGSI) y así poder mitigar los riesgos actuales y futuros e ir reduciendo la brecha en el cumplimiento de los requisitos de la norma ISO 27001.

7.2. ANALISIS DE LOS INDICADORES

OBJETIVO 1: Contar con una política de seguridad de la información que sea entendible y esté disponible a todo el personal

Al inicio del proyecto el conocimiento de la política de seguridad de la información era mínima 4%, posterior al proyecto se realizaron capacitaciones (charlas, correos, boletines) y el personal en su totalidad conoce la política de seguridad de la información.

OBJETIVO 2: Cumplir con las regulaciones aplicables en torno a la seguridad de la información

La satisfacción del cliente aumento en comparación al inicio del proyecto (de 78% a 96%) debido a la mejora en el cumplimiento y calidad del servicio brindado por GMD.

Al inicio de la implementación los SLA (acuerdos de niveles de servicios) no se cumplían en su totalidad, debido a incidentes de indisponibilidad de los servicios brindados, posterior a la implementación, se aplicaron controles de monitoreo para un mejor y total cumplimiento de los SLA (100%)

Al finalizar el proyecto no se obtuvieron penalidades o multas monetarias por incumplimiento en acuerdos contractuales como contratos, requisitos legales, requisitos técnicos, cumplimiento en los plazos de entrega, o por perdida en la información del negocio.

OBJETIVO 3: Mantener una cultura organizacional que aliente a todos los trabajadores a asumir una responsabilidad por la seguridad de la información

Al inicio del proyecto el personal no se encontraba capacitado o no tenía conocimiento de la importancia y definición de la seguridad de la información en la totalidad del personal solo en un 4%, por lo cual luego de la implementación se pudo capacitar a todo el personal del proyecto en un 100% las cuales aprobaron la evaluación en su totalidad.

Los temas que se tomaron en la concienciación fueron:

- Definición de la seguridad de la información
- Política y objetivos de la seguridad de la información
- Incidentes de seguridad de la información
- Consecuencias / Beneficios de la seguridad de la información

OBJETIVO 4: Mejorar continuamente la eficacia del SGSI

Al iniciar el proyecto el analisis GAP (Brechas) indico un cumplimiento de las cláusulas y controles en un 46%, luego de la implementación de controles preventivos, correctivos y/o detectivos se obtuvo una mejora significativa del 86% de cumplimiento de la norma ISO 27001:2013; según el encunciado de aplicabilidad aprobado por la organización.

OBJETIVO 5: Proteger la información y sus activos de información a través de un SGSI para garantizar su confidencialidad, integridad y disponibilidad.

Al inicio del proyecto no se tenia una metodología para el análisis, evaluación y tratamiento del riesgo por lo que solo se podían identificar y atender un 58% de los mismos, posterior a la implementación se puede identificar mejor los riesgos en función de sus activos de información; y por ende se pueden implementar planes de acción para su mitigación.

Asimismo, no se tenía planes de emergencia (contingencia u continuidad) en caso de pérdida de la información por factores como: daño en las instalaciones, corrupción en las bases de datos, indisponibilidad de los servicios del proyecto, etc.)

Luego de la implementación se implementaron los controles para asegurar que se proteja la información mediante la planificación de pruebas o ejercicios (100%) ante supuestos eventos que atenten contra la información, a fin de que se si materializase alguno de ellos, se pueda tomar acción de inmediato (acción preventiva / correctiva).

OBJETIVO 6: Dar respuesta inmediata a los incidentes que se presenten

Antes de iniciar el proyecto no se podían identificar incidentes de seguridad por lo que solo se registraban de manera correcta un 46% del total, posterior a la implementación del sistema de gestión se definieron mecanismos para diferenciar entre eventos e incidentes de seguridad por lo que mejoro significativamente su identificación en un 93%.

Asimismo, solo se resolvían al inicio un 80% de los mismos, al finalizar el proyecto, se cuenta con un equipo especializado para la resolución de incidentes de seguridad de la información, lo cual permitió su atención en un 96%.

CONCLUSIONES

- Se destaca que el apoyo brindado de la alta gerencia para la implementación del sistema de gestión fue imprescindible, debido a que fue necesaria su intervención para ayudar a concientizar a los jefes de área y dueños de los procesos a participar de las entrevistas de levantamiento de información y ayudó a que entendieran que el SGSI busca proteger la información crítica del negocio.
- Al contar con una política de seguridad de la información y que esta sea difundida y de conocimiento de todo el personal, permite a la organización tener una visión de cómo con sus actividades diarias y como estas pueden contribuir a la mejora del sistema de gestión.
- A pesar de contar con un sistema de gestión de seguridad de la información, el mercado actual está en continua actualización y mejoras en sus tecnologías, lo que conlleva a la existencia de nuevas amenazas y oportunidades para la organización; por lo cual se debe revisar de manera periódica la política de seguridad de la información, objetivos de seguridad y la metodología de la gestión de riesgos.
- Cuando la metodología de gestión de riesgos es aplicada de manera correcta, permite identificar los activos de información importantes para el negocio, así como los riesgos y el impacto sobre los mismos, asimismo permite elaborar planes de trabajo con los controles adecuados para su mitigación y reducir los niveles de riesgos a un nivel aceptable.
- Debido a que el personal es un factor importante y es quien opera en su mayoría los procesos del negocio, es necesario que esté capacitado en temas técnicos para la operación del proyecto y concientizado en la importancia de la seguridad de la información y en que sus actividades contribuyen a la protección de la información.
- La documentación que se genere en el proyecto es importante para la operativa del día a día por ello debe tenerse actualizada y resguardada para solos fines que fueron elaborados.
- La norma ISO 27001:2013 puede integrarse a las diversas normas debido a su estructura a las demás normas ISO 9001, ISO 14000, etc.

RECOMENDACIONES

- Se recomienda debe revisar periódicamente las políticas de seguridad de la información para verificar que estén alineadas a los objetivos del negocio.
- Se recomienda revisar la metodología de riesgos a fin de evaluar su eficacia y aplicar mejoras en su implementación.
- Se recomienda idear nuevas técnicas de enseñanza al personal mediante (videos, trípticos, boletines, etc.)
- Se deben realizar pruebas periódicas para identificar los controles que aplicarían antes posibles escenarios que atenten contra la información.
- Se recomienda contar con una bitácora para almacenar los eventos, riesgos e incidentes de seguridad de la información a fin de recolectar evidencias (lecciones aprendidas), en el cual se describan las acciones tomadas y mejoras en los mismos, con el objetivo de prevenir que dichos sucesos vuelvan a ocurrir.
- El sistema de gestión de seguridad de la información no solo aplica para organización que brinden servicios de TI (tecnología de información) sino para cualquier empresa (grande o pequeña) y de cualquier rubro (pesquero, industria, público, privado, etc.) que quiera implementar controles para proteger su información.
- Para implementar adecuadamente el SGSI, se recomienda utilizar estándares y buenas prácticas que sean ampliamente aceptadas. La implementación va a depender de las necesidades de la organización. Cabe resaltar que la norma ISO/IEC 27001:2013 te indican que es aquello que se debe controlar, pero no indica el cómo; por lo que esto depende de la organización.
- Todas las empresas que cuenten con un SGSI implementado, se les recomienda que el enfoque de su SGSI se encuentre alineado con las necesidades y objetivos del negocio. Asimismo, se debe tratar de obtener un retorno de inversión que justifique, de alguna manera, los gastos realizados en el año.
- Es necesario mejorar la comunicación con el área de logística para acelerar los procesos de compra de aquellos activos que ayudaran en el

tratamiento de riesgos detectados, especialmente, si estos riesgos son considerados altos o graves por la organización

- Se recomienda evaluar la factibilidad de adquirir de una herramienta que les permita gestionar los riesgos SGSI de una forma más rápida y eficiente por ejemplo Meykor KP, SE Risk, etc.
- Se recomienda establecer, como mínimo, reuniones mensuales del comité de seguridad de la información para dar un seguimiento adecuado del sistema de gestión y validar la ampliación del alcance del sistema de gestión.
- Es necesario que la organización asigne un presupuesto orientado a la implementación de los controles del SGSI, así como para las capacitaciones, charlas de concientización y las revisiones anuales que se darán para asegurar la continuidad del sistema.

REFERENCIAS BIBLIOGRAFICAS

- Norma internacional ISO/IEC 27001:2013 tecnología de la información – técnicas de seguridad – sistemas de gestión de la seguridad de la información – requisitos.
- Norma internacional ISO 31000:2009 gestión de riesgos – principios y guías
- International Standard ISO/IEC 27002:2013 Information technology – Security techniques – code of practice for information security controls
- International Standard ISO 27006:2011 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
- Guía del PMBOK 5ta edición
- Página web de GMD® www.gmd.com.pe
- Página web de ONP www.onp.gob.pe
- Bases integradas CP 0003-2017-ONP
- Bases integradas CP 0004-2017-ONP
- Web de buenas prácticas de seguridad de la información https://advisera.com/27001academy/blog/2013/06/18/one-information-security-policy-or-several-policies/
- Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552
- Barrantes, C., Herrera, J. (2012). Diseño e Implementación de un sistema de gestión de seguridad de información en procesos tecnológicos. http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/609/3/barrantes_ce.pdf (Visitado 2018-02-09)
- Ampuero, C. (2011). Diseño de un Sistema de Gestión de Seguridad de Información para una Compañía de Seguros. http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/933/AMPUERO_CHANG_CARLOS_INFORMACION_COMPAÑIA_SEGUROS.pdf?sequence=1 (Visitado 2018-02-09)
- Villena, M. (2006). Sistema de gestión de seguridad de información para una institución financiera. http://mendillo.info/seguridad/tesis/Villena.pdf (Visitado 2018-02-09)

- Aguirre, D. (2014). Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A. http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5677/AGUIRRE_DAVID_SISTEMA_GESTION_SEGURIDAD_INFORMACION_SERVICIOS_POSTALES.pdf?sequence=1&isAllowed=y (Visitado 2018-02-09)
- Aguirre, J. y Aristizabal, C. (2012). Diseño del sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda. http://repositorio.utp.edu.co/mwg-internal/de5fs23hu73ds/progress?id=Jn-cRZMTWV27lm4TWE9AMfbPnTB4jSZOlmb8sZPMof0 (Visitado 2018-02-09)

ANEXOS

ANEXO I: MATRIZ DE CONSISTENCIA

Título	Definición del Problema	Objetivos	Formulación de Hipótesis	Variables	Indicadores	Metodología	Población/ Muestra	Técnicas Instrumentos
Implementación de un sistema de gestión ISO 27001:2013 para proteger la información en los procesos de TI	**Problema Principal** ¿De qué manera la implementación del sistema de gestión ISO 27001:2013 permite proteger la información en los procesos de TI **Problemas Específicos** **PE1** ¿En qué medida la política de seguridad de la información influye en el sistema de gestión de seguridad de la información? **PE2** ¿Cómo influye el cumplimiento de las regulaciones legales y contractuales en la seguridad de la información? **PE3** ¿Cómo influye la mejora continua en la eficacia del SGSI? **PE4** ¿Cómo se influye el mantener una cultura organizacional a que el personal asuma su responsabilidad por la seguridad de la información? **PE5** ¿Cómo proteger la información y sus activos de información a través de un SGSI? **PE6** ¿Cómo se deben atender los incidentes de seguridad de la información?	**Objetivo General** Implementar el sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI. **Objetivos específicos** **OE1** Contar con una política de seguridad de la información que sea entendible y esté disponible a todo el personal **OE2** Cumplir con todas las regulaciones aplicables en torno a la seguridad de la información **OE3** Mejorar continuamente la eficacia del SGSI **OE4** Mantener una cultura organizacional que aliente a todos los trabajadores a asumir una responsabilidad por la seguridad de la información **OE5** Proteger la información y sus activos de información a través de un SGSI para garantizar su confidencialidad, integridad y disponibilidad. **OE6** Dar respuesta inmediata a los incidentes que se presenten.	**Hipótesis general** Con la implementación del sistema de gestión ISO 27001:2013, se garantiza la protección de la información en los procesos de tecnología de la información. **Hipótesis Específicas** **HE1** La política de seguridad de la información establece los lineamientos y el compromiso de la alta dirección en el cumplimiento del sistema de gestión de seguridad de la información **HE2** Al cumplir con los requisitos regulatorios y/o las obligaciones contractuales referentes a la seguridad de la información permite evitar multas de incumplimiento legal **HE3** La mejora continua contribuye a la mejora en la eficacia del SGSI mediante la revisión del cumplimiento de los estándares y la identificación de mejoras en los procesos de TI **HE4** La cultura organización alienta al personal a asumir una responsabilidad en relación con la seguridad de la información **HE5** La protección de la información y sus activos de información se garantizan mediante la protección de la confidencialidad, integridad y disponibilidad de la información **HE6** El atender los incidentes de seguridad permiten reducir el impacto negativo en la información	**Variable independiente (V1)** Implementación del sistema de gestión ISO 27001:2013 en los procesos de TI **Variable dependiente (V2)** Protección de la información en los procesos de tecnología de la información (TI).	Certificación del sistema de gestión (Certificado internacional) Cantidad de personas que conocen la política de seguridad de la información Clientes satisfechos con el servicio SLA establecidos que se han cumplidos Penalidades por incumplimiento contractuales Cumplimiento de la norma ISO 27001:2013 Cantidad de personas capacitadas en temas de seguridad de la información Cantidad de Personas que aprobaron el examen de las charlas de seguridad de la información Riesgos atendidos (confidencialidad, integridad y disponibilidad de la información) Pruebas de continuidad ejecutadas Incidentes reportados correctamente Incidentes atendidos correctamente	**Tipo de investigación** El presente trabajo de investigación está enmarcado dentro del tipo de investigación descriptiva aplicada, ya que describe, explica la influencia o relación entre las variables de investigación en la realidad concreta del universo. **Diseño de la investigación** El estudio responde a un Diseño experimental ya que se fundamenta en el Método Científico y utiliza como procesos lógicos la inducción y la deducción. Consiste en realizar actividades con la finalidad de comprobar, demostrar o reproducir ciertos fenómenos hechos o principios en forma natural o artificial, de tal forma que permita establecer experiencias para formular hipótesis que permitan a través del proceso científico conducir a generalizaciones científicas, que puedan verificarse en hechos concretos en la vida diaria.	**Población** La población está conformada por todo el personal que pertenece al proyecto (56 personas) **Muestra** La muestra la representará 56 personas	El estudio ha establecido la siguiente técnica de recolección de datos: Encuestas Revisión documental Auditorías

ANEXO II: FORMATO GAP DE CLÁUSULA

CLAUSULA	Requisito obligatorio para el SGSI	Estado (Evaluación)	Evidencia de cumplimiento
4	**CONTEXTO DE LA ORGANIZACIÓN**		
4.1	**Comprender la organización y su contexto**		
4.1	La organización debe determinar los asuntos externos e internos que son importantes para su objetivo y que afecte su capacidad para lograr e(los) resultado(s) esperado(s) de su sistema de gestión de la seguridad de la información.		
4.2	**Comprender las necesidades y expectativas de las partes interesadas**		
4.2	La organización debe determinar: a) las partes interesadas que son pertinentes para el sistema de gestión de la seguridad de la información; y		
4.2	b) los requisitos de estas partes interesadas que sean pertinentes para la seguridad de la información.		
4.3	**Determinar el alcance del sistema de gestión de seguridad de la información**		
4.3	La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.		
4.3	Al determinar este alcance, la organización debe considerar: a) los asuntos externos e internos tratados en 4.1		
4.3	b) los requerimientos tratados en 4.2; y		
4.3	c) interferencias y dependencias entre las actividades realizadas por la organización y aquellas realizadas por otras organizaciones.		
4.3	El alcance estará disponible como información documentada.		
4.4	**Sistema de gestión de la seguridad de la información**		
4.4	La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, según los requerimientos de esta norma.		
5	**LIDERAZGO**		
5.1	**Liderazgo y compromiso**		
5.1	La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información al: a) asegurar que los objetivos de la política de seguridad de la información y la seguridad de la información se establezcan y sean compatibles con la dirección estratégica de la organización;		
5.1	b) asegurar la integración de los requisitos del sistema de gestión de la seguridad de la información a los procesos de la organización;		
5.1	c) asegurar que los recursos necesarios para el sistema de gestión de la seguridad de la información están disponibles;		
5.1	d) comunicar la importancia de la gestión de seguridad de la información efectiva y del cumplimiento de los requisitos del sistema de gestión de la seguridad de la información;		
5.1	e) asegurar que el sistema de gestión de la seguridad de la información logre su(s) resultado(s) esperado(s);		
5.1	f) dirigir y apoyar a las personas para que contribuyan a la eficacia del sistema de gestión de la seguridad de la información;		
5.1	g) promover la mejora continua; y		
5.1	h) apoyar otros roles de gestión relevantes para demostrar su liderazgo, según corresponda a sus áreas de responsabilidad.		
5.2	**Política**		
5.2	La alta dirección debe establecer una política de seguridad de la información que: a) es pertinente al objetivo de la organización;		
5.2	b) incluya los objetivos de seguridad de la información (consulte 6.2) o que proporcione el marco de trabajo para establecer los objetivos de seguridad de la información;		
5.2	c) incluye un compromiso para satisfacer los requisitos aplicables, relacionados a la seguridad de la información; y		
5.2	d) incluya un compromiso para la mejora continua del sistema de gestión de la seguridad de la información.		
5.2	La política de seguridad de la información debe: e) estar disponible como información documentada;		
5.2	f) ser comunicada dentro de la organización; y		
5.2	g) estar disponible para las partes interesadas, según corresponda.		
5.3	**Roles organizacionales, responsabilidades y autoridades**		
5.3	La alta dirección debe asegurar que las responsabilidades y las autoridades para los roles pertinentes a la seguridad de la información son asignados y comunicados.		
5.3	La alta dirección debe asignar la responsabilidad y la autoridad para: a) asegurar que el sistema de gestión de la seguridad de la información cumple con los requisitos de esta norma; y		

CLAUSULA	Requisito obligatorio para el SGSI	Estado (Evaluación)	Evidencia de cumplimiento
5.3	b) informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información.		
6	**PLANIFICACIÓN**		
6.1.1	**General - Acciones para abordar los riesgos y las oportunidades**		
6.1.1	Al planificar el sistema de gestión de la seguridad de la información, la organización debe considerar los asuntos tratados en 4.1 y los requisitos tratados en 4.2 y determinar los riesgos y oportunidades que necesitan ser cubiertos para: a) asegurar que el sistema de gestión de la seguridad de la información pueda lograr su(s) resultado(s) esperado(s); b) evitar o disminuir efectos no deseados; y c) lograr una mejora continua.		
6.1.1	La organización debe planificar: d) acciones para abordar estos riesgos y oportunidades; y		
6.1.1	e) cómo e.1) integrar e implementar las acciones en los procesos del sistema de gestión de la seguridad de la información; y		
6.1.1	e) cómo e.2) evaluar la eficacia de estas acciones.		
6.1.2	**Evaluación de riesgo de la seguridad de la información**		
6.1.2	La organización debe definir y aplicar un proceso de evaluación de riesgo de la seguridad de la información que:		
6.1.2	a) establezca y mantenga los criterios de riesgo de la seguridad de la información que incluya: a.1) los criterios de aceptación del riesgo; y		
6.1.2	a.2) los criterios para realizar las evaluaciones de riesgo de la seguridad de la información;		
6.1.2	b) asegure que las evaluaciones de riesgo de la seguridad de la información producen resultados consistentes, válidos y comparables, una y otra vez;		
6.1.2	c) identifica los riesgos de la seguridad de la información: c.1) aplica el proceso de evaluación del riesgo de la seguridad de la información para identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad para la información dentro del alcance del sistema de gestión de la seguridad de la información; y		
6.1.2	c.2) identifica los propietarios del riesgo;		
6.1.2	d) analiza los riesgos de la seguridad de la información: d.1) evalúa las posibles consecuencias que podrían resultar si los riesgos identificados en 6.1.2 c) 1) se hicieran realidad;		
6.1.2	d.2) evalúa la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 c) 1); y		
6.1.2	d.3) determina los niveles de riesgo;		
6.1.2	e) evalúa los riesgos de la seguridad de la información: e.1) compara los resultados del análisis de riesgo con los criterios de riesgo definidos en 6.1.2 a); y		
6.1.2	e.2) prioriza los riesgos analizados para el tratamiento de riesgo.		
6.1.2	La organización debe conservar la información documentada acerca del proceso de evaluación de riesgo de la seguridad de la información.		
6.1.3	**Tratamiento de riesgo de la seguridad de la información**		
6.1.3	La organización debe definir y aplicar un proceso de tratamiento de riesgo de la seguridad de la información para: a) seleccionar las opciones apropiadas de tratamiento de riesgo de la seguridad de la información, tomando en consideración los resultados de la evaluación de riesgo;		
6.1.3	b) determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgo de la seguridad de la información escogida;		
6.1.3	c) comparar los controles definidos en 6.1.3 b) más arriba con aquellos en Anexo A y verificar que ningún control necesario fue omitido;		
6.1.3	d) generar una Declaración de Aplicabilidad que contenga los controles necesarios [consultar 6.1.3 b) y c)], y además la justificación de inclusiones, sean estas implementadas o no y la justificación para exclusiones de controles de Anexo A;		
6.1.3	e) formular un plan de tratamiento del riesgo de seguridad de la información; y		
6.1.3	f) obtener la aprobación del propietario del riesgo del plan de tratamiento del riesgo de la seguridad de la información y la aceptación de los riesgos de la seguridad de la información residual.		
6.1.3	La organización debe conservar la información documentada acerca del proceso de tratamiento del riesgo de la seguridad de la información.		
6.2	**Objetivos de seguridad de la información y planificación para lograrlos**		
6.2	La organización debe establecer los objetivos de seguridad de la información en niveles y funciones relevantes.		
6.2	Los objetivos de seguridad de la información deben: a) ser consistentes con la política de seguridad de la información;		
6.2	b) ser medible (si es posible);		

CLAUSULA	Requisito obligatorio para el SGSI	Estado (Evaluación)	Evidencia de cumplimiento
6.2	c) tomar en consideración los requisitos de seguridad de la información aplicable y los resultados de la evaluación de riesgo y el tratamiento de riesgo;		
6.2	d) ser comunicados; y		
6.2	e) estar actualizados según corresponda.		
6.2	La organización debe conservar la información documentada sobre los objetivos de la seguridad de la información.		
6.2	Al planificar cómo lograr sus objetivos de seguridad de la información, la organización debe determinar: f) qué se hará; g) qué recursos se necesitarán; h) quién será responsable; i) cuándo se terminará; y j) cómo se evaluarán los resultados.		
7	**APOYO**		
7.1	**Recursos**		
7.1	La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.		
7.2	**Competencias**		
7.2	La organización debe: a) determinar las competencias necesarias de las personas que trabajan bajo su control que afecta su desempeño de seguridad de la información;		
7.2	b) asegurar que estas personas sean competentes basados en una educación, capacitación o experiencia adecuada;		
7.2	c) cuando corresponda, tomar las acciones para adquirir las competencias necesarias y evaluar la efectividad de las acciones tomadas; y		
7.2	d) retener la información documentada adecuada como evidencia de competencia.		
7.3	**Conocimiento**		
7.3	Las personas que trabajen bajo el control de la organización deben estar al tanto de: a) la política de seguridad de la información;		
7.3	b) su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluidos los beneficios del desempeño mejorado de la seguridad de la información; y		
7.3	c) las implicaciones de no cumplir con los requisitos del sistema de gestión de la seguridad de la información.		
7.4	**Comunicación**		
7.4	La organización debe determinar la necesidad de comunicaciones internas y externas que sean pertinentes al sistema de gestión de seguridad de la información que incluya: a) qué comunicar; b) cuándo comunicarlo; c) con quién comunicarlo; d) quién debe comunicarlo; y e) los procesos que se verán afectados por la comunicación.		
7.5.1	**Información documentada**		
7.5.1	El sistema de gestión de la seguridad de la información debe incluir: a) información documentada necesaria para esta norma; y		
7.5.1	b) información documentada, definida por la organización como necesaria para la efectividad del sistema de gestión de la seguridad de la información.		
7.5.2	**Creación y actualización**		
7.5.2	Al crear y actualizar la información documentada, la organización debe asegurar la correspondiente: a) identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia);		
7.5.2	b) formato (por ejemplo, idioma, versión de software, gráficos) y medio (por ejemplo, papel, digital); y		
7.5.2	c) revisión y aprobación para conveniencia y suficiencia.		
7.5.3	**Control de la información documentada**		
7.5.3	La información documentada necesaria por el sistema de gestión de la seguridad de la información y por la norma debe ser controlada para asegurar que: a) está disponible y apropiada para su uso, donde y cuando sea necesario; y		
7.5.3	b) está debidamente protegida (por ejemplo, de pérdidas de confidencialidad, uso inapropiado o pérdida de integridad).		
7.5.3	Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda: c) distribución, acceso, recuperación y uso;		
7.5.3	d) almacenamiento y conservación, incluida la conservación de la legibilidad;		
7.5.3	e) control de cambios (por ejemplo, control de versión); y		

CLAUSULA	Requisito obligatorio para el SGSI	Estado (Evaluación)	Evidencia de cumplimiento
7.5.3	f) retención y disposición.		
7.5.3	Información documentada de origen externo, determinada por la organización, de ser necesario, para la planificación y operación del sistema de gestión de la seguridad de la información debe ser identificado como apropiado y controlado.		
8	**OPERACIÓN**		
8.1	**Control y planificación operacional**		
8.1	La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información y para implementar las acciones definidas en 6.1. La organización además debe implementar los planes para lograr los objetivos de seguridad de la información, definidos en 6.2.		
8.1	La organización debe mantener la información documentada hasta que sea necesario y tener la certeza que los procesos se llevaron a cabo según lo planeado.		
8.1	La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no planificados, al tomar acciones para mitigar cualquier efecto adverso, según sea necesario. La organización se debe asegurar de que los procesos externalizados se determinan y controlan.		
8.2	**Evaluación de riesgo de la seguridad de la información**		
8.2	La organización debe realizar evaluaciones de riesgo de la seguridad de la información, en intervalos planificados o cuando se propongan u ocurran cambios significativos, considerando los criterios establecidos en 6.1.2 a).		
8.2	La organización debe conservar la información documentada de los resultados de las evaluaciones de riesgo de la seguridad de la información.		
8.3	**Tratamiento de riesgo de la seguridad de la información**		
8.3	La organización debe implementar el plan de tratamiento del riesgo de la seguridad de la información.		
8.3	La organización debe conservar la información documentada de los resultados del tratamiento del riesgo de la seguridad de la información.		
9	**EVALUACIÓN DEL DESEMPEÑO**		
9.1	**Monitoreo, medición, análisis y evaluación**		
9.1	La organización debe evaluar el desempeño de la seguridad de la información y la efectividad del sistema de gestión de la seguridad de la información. La organización debe determinar: a) qué se necesita monitorear y medir, incluidos los controles y procesos de la seguridad de la información;		
9.1	b) los métodos para monitorear, medir, analizar y evaluar, según corresponda, para asegurar resultados válidos;		
9.1	c) cuándo se deben llevar a cabo el monitoreo y la medición;		
9.1	d) quién debe monitorear y medir;		
9.1	e) cuándo se deben analizar y evaluar los resultados del monitoreo y la medición; y		
9.1	f) quién debe analizar y evaluar estos resultados.		
9.1	La organización debe conservar la información documentada correspondiente, como evidencia de los resultados del monitoreo y medición.		
9.2	**Auditoría Interna**		
9.2	La organización debe llevar a cabo auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de la seguridad de la información: a) cumple con: a.1) los propios requisitos de la organización para su sistema de gestión de la seguridad de la información; y a.2) los requisitos de esta norma;		
9.2	b) está debidamente implementada y mantenida. La organización debe:		
9.2	c) planificar, establecer, implementar y mantener programa(s) de auditoría, incluida la frecuencia, métodos, responsabilidades, requisitos de planificación e informes. El (los) programa(s) de auditoría debe(n) considerar la importancia de los procesos en cuestión y los resultados de las auditorías anteriores;		
9.2	d) definir los criterios de auditoría y el alcance para cada auditoría;		
9.2	e) seleccionar auditores y realizar auditorías que aseguren la objetividad y la imparcialidad del proceso de auditoría;		
9.2	f) asegurar que los resultados de las auditorías son informados a la dirección pertinente; y		
9.2	g) conservar la información documentada como evidencia de los programas de auditoría y los resultados de la auditoría.		
9.3	**Revisión de gestión**		
9.3	La alta dirección debe revisar el sistema de gestión de la seguridad de la información en los plazos planificados para asegurar su conveniencia, suficiencia y efectividad continua. La revisión de la dirección debe considerar: a) el estado de las acciones, a partir de las revisiones de gestión anteriores;		

CLAUSULA	Requisito obligatorio para el SGSI	Estado (Evaluación)	Evidencia de cumplimiento
9.3	b) los cambios en los asuntos externos e internos que son pertinentes al sistema de gestión de la seguridad de la información;		
9.3	c) los comentarios sobre el desempeño de la seguridad de la información, incluidas tendencias en: 1) no conformidades y acciones correctivas;		
9.3	2) resultados del monitoreo y mediciones;		
9.3	3) resultados de auditoría; y		
9.3	4) cumplimiento de los objetivos de seguridad de la información;		
9.3	d) comentarios de las partes interesadas;		
9.3	e) resultados de la evaluación de riesgo y el estado del plan de tratamiento de riesgo; y		
9.3	f) las oportunidades para la mejora continua.		
9.3	Los resultados de la revisión de dirección deben incluir las decisiones relacionadas a las oportunidades de mejora y cualquier necesidad de cambios al sistema de gestión de la seguridad de la información.		
9.3	La organización debe conservar la información documentada como evidencia de los resultados de las revisiones de gestión.		
10	**MEJORA**		
10.1	**No Conformidades y acciones correctivas**		
10.1	Cuando ocurre una no conformidad, la organización debe: a) reaccionar frente a la no conformidad y si corresponde: a.1) tomar acciones para controlarlo y corregirlo; y		
10.1	a.2) encargarse de las consecuencias;		
10.1	b) evaluar la necesidad de acción para eliminar las causas de no conformidad, y que así esto no vuelva a ocurrir o que ocurra en otro lugar, al: 1) revisar la no conformidad;		
10.1	2) determinar las causas de las no conformidades; y		
10.1	3) determinar si existe una no conformidad similar o podría ocurrir;		
10.1	c) implementar cualquier acción necesaria;		
10.1	d) revisar la efectividad de cualquier acción correctiva implementada; y		
10.1	e) hacer cambios al sistema de gestión de la seguridad de la información, si es necesario.		
10.1	Las acciones correctivas deben ser pertinentes a los efectos de las no conformidades halladas.		
10.1	La organización debe conservar la información documentada como evidencia de: f) la naturaleza de las no conformidades y las subsecuentes acciones implementadas, y		
10.1	g) los resultados de cualquier acción correctiva.		
10.2	**Mejora continua**		
10.2	La organización debe mejorar de manera continua la conveniencia, suficiencia y efectividad del sistema de gestión de la seguridad de la información.		

ANEXO III: FORMATO GAP DE CONTROLES

Anexo A	Título del control	Descripción del control	Estado (Evaluación)	Evidencia de cumplimiento
A.5	**Políticas de seguridad de la información**			
A.5.1	**Orientación de la dirección para la seguridad de la información**	**Objetivo: Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.**		
A.5.1.1	Políticas para la seguridad de la información	La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información.		
A.5.1.2	Revisión de las políticas de seguridad de la información	Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continua.		
A.6	**Organización de la seguridad de la información**			
A.6.1	**Organización interna**	**Objetivo: Establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización.**		
A.6.1.1	Roles y responsabilidades de la seguridad de la información	Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas.		
A.6.1.2	Segregación de funciones	Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización.		
A.6.1.3	Contacto con autoridades	Se deben mantener los contactos apropiados con las autoridades pertinentes.		
A.6.1.4	Contacto con grupos especiales de interés	Se deben mantener los contactos apropiados con los grupos especiales de interés u otros foros especializados en seguridad, así como asociaciones de profesionales.		
A.6.1.5	Seguridad de la información en la gestión de proyecto	Se debe abordar la seguridad de la información en la gestión de proyecto, sin importar el tipo de proyecto.		
A.6.2	**Dispositivos móviles y trabajo remoto**	**Objetivo: garantizar la seguridad del trabajo remoto y el uso de dispositivos móviles.**		
A.6.2.1	Política de dispositivos móviles	Se debe adoptar una política y medidas de apoyo a la seguridad para gestionar los riesgos presentados al usar dispositivos móviles.		
A.6.2.2	Trabajo remoto	Se debe implementar una política y medidas de apoyo a la seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto.		
A.7	**Seguridad ligada a los recursos humanos**			
A.7.1	**Previo al empleo**	**Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y que sea aptos para los roles para los cuales están siendo considerados.**		
A.7.1.1	Selección	Se debe realizar la verificación de antecedentes en todos los candidatos al empleo, de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos.		
A.7.1.2	Términos y condiciones de la relación laboral	Los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y las de la organización en cuanto a seguridad de la información.		
A.7.2	**Durante el empleo**	**Objetivo: Asegurar que los empleados y contratistas estén en conocimiento y cumplan con sus responsabilidades de seguridad de la información.**		
A.7.2.1	Responsabilidades de la dirección	La dirección debe solicitar a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.		
A.7.2.2	Concientización, educación y formación en seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas deben recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales, pertinentes para su función laboral.		
A.7.2.3	Proceso disciplinario	Debe existir un proceso disciplinario formal y sabido por los empleados para tomar acciones en contra de los empleados que hayan cometido una infracción a la seguridad de la información.		
A.7.3	**Desvinculación y cambio de empleo**	**Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o desvinculación del empleo.**		
A.7.3.1	Responsabilidades en la desvinculación o cambio de empleo	Se deben definir y comunicar las responsabilidades y funciones de la seguridad de la información que siguen en vigor después de la desvinculación o cambio de relación laboral.		
A.8	**Administración de activos**			
A.8.1	**Responsabilidad por los activos**	**Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección pertinentes.**		
A.8.1.1	Inventario de activos	Los activos asociados a la información y a las instalaciones de procesamiento de la información deben ser identificados y se deben mantener y realizar un inventario de dichos activos.		

Anexo A	Título del control	Descripción del control	Estado (Evaluación)	Evidencia de cumplimiento
A.8.1.2	Propiedad de los activos	Los activos que se mantienen en inventario deben pertenecer a un dueño.		
A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con la información y las instalaciones de procesamiento de información.		
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder como consecuencia de la finalización de su relación laboral, contrato o acuerdo.		
A.8.2	**Clasificación de la información**	**Objetivo: Asegurar que la información recibe el nivel de protección adecuado, según su importancia para la organización.**		
A.8.2.1	Clasificación de la información	La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad para la divulgación o modificación sin autorización.		
A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo al esquema de clasificación de información adoptado por la organización.		
A.8.2.3	Manejo de activos	Se deben desarrollar e implementar los procedimientos para el manejo de activos, de acuerdo al esquema de clasificación de información adoptado por la organización.		
A.8.3	**Manejo de los medios**	**Objetivo: Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios**		
A.8.3.1	Gestión de los medios removibles	Se deben implementar los procedimientos para la gestión de los medios removibles, de acuerdo al esquema de clasificación adoptado por la organización.		
A.8.3.2	Eliminación de los medios	Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales		
A.8.3.3	Transferencia física de medios	Los medios que contengan información se deben proteger contra acceso no autorizado, uso inadecuado o corrupción durante el transporte.		
A.9	**Control de acceso**			
A.9.1	**Requisitos de negocio para el control de acceso**	**Objetivo: Restringir el acceso a la información y a las instalaciones de procesamiento de información.**		
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basadas en los requisitos del negocio y de seguridad de la información.		
A.9.1.2	Accesos a las redes y a los servicios de la red	Los usuarios solo deben tener acceso directo a la red y a los servicios de la red para los que han sido autorizados específicamente.		
A.9.2	**Gestión de acceso del usuario**	**Objetivo: Asegurar el acceso de usuarios autorizados y evitar el acceso sin autorización a los sistemas y servicios.**		
A.9.2.1	Registro y cancelación de registro de usuario	Se debe implementar un proceso de registro y cancelación de registro de usuario para habilitar la asignación de derechos de acceso.		
A.9.2.2	Asignación de acceso de usuario	Debe existir un procedimiento formal de asignación de acceso de usuario para asignar o revocar los derechos de acceso para todos los tipos de usuarios, a todos los sistemas y servicios.		
A.9.2.3	Gestión de derechos de acceso privilegiados	Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.		
A.9.2.4	Gestión de información secreta de autenticación de usuarios	Se debe controlar la asignación de información de autenticación secreta mediante un proceso de gestión formal.		
A.9.2.5	Revisión de los derechos de acceso de usuario	Los propietarios de activos deben revisar los derechos de acceso de los usuarios de manera periódica.		
A.9.2.6	Eliminación o ajuste de los derechos de acceso	Se deben retirar los derechos de acceso de todos los empleados y usuarios externos a la información y a las instalaciones de procesamiento de información, una vez que termine su relación laboral, contrato o acuerdo o se ajuste según el cambio.		
A.9.3	**Responsabilidades del usuario**	**Objetivo: Responsabilizar a los usuarios del cuidado de su información de autenticación.**		
A.9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios el cumplimiento de las prácticas de la organización en el uso de la información de autenticación secreta.		
A.9.4	**Control de acceso al sistema y aplicaciones**	**Objetivo: Evitar el acceso sin autorización a los sistemas y aplicaciones.**		
A.9.4.1	Restricción de acceso a la información	Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso.		
A.9.4.2	Procedimientos de inicio de sesión seguro	Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro.		

Anexo A	Título del control	Descripción del control	Estado (Evaluación)	Evidencia de cumplimiento
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.		
A.9.4.4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden estar en capacidad de anular el sistema y los controles de aplicación.		
A.9.4.5	Control de acceso al código fuente de los programas	Se debe restringir el acceso al código fuente de los programas.		
A.10	**Criptografía**			
A.10.1	**Controles criptográficos**	**Objetivo: Asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información.**		
A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.		
A.10.1.2	Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas durante toda su vida útil.		
A.11	**Seguridad física y del ambiente**			
A.11.1	**Áreas seguras**	**Objetivo: Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y la información de la organización.**		
A.11.1.1	Perímetro de seguridad física	Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen ya sea información sensible o crítica y las instalaciones de procesamiento de información.		
A.11.1.2	Controles de acceso físico	Las áreas seguras deben estar protegidas por controles de entrada apropiados que aseguren que solo se permite el acceso a personal autorizado.		
A.11.1.3	Seguridad de oficinas, salas e instalaciones	Se debe diseñar y aplicar la seguridad física en oficinas, salas e instalaciones.		
A.11.1.4	Protección contra amenazas externas y del ambiente	Se debe diseñar y aplicar la protección física contra daños por desastre natural, ataque malicioso o accidentes.		
A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajar en áreas seguras.		
A.11.1.6	Áreas de entrega y carga	Se deben controlar los puntos de acceso tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas puedan acceder a las instalaciones, y si es posible, aislarlas de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.		
A.11.2	**Equipamiento**	**Objetivo: Prevenir pérdidas, daños, hurtos o el compromiso de los activos, así como la interrupción de las actividades de la organización.**		
A.11.2.1	Ubicación y protección del equipamiento	El equipamiento se debe ubicar y proteger para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.		
A.11.2.2	Elementos de soporte	Se debe proteger el equipamiento contra fallas en el suministro de energía y otras interrupciones causadas por fallas en elementos de soporte.		
A.11.2.3	Seguridad en el cableado	Se debe proteger el cableado de energía y de telecomunicaciones que transporta datos o brinda soporte a servicios de información contra interceptación, interferencia o daños.		
A.11.2.4	Mantenimiento del equipamiento	El equipamiento debe recibir el mantenimiento correcto para asegurar su permanente disponibilidad e integridad.		
A.11.2.5	Retiro de activos	El equipamiento, la información o el software no se deben retirar del local de la organización sin previa autorización.		
A.11.2.6	Seguridad del equipamiento y los activos fuera de las instalaciones	Se deben asegurar todos los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.		
A.11.2.7	Seguridad en la reutilización o descarte de equipos	Todos los elementos del equipamiento que contenga medios de almacenamiento deben ser revisados para asegurar que todos los datos sensibles y software licenciado se hayan removido o se haya sobrescrito con seguridad antes de su descarte o reutilización.		
A.11.2.8	Equipo de usuario desatendido	Los usuarios se deben asegurar de que a los equipos desatendidos se les da protección apropiada.		
A.11.2.9	Política de escritorio y pantalla limpios	Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información.		
A.12	**Seguridad de las operaciones**			
A.12.1	**Procedimientos operacionales y responsabilidades**	**Objetivo: Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.**		
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.		

Anexo A	Título del control	Descripción del control	Estado (Evaluación)	Evidencia de cumplimiento
A.12.1.2	Gestión de cambios	Se deben controlar los cambios a la organización, procesos de negocio, instalaciones de procesamiento de información y los sistemas que afecten la seguridad de la información.		
A.12.1.3	Gestión de la capacidad	Se debe supervisar y adaptar el uso de los recursos, y se deben hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.		
A.12.1.4	Separación de los ambientes de desarrollo, prueba y operacionales	Los ambientes para desarrollo, prueba y operación se deben separar para reducir los riesgos de acceso no autorizado o cambios al ambiente de operación.		
A.12.2	**Protección contra código malicioso**	**Objetivo: Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el código malicioso.**		
A.12.2.1	Controles contra código malicioso	Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios.		
A.12.3	**Respaldo**	**Objetivo: Proteger en contra de la pérdida de datos.**		
A.12.3.1	Respaldo de la información	Se deben hacer copias de respaldo y pruebas de la información, del software y de las imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordada.		
A.12.4	**Registro y monitoreo**	**Objetivo: Registrar eventos y generar evidencia.**		
A.12.4.1	Registro de evento	Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, faltas y eventos de seguridad de la información.		
A.12.4.2	Protección de la información de registros	Las instalaciones de registro y la información de registro se deben proteger contra alteraciones y accesos no autorizados.		
A.12.4.3	Registros del administrador y el operador	Se deben registrar las actividades del operador y del administrador del sistema, los registros se deben proteger y revisar con regularidad.		
A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinente dentro de una organización o dominio de seguridad deben estar sincronizados a una sola fuente horaria de referencia.		
A.12.5	**Control del software de operación**	**Objetivo: Asegurar la integridad de los sistemas operacionales.**		
A.12.5.1	Instalación del software en sistemas operacionales	Se deben implementar los procedimientos para controlar la instalación del software en los sistemas operacionales.		
A.12.6	**Gestión de la vulnerabilidad técnica**	**Objetivo: Evitar la explotación de las vulnerabilidades técnicas.**		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener la información acerca de las vulnerabilidades técnicas de los sistemas de información usados se debe obtener de manera oportuna, evaluar la exposición de la organización a estas vulnerabilidades y se deben tomar las medidas apropiadas para abordar el riesgo asociado.		
A.12.6.2	Restricciones sobre la instalación de software	Se deben establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.		
A.12.7	**Consideraciones de la auditoría de los sistemas de información**	**Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.**		
A.12.7.1	Controles de auditoría de sistemas de información	Los requisitos y las actividades de auditoría que involucran verificaciones de los sistemas operacionales se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones en los procesos del negocio.		
A.13	**Seguridad de las comunicaciones**			
A.13.1	**Gestión de la seguridad de red**	**Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.**		
A.13.1.1	Controles de red	Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones.		
A.13.1.2	Seguridad de los servicios de red	Los mecanismos de seguridad, los niveles del servicio y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios son prestados dentro de la organización o por terceros.		
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes.		
A.13.2	**Transferencia de información**	**Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.**		
A.13.2.1	Políticas y procedimientos de transferencia de información	Las políticas, procedimientos y controles de transferencia formal deben estar en efecto para proteger la transferencia de la información mediante el uso de todos los tipos de instalaciones de comunicación.		

Anexo A	Título del control	Descripción del control	Estado (Evaluación)	Evidencia de cumplimiento
A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben abarcar la transferencia segura de la información del negocio entre la organización y terceros.		
A.13.2.3	Mensajería electrónica	La información involucrada en la mensajería electrónica debe ser debidamente protegida.		
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Se deben identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejan las necesidades de protección de la información de la organización.		
A.14	**Adquisición, desarrollo y mantenimiento del sistema**			
A.14.1	**Requisitos de seguridad de los sistemas de información**	**Objetivo: Asegurar que la seguridad de la información es parte integral de los sistemas de información en todo el ciclo. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios en las redes públicas.**		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados a la seguridad de la información deben ser incluidos en los requisitos para los sistemas de información nuevos o las mejoras para los sistemas de información existentes.		
A.14.1.2	Aseguramiento de servicios de aplicación en redes públicas	La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, y su divulgación y modificación no autorizada.		
A.14.1.3	Protección de las transacciones de servicios de aplicación	La información implicada en transacciones de servicio de aplicación se debe proteger para evitar la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.		
A.14.2	**Seguridad en procesos de desarrollo y soporte**	**Objetivo: Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información.**		
A.14.2.1	Política de desarrollo seguro	Las reglas para el desarrollo de software y de sistemas deben ser establecidas y aplicadas a los desarrollos dentro de la organización.		
A.14.2.2	Procedimientos de control de cambios del sistema	Los cambios a los sistemas dentro del ciclo de desarrollo deben ser controlados mediante el uso de procedimientos formales de control de cambios.		
A.14.2.3	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación	Cuando se cambien las plataformas de operación, se deben revisar y poner a prueba las aplicaciones críticas del negocio para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización.		
A.14.2.4	Restricciones en los cambios a los paquetes de software	Se debe desalentar la realización de modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, los que deben ser controlados de manera estricta.		
A.14.2.5	Principios de ingeniería de sistema seguro	Se deben establecer, documentar, mantener y aplicar los principios para los sistemas seguros de ingeniería para todos los esfuerzos de implementación del sistema de información.		
A.14.2.6	Entorno de desarrollo seguro	Las organizaciones deben establecer y proteger los entornos de desarrollo seguro, de manera apropiada, para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de desarrollo del sistema.		
A.14.2.7	Desarrollo tercerizado	La organización debe supervisar y monitorear la actividad del desarrollo del sistema tercerizado.		
A.14.2.8	Prueba de seguridad del sistema	Durante el desarrollo se debe realizar la prueba de funcionalidad de seguridad		
A.14.2.9	Prueba de aprobación del sistema	Se deben definir los programas de prueba de aceptación y los criterios pertinentes para los nuevos sistemas de información, actualizaciones y versiones nuevas.		
A.14.3	**Datos de prueba**	**Objetivo: Asegurar la protección de los datos usados para prueba.**		
A.14.3.1	Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar de manera muy rigurosa.		
A.15	**Relaciones con el proveedor**			
A.15.1	**Seguridad de la información en las relaciones con el proveedor**	**Objetivo: Asegurar la protección de los activos de la organización a los que tienen acceso los proveedores.**		
A.15.1.1	Política de seguridad de la información para las relaciones con el proveedor	Se deben acordar y documentar, junto con el proveedor, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del proveedor a los activos de la organización.		
A.15.1.2	Abordar la seguridad dentro de los acuerdos del proveedor	Todos los requisitos de seguridad de la información pertinente deben ser definidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.		
A.15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones	Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociados a los		

Anexo A	Título del control	Descripción del control	Estado (Evaluación)	Evidencia de cumplimiento
		servicios de la tecnología de la información y las comunicaciones y la cadena de suministro del producto.		
A.15.2	**Gestión de entrega del servicio del proveedor**	**Objetivo: Mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos del proveedor**		
A.15.2.1	Supervisión y revisión de los servicios del proveedor	Las organizaciones deben supervisar, revisar y auditar la entrega del servicio del proveedor.		
A.15.2.2	Gestión de cambios a los servicios del proveedor	Se deben gestionar los cambios al suministro de los servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, al considerar la criticidad de la información del negocio, los sistemas y procesos involucrados y la reevaluación de los riesgos.		
A.16	**Gestión de incidentes de seguridad de la información**			
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras**	**Objetivo: Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.**		
A.16.1.1	Responsabilidades y procedimientos	Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información.		
A.16.1.2	Informe de eventos de seguridad de la información	Se deben informar, lo antes posible, los eventos de seguridad de la información mediante canales de gestión apropiados.		
A.16.1.3	Informe de las debilidades de seguridad de la información	Se debe requerir que los empleados y contratistas que usen los sistemas y servicios de información de la organización observen e informen cualquier debilidad en la seguridad de la información en los sistemas o servicios, observada o que se sospeche.		
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Los eventos de seguridad de la información se deben evaluar y decidir su van a ser clasificados como incidentes de seguridad de la información.		
A.16.1.5	Respuesta ante incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados.		
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Se debe utilizar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros.		
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia.		
A.17	**Aspectos de seguridad de la información en la gestión de la continuidad del negocio**			
A.17.1	**Continuidad de la seguridad de la información**	**Objetivo: Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad del negocio de la organización**		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.		
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.		
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar, de manera periódica, los controles de continuidad de la seguridad de la información definida e implementada para asegurar que son válidos y eficaces durante situaciones adversas.		
A.17.2	**Redundancias**	**Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de la información**		
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	Las instalaciones de procesamiento de la información deben ser implementadas con la redundancia suficiente para cumplir con los requisitos de disponibilidad.		
A.18	**Cumplimiento**			
A.18.1	**Cumplimiento con los requisitos legales y contractuales**	**Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información y todos los requisitos de seguridad.**		
A.18.1.1	Identificación de la legislación vigente y los requisitos contractuales	Todos los requisitos estatutarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.		
A.18.1.2	Derechos de propiedad intelectual	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y al uso de productos de software patentados.		
A.18.1.3	Protección de los registros	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.		

Anexo A	Título del control	Descripción del control	Estado (Evaluación)	Evidencia de cumplimiento
A.18.1.4	Privacidad y protección de la información de identificación personal	Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda.		
A.18.1.5	Regulación de los controles criptográficos	Se deben utilizar controles criptográficos que cumplan con todos los acuerdos, leyes, y regulaciones pertinentes.		
A.18.2	**Revisiones de seguridad de la información**	**Objetivo: Asegurar que la seguridad de la información se implemente y funcione de acuerdo a las políticas y procedimientos de la organización.**		
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se debe revisar en forma independiente, a intervalos planificados, o cuando ocurran cambios significativos.		
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Los gerentes deben revisar con regularidad el cumplimiento del procesamiento y los procedimientos de seguridad que están dentro de su área de responsabilidad, de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes.		
A.18.2.3	Verificación del cumplimiento técnico	Se deben verificar regularmente los sistemas de información en cuanto a su cumplimiento con las políticas y normas de seguridad de la información de la organización.		

ANEXO IV: CATALOGO DE SERVICIOS

CATÁLOGO DE SERVICIOS					
N°	CODIGO	TIPO DE SERVICIO	NOMBRE DEL SERVICIO	CLIENTES	PRIORIDAD
1	ONPMSE0001	MACROSERVICIO	SERVICIO DE GESTIÓN PARA EL SOPORTE MICROINFORMÁTICO EN SOFTWARE Y APLICACIONES.	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
1.1	ONPSER0001	SERVICIO	SOPORTE TÉCNICO PARA SOFTWARE Y APLICACIONES - SISTEMAS OPERATIVOS	Usuarios internos y externos de la OTI	ALTO
1.1.1	ONPSSE0001	SUBSERVICIOS	Soporte Técnico para Sistemas Operativos Windows	Usuarios internos y externos de la OTI	ALTO
1.1.2	ONPSSE0002	SUBSERVICIOS	Soporte Técnico para Sistemas Operativos para MAC	Usuarios internos y externos de la OTI	ALTO
1.1.3	ONPSSE0003	SUBSERVICIOS	Soporte Técnico para Sistemas Operativos Linux	Usuarios internos y externos de la OTI	MEDIO
1.2	ONPSER0002	SERVICIO	SOPORTE TÉCNICO PARA SOFTWARE Y APLICACIONES DE OFIMÁTICA	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
1.2.1	ONPSSE0004	SUBSERVICIOS	Soporte para Paquetes o Suite de Oficina	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
1.2.2	ONPSSE0005	SUBSERVICIOS	Soporte para Clientes de Correo Electrónico	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
1.2.3	ONPSSE0006	SUBSERVICIOS	Soporte para Clientes de Base de Datos	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
1.2.4	ONPSSE0007	SUBSERVICIOS	Soporte para Utilitarios y herramientas	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
1.2.5	ONPSSE0008	SUBSERVICIOS	Soporte para Aplicaciones ONP	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
2	ONPMSE0002	MACROSERVICIO	SERVICIO DE GESTIÓN PARA EL SOPORTE MICROINFORMÁTICO EN HARDWARE, EQUIPOS Y COMPONENTES	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
2.1	ONPSER0003	SERVICIO	SOPORTE TÉCNICO PARA EQUIPOS	Usuarios internos y externos de la OTI	ALTO
2.1.1	ONPSSE0009	SUBSERVICIOS	Soporte Técnico para PC/MAC - Desktop	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
2.1.2	ONPSSE0010	SUBSERVICIOS	Soporte Técnico para PC/MAC - Laptop	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
2.2	ONPSER0004	SERVICIO	SOPORTE TÉCNICO PARA PERIFÉRICOS	Usuarios internos y externos de la OTI	BAJO
2.2.1	ONPSSE0011	SUBSERVICIOS	Soporte Técnico para Periféricos - Monitor	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
2.2.2	ONPSSE0012	SUBSERVICIOS	Soporte Técnico para Periféricos - Teclado	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
2.2.3	ONPSSE0013	SUBSERVICIOS	Soporte Técnico para Periféricos - Mouse	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
2.2.4	ONPSSE0014	SUBSERVICIOS	Soporte Técnico para Periféricos - Impresoras/Escáneres	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
2.2.5	ONPSSE0015	SUBSERVICIOS	Soporte Técnico para Periféricos - Lector de Código de Barras	Usuarios internos de ONP a nivel nacional (según bases)	BAJO

CATÁLOGO DE SERVICIOS					
N°	CODIGO	TIPO DE SERVICIO	NOMBRE DEL SERVICIO	CLIENTES	PRIORIDAD
2.2.6	ONPSSE0016	SUBSERVICIOS	Soporte Técnico para Periféricos - Otros periféricos	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
2.3	ONPSER0005	SERVICIO	SOPORTE TÉCNICO PARA COMPONENTES DE PC	Usuarios internos y externos de la OTI	ALTO
2.3.1	ONPSSE0017	SUBSERVICIOS	Soporte Técnico para Componentes - Disco Duro	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
2.3.2	ONPSSE0018	SUBSERVICIOS	Soporte Técnico para Componentes - Memoria RAM	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
2.3.3	ONPSSE0019	SUBSERVICIOS	Soporte Técnico para Componentes - Placa Base	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
2.3.4	ONPSSE0020	SUBSERVICIOS	Soporte Técnico para Componentes - Fuente de Poder	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
2.3.5	ONPSSE0021	SUBSERVICIOS	Soporte Técnico para Componentes - Lector de CD/DVD	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
2.3.6	ONPSSE0022	SUBSERVICIOS	Soporte Técnico para Otro Tipo de Componentes	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
3	ONPMSE0003	MACROSERVICIO	SERVICIO DE GESTIÓN DE SOLUCIONES, APLICACIONES Y BASES DE DATOS	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
3.1	ONPSER0006	SERVICIO	GESTIÓN DE SOLUCIONES Y APLICACIONES CORE	Usuarios internos de la OTI	ALTO
3.1.1	ONPSSE0023	SUBSERVICIOS	Gestión y Despliegue de Nuevas Aplicaciones Core de Negocio	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
3.1.2	ONPSSE0024	SUBSERVICIOS	Gestión y Ejecución del Mantenimiento de Aplicaciones Core de Negocio	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
3.1.3	ONPSSE0025	SUBSERVICIOS	Gestión y Ejecución de Pruebas de Esfuerzo a Demanda para aplicaciones Core de Negocio	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
3.2	ONPSER0007	SERVICIO	GESTIÓN DE SOLUCIONES Y APLICACIONES DE APOYO	Usuarios internos de la OTI	MEDIO
3.2.1	ONPSSE0026	SUBSERVICIOS	Gestión y Despliegue de Nuevas Aplicaciones de Apoyo	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
3.2.2	ONPSSE0027	SUBSERVICIOS	Gestión y Ejecución del Mantenimiento de Aplicaciones de Apoyo	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO
3.2.3	ONPSSE0028	SUBSERVICIOS	Gestión y Ejecución de Pruebas de Esfuerzo a Demanda para Aplicaciones de Apoyo	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO
3.3	ONPSER0008	SERVICIO	GESTIÓN Y AUDITORÍAS DE BASES DE DATOS	Usuarios internos de la OTI	ALTO
3.3.1	ONPSSE0029	SUBSERVICIOS	Gestión y administración de BD	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO
3.3.2	ONPSSE0030	SUBSERVICIOS	Auditoria de BD	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO
4	ONPMSE0004	MACROSERVICIO	SERVICIO DE GESTIÓN DE ACCESOS A APLICACIONES, BASE DE DATOS, SERVICIOS TECNOLÓGICOS Y EQUIPOS	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
4.1	ONPSER0009	SERVICIO	GESTIÓN DE ACCESO A APLICACIONES Y BASES DE DATOS	Usuarios internos y externos de la OTI	MEDIO
4.1.1	ONPSSE0031	SUBSERVICIOS	Gestión de Acceso a Aplicaciones	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO

CATÁLOGO DE SERVICIOS					
N°	CODIGO	TIPO DE SERVICIO	NOMBRE DEL SERVICIO	CLIENTES	PRIORIDAD
4.1.2	ONPSSE0032	SUBSERVICIOS	Gestión de Acceso a Bases de Datos	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO
4.2	ONPSER0010	SERVICIO	GESTIÓN DE ACCESO A SERVICIOS TECNOLÓGICOS Y DE TELEFONÍA	Usuarios internos y externos de la OTI	ALTO
4.2.1	ONPSSE0033	SUBSERVICIOS	Gestión de Acceso a Cuenta de Red Corporativa	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
4.2.2	ONPSSE0034	SUBSERVICIOS	Gestión de Acceso al Correo Electrónico	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
4.2.3	ONPSSE0035	SUBSERVICIOS	Gestión de Acceso al Internet Corporativo	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
4.2.4	ONPSSE0036	SUBSERVICIOS	Gestión de Acceso a la Red Privada Virtual (VPN)	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
4.2.5	ONPSSE0037	SUBSERVICIOS	Gestión de Acceso a Recursos Compartidos	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
4.2.6	ONPSSE0038	SUBSERVICIOS	Gestión de Acceso a Telefonía	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO
4.3	ONPSER0011	SERVICIO	GESTIÓN DE CONTROL DE ACCESO A EQUIPOS	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
4.3.1	ONPSSE0039	SUBSERVICIOS	Gestión de Control de Acceso a Puertos y Conexiones de PC	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
4.3.2	ONPSSE0040	SUBSERVICIOS	Gestión de Control de Acceso a Escáner, Fotocopiadora e Impresión en red	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
5	ONPMSE0005	MACROSERVICIO	SERVICIO DE GESTIÓN DE PLATAFORMAS FÍSICAS, VIRTUALES Y DE ALMACENAMIENTO Y SERVICIOS DE RED	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
5.1	ONPSER0012	SERVICIO	GESTIÓN Y SOPORTE DE PLATAFORMAS FÍSICAS Y DE ALMACENAMIENTO	Usuarios internos de la OTI	BAJO
5.1.1	ONPSSE0041	SUBSERVICIOS	Gestión de Plataformas Físicas para WINDOWS	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
5.1.2	ONPSSE0042	SUBSERVICIOS	Gestión de Plataformas Físicas para UNIX	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
5.1.3	ONPSSE0043	SUBSERVICIOS	Gestión de Plataformas Físicas para VMWARE	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
5.1.4	ONPSSE0044	SUBSERVICIOS	Gestión de Sistema de Almacenamiento	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
5.2	ONPSER0013	SERVICIO	GESTIÓN Y SOPORTE DE PLATAFORMAS VIRTUALES	Usuarios internos de la OTI	MEDIO
5.2.1	ONPSSE0045	SUBSERVICIOS	Gestión de Plataformas Virtuales para WINDOWS	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO
5.2.2	ONPSSE0046	SUBSERVICIOS	Gestión de Plataformas Virtuales para UNIX	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
5.2.3	ONPSSE0047	SUBSERVICIOS	Gestión de Plataformas Virtuales para LINUX	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
5.3	ONPSER0014	SERVICIO	GESTIÓN DE SERVICIOS DE RED	Usuarios internos de la OTI	ALTO
5.3.1	ONPSSE0048	SUBSERVICIOS	Gestión de Directorio Activo	Usuarios internos de ONP a nivel nacional (según bases)	ALTO

CATÁLOGO DE SERVICIOS					
N°	CODIGO	TIPO DE SERVICIO	NOMBRE DEL SERVICIO	CLIENTES	PRIORIDAD
5.3.2	ONPSSE0049	SUBSERVICIOS	Gestión de Herramientas de Colaboración	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
5.3.3	ONPSSE0050	SUBSERVICIOS	Gestión de Servidores de Archivo	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
6	ONPMSE0006	MACROSERVICIO	SERVICIO DE GESTIÓN Y SOPORTE A LAS COMUNICACIONES Y SEGURIDAD INFORMÁTICA Y PERIMETRAL	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO
6.1	ONPSER0015	SERVICIO	GESTIÓN PARA EL SOPORTE DE REDES LAN/WAN	Usuarios internos de la OTI	ALTO
6.1.1	ONPSSE0051	SUBSERVICIOS	Gestión para Instalación y Mantenimiento de Cableado Estructurado	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
6.1.2	ONPSSE0052	SUBSERVICIOS	Gestión para el soporte a Switch	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
6.1.3	ONPSSE0053	SUBSERVICIOS	Gestión para el soporte a Router	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
6.1.4	ONPSSE0054	SUBSERVICIOS	Gestión para el soporte a Access Point	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO
6.1.5	ONPSSE0055	SUBSERVICIOS	Gestión para el soporte a WAAS	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO
6.2	ONPSER0016	SERVICIO	GESTIÓN DE SOPORTE DE REDES DE TELEFONÍA	Usuarios internos de la OTI	BAJO
6.2.1	ONPSSE0056	SUBSERVICIOS	Gestión y Soporte de Central Telefónica IP	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO
6.2.2	ONPSSE0057	SUBSERVICIOS	Gestión, soporte e instalación de Telefonía IP	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
6.3	ONPSER0017	SERVICIO	GESTIÓN Y SOPORTE DE SEGURIDAD INFORMÁTICA Y PERIMETRAL	Usuarios internos de la OTI	ALTO
6.3.1	ONPSSE0058	SUBSERVICIOS	Gestión para el soporte a Proxy	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
6.3.2	ONPSSE0059	SUBSERVICIOS	Gestión para el soporte a Firewall	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
6.3.3	ONPSSE0060	SUBSERVICIOS	Gestión para el soporte a IDS/IPS	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
6.3.4	ONPSSE0061	SUBSERVICIOS	Gestión para el soporte a Antispam	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
6.3.5	ONPSSE0062	SUBSERVICIOS	Gestión para el soporte a Consola de Seguridad	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
6.3.6	ONPSSE0063	SUBSERVICIOS	Gestión para el soporte a Load Balancer	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
6.3.7	ONPSSE0064	SUBSERVICIOS	Gestión para el soporte a la Solución de Antivirus	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
7	ONPMSE0007	MACROSERVICIO	SERVICIO DE GESTIÓN PARA EL SOPORTE A LAS OPERACIONES DE TI	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
7.1	ONPSER0018	SERVICIO	GESTIÓN DE RESPALDO DE LA INFORMACIÓN	Usuarios internos de la OTI	BAJO
7.1.1	ONPSSE0065	SUBSERVICIOS	Gestión de Respaldo de la Información - Copia de Seguridad	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
7.1.2	ONPSSE0066	SUBSERVICIOS	Gestión de Respaldo de la Información - Restauración	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
7.1.3	ONPSSE0067	SUBSERVICIOS	Gestión de Respaldo de información - Migración de Medios Magnéticos	Usuarios internos de ONP a nivel nacional (según bases)	BAJO

CATÁLOGO DE SERVICIOS					
N°	CODIGO	TIPO DE SERVICIO	NOMBRE DEL SERVICIO	CLIENTES	PRIORIDAD
7.2	ONPSER0019	SERVICIO	GESTIÓN Y EJECUCIÓN DE SCRIPTS O PASES A PRODUCCIÓN O QA	Usuarios internos de la OTI	ALTO
7.2.1	ONPSSE0068	SUBSERVICIOS	Gestión y Ejecución de Scripts o Pases a Producción o QA	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO
7.3	ONPSER0020	SERVICIO	GESTIÓN Y EJECUCIÓN DE MONITOREO DE PLATAFORMA.	Usuarios internos de la OTI	BAJO
7.3.1	ONPSSE0069	SUBSERVICIOS	Gestión y Ejecución de monitoreo de plataforma	Usuarios internos de ONP a nivel nacional (según bases)	BAJO
7.4	ONPSER0021	SERVICIO	GESTIÓN Y EJECUCIÓN DE ALINEAMIENTO DE BASES DE DATOS DE QA Y PRODUCCIÓN.	Usuarios internos de la OTI	MEDIO
7.4.1	ONPSSE0070	SUBSERVICIOS	Gestión y Ejecución de alineamiento de bases de datos de QA y Producción	Usuarios internos de ONP a nivel nacional (según bases)	MEDIO
7.5	ONPSER0022	SERVICIO	GESTIÓN Y SOPORTE DE EQUIPOS DE APOYO DEL CENTRO DE COMPUTO	Usuarios internos de la OTI	ALTO
7.5.1	ONPSSE0071	SUBSERVICIOS	Soporte a Conexiones Eléctricas	Usuarios internos de ONP a nivel nacional (según bases)	ALTO
7.5.2	ONPSSE0072	SUBSERVICIOS	Gestión y Soporte de equipos de apoyo del Centro de Cómputo	Usuarios internos de ONP a nivel nacional (según bases)	BAJO

ANEXO V: SOLICITUD DE CAMBIO (RFC)

ÍTEM	FUENTE	NOMBRE DEL SOLICITANTE	FECHA DE LA SOLICITUD	CLASIFICACIÓN DEL CAMBIO	DESCRIPCIÓN DEL CAMBIO	PROPOSITO DEL CAMBIO	ELEMENTO QUE REQUIERESE CAMBIADO	PRIORIDAD	ANALISIS DE LAS CONSECUENCIAS					FECHA DE INICIO	FECHA DE TERMINO	RESPONSABLE DE IMPLEMENTAR EL CAMBIO	ESTADO DEL CAMBIO	COMENTARIO DE SEGUIMIENTO
									DESCRIPCIÓN DE LAS CONSECUENCIAS	PROBABILIDAD	IMPACTO	NIVEL DE EXPOSICIÓN	DESCRIPCIÓN DE LAS ACCIONES A TOMAR					

ANEXO VI: SOLICITUD DE ACCIÓN CORRECTIVA

<table>
<tr><td colspan="2">☐ ACCIONES CORRECTIVAS</td><td colspan="2">☐ ACCIONES PREVENTIVAS</td><td>PROCESO:</td></tr>
<tr><td rowspan="2">Proviene de:</td><td>☐ Queja del cliente</td><td>☐Revisión por la Dirección</td><td>☐ Análisis de datos (Gestión de Problemas)</td><td>☐Observaciones del personal</td></tr>
<tr><td>☐ Auditoria Interna</td><td>☐ Auditoria Externa</td><td>☐ Producto No Conforme</td><td>☐ Otras</td></tr>
<tr><td colspan="5">DESCRIPCIÓN DE LA NC O PROBLEMA</td></tr>
<tr><td colspan="5">• Norma/Requisito:</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td colspan="4">Informado por:</td><td>Fecha:</td></tr>
<tr><td colspan="5">CAUSA RAIZ (Utilizar segunda hoja Investigación de la Causa Raíz)</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td colspan="4">Responsable:</td><td>Fecha:</td></tr>
<tr><td colspan="5">ACCION CORRECTIVA O PREVENTIVA (Si el espacio no es suficiente, utilizar el reverso o adjuntar una hoja)</td></tr>
<tr><td>Actividades</td><td colspan="2">Responsable</td><td colspan="2">Plazos</td></tr>
<tr><td></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>Responsable:</td><td colspan="2">Fecha:</td><td colspan="2">Fecha de Cierre Propuesta:</td></tr>
<tr><td colspan="5">VERIFICACIÓN (Si el espacio no es suficiente, utilizar el reverso o adjuntar una hoja)
☐ CONFORME ☐ NO CONFORME</td></tr>
<tr><td colspan="5"></td></tr>
<tr><td colspan="4">Responsable:</td><td>Fecha de cierre real:</td></tr>
<tr><td colspan="4">PROX FECHA DE VERIFICACIÓN: Solo llenar en caso de que en la etapa de verificación sea NO CONFORME</td><td></td></tr>
<tr><td colspan="5">VERIFICACIÓN ☐ CONFORME ☐ NO CONFORME</td></tr>
<tr><td colspan="5"></td></tr>
</table>

ANEXO VII: ANALISIS DE CAUSA

ANÁLISIS UTILIZANDO LOS 5 PORQUÉS
Consiste en establecer la no conformidad y luego preguntarse ¿Por qué?, al resultado de ésa pregunta volver a preguntarse ¿Por qué? y así sucesivamente hasta que se agoten los ¿Por qué?, el resultado del último ¿Por qué? es la causa raíz.
1. ¿Por qué pasó esto?
2. ¿Por qué pasó esto?
3. ¿Por qué pasó esto?
4. ¿Por qué pasó esto?
5. ¿Por qué pasó esto?
CAUSA RAIZ DE LA NO CONFORMIDAD