



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

**Implementación de controles de ciberseguridad bajo el
marco NIST para la protección de los servicios
tecnológicos de una entidad de microfinanzas**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Luis Fernando CORRO QUISPE

ASESOR

Raúl Marcelo ARMAS CALDERÓN

Lima, Perú

2024



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

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

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

Referencia bibliográfica

Corro, L. (2024). *Implementación de controles de ciberseguridad bajo el marco NIST para la protección de los servicios tecnológicos de una entidad de microfinanzas*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Sistemas e Informática, Escuela Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Luis Fernando Corro Quispe
Tipo de documento de identidad	DNI
Número de documento de identidad	40036211
URL de ORCID	https://orcid.org/0009-0000-0921-1574
Datos de asesor	
Nombres y apellidos	Raúl Marcelo Armas Calderón
Tipo de documento de identidad	DNI
Número de documento de identidad	07156168
URL de ORCID	https://orcid.org/0000-0003-4624-3705
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Javier Elmer Cabrera Díaz
Tipo de documento	DNI
Número de documento de identidad	08692591
Miembro del jurado 1	
Nombres y apellidos	Cayo Víctor León Fernandez
Tipo de documento	DNI
Número de documento de identidad	07001405
Datos de investigación	
Línea de investigación	No aplica
Grupo de investigación	No aplica
Agencia de financiamiento	Sin financiamiento

Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima
	Distrito: Cercado de Lima Jr. Carlos Amezaga No. 375 Universidad Nacional Mayor de San Marcos Latitud: -12.0564232 Longitud: -77.0843327
Año o rango de años en que se realizó la investigación	2023
URL de disciplinas OCDE	Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
Escuela Profesional de Ingeniería de Sistemas

Acta Virtual de Sustentación
del Trabajo de Suficiencia Profesional

Siendo las 11:00 horas del día 03 de febrero del año 2024, se reunieron virtualmente los docentes designados como Miembros de Jurado del Trabajo de Suficiencia Profesional, presidido por el Mg. Cabrera Díaz Javier Elmer (Presidente), Dr. León Fernandez Cayo Victor (Miembro) y el Ing. Armas Calderón Raúl Marcelo (Miembro Asesor), usando la plataforma Meet (<https://meet.google.com/ets-flxi-urx?hs=224>), para la sustentación virtual del Trabajo de Suficiencia Profesional intitulado: **“IMPLEMENTACIÓN DE CONTROLES DE CIBERSEGURIDAD BAJO EL MARCO NIST PARA LA PROTECCIÓN DE LOS SERVICIOS TECNOLÓGICOS DE UNA ENTIDAD DE MICROFINANZAS”**, por el Bachiller **Corro Quispe Luis Fernando**; para obtener el Título Profesional de Ingeniero de Sistemas.

Acto seguido de la exposición del Trabajo de Suficiencia Profesional, el Presidente invitó al Bachiller a dar las respuestas a las preguntas establecidas por los miembros del Jurado.

El Bachiller en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros del Jurado, el Bachiller obtuvo la nota de **18 (DIECIOCHO)**.

A continuación el Presidente de Jurados el Mg. Cabrera Díaz Javier Elmer, declara al Bachiller **Ingeniero de Sistemas**.

Siendo las 12:00 horas, se levantó la sesión.

Presidente

Mg. Cabrera Díaz Javier Elmer

Miembro

Dr. León Fernandez Cayo Victor

Miembro Asesor

Ing. Armas Calderón Raúl Marcelo



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Vicerrectorado de Investigación y Posgrado



CERTIFICADO DE SIMILITUD

Yo RAÚL MARCELO ARMAS CALDERÓN en mi condición de asesor acreditado con la Resolución Decanal N° 001246-2023-D-FISI y Oficio N° 004-PTTSP-FISI-2023 del Trabajo de Suficiencia Profesional cuyo título es IMPLEMENTACIÓN DE CONTROLES DE CIBERSEGURIDAD BAJO EL MARCO NIST PARA LA PROTECCIÓN DE LOS SERVICIOS TECNOLÓGICOS DE UNA ENTIDAD DE MICROFINANZAS, presentado por el bachiller CORRO QUISPE LUIS FERNANDO para optar el título de Ingeniero de Sistemas CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de 12% de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional**.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título correspondiente.

Firma del Asesor

DNI: 07156168

Nombres y apellidos del asesor: RAÚL M. ARMAS CALDERÓN



Huella
digital

DEDICATORIA

A mi amada familia y seres queridos, Erlinda, Mary, Shaggy y Pepe: Agradezco profundamente su inquebrantable apoyo, que ha sido el cimiento de mi crecimiento personal y profesional. Sus contribuciones muy valoradas fortalecieron mis valores y conocimientos, permitiéndome llevar a cabo acciones significativas como satisfactorias a lo largo de mi carrera.

Esta dedicatoria también se extiende a todos aquellos profesionales que comparten la misma pasión por la ciberseguridad y aspiran a transformar este mundo con pequeñas pero notables acciones.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

**Implementación de controles de ciberseguridad bajo el marco NIST para la
protección de los servicios tecnológicos de una Entidad de Microfinanzas**

Autor: Corro Quispe, Luis Fernando

Asesor: Armas Calderón, Raúl Marcelo

Título: Trabajo de Suficiencia Profesional para optar el Título Profesional de
Ingeniero de Sistemas

Fecha: Enero de 2024

RESUMEN

El presente documento refleja el complejo trabajo realizado para la implementación de los controles más críticos de ciberseguridad adoptando el marco de referencia internacional NIST (National Institute of Standards and Technology). El objetivo primordial de este trabajo ha sido salvaguardar los activos de información y los servicios tecnológicos de la Entidad de Microfinanzas. Esta implementación recoge las mejores recomendaciones de la industria bajo estándares tecnológicos apoyadas por la experiencia que obtuve a lo largo de los años como profesional como consultor de riesgo y cumplimiento de ciberseguridad.

Dicha implementación permitió a la Entidad de Microfinanzas tener un control y posterior reducción de los diferentes niveles de riesgos que fueron identificados en las etapas previas en las auditorías internas y externas; así como, para poder cumplir con las exigencias del mercado y el frente regulatorio que una entidad financiera debe cubrir.

Dentro del marco regulatorio, toda entidad financiera está sujeta a cumplir la Resolución 504-2021 de la Superintendencia de Banca, Seguros y AFP (SBS) y el estándar PCI-DSS (que en sus siglas en inglés significa Payment Card Industry Data Security Standard).

La implementación de estos controles de ciberseguridad se hizo bajo una metodología ágil compuesto por profesionales tanto de Tecnologías de la Información como del área de negocios. Todo el equipo comprometido con los objetivos se alineó a los estándares vigentes, a las política, procedimientos y normas sin perder el enfoque en los objetivos establecidos durante la estrategia análisis e implementación.

Durante la implementación de los controles, se siguió de forma rigurosa los procesos internos tales como: la gestión de vulnerabilidades, gestión de cambios, gestión de incidentes y la gestión de la continuidad basados en ITIL que dieron un orden y control sobre todas las actividades ejecutadas.

Palabras Clave: Controles de ciberseguridad, NIST (Instituto Nacional de Estándares Tecnológicos), IT (Tecnologías de la Información), Estándares tecnológicos, marcos regulatorios, sistema financiero, PCI-DSS.

MAJOR NATIONAL UNIVERSITY OF SAN MARCOS
FACULTY OF SYSTEMS AND INFORMATICS ENGINEERING
PROFESSIONAL SCHOOL OF SYSTEMS ENGINEERING

**Implementation of cybersecurity controls under the NIST framework for the
protection of technological services of a Microfinance Entity**

Author: Corro Quispe, Luis Fernando

Advisor: Armas Calderón, Raúl Marcelo

**Title: Professional Sufficiency Work to opt for the Professional Title of Systems
Engineer**

Date: January 2024

ABSTRACT

This document reflects the intricate work carried out for the implementation of the most critical cybersecurity controls, adopting the international framework of NIST (National Institute of Standards and Technology). The primary objective of this endeavor has been to safeguard the information assets and technological services of the Microfinance Entity. This implementation incorporates industry best practices supported by the experience I gained over the years as a cybersecurity risk and compliance consultant.

Such implementation enabled the Microfinance Entity to gain control and subsequently reduce various levels of risks identified in previous stages of internal and external audits. It also positioned the entity to meet market demands and regulatory requirements incumbent upon a financial institution.

Within the regulatory framework, every financial entity is obliged to comply with Resolution 504-2021 of the Superintendence of Banking, Insurance, and Pension Fund Administrators (SBS) and the PCI-DSS standard (Payment Card Industry Data Security Standard).

The implementation of these cybersecurity controls was conducted using an agile methodology involving professionals from both Information Technology and business domains. The entire team, committed to the objectives, adhered to current standards, policies, procedures, and norms without losing sight of the established goals during the strategy analysis and implementation phases.

Throughout the implementation of the controls, internal processes were rigorously followed, including vulnerability management, change management, incident management, and continuity management based on ITIL, providing structure and control over all executed activities.

Keywords: Cybersecurity Controls, NIST (National Institute of Standards and Technology), IT (Information Technology), Technological standards, Financial Sector, regulatory frameworks, PCI-DSS

TABLA DE CONTENIDO

RESUMEN	iv
ABSTRACT	vi
TABLA DE CONTENIDO	viii
INTRODUCCIÓN	1
CAPÍTULO I - TRAYECTORIA PROFESIONAL	3
CAPÍTULO II - CONTEXTO EN EL QUE SE DESARROLLA LA EXPERIENCIA	7
2.1. EMPRESA - ACTIVIDAD QUE REALIZA	7
2.2. VISIÓN	7
2.3. MISIÓN	7
2.4. ORGANIZACIÓN DE LA EMPRESA	7
2.5. ÁREA, CARGO Y FUNCIONES DESEMPEÑADAS	9
2.6. EXPERIENCIA PROFESIONAL REALIZADA EN LA ORGANIZACIÓN	10
CAPÍTULO III - ACTIVIDADES DESARROLLADAS	11
3.1. SITUACIÓN PROBLEMÁTICA	11
3.1.1. DEFINICIÓN DEL PROBLEMA	11
3.2. SOLUCIÓN	12
3.2.1. OBJETIVOS	13
3.2.1.1. Objetivo General	13
3.2.1.2. Objetivos específicos	13
3.2.2. ALCANCE	13
3.2.3. ETAPAS Y METODOLOGÍA	15
3.2.3.1. Etapa 1: Establecimiento del equipo de gobierno.	15
3.2.3.2. Etapa 2: Análisis de las amenazas y brechas de seguridad actuales.	16
3.2.3.3. Etapa 3: Priorización según el análisis del riesgo	16
3.2.3.4. Etapa 4: Despliegue e implementación de los controles	16
3.2.3.5. Etapa 5: Pruebas de efectividad de los controles.	17
3.2.3.6. Etapa 6: Cierre de las observaciones de auditoría	17
3.2.4. FUNDAMENTOS UTILIZADOS	18
3.2.4.1. Marco de referencia NIST	18

3.2.4.1.1.	Gestión del riesgo de ciberseguridad	19
3.2.4.1.2.	Las funciones del NIST	20
3.2.4.1.3.	Niveles de madurez de ciberseguridad	22
3.2.4.1.4.	Programa de ciberseguridad	23
3.2.4.2.	Capacidades de seguridad de la información y ciberseguridad.	24
3.2.4.2.1.	Las 3 líneas de defensa del gobierno	25
3.2.4.3.	Amenazas de ciberseguridad – Modelo de amenazas MITRE ATT&CK	27
3.2.5.	IMPLEMENTACIÓN DE LAS BUENAS PRÁCTICAS	29
3.2.5.1.	Etapa 1: Establecimiento del equipo de gobierno.	30
3.2.5.2.	Etapa 2: Análisis de las amenazas y brechas de seguridad	33
3.2.5.3.	Etapa 3: Priorización de los controles según el riesgo	37
3.2.5.4.	Etapa 4: Despliegue e implementación de los controles	44
3.2.5.5.	Etapa 5: Pruebas de efectividad de los controles	49
3.2.5.6.	Etapa 6: Cierre de las observaciones de auditoría	52
3.3.	EVALUACIÓN	53
3.3.1.	EVALUACIÓN COSTO-BENEFICIO	53
<i>CAPÍTULO IV. REFLEXIÓN CRÍTICA DE LA EXPERIENCIA</i>		54
5.1.	APORTE / LECCIONES APRENDIDAS	54
<i>CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES</i>		55
5.2.	CONCLUSIONES	55
5.3.	RECOMENDACIONES	56
5.4.	FUENTES DE INFORMACIÓN	57
5.4.	GLOSARIO	58
<i>ANEXOS</i>		60
1.	CERTIFICACIONES	60

INTRODUCCIÓN

Las amenazas constantes de ciberseguridad en las organizaciones y el uso de controles poco eficaces para contenerlos, hacen que se materialicen incidentes que se traducen en impactos económico-financiero, operacional, reputacional e incluso regulatorio. Día a día los adversarios tecnológicos que buscan vulnerar dichos controles se nutren de capacidades de recursos y conocimientos; y este, es el gran desafío de las personas dedicadas a protegerlos de estos cibercriminales.

El marco de referencia NIST es una guía para que las organizaciones puedan adoptar estas recomendaciones e implementar los controles bajo un conjunto de pautas dentro de las funciones específicas de la ciberseguridad como es identificación protección, detección, respuesta y recuperación de las amenazas desde un enfoque de riesgos de ciberseguridad. Este marco de origen estadounidense que nació con el objetivo de aumentar la competitividad de su industria y hoy sirve de guía a nivel mundial. El marco NIST está escrito en un lenguaje que pueda ser llevado a todos los niveles de la organización con la finalidad de alinear los objetivos de negocio, apetito y tolerancia del riesgo.

Toda entidad financiera tiene que cumplir los diferentes marcos regulatorios tecnológicos con el fin de proteger todos los activos de información, gestionar adecuadamente sus riesgos y ofrecer productos financieros seguros y confiables para sus clientes. Dentro del marco regulatorio tenemos principalmente la Resolución 504 de la SBS con su reglamento, el estándar PCI-DSS para aquellas instituciones que emiten tarjetas de créditos y la ley de protección de datos personales del Ministerio de Justicia.

Para llevar a cabo esta implementación, tomé control sobre un equipo de trabajo como Líder de Tecnología en mi rol de Jefe de Seguridad de Tecnologías de la Información de la Entidad de Microfinanzas. Como parte de mi experiencia como consultor de riesgos y amenazas de ciberseguridad pude iniciar las primeras coordinaciones con el fin de armar la estrategia de implementación teniendo como base los resultados de las auditorias pasadas tanto externas como las internas. Todo ello, motivo semanas de arduo trabajo con un equipo conformado por especialistas de redes, especialistas de gestión de servidores, consultores terceros de ciberseguridad, líderes de TI de casi todas las líneas y del negocio mismo.

- En el Capítulo I, describiremos mi experiencia profesional, que me permitió liderar la implementación de controles de ciberseguridad.

- En el Capítulo II, se detalla el contexto en el que se llevó a cabo dicha implementación, parafraseando la visión y misión de la institución financiera, su organigrama y mis funciones.
- En el Capítulo III, se formula el problema, los objetivos, el alcance, las etapas y las fases ejecutadas. Se incluyen la definición de los estándares utilizados y la estimación del valor del trabajo realizado.
- En el Capítulo IV, se indica una reflexión crítica de mi experiencia.
- En el Capítulo V, explicaremos las conclusiones y las recomendaciones del trabajo de suficiencia profesional que presento.

CAPÍTULO I - TRAYECTORIA PROFESIONAL

Describiré en este capítulo una síntesis de mi trayectoria profesional en estos 22 años de experiencia en Tecnologías de Información, en su mayoría en entidades financieras y afines, hasta desempeñarme en la actualidad como Auditor Corporativo de TI del Grupo Gloria S.A.

Siendo líder en la Entidad de Microfinanzas desarrollé un nuevo modelo de gobierno de ciberseguridad y realicé la planificación de un plan director con actividades propias de la operación, que permitieron a mediano y largo plazo alcanzar los objetivos, tales como los objetivos estratégicos de TI y del negocio, así como los regulatorios.

He tenido diferentes encargos y reconocimientos de parte de mis empleadores por haber liderado con resultados satisfactorios y haber actuado de forma disruptiva con mucha resiliencia varios equipos de trabajo, aumentado la productividad y competitividad interna.

Me apasiona la ciberseguridad y por eso estoy en constante crecimiento profesional, tengo certificado ITIL, ISO 27001, 27032, 31000, SCRUM Master, así como conocimiento experto en PCI DSS, Resolución SBS 504, Ley de protección de datos, PMI, tecnologías emergentes como Blockchain, IA, Open Banking.

A continuación, el detalle de mi trayectoria profesional

TABLA 1

Experiencia Profesional

Grupo Gloria

Mayo 2023 -Actualidad

Cargo

Auditor Corporativo de Tecnologías de la Información

Funciones	• Revisar los controles generales de TI y los controles programados en sistemas de información que soportan procesos de negocio tanto de la red administrativa (por ejemplo, SAP, directorio activo, gestión de accesos, etc.) como de redes industriales (por ejemplo, SCADA) • Revisar los procesos y entornos tecnológicos, revisar el planeamiento estratégico de TI, revisar la gestión de gobierno de TI basados en COBIT, revisar la seguridad de la infraestructura tecnológica basados en NIST e ISO-27000, revisar la segregación de funciones y revisar gestión de procesos de la tecnología basados en ITIL. • 3. Elaboración y ejecución del plan anual de las auditorías internas y externas para las diferentes sociedades del grupo en los diferentes países.
------------------	---

Banco Pichincha del Perú
Mayo 2021 – Mayo 2023

Cargo Jefe de Seguridad de TI

Funciones	• Asegurar la ejecución y cumplimiento de los indicadores claves de rendimiento (KPIs) y reporte a través de la elaboración de presentaciones a la VP de Operaciones y Tecnología y a la Gerencia de Operaciones TI. • Gestionar los servicios de terceros a través de la revisión de contratos y cumplimiento de los acuerdos de los niveles de servicio. • Asegurar la continuidad operativa de los servicios de TI incluyendo la atención de incidentes y requerimientos. • Elaborar y revisar el presupuesto de la unidad de Seguridad TI. • Planificar anualmente las actividades de la unidad de Seguridad TI. • Monitorear el plan Director de Seguridad de la Información y Ciberseguridad a través de la comunicación eficaz con los líderes técnicos. • Gestionar los riesgos de TI a través del monitoreo e implementación de planes de acción y controles compensatorios. • Participar en los comités CAI y CAB.
------------------	---

IBM del Perú
Setiembre 2015 - Mayo 2021

Cargo Security, Risk & Compliance Management Specialist Senior

Funciones	• Security and Risk Management Specialist Senior (dic/2018-may/2021): asegurar el cumplimiento de los procesos globales de seguridad, riesgos de TI y cumplimiento para el cliente Interbank. • Security and Risk Management Specialist (set/2017-nov/2018): asegurar los procesos globales de seguridad, gestión de riesgos de TI y cumplimientos para las 80 cuentas principales de IBM. • Configuration Management Process Owner (abr/2017-ago/2017): asegurar el cumplimiento del proceso global de la gestión de activos tecnológicos. • Service Level Management Specialist and Global Server Build Process Owner (may/2016-mar/2017): gestionar los procesos de acuerdos de niveles de servicios con cada cliente y servicios internos, así como asegurar el aprovisionamiento de la infraestructura bajo los lineamientos globales de IBM. • Reporting Team Leader (set/2015-abr/2016): liderar equipo para elaborar informes de servicios de TI contratados a los más de 100 clientes de IBM del Perú.
------------------	---

Consultor en Tecnologías de la Información
Setiembre 2013 - Octubre 2015

Cargo	Consultor de TI
Funciones	• Elaborar y ejecutar un plan de implementación de procesos ITIL en entidades públicas como el Ministerio del Ambiente, SUNAFIL. • Implementar los controles para el cumplimiento de la Ley de Protección de Datos Personales en el Grupo PASESA y Superintendencia Nacional de Pesquería. • Evaluar el estado del centro de datos de la Caja Municipal de Maynas.

Banco de Crédito del Perú
Julio 2001 – Octubre 2013

Cargo	Subgerente Adjunto de Gestión de Servicios de TI
Funciones	• Subgerente Adjunto de Gestión de Servicios de TI (feb/2011-oct/2013): Implementar un modelo de costo y precio de los servicios de TI mediante integraciones en diferentes plataformas usando analítica de datos. • Comprador Senior de TI (ene/2010-mar/2011): negociar las compras con proveedores de TI, elaborar y ejecutar el presupuesto OPEX. • Analista de Gestión de TI (ene/2007-dic/2010): controlar el OPEX, gestionar los SLA con los diferentes proveedores de TI y elaborar los KPI de gestión de servicios de TI. • Especialista de Infraestructura de TI (oct/2002-dic/2006): DBA de sistemas de oficinas, elaborar indicadores operativos y gestionar los pagos de TI a proveedores.

- Operador de Mesa de Ayuda (jul/2001-set/2002): asistir los clientes internos y externos del BCP.

Nota: Elaboración propia

TABLA 2

Formación Académica

Programa	Institución	Grado Obtenido	Período
Gestión de Riesgos de TI y Ciberseguridad	Universidad del Pacífico	Diplomado	2023 – 2023
Gerencia de Proyectos de Tecnologías de Información	ESAN	Diplomado	2006 - 2006
Ingeniería de Sistemas	Universidad Nacional Mayor de San Marcos	Bachiller	1997 - 2002

Nota: Elaboración propia.

TABLA 3

Formación Complementaria

Programa	Institución	Tipo	Año
ISO 31000 – Risk Manager	PECB	Certificado	2019
ISO 27001 – Lead Implementer	PECB	Certificado	2020
ISO 27032 – Lead Cybersecurity Manager	PECB	Certificado	2021
Preparación para el examen CISM	ISACA	Curso	2020
Diversos cursos en IBM: Watson Analytics, Blockchain, Think like a Hacker, IBM Agile, Cloud Computing, Python, Bigdata	IBM del Perú	Certificados	2015 - 2021
Scrum Master	New Horizons	Certificado	2018
ITIL v3	Netcomp	Certificado	2012
Controlling y Activos fijos	SAP Andina	Curso	2008
PMP	New Horizons	Curso	2007
Administración de Servidores Windows	Cibertec	Certificado	2009
Oracle Certified Professional	Cibertec	Certificado	2006
Desarrollo Aplicaciones Web .NET	Cibertec	Certificado	2012

Nota: Elaboración propia, esta relación de aptitudes adquiridas son los principales referentes dentro de mi desarrollo profesional.

CAPÍTULO II - CONTEXTO EN EL QUE SE DESARROLLA LA EXPERIENCIA

2.1. EMPRESA - ACTIVIDAD QUE REALIZA

La Entidad de Microfinanzas forma parte de un grupo financiero fundado en Ecuador en 1906, estando comprometido con el desarrollo de los países en los que opera y de sus habitantes. Cuenta con una posición de liderazgo en el mercado ecuatoriano, donde es la mayor institución bancaria. En adición, tiene presencia también en Perú, Colombia, España y Miami.

2.2. VISIÓN

Ser reconocido como el mejor grupo financiero por sus clientes y sus comunidades.

2.3. MISIÓN

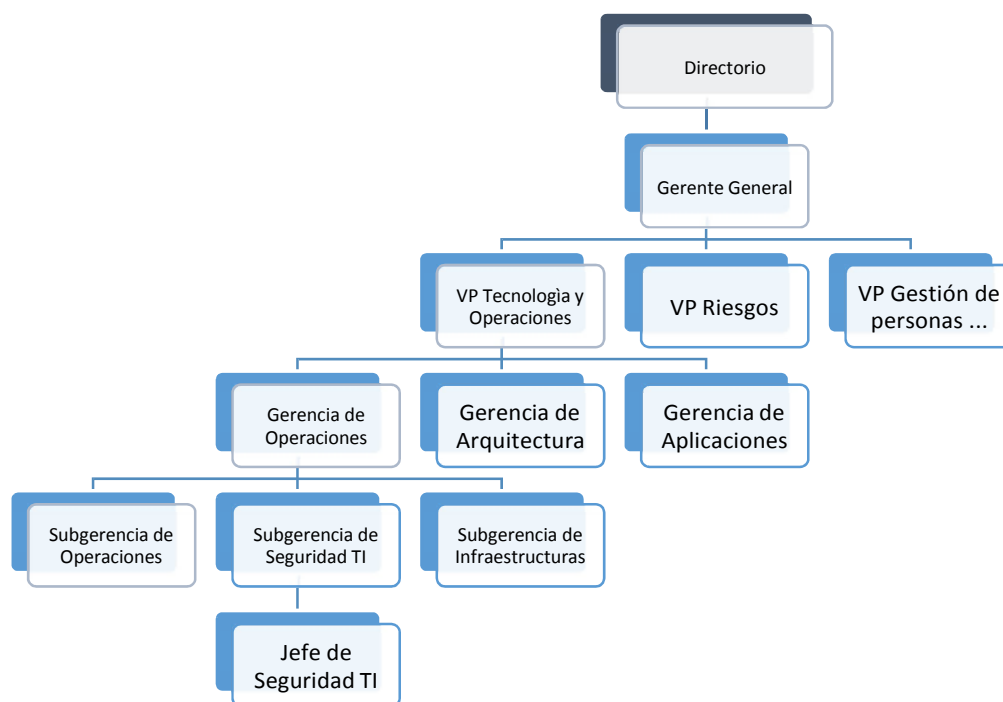
Crear soluciones y ofrecer servicios que generen valor a nuestros clientes y a la sociedad.

2.4. ORGANIZACIÓN DE LA EMPRESA

La empresa está conformada por un directorio de accionistas liderado por el gerente general que reportan a la matriz en Ecuador. La Entidad de Microfinanzas está conformada por 8 vicepresidencias y la Gerencia de Auditoria Interna sumando un aproximado de 2500 colaboradores con presencia en las principales ciudades de Perú distribuido en 54 oficinas a nivel nacional.

El Gráfico 1 es un extracto de la estructura orgánica de la Entidad de Microfinanzas. Las unidades de tecnologías incluyen a la jefatura de Seguridad TI y son responsables de los servicios tecnológicos que dan soporte a los servicios financieros. Como Seguridad TI tiene la principal labor de mantener los servicios de ciberseguridad operativos y en constante mejora continua; es por ello, que tiene mucha interacción con otras unidades, como la Vicepresidencia de Seguridad de la Información que pertenece a la Vicepresidencia de Riesgos. Además, otras unidades como Gestión de Personas, Banca Persona, Banca Empresa, Auditoria, etc.

Gráfico 1: Organigrama empresa financiera



Fuente: Elaboración propia del extracto organizacional de la Entidad de Microfinanzas

2.5. ÁREA, CARGO Y FUNCIONES DESEMPEÑADAS

Toda entidad financiera mantiene una estructura similar y las unidades de tecnología forman parte de una vertical para dar soporte a todos los servicios financieros de forma cruzada. Las unidades de TI responsables de las operaciones y desarrollo de productos ejecutan sus procesos bajos lineamientos y estándares acordados, y alineados a los objetivos estratégicos del negocio. La gerencia que gobierna la seguridad de la información y ciberseguridad es quien brinda estos lineamientos y los difunde a toda la organización para reducir las brechas y controlar los riesgos. Todo esto no sería posible si no existiera una unidad de TI Operativa de Seguridad que es la unidad a la que pertenecía como jefe de Seguridad TI. En este cargo, tenía las siguientes funciones:

- Presentar a la vicepresidencia de forma bimestral los resultados de la operación de seguridad TI, los proyectos en cursos, planes de acción ejecutados y presupuestos de la unidad de seguridad TI.
- Asegurar el cumplimiento de los servicios de seguridad prestados por terceros, mediante un comité mensual realizado con la unidad de riesgos.
- Asegurar que los servicios de seguridad estén siempre disponibles, para garantizar los principios de la seguridad de la información: confidencialidad, integridad y disponibilidad.
- Asegurar la correcta ejecución del plan director como parte de la estrategia de ciberseguridad.
- Gestionar los riesgos tecnológicos bajo la metodología vigente, implementando planes de acción y controles compensatorios.
- Liderar y gestionar los recursos internos como personal, horarios y vacaciones de la unidad de Seguridad de TI.
- Participar y ser consultor de Seguridad TI para los distintos comités de tecnología: CAI, CAB, Auditoria.

2.6. EXPERIENCIA PROFESIONAL REALIZADA EN LA ORGANIZACIÓN

En la Entidad de Microfinanzas asumí el rol como Jefe de Seguridad TI, pero dada la coyuntura del momento donde algunas posiciones de ciberseguridad claves estaban ausentes, extraoficialmente asumía roles de arquitecto, Gestor de Riesgos y auditor interno. Como principales acciones realicé lo siguiente:

- a. Asumí el rol de Jefe de Seguridad de TI con un equipo conformado por 7 personas bajo mi liderazgo entre analistas para el control de accesos, especialistas de seguridad para la administración de infraestructura como firewall, directorio activo, balanceadores de enlaces, antivirus, cajas criptográficas, filtros web, EDR, DLP, servicios Office 365, Azure AD, WAF, certificados digitales, dominios internos y públicos.
- b. Desarrollé un plan de capacitación en seguridad de la información y ciberseguridad para todo el personal de TI.
- c. Junto con mi equipo, revisamos las arquitecturas vigentes para encontrar oportunidades de mejorar con el fin de reducir riesgos tecnológicos estableciendo planes de acción a corto, mediano y largo plazo.
- d. Aseguré y prioricé el cumplimiento de los marcos normativos y regulatorios, así como la identificación de los controles que debían mejorarse o implementarse de acuerdo a las recomendaciones de la Resolución 504 de la SBS, PCI-DSS y la ley de protección de los datos personales.

Es necesario mencionar que todas estas acciones ayudaron a la Entidad de Microfinanzas y principalmente a sus líderes a comprometerse con los objetivos estratégicos de tecnología así como los de Seguridad TI, Seguridad de la Información y Ciberseguridad.

CAPÍTULO III - ACTIVIDADES DESARROLLADAS

3.1. SITUACIÓN PROBLEMÁTICA

El aumento de las amenazas y riesgos de ciberseguridad, sumado a las situaciones en un mundo post pandemia en donde el uso de recursos casi ilimitados y la accesibilidad a la tecnología para perpetrar hechos delictivos por parte de ciberdelinquentes, ha ido en aumento. Esto ha motivado elevar las barreras de control para proteger los activos de información para cualquier institución. Más aún para una entidad financiera en donde casi todos sus productos están soportados por servicios tecnológicos o de alguna forma, tienen una importante dependencia de los sistemas de información.

Esto no ha sido ajeno para la Entidad de Microfinanzas, por ellos se ejecutaron durante el año 2020 y 2021 auditorías internas y externas que evidenciaron la falta de controles que contrarresten las amenazas de los adversarios.

El ente regulador sumado a esta preocupación y para poder aumentar la competitividad, confianza y seguridad de las entidades financieras para sus clientes, emitieron una resolución con su respectivo reglamento denominado Resolución N° 504-2021 para la gestión de seguridad de la información y ciberseguridad. Dicho reglamento, especifica un conjunto de artículos destinados a cumplir lineamientos específicos relacionados a la norma ISO 27001:2013 y exige que cada institución elabore y ejecute un plan de adecuación de la norma.

Por otro lado, existe otros entes reguladores y aspiraciones de las instituciones para cumplir sus objetivos estratégicos, como alinearse al estándar PCI-DSS, cumplir con la ley de protección de datos personales o acreditar una certificación ASA (Método Estándar Alternativo), que permite un mayor nivel de confianza en el mercado para una gestión del riesgo operacional.

Entonces, todos esos componentes sumados a los informes y observaciones de auditoría motivaron mi contratación como Jefe de Seguridad de TI en la Entidad de Microfinanzas para elaborar y ejecutar un plan agresivo de implementación de los controles que permitan ir por el camino correcta, de cara a cumplir todo lo expuesto.

3.1.1. DEFINICIÓN DEL PROBLEMA

Para la Entidad de Microfinanzas era relevante tomar acción sobre todas las debilidades encontradas durante las revisiones de auditorías y gestionar de la mejor forma

los riesgos que ellas gatillaban, así como alienarse a las exigencias de las entidades reguladoras, sumado todo ello a alcanzar los objetivos estratégicos.

Como parte de las revisiones iniciales de los informes de auditoría ejecutados por la Entidad de Microfinanzas durante los años 2020 y 2021, se detectaron muchas debilidades, tales como:

- Ausencia de indicadores claves de rendimiento, para conocer el estado de salud de los servicios de seguridad.
- Inexistencia de un inventario de activos y servicios tecnológicos de seguridad.
- Muchos de los servicios tecnológicos de seguridad no cumplían un nivel básico para prevenir incidentes de ciberseguridad.
- No se contaba con el personal idóneo para gestionar, actuar y mejorar los cambios necesarios para elevar el nivel de seguridad de los servicios tecnológicos y productos financieros.
- Ausencia una línea de gobierno que brinde los lineamientos, políticas y revisión de los controles necesario para una operación saludable.
- No existía un correo de monitoreo y gestión de servicios de terceros hacia la Entidad de Microfinanzas.

3.2. SOLUCIÓN

El primer paso para elaborar un plan agresivo y eficaz para implementar los controles de seguridad alienados al marco NIST, era realizar una revisión en todos los niveles de los servicios tecnológicos para conocer que tal grande es el problema y tomar acción inmediata sobre lo más crítico, para luego, pasar a lo urgente y terminando por aquellos que generaban un riesgo medio o menor.

Una vez dimensionado el problema, mediante el uso de la metodología ágil Lean Kanban se pudo clasificar los riesgos, recursos, tiempos y acciones concretas como, por ejemplo:

- Sincerar el inventario de los servicios y equipos de seguridad mediante un formato con datos que permitan identificar riesgos de obsolescencia, gestión de parches, contactos y detalles técnicos.
- Implementación del proceso de revisión de reglas en los firewall perimetral e interno.
- Identificación de los usuarios privilegiados de las plataformas de seguridad.

- Revisión de los contratos y alcances de servicios de los proveedores de ciberseguridad.
- Revisión de los indicadores de desempeño y definición de los nuevos indicadores que generen valor.
- Redistribución de las funciones operativas dentro del equipo y contratación de dos especialistas de seguridad perimetral.
- Identificación de las oportunidades de mejora técnicas en las plataformas WAF, Antivirus, Filtros web y directorio activo.

3.2.1. OBJETIVOS

3.2.1.1. Objetivo General

Implementar controles eficaces en las plataformas y servicios de seguridad para cumplir con los marcos regulatorios, elevar el nivel de madurez de seguridad y alcanzar los objetivos estratégicos para un mejor posicionamiento en el mercado.

3.2.1.2. Objetivos específicos

- Mejorar los indicadores de gestión y performance de los servicios y plataformas de seguridad.
- Responder las observaciones de auditoria emitidos tanto por la SBS como por la unidad de auditoria interna.
- Habilitar funcionalidades de seguridad técnicas en cada una de las plataformas.
- Mejorar la calidad de los servicios con personal altamente calificado y poder con un ente rector y consultor en ciberseguridad para todas las unidades de tecnología y del negocio.

3.2.2. ALCANCE

Durante la etapa previa para el levantamiento de los inventarios, la recopilación de las observaciones de auditoria, la toma de conocimientos de los objetivos estratégicos del negocio, los marcos regulatorios y la ponderación de los riesgos de cada una de plataformas, se identificaron los controles más críticos que debían implementarse y

mejorarse. El alcance incluye, un conjunto de controles definidos para las plataformas como los firewalls internos y perimetrales, WAF, DLP, antivirus, Azure AD, directorio activo, O365, IPS, IDS, cajas criptográficas, CyberSOC, Antispam, balanceadores de enlaces de internet, equipos de seguridad de contingencia y gobierno de ciberseguridad.

La Tabla-4 representa las principales plataformas y servicios de seguridad. Pero existen otros muchas más cuya mejora continua era parte de la operación tales como: control de acceso lógico a la infraestructura, servicios y aplicaciones; gestión de certificados digitales; controles en los proyectos para el desarrollo seguro de las aplicaciones y servicios; protección de marca de la Entidad de Microfinanzas en el ciberespacio, etc.

TABLA 4

Plataformas y servicios de seguridad dentro del alcance

Plataforma / Servicio	Tipo	Marca	Modelo	Acción
Firewall Perimetral (HA)	On-premise	Palo Alto	PA-3220	Mejora
Firewall Interno (HA)	On-premise	Palo Alto	PA-3250	Mejora
Firewall Sede San Isidro	On-premise	Palo Alto	PA-820	Mejora
Firewall Sede Tarjeta	On-premise	Palo Alto	PA-820	Mejora
Panorama Palo Alto	On-premise	Palo Alto	n/a	Mejora
VPN Palo Alto	On-premise	Palo Alto	5.1.1	Nuevo
Filtro Web Trellix	On-premise	Trellix		Mejora
Consola AV ePO Trellix	On-premise	Trellix		Mejora
EDR Trellix	Cloud	Trellix	n/a	Nuevo
DLP Trellix	On-premise	Trellix	n/a	Nuevo
SIEM IBM QRadar	On-premise	IBM		Nuevo
Seguridad O365	Cloud	Microsoft	n/a	Nuevo
Directorio Activo	On-premise	Microsoft		Mejora
WAF Imperva	Cloud	Imperva	n/a	Nuevo
Thales HSM Payshield 10K	On-premise	Thales	HSM10K	Nuevo
Balanceador Citrix ADC	On-premise	Citrix		Mejora
CyberSOC + Gestión Plataforma	Service	n/a	n/a	Mejora

Fuente: Elaboración propia.

3.2.3. ETAPAS Y METODOLOGÍA

Durante la ejecución del proyecto, tomé como referencia la metodología de riesgos recomendado por NIST que está alineado al estándar ISO/IEC 27005:2018; así como, las recomendaciones de los controles a aplicar también alineado a la ISO/IEC 27001 y 27002. La ejecución en cada una de las fases de análisis, medición, implementación y pruebas de efectividad de los controles se hizo bajo un enfoque ágil con iteraciones para visualizar las entregas parciales, con seguimiento continuo con sesiones programadas con todo el equipo de seguridad de TI que estaba bajo mi supervisión y con interacciones con niveles directivos y unidades interesadas de la Entidad de Microfinanzas. Cada etapa se realizó siguiendo una metodología propia producto de la experiencia profesional. Las etapas efectuadas fueron:

- Etapa 1: Establecimiento del equipo de gobierno.
- Etapa 2: Análisis de las amenazas y brechas de seguridad actuales.
- Etapa 3: Identificación de los riesgos y medición de los mismos.
- Etapa 4: Despliegue e implementación de los controles.
- Etapa 5: Pruebas de efectividad de los controles.
- Etapa 6: Cierre de las observaciones de auditoría.

3.2.3.1. Etapa 1: Establecimiento del equipo de gobierno.

Esta es una etapa importante porque permitió establecer y fortalecer un gobierno de ciberseguridad junto con los sponsors y stakeholders para determinar si los recursos, en especial las personas de las unidades de TI (Seguridad TI), eran capaces de lograr el objetivo planteado.

El conocimiento y aptitudes de los analistas y especialistas de Seguridad TI no era uniforme y se debía identificar estas oportunidades de mejora de aptitudes y actitudes, que como líder estaba bajo mi responsabilidad.

El talento no sólo debía garantizarse dentro de la Entidad de Microfinanzas, sino también en las unidades que tenían una participación importante, como la unidad de Seguridad de la Información, que pertenecía a la vicepresidencia de

Riesgos o con proveedores de servicios cuyas acreditaciones debían ser comprobadas.

3.2.3.2. Etapa 2: Análisis de las amenazas y brechas de seguridad actuales.

La Entidad de Microfinanzas contaba con un conjunto de observaciones de las auditorías, tanto externas como interna, que debían ser levantadas para cumplir en los plazos establecidos, así como una recopilación de amenazas detectadas durante los escaneos proactivos como parte de la operación. Igual de relevante fue tener presente las exigencias regulatorias, como la resolución 504 de la SBS, SWIFT o PCI-DSS.

Atender toda esta relación de compromisos mencionados nos llevó a la necesidad de priorizar la revisión o implementación de cada control por cada una de las plataformas y servicios de Seguridad Tecnológica, bajo un enfoque de riesgos basados en NIST.

3.2.3.3. Etapa 3: Priorización según el análisis del riesgo

La implementación de cada control se ejecutó según la ponderación del riesgo como producto de impacto versus la probabilidad de ocurrencia de un incidente de ciberseguridad. Algunos controles existentes debían pasar por una mejora que fortalezca su efectividad.

Al terminar esta ponderación de los riesgos, se expuso a la Alta Dirección en varios comités el presupuesto necesario de gasto e inversión o simplemente la presentación de los planes con los recursos internos y una buena gestión de proveedores estratégicos de seguridad tecnológica.

3.2.3.4. Etapa 4: Despliegue e implementación de los controles

En esta etapa, se detalla con acciones concretas ejecutadas para la implementación de cada control. La decisión de ejecución fue el resultado de revisiones técnicas de todo el equipo en donde se definieron fechas, actividades y pruebas siguiendo un estricto cumplimiento del proceso de cambio como parte de las políticas de gestión de servicios de TI.

Muchas de las fechas planificadas para la implementación de los controles estaban relacionados con compromisos asumidos con auditoria interna y la SBS que a su vez estaban alienados a los objetivos estratégicos de la Entidad de Microfinanzas.

3.2.3.5. Etapa 5: Pruebas de efectividad de los controles.

Una vez completada cada implementación de un control específico, era parte de las actividades de cada iteración del proyecto, que el equipo de Seguridad de la información pueda realizar pruebas controladas de penetración. Este equipo, altamente calificado con perfil de Hacker Ético intentaba vulnerar los controles para determinar el nivel de eficacia en la contención las amenazas de ciberseguridad.

3.2.3.6. Etapa 6: Cierre de las observaciones de auditoria

Por cada control implementado, se elaboró un informe de implementación para dar una respuesta formal a las observaciones de auditoria o notificar al regulador el cumplimiento de los compromisos pactados.

Esta parte era muy importante porque de su buen desempeño dependía el levantamiento de observaciones, que casi siempre estaba asociado a multas por incumplimiento y que podría haber afectado no sólo en el ámbito financiero y regulatorio, sino también en el reputacional.

3.2.4. FUNDAMENTOS UTILIZADOS

Es primordial conocer los marcos de trabajo y la metodología utilizada que sumado a la experiencia y trayectoria aplicada para liderar un equipo altamente calificado, permitieron que, en casi 24 meses de arduo esfuerzo, culminar con la implantación de los controles en las distintas plataformas y servicios de ciberseguridad.

3.2.4.1. Marco de referencia NIST

Este marco es la principal referencia usada para determinar los controles basado en la gestión de riesgos de ciberseguridad. Su origen surge como necesidad del gobierno de los Estados Unidos de contar con un conjunto de pautas, recomendaciones y controles que debieran aplicar cada una de los operadores de tecnología en sus diferentes industrias con el fin de poder hacer frente a los riesgos de ciberseguridad y amenazas crecientes a nivel mundial.

NIST que en sus siglas en ingles significa National Institute of Standards and Technology, recoge todos los acuerdos, políticas, estándares, referencias tecnológicas mundialmente reconocidas y coordinaciones en todos los niveles tanto del gobierno norteamericano y las principales industrias. Fue clave conocer que este marco era flexible, fácil de comprender y utilizar, sin importar el tamaño o tipo de industria y que estas pudieran manejar de la forma oportuna sus propios riesgos de ciberseguridad y así aumentar la competitividad y eficiencia.

Este marco NIST es aplicable no solo en ámbito de TI, sino también en los sistemas de control industrial, Internet de las cosas, plataformas físicas de seguridad y cualquier componente tecnológico. Hoy NIST forma parte de un estándar internacional en donde muchos países contribuyen a fortalecerlo y es un instrumento clave para sus propias gestiones de los riesgos de ciberseguridad.

La gran fortaleza de NIST es la de permitir a las industrias mejorar sus procesos, gestionar y asegurar la rentabilidad de sus inversiones y optimizar el uso de sus recursos cuando estas operan sus infraestructuras tecnológicas críticas en un ecosistema cambiante y desafiante y cada vez más interconectado hacia la internet y con los desafíos de la Inteligencia Artificial.

El marco de NIST se compone de varias áreas clave, que abarcan desde la evaluación de riesgos y la implementación de controles de seguridad, hasta la monitorización continua y la mejora proactiva de las prácticas de seguridad.

3.2.4.1.1. Gestión del riesgo de ciberseguridad

La gestión de los riesgos de ciberseguridad bajo el enfoque NIST fue la mejor guía que ayudó a la Entidad de Microfinanzas tomar esas decisiones importantes y poder priorizar cuando se disponía de recursos limitados. NIST recomienda seguir las siguientes fases:

- Identificación de activos: Este paso implica identificar y catalogar los activos críticos de información y sistemas en una organización, incluidos datos confidenciales, hardware, software y recursos de red, así como servicios de tecnología gestionados por terceras partes.
- Evaluación de riesgos: Se lleva a cabo una evaluación exhaustiva de las amenazas potenciales y las vulnerabilidades existentes que podrían afectar a los activos identificados. Esto implica, determinar la probabilidad para materializar las amenazas y el impacto potencial cuando ocurre un incidente de ciberseguridad.
- Implementación de controles: Aquí, se implementan los controles y medidas de seguridad adecuados para el tratamiento de los riesgos identificados. Estos controles pueden incluir medidas de prevención, detección y respuesta como firewalls y el afinamiento de sus reglas, sistemas de detección y protección de intrusos, encriptación de servicios y tráfico en la red y no menos importante, con políticas de acceso, así como un conjunto de lineamientos para fijar un norte.
- Monitoreo continuo: El propósito es poder establecer procesos de monitoreo y revisión periódica para garantizar que los controles implementados sean efectivos y estén alineados con los cambios en el entorno de riesgos y así alcanzar los objetivos estratégicos de la Entidad de Microfinanzas.
- Respuesta y recuperación: Se debieron establecer planes de respuesta a incidentes y de recuperación posterior a incidentes, para minimizar los impactos negativos en caso de que ocurra un evento de seguridad, todo esto bajo procedimientos claros denominados playbooks. Esto implica, un enfoque coordinado y sistemático para mitigar y remediar los efectos de los incidentes de seguridad que

casi siempre involucra un esfuerzo coordinado entre las distintas disciplinas de tecnología.

3.2.4.1.2. Las funciones del NIST

NIST proporciona una serie de funciones y controles que se pueden implementar para fortalecer la postura de ciberseguridad de una organización. Se identifican cinco funciones principales más una denominada gobernanza, dentro de un programa de ciberseguridad. Las 5 funciones principales para gestionar y fortalecer la seguridad de la información de una organización son:

- Identificar: Esta función implica la comprensión de los activos de información críticos, los sistemas, las personas y los procesos de una organización. Identificar los recursos clave y evaluar los riesgos asociados, es crucial para desarrollar estrategias efectivas de seguridad cibernética.
- Proteger: Esta función se centra en la implementación de medidas de seguridad adecuadas para proteger los activos de información identificados. Esto incluye: la aplicación de controles de acceso, la capacitación de empleados en prácticas de seguridad y la implementación de medidas de seguridad física y lógica.
- Detectar: Implica la implementación de sistemas y procesos que permitan la detección temprana de posibles amenazas y actividades maliciosas. Esto incluye: el monitoreo de la red, el análisis de registros y la implementación de sistemas de detección de intrusos.
- Responder: Esta función implica la capacidad de responder rápidamente a incidentes de seguridad cibernética. Esto implica: la implementación de planes de respuesta a incidentes detallados que permitan una acción rápida y efectiva para contener y mitigar cualquier amenaza en curso.
- Recuperar: Se refiere a la capacidad de una organización para recuperarse rápidamente de un incidente de seguridad cibernética y restaurar sus operaciones normales. Esto implica: la implementación de planes de recuperación de desastres, la restauración de datos y sistemas y el análisis de lecciones aprendidas para mejorar las prácticas de seguridad futuras.

Estas funciones trabajan de manera integral para fortalecer la postura de ciberseguridad de una organización y proteger sus activos críticos de información de un conjunto de amenazas y vulnerabilidades de ciberseguridad cada vez más sofisticadas.

Cada función cuenta con controles diseñados para este mismo fin, estos incluyen capacidades para:

- Identificación y autenticación: Implica la implementación de mecanismos para identificar y autenticar a usuarios y dispositivos que acceden a sistemas y datos críticos. Esto puede incluir el uso de contraseñas seguras, autenticación de dos factores y biometría.
- Control de acceso: Se refiere a la gestión de permisos y restricciones de acceso a recursos de información y sistemas críticos. Esto garantiza que solo los usuarios autorizados tengan acceso a los datos y sistemas pertinentes, y ayuda a prevenir accesos no autorizados.
- Auditoría y rendición de cuentas: Comprende la implementación de mecanismos de registro y seguimiento de actividades de usuarios y sistemas. Esto facilita la capacidad de supervisar y auditar eventos relevantes para detectar posibles incidentes de seguridad y realizar un seguimiento de las acciones realizadas por los usuarios.
- Protección de datos: Incluye la implementación de medidas de cifrado y protección de datos para garantizar la confidencialidad e integridad de la información sensible. Esto puede incluir el uso de técnicas de encriptación robustas y la aplicación de políticas de manejo de datos.
- Gestión de incidentes de seguridad: Implica establecer procesos y protocolos para detectar, reportar y responder a incidentes de seguridad de manera oportuna y eficaz. Esto implica tener planes de respuesta a incidentes bien definidos y realizar análisis forenses para comprender las causas y mitigar los impactos de los incidentes.
- Seguridad de red: Incluye la implementación de medidas de seguridad en la infraestructura de red, como firewalls, detección de intrusos y prevención de intrusiones, para proteger la red de accesos no autorizados y actividades malintencionadas.
- Seguridad física: Se refiere a la protección de activos de información crítica a través de medidas de seguridad física, como el control de acceso a instalaciones, la protección de equipos y la gestión de la seguridad en el lugar de trabajo.

3.2.4.1.3. Niveles de madurez de ciberseguridad

Este marco incluye un enfoque de niveles o "Tiers" que ayuda a las organizaciones a evaluar y mejorar su postura de ciberseguridad. Los Tiers de NIST representan niveles de madurez en la implementación de prácticas de ciberseguridad y la capacidad de gestionar y responder a las amenazas cibernéticas. Estos Tiers se pueden resumir de la siguiente manera:

- Tier 1 - Riesgos no estructurados: En este nivel, las prácticas de ciberseguridad son ad hoc, lo que significa que las organizaciones tienen una comprensión limitada de los riesgos y carecen de una estrategia formal de gestión de riesgos cibernéticos.
- Tier 2 - Riesgos gestionados: En este nivel, las organizaciones comienzan a implementar controles de ciberseguridad básicos y tienen una comprensión más clara de los riesgos cibernéticos. Sin embargo, aún pueden carecer de un enfoque integral para gestionar proactivamente los riesgos y responder a incidentes de ciberseguridad.
- Tier 3 - Riesgos mitigados: Aquí, las organizaciones implementan controles de ciberseguridad más robustos y tienen una comprensión sólida de los riesgos de ciberseguridad específicos a los que se enfrentan. Tienen la capacidad de detectar y responder a amenazas de ciberseguridad de manera más efectiva y cuentan con una estrategia formal de gestión de riesgos en su lugar.
- Tier 4 - Riesgos revisados: En este nivel, las organizaciones tienen implementadas prácticas de ciberseguridad avanzadas y proactivas. Tienen la capacidad de monitorear continuamente su postura de ciberseguridad, anticipar y responder a las amenazas emergentes, y ajustar su estrategia de seguridad en consecuencia.

Estos Tiers proporcionó un marco para que Entidad de Microfinanzas evalúe su madurez en ciberseguridad y establezcan metas para mejorar su capacidad de gestión de riesgos. El objetivo de esta evaluación fue ayudar a progresar hacia un estadio más sólido y efectivo de ciberseguridad, lo que les permitió proteger mejor sus activos críticos de información y adaptarse a las amenazas de ciberseguridad en constante evolución.

3.2.4.1.4. Programa de ciberseguridad

El programa de ciberseguridad es aquel plan con tareas y compromisos a corto, mediano y largo plazo para fortalecer los procesos con controles de seguridad capaces de contrarrestar las amenazas del entorno. Un programa de ciberseguridad está compuesto por recursos, talento humano que lo acompañe, roles, responsabilidades, presupuesto, lineamientos y políticas, fechas y responsables en todos los niveles.

Los pasos que una organización podría seguir para establecer un nuevo programa de ciberseguridad o mejorar uno existente utilizando el Marco de Ciberseguridad del NIST, requieren de un conocimiento profundo del mismo sumado a la experiencia comprobada. Estos pasos deben repetirse en iteraciones constante con mejora continua, según sea necesario para elevar el nivel de madurez de la ciberseguridad. Estos pasos recomendados para establecer un programa de ciberseguridad son:

- Paso 1: Priorizar y delimitar. La organización debe identificar sus objetivos estratégicos y prioridades organizativas generales. Utilizando esta información, la organización toma decisiones estratégicas sobre implementaciones de ciberseguridad y determina el alcance de los sistemas y activos que respaldan la línea de negocio o proceso seleccionado.
- Paso 2: Orientación. Una vez determinado el alcance del programa de ciberseguridad para la línea de negocio o proceso, la organización identifica los sistemas y activos relacionados, requisitos reglamentarios y enfoque general de riesgos. La organización consulta fuentes para identificar amenazas y vulnerabilidades aplicables a esos sistemas y activos.
- Paso 3: Crear un perfil actual. La organización desarrolla un perfil actual indicando qué resultados de categoría y subcategoría del Marco se están logrando actualmente. Si un resultado se logra parcialmente, señalar este hecho ayudará a respaldar los pasos posteriores al proporcionar información de línea de base.
- Paso 4: Realizar una evaluación de riesgos. La organización analiza el entorno operativo para discernir la probabilidad de un evento de ciberseguridad y el impacto que el evento podría tener en la organización. Es importante que las organizaciones identifiquen riesgos emergentes y utilicen información de amenazas de ciberseguridad de fuentes internas y externas para comprender mejor la probabilidad e impacto de los eventos de los mismos.

- Paso 5: Crear un perfil objetivo. La organización crea un perfil objetivo que se centra en la evaluación de las categorías y subcategorías del Marco que describen los resultados de ciberseguridad deseados de la organización.
- Paso 6: Determinar, analizar y priorizar brechas. La organización compara el perfil actual y el perfil objetivo para determinar brechas. Luego, crea un plan de acción priorizado para abordar estas brechas, reflejando los impulsores de la misión, costos y beneficios, y riesgos, para lograr los resultados en el perfil objetivo.
- Paso 7: Implementar el plan de acción. La organización determina qué acciones tomar para abordar las brechas identificadas en el paso anterior y ajusta sus prácticas actuales de ciberseguridad para lograr el perfil objetivo. Las organizaciones pueden repetir estos pasos, según sea necesario para evaluar y mejorar continuamente su ciberseguridad, y alinear su programa de ciberseguridad con su nivel de implementación deseado en el Marco.

3.2.4.2. Capacidades de seguridad de la información y ciberseguridad.

Para garantizar la seguridad de la información en el ámbito de las tecnologías de la información (TI), es fundamental contar con una serie de capacidades y prácticas en el gobierno de la seguridad de la información. Algunas de estas capacidades incluyen:

- Conciencia de la seguridad de la información: Comprender la importancia de la seguridad de la información y fomentar una cultura organizacional que la respalde.
- Gestión de riesgos de seguridad: Identificar, evaluar y gestionar los riesgos de seguridad de la información de manera proactiva.
- Políticas y procedimientos de seguridad: Establecer y hacer cumplir políticas y procedimientos claros de seguridad de la información en toda la organización.
- Gestión de accesos: Implementar controles de acceso adecuados para garantizar que solo las personas autorizadas tengan acceso a la información confidencial.
- Gestión de identidades: Administrar y controlar la identificación y autenticación de los usuarios y su acceso a los recursos de TI.

- Seguridad en la red: Implementar medidas de seguridad robustas, como firewalls, detección de intrusiones y prevención de ataques maliciosos.
- Gestión de incidentes de seguridad: Tener un plan de respuesta a incidentes que permita detectar, responder y recuperarse de posibles violaciones de seguridad de la información de manera eficiente.
- Cumplimiento normativo: Cumplir con los requisitos regulatorios y normativos relacionados con la seguridad de la información, como el cumplimiento de la GDPR o la ley de protección de datos personales, Resolución 504 de la SBS, PCI-DSS, ASA.
- Concienciación y formación: Capacitar a los empleados en prácticas seguras de manejo de datos y concienciar sobre la importancia de la seguridad de la información.
- Gestión de proveedores: Evaluar y gestionar los riesgos de seguridad asociados con proveedores y terceros que tienen acceso a datos sensibles de la organización.

Además, es esencial mantenerse actualizado sobre las últimas amenazas de seguridad de la información y adoptar un enfoque proactivo para la protección de datos y la privacidad en el entorno de las TI.

3.2.4.2.1. Las 3 líneas de defensa del gobierno

Con respecto a las "tres líneas de defensa" que es un modelo de gobernanza de riesgos que se utiliza en muchos sectores, incluido el de la seguridad de la información. Estas tres líneas representan diferentes funciones y responsabilidades dentro de una organización que trabajan en conjunto para garantizar una gestión efectiva de los riesgos. Aunque originalmente se utilizó en el ámbito de la gestión de riesgos empresariales, también se puede aplicar a la seguridad de la información y ciberseguridad. Las tres líneas de defensa del gobierno de seguridad de la información y ciberseguridad son:

- a. Primera línea de defensa
 - Responsabilidad operativa directa.
 - Propietarios de riesgos y controles.
 - Se ocupan de identificar y gestionar proactivamente los riesgos en su área de responsabilidad.

- Ejemplos en seguridad de la información: los equipos de TI y de seguridad de la información en las empresas son parte de la primera línea de defensa, ya que son responsables de implementar controles de seguridad y mitigar riesgos de seguridad.
- b. Segunda línea de defensa
- Supervisión y monitoreo de la gestión de riesgos.
 - Establecimiento de políticas y estándares.
 - Ofrece orientación y supervisión a la primera línea de defensa.
 - Ejemplos en seguridad de la información: los equipos de gestión de riesgos y cumplimiento de normativas, así como los equipos de seguridad de la información que supervisan las actividades de la primera línea de defensa, forman parte de la segunda línea de defensa.
- c. Tercera línea de defensa
- Evaluación independiente y aseguramiento.
 - Auditoría interna u otras funciones de aseguramiento interno.
 - Proporciona una evaluación independiente de la efectividad de la gestión de riesgos y los controles.
 - Ejemplos en seguridad de la información: los equipos de auditoría de seguridad y los auditores internos o externos que realizan evaluaciones independientes de los controles de seguridad y riesgos, forman parte de la tercera línea de defensa.

El modelo de las tres líneas de defensa proporcionó una estructura clara para la gestión de riesgos y la gobernanza dentro de la Entidad de Microfinanzas, lo que garantizó una supervisión efectiva de los riesgos y controles en todas las unidades, principalmente en la Seguridad de la información y Seguridad TI.

Gráfico 2: Estructura de las 3 líneas de gobierno de seguridad de la información y ciberseguridad



Fuente: Elaboración propia. Gráfico basado en la recomendación para establecer un gobierno bajo COBIT, esta propuesta presentada a la Entidad de Microfinanzas es la que se usó para establecer y fortalecer en las distintas unidades de las vicepresidencias.

3.2.4.3. Amenazas de ciberseguridad – Modelo de amenazas MITRE ATT&CK

El modelo de amenazas MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) es un marco de trabajo que se utiliza para comprender y categorizar las tácticas y técnicas que los adversarios pueden emplear durante un ciberataque. Este modelo proporciona un conjunto de conocimientos detallados sobre cómo los atacantes pueden operar a lo largo de las diferentes etapas de un ciclo de vida de un ataque y se deben considerar los siguientes aspectos claves del modelo de amenazas MITRE ATT&CK:

- **Matriz de tácticas y técnicas:** La matriz MITRE ATT&CK organiza las tácticas en etapas de un ataque, desde la etapa de inicialización hasta la filtración de datos. Además, identifica una amplia gama de técnicas específicas que los atacantes pueden utilizar para lograr sus objetivos en cada etapa.
- **Descripción detallada de técnicas:** Cada técnica identificada en el marco MITRE ATT&CK viene acompañada de una descripción detallada que explica cómo funciona la técnica, qué sistemas o aplicaciones pueden verse afectados y cómo se puede detectar y mitigar esa técnica en particular.

- Uso de adversarios: El modelo MITRE ATT&CK proporciona información sobre el comportamiento de adversarios específicos y grupos de amenazas, incluyendo detalles sobre sus motivaciones, capacidades y las tácticas y técnicas que son propensos a emplear.
- Referencias cruzadas de herramientas: El modelo MITRE ATT&CK también incluye referencias cruzadas de herramientas y software malicioso conocido que se ha asociado con las diferentes tácticas y técnicas identificadas en la matriz, lo que proporciona a los analistas de seguridad una comprensión más profunda de las posibles herramientas que pueden estar en uso durante un ataque.

En resumen, el modelo de amenazas MITRE ATT&CK es una herramienta valiosa para los profesionales de la ciberseguridad, ya que les permite comprender mejor las tácticas y técnicas utilizadas por los atacantes, lo que les ayuda a fortalecer la postura de seguridad de una organización y a estar mejor preparados para detectar y mitigar posibles amenazas cibernéticas.

Gráfico 3: Extracto de las técnicas de los adversarios de la ciberseguridad según el marco de modelo de amenazas MITRE ATT&CK

Reconnaissance 10 techniques	Intelligence Gathering 8 techniques	Initial Access 10 techniques	Execution 10 techniques	Persistence 10 techniques	Privilege Escalation 14 techniques	Defense Evasion 10 techniques	Credential Access 17 techniques	Discovery 22 techniques	Lateral Movement 8 techniques	Collection 11 techniques	Command and Control 11 techniques	Exfiltration 8 techniques	Impact 14 techniques
Active Scanning (T1046)	Active Scanning (T1046)	Drive-by Compromise (T1203)	Command and Control (T1021)	Command and Control (T1021)	Local Security Authority Access (T1055)	Process Injection (T1055)	Local Security Authority Access (T1055)	Process Injection (T1055)	Process Injection (T1055)	Process Injection (T1055)	Process Injection (T1055)	Process Injection (T1055)	Process Injection (T1055)

Fuente: ATT&CK Matrix for EnterpriseGroup (<https://attack.mitre.org/>)

3.2.5. IMPLEMENTACIÓN DE LAS BUENAS PRÁCTICAS

Para la implementación de los controles bajo el marco NIST se necesitó de una coordinación efectiva entre múltiples unidades de tecnología de la entidad de Microfinanzas. La coordinación fue esencial para garantizar que las diversas funciones y controles de ciberseguridad se implementen de manera coherente y eficiente. A continuación, algunos aspectos clave de la coordinación que se tomaron durante la implementación del marco NIST:

- Comunicación interdepartamental: Fue crucial fomentar una comunicación clara y abierta entre los diferentes departamentos y equipos que estuvieron involucrados en la implementación del marco NIST. Esto, garantizó que todos los equipos estén alineados en términos de objetivos, prioridades y estrategias de ciberseguridad.
- Colaboración en la toma de decisiones: La implementación exitosa del marco NIST requirió de una toma de decisiones colaborativa teniendo en cuenta las perspectivas y los conocimientos de diferentes equipos y partes interesadas. La coordinación efectiva permitió la colaboración en la evaluación de riesgos, la selección de controles de seguridad y la planificación de la implementación.
- Asignación clara de responsabilidades: Fue esencial asignar claramente las responsabilidades específicas a equipos y miembros individuales que garantizó que cada tarea y objetivo claramente definido haya calado y rendido cuentas con el compromiso de las posiciones claves para la toma de decisiones,
- Formación y capacitación: La coordinación incluyó la implementación de programas de formación y capacitación para garantizar que todos los empleados estén familiarizados con los procedimientos y controles de ciberseguridad y puedan cumplir con sus responsabilidades de manera efectiva en los aspectos básicos de ciberseguridad.
- Revisión y mejora continua: La coordinación efectiva implicó establecer procesos para revisar y mejorar continuamente las prácticas de ciberseguridad en función de los cambios en el entorno de riesgos y las amenazas emergentes. En adición, la retroalimentación de múltiples equipos y la adaptación ágil a los cambios en el panorama de la ciberseguridad.

Gráfico 4: Flujo de coordinación dentro de una organización para la mejora continua

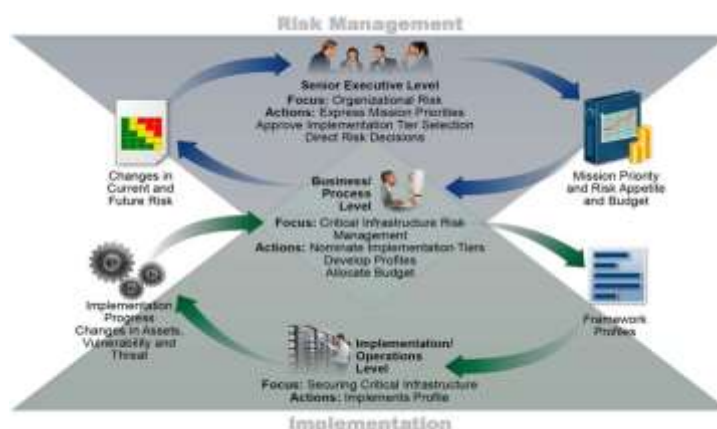


Figure 2: Notional Information and Decision Flows within an Organization

Fuente: *Cybersecurity Framework* (National Institute of Standards and Technology – Version 1.0)

3.2.5.1. Etapa 1: Establecimiento del equipo de gobierno.

Al establecer un equipo de seguridad de TI es fundamental considerar una serie de roles y responsabilidades, clave para garantizar una defensa sólida contra las amenazas y riesgos de seguridad; y, además, puedan aplicar permanentemente las mejoras continuas con la finalidad de contrarrestar los desafíos y riesgos del entorno.

Es importante conocer el nivel técnico y de gestión para garantizar una correcta implementación de los controles. Algunos roles comunes en un equipo de seguridad de TI incluyen:

- Gerente de Seguridad de la Información (CISO): Responsable de la estrategia general de seguridad de TI, el cumplimiento normativo y la protección de los activos de información crítica. Este rol está fuera de la organización de TI y usualmente pertenece a la unidad de Riesgos. En adición, este rol es crítico porque define el rumbo y a estrategia a nivel de lineamientos y políticas.
- Jefe de Seguridad TI: Responsable de la ejecución de la estrategia, implementación de controles, garantizar la mejora continua de los servicios

y dar respuesta a las auditorías relacionado a la seguridad de la información y ciberseguridad.

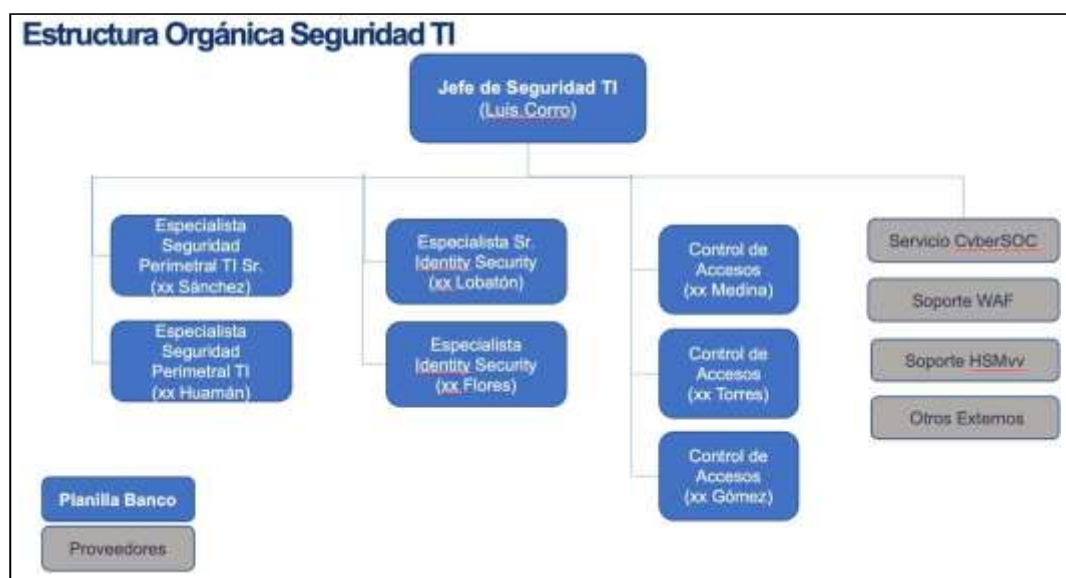
- Analistas de seguridad TI: Encargados de monitorear y analizar las amenazas de seguridad, investigar posibles incidentes y mitigar riesgos de seguridad. Este rol lo tiene asignado el especialista del equipo según la plataforma que tiene bajo su responsabilidad.
- Especialidad de seguridad Perimetral: Responsables de implementar y mantener medidas de seguridad de red, como firewalls, detección de intrusiones y prevención de ataques. Este rol lo tiene asignado el especialista del equipo según la plataforma que tiene bajo su responsabilidad.
- Analista de Control de Accesos: Encargados de administrar y controlar la identificación y autenticación de usuarios, así como, de gestionar los accesos a los recursos de TI.
- Analistas de riesgos de seguridad: Responsables de identificar y evaluar los riesgos de seguridad de TI y de proponer soluciones y controles adecuados. Este rol recae sobre todos los integrantes del equipo incluyendo al Jefe de Seguridad TI.
- Expertos en cumplimiento normativo: Encargados de garantizar que la organización cumpla con las regulaciones y normativas de seguridad de TI relevantes. Este rol recae sobre todos los integrantes del equipo.
- Analistas de seguridad de aplicaciones: Responsables de evaluar la seguridad de las aplicaciones y de identificar posibles vulnerabilidades o debilidades en el software utilizado por la organización. Este rol no estaba aún disponible en el equipo.
- Administradores de sistemas seguros: Encargados de implementar y mantener la seguridad en los sistemas operativos y aplicaciones utilizados en la organización.
- Especialistas en respuesta a incidentes: Responsables de desarrollar y ejecutar planes de respuesta a incidentes en caso de violaciones de seguridad y de coordinar las acciones de mitigación. Este rol recae sobre

todos los integrantes del equipo incluyendo al Jefe de Seguridad TI y proveedores del servicio del CyberSOC.

- Especialistas en concienciación y formación en seguridad: Encargados de educar a los empleados sobre las prácticas de seguridad de TI y de fomentar una cultura de seguridad en toda la organización. Este rol es asignado a todos los integrantes del equipo incluyendo al Jefe de Seguridad TI.

Al establecer un equipo de seguridad de TI con roles y responsabilidades bien definidos, una organización puede mejorar su capacidad para detectar, prevenir y responder a las amenazas de seguridad cibernética en un entorno tecnológico en constante evolución. Para el caso de la Entidad de Microfinanzas, algunos de estos roles estaban concentrados en una misma persona. Luego, en una primera etapa, estuvo conformado por un total de 7 personas, que junto con el Jefe de Seguridad TI y los servicios contratados con proveedores de seguridad lograron implementar los controles más urgentes en las plataformas y servicios de seguridad.

Gráfico 5: Estructura organizacional de la Jefatura de Seguridad TI



Fuente: Elaboración propia. Esta estructura orgánica es la que permaneció vigente durante el periodo del trabajo realizado para la implementación de los controles de ciberseguridad que fue desde mayo del 2021 hasta mayo del 2023.

3.2.5.2. Etapa 2: Análisis de las amenazas y brechas de seguridad

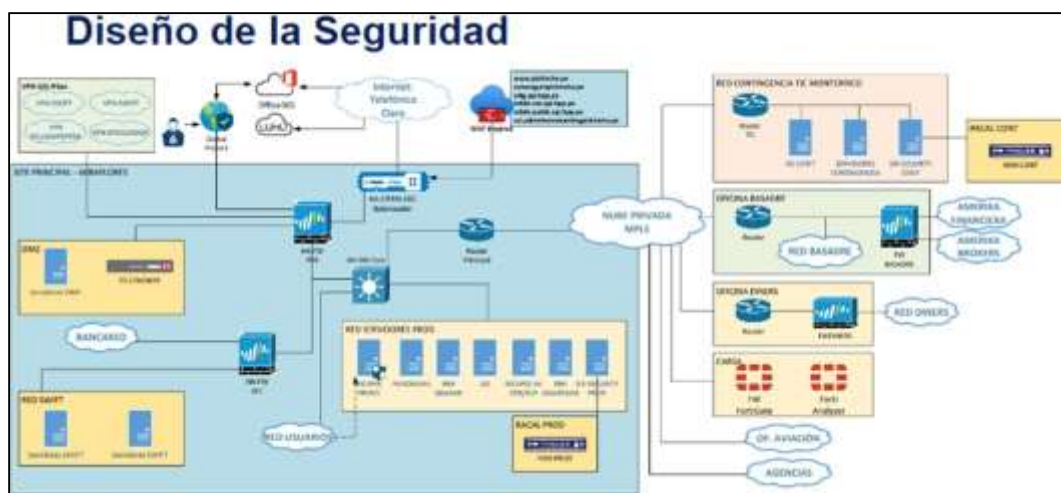
Como primer paso y siguiendo las buenas prácticas de NIST bajo la metodología de Gestión de riesgos de seguridad antes de tener el mapa completo de las amenazas existentes, se ejecutó una auto revisión de las plataformas y servicios de seguridad para identificar los activos, arquitectura de seguridad y bajo las funciones de NIST.

3.2.5.2.1. Identificación de activos

La elaboración del diagrama de seguridad ayudó a entender los puntos de contacto de la infraestructura y servicios tecnológicos de seguridad con los ecosistemas.

En el diagrama del Gráfico-6 que se presenta a continuación muestra a muy alto nivel la infraestructura y su ubicación estratégica según las necesidad y riesgos que debe cubrir.

Gráfico 6: Mapa conceptual a muy alto nivel de los servicios y plataformas de seguridad dentro de la red de la Entidad de Microfinanzas

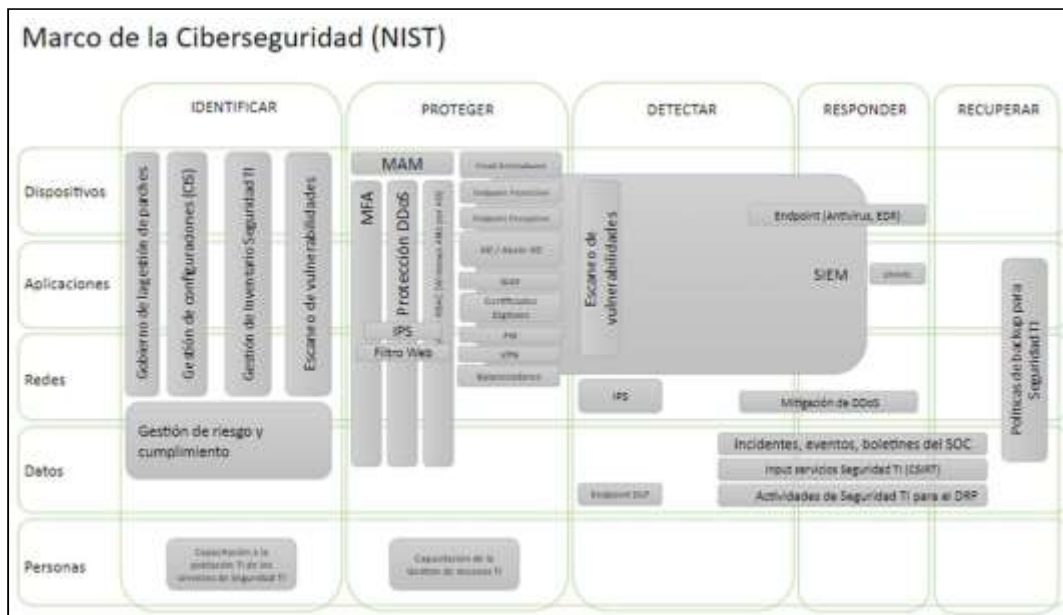


Fuente: Elaboración propia. Este diagrama muestra estratégicamente las plataformas y servicios de seguridad ubicados en la sede principal de la Entidad de Microfinanzas y sedes secundarias.

Al iniciar mis responsabilidades como jefe de Seguridad TI, realicé una revisión de todos los controles existentes bajo un enfoque de las funciones del marco NIST y su relación con las dimensiones tecnológicas. Esta acción, permitió

detectar la ausencia de los controles claves y encontrar oportunidades de mejora de los controles ya existentes.

Gráfico 7: Mapeo de los servicios y plataformas de seguridad bajo las dimensiones tecnológicas contra las funciones de NIST



Fuente: Elaboración propia. Este mapa muestra el resumen de las capacidades y controles de ciberseguridad con que se contaban, pero no necesario correctamente implementados.

Conociendo por completo las plataformas, activos y servicios de seguridad, se pudo precisar y mantener en un inventario de mucho valor, realizado con el mayor detalle técnico posible. Se implementó la gestión de la configuración con los inventarios de activos tecnológicos, inventarios de los servicios de TI y seguridad de todas las cuentas de correo y del directorio activo, inventarios de las estaciones, servidores y dispositivos móviles; además, se ejecutó el inventario de los agentes desplegados en los dispositivos y el inventario de certificados digitales internos y externos.

El resultado de estas revisiones y relevamiento de información dio lugar a un inventario centralizado, con un responsable asignado y los suficientes detalles técnicos para responder escalamientos durante los incidentes o requerimientos de la operación.

Gráfico 8: Extracto del inventario de las plataformas y servicios de Seguridad TI

Cat	Equipo	Marca	Nombre referencial	Hardware	Version
1	Penetration	Palo Alto	Penetration	VMware ESXi	9.1.9
2	Firewall	Palo Alto	Firewall Interno Principal	PA-3250	9.1.9
	Firewall	Palo Alto	Firewall Interno Secundario	PA-3250	9.1.9
2	Firewall	Palo Alto	Firewall Perimetral Principal	PA-3220	9.1.4
	Firewall	Palo Alto	Firewall Perimetral Secundario	PA-3220	9.1.4
1	Firewall	Fortinet	Firewall Cora	FG7000	V5.6.12
2	Proxy	McAfee	Proxy McAfee 01	5000-D	9.2.4
	Proxy	McAfee	Proxy McAfee 02	5000-D	9.2.4
1	WAF	FS	WAF FS	BIG-IP 2200 (C112)	13.1.1.3
1	Antivirus	McAfee	McAfee EPD	-	5.10.0 Update8
1	ATO	McAfee	ATO	ATD-3100	4.6.2.13
1	TIE	McAfee	TIE	Virtual Appliance	3.0.1.119
2	Antidddos	Clara	Clara Netscaler 01	227-1.mlos2.x86_64	NS12.1 56.22.nc
	Antidddos	Clara	Clara Netscaler 02	NS4APX-5900	NS12.1 56.22.nc
	Firewall	Palo Alto	PW BASADRE	NS4APX-5900	NS12.1 56.22.nc
3	Firewall	Palo Alto	Pw basadre		

Fuente: Elaboración propia.

3.2.5.2.2. Brechas de seguridad detectadas

La entidad de Microfinanzas contaba con una lista de vulnerabilidades, observaciones de auditoría y compromisos regulatorios que se debían gestionar con procesos y que permitan la posterior remediación y resolución de las mismas.

Una de las listas disponibles eran los planes de acción diseñados para contrarrestar las amenazas de grupos hacktivistas, amenazas del momento como los ransomware, campañas de phishing, ataques de denegación de servicios, fuerza bruta para cuentas M365, entre otros.

Gráfico 9: Extracto del plan de acción a corto plazo para los controles críticos

Id	A	B	C	D	E	F	G	H
Id	Actividades	Prioridades	Impacto	Nº de Casos	Fecha Inicio	Área Responsable	Comentarios	
1	Cargue OCs	0	00	100%	10/1/2021	Seguridad TI	Cargado el mismo 11/01/21, se viene aplicando las recomendaciones de seguridad de todos los servidores, eventos e incidentes desde la plataforma de seguridad (SI). Antivirus, Proxy, Backups, etc.	
2	Transferir las centralizadas CDR 2021-2029, CDR 2021-2027 y Actualización de uso móvil (JOC)	1	00	100%	01/01/2021	Seguridad de la Información	CDR 2021-2029, se transfiere todos los datos para cargar en CDR 2021-2027 en los sistemas existentes con soporte de datos de wireless en acceso. Para los sistemas existentes en backhaul, se produce la alternativa de usar la conexión al "terminal backbone" de Transo Mingo. Se va a migrar los datos de los sistemas de acceso a CDR 2021-2027.	
3	Transferir las centralizadas CDR 2021-2029, CDR 2021-2027 y Actualización de uso móvil (JOC)	1	00	100%	01/01/2021	Seguridad TI, TCS	CDR 2021-2029, se transfiere todos los datos para cargar en CDR 2021-2027 en los sistemas existentes con soporte de datos de wireless en acceso. Para los sistemas existentes en backhaul, se produce la alternativa de usar la conexión al "terminal backbone" de Transo Mingo. Se va a migrar los datos de los sistemas de acceso a CDR 2021-2027.	
4	Transferir las centralizadas CDR 2021-2029, CDR 2021-2027 y Actualización de uso móvil (JOC)	1	00	100%	01/01/2021	Seguridad TI, TCS	CDR 2021-2029, se transfiere todos los datos para cargar en CDR 2021-2027 en los sistemas existentes con soporte de datos de wireless en acceso. Para los sistemas existentes en backhaul, se produce la alternativa de usar la conexión al "terminal backbone" de Transo Mingo. Se va a migrar los datos de los sistemas de acceso a CDR 2021-2027.	
5	Transferir las centralizadas CDR 2021-2029, CDR 2021-2027 y Actualización de uso móvil (JOC)	1	00	100%	01/01/2021	Seguridad TI, TCS	CDR 2021-2029, se transfiere todos los datos para cargar en CDR 2021-2027 en los sistemas existentes con soporte de datos de wireless en acceso. Para los sistemas existentes en backhaul, se produce la alternativa de usar la conexión al "terminal backbone" de Transo Mingo. Se va a migrar los datos de los sistemas de acceso a CDR 2021-2027.	
6	Transferir las centralizadas CDR 2021-2029, CDR 2021-2027 y Actualización de uso móvil (JOC)	1	00	100%	01/01/2021	Seguridad TI, TCS	CDR 2021-2029, se transfiere todos los datos para cargar en CDR 2021-2027 en los sistemas existentes con soporte de datos de wireless en acceso. Para los sistemas existentes en backhaul, se produce la alternativa de usar la conexión al "terminal backbone" de Transo Mingo. Se va a migrar los datos de los sistemas de acceso a CDR 2021-2027.	
7	Transferir las centralizadas CDR 2021-2029, CDR 2021-2027 y Actualización de uso móvil (JOC)	1	00	100%	01/01/2021	Seguridad TI, TCS	CDR 2021-2029, se transfiere todos los datos para cargar en CDR 2021-2027 en los sistemas existentes con soporte de datos de wireless en acceso. Para los sistemas existentes en backhaul, se produce la alternativa de usar la conexión al "terminal backbone" de Transo Mingo. Se va a migrar los datos de los sistemas de acceso a CDR 2021-2027.	
8	Transferir las centralizadas CDR 2021-2029, CDR 2021-2027 y Actualización de uso móvil (JOC)	1	00	100%	01/01/2021	Seguridad TI, TCS	CDR 2021-2029, se transfiere todos los datos para cargar en CDR 2021-2027 en los sistemas existentes con soporte de datos de wireless en acceso. Para los sistemas existentes en backhaul, se produce la alternativa de usar la conexión al "terminal backbone" de Transo Mingo. Se va a migrar los datos de los sistemas de acceso a CDR 2021-2027.	
9	Transferir las centralizadas CDR 2021-2029, CDR 2021-2027 y Actualización de uso móvil (JOC)	1	00	100%	01/01/2021	Seguridad TI, TCS	CDR 2021-2029, se transfiere todos los datos para cargar en CDR 2021-2027 en los sistemas existentes con soporte de datos de wireless en acceso. Para los sistemas existentes en backhaul, se produce la alternativa de usar la conexión al "terminal backbone" de Transo Mingo. Se va a migrar los datos de los sistemas de acceso a CDR 2021-2027.	
10	Transferir las centralizadas CDR 2021-2029, CDR 2021-2027 y Actualización de uso móvil (JOC)	1	00	100%	01/01/2021	Seguridad TI, TCS	CDR 2021-2029, se transfiere todos los datos para cargar en CDR 2021-2027 en los sistemas existentes con soporte de datos de wireless en acceso. Para los sistemas existentes en backhaul, se produce la alternativa de usar la conexión al "terminal backbone" de Transo Mingo. Se va a migrar los datos de los sistemas de acceso a CDR 2021-2027.	

Fuente: Elaboración propia

3.2.5.3. Etapa 3: Priorización de los controles según el riesgo

3.2.5.3.1. Evaluación de riesgos

Los componentes claves para la evaluación del riesgo previo a la implementación de los controles son el inventario de los activos de seguridad, la relación de las vulnerabilidades y amenazas detectadas, así como el factor de impacto.

Lo que describe la TABLA-5 es un resumen por cada una de las plataformas y servicios de seguridad en donde se desarrolló un análisis de riesgo midiendo la probabilidad e impacto financiero, así como los controles que debían revisarse y/o mejorarse. A continuación se detalla el resultado de esta evaluación de riesgo:

TABLA 5

Plataformas y servicios de seguridad con las vulnerabilidades detectadas y los resultados de la evaluación del riesgo de los controles existentes y aquellos que debían implementarse

Plataforma o Servicio	Firewall	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	- Equipo perimetral no se encuentra en un nivel de actualización recomendada por marca Palo Alto (N-1) - No se encuentran funcionalidades de seguridad activadas en el appliance como el antispoofting, antimalware. - No se encuentran activas las funcionalidades IDS e IPS - El nivel de madurez de la reglas está por debajo del 95% aceptable.		
Control	Objetivo	Criticidad Riesgo	
Actualizaciones	- Elevar el nivel de actualización del firewall a la recomendada por marca. (N-1)	ALTA	
Configuración base segura	- Definir una línea base de seguridad para aplicarla en la configuración. - Habilitar funcionalidades antimalware, antispoofting, IDS y IPS en el equipo perimetral.	ALTA	
Madurez de reglas	- Afinar las reglas de protección para las red protegida SWIFT y eliminar el resto de las reglas expuestas "ANY-to-ANY".	ALTA	

Nota: Elaboración propia

Plataforma o Servicio	Panorama Palo Alto	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	- La gestión de usuarios no está integrada al servicio LDAP para implementar controles MFA. - Los usuarios de administración no tienen política fuerte de contraseñas. - No todos los firewalls están integrados a la consola de administración Panorama.		

	- La versión no se encuentra actualizada a una recomendada por marca.	
Control	Objetivo	Criticidad Riesgo
Actualizaciones	- Elevar el nivel de parchado a la versión N-1.	ALTA
Configuración base segura	- Integrar funcionalidades con el directorio activo para aplicarlo en los firewall y el filtro web de Trellix.	ALTA
Control de acceso	- Inventariar los usuario y aplicar la política de control de acceso y contraseñas.	ALTA

Nota: Elaboración propia

Plataforma o Servicio	VPN Palo Alto	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	- El servicio no tiene habilitado el doble factor de autenticación para integrarlo con el Azure AD. - No existe registros de auditorías habilitados y recopilados por el SIEM - No se tiene un ordenamiento de los perfiles VPN y no hay una gestión de accesos para las bajas.		
Control	Objetivo	Criticidad Riesgo	
Políticas de firewall	- Asegurar que las reglas VPN cuenten con controles de firewall antimalware, antispoofing, IDS e IPS.	ALTA	
Perfiles de seguridad	- Definir una política y procedimiento de acceso para gestionar las ALTAS, BAJAS y MODIFICACIÓN de los usuarios por cada grupo de seguridad definido.	ALTA	
Doble factor de autenticación	- Robustecer el acceso con un segundo control como factor de autenticación con Azure AD.	ALTA	
Configuración segura	- Asegurar que tenga los mecanismos de encriptación adecuados con certificados robustos, también tengan habilitados los registros de auditorías integrados al SIEM.	ALTA	

Nota: Elaboración propia

Plataforma o Servicio	Filtro Web Trellix	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	- La plataforma Trellix no se encuentra en su último nivel de actualización recomendado. - No se tiene bien definida las listas de control de acceso web con perfiles de navegación y una política con procedimiento que lo respalde. - Los sitios Web no están categorizados en la herramienta. - El filtrado web necesita un afinamiento.		
Control	Objetivo	Criticidad Riesgo	
Actualizaciones	- Elevar el nivel de parchado a la versión N-1.	ALTA	
Listas de control de acceso	- Definir una política y procedimiento y hacer un reordenamiento de los accesos de navegación según el perfil del usuario.	ALTA	
Categorización de los sitios web	- Habilitar las clasificación automática de reputación y categorización de sitios web.	MEDIA	
Filtrado de contenido	- Afinar la reglas de filtrado para hacerlo más sensible y restrictivo.	MEDIA	
Configuración segura	- Asegurar que los registros de auditoria estén integrados al SIEM.	MEDIA	

Nota: Elaboración propia

Plataforma o Servicio	Consola AV ePO Trellix	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	Elevar el nivel de parchado a la versión N-1.		
Control	Objetivo	Criticidad Riesgo	
Actualizaciones	- Elevar el nivel de parchado a la versión N-1.	MEDIA	
Control de dispositivos	- Definir los grupos y reglas para dispositivos enrolados en la consola.	ALTA	

Gestión de amenazas	- Asegurar que la detección, cuarentena y remediación se ejecute de forma automática con políticas afinadas para todos los dispositivos conectados a la red.	ALTA
Políticas de seguridad	- Asegurar que existan directivas de escaneo continuo tanto preventiva como reactiva.	MEDIA
Configuración segura	- Asegurar que los registros de auditoría estén integrados al SIEM.	MEDIA

Nota: Elaboración propia

Plataforma o Servicio	EDR Trellix	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	- No existe un control que permita identificar amenazas de malware tipo ransomware e identifique comportamientos sospechosos en los dispositivos y pueda asociarlos con un mismo origen. - No se tiene un control que aisle los dispositivos cuando se detecten amenazas que no puedan ser contenida en una primera instancia por el antivirus.		
Control	Objetivo	Criticidad Riesgo	
Detección y respuesta a los comportamientos anómalos	- Asegurar que se configuren directivas que permitan la detección temprana de amenazas y su respectiva acción inmediata como el aislamiento de los dispositivos conectados a la red.	ALTA	
Análisis en tiempo real sobre toda la red	- Asegurar el monitoreo permanente por parte del CyberSOC con un tablero de control.	ALTA	
Configuración segura	- Asegurar que los registros de auditoría estén monitoreados por un SIEM y configurar las conexiones seguras a la consola junto con una adecuada gestión de acceso.	ALTA	

Nota: Elaboración propia

Plataforma o Servicio	DLP Trellix	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	- No se cuenta con directiva DLP activas posibilitando fuga de información. - No se tiene desplegado DLP en todos los dispositivos.		
Control	Objetivo	Criticidad Riesgo	
Directivas DLP	- Asegurar existas reglas para detección de patrones y prevenir fuga de información junto con políticas y plan de concientización. - Asegurar que las directivas se apliquen al 100% de los dispositivos de la red.	MEDIA	
Inspección de contenido	- Habilitar capacidades forenses y alertas de incumplimiento de la política DLP.	MEDIA	
Configuración segura	- Asegurar que los registros de auditoría estén monitoreados por un SIEM.	MEDIA	

Nota: Elaboración propia

Plataforma o Servicio	SIEM IBM QRadar	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	- No se cuenta con una solución que integre registros de auditorías y eventos de las diferentes fuentes para la alertas preventivas y correctivas de las amenazas de ciberseguridad.		
Control	Objetivo	Criticidad Riesgo	
Actualizaciones	- Asegurar que la plataforma On-premise se encuentre en el último nivel de actualización recomendado por la marca	MEDIA	
Recopilación, normalización y correlación de eventos	- Asegurar que todas las plataformas críticas se integren al SIEM y se puedan crear reglas con casos de uso efectivos que permitan el relacionamiento de los eventos y su oportuna acción de contención.	ALTA	

Fuentes de amenazas	- Asegurar que el SIEM se integra con las fuentes de amenazas globales para extender su alcance de detección y cobertura.	ALTA
Sistema de respuesta automatizada	- Asegurar que la contención de las amenazas se ejecute de forma automatizada con integraciones directa con cada plataforma como Firewall, Antivirus, EDR, Filtro Web.	MEDIA
Gestión de incidentes	- Asegurar que los eventos sean tratados como incidentes y puedan ejecutarse las acciones correctivas.	ALTA
Tablero de control	- Contar con un acceso oportuno y con el mayor nivel de detalle para la revisión de los controles y eventos junto con los niveles de cumplimiento definidos en los casos de uso.	MEDIA
Auditoría y cumplimiento	- Permitir actividad forense y cumplimiento de los acuerdos de niveles de servicios definidos	MEDIA

Nota: Elaboración propia

Plataforma o Servicio	Seguridad O365	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	- No se tiene habilitado el multifactor de autenticación (MFA) para todos los usuarios del M365. - No se ha implementado una política de contraseña segura. - No se han habilitado funcionalidades de seguridad como al antispam, antimalware y DLP del M365. - No se ha habilitado políticas de retención y registros de auditorías. - No se monitorea los dispositivos móviles enlazados a las cuentas M365.		
Control	Objetivo	Criticidad	Riesgo
Autenticación MFA	- Asegurar con una segunda protección de autenticación tipo OTP (one-time password) contra ataques de compromiso de cuentas por fuerza bruta u otra técnica y que sirva como control MFA para otras plataformas.	ALTA	
Políticas de contraseña	- Desplegar políticas de contraseñas y directivas tanto para cuentas del directorio activo como cuentas propias de los servicios en nube.	ALTA	
Funciones antimalware, antiphishing, antispam, DLP	- Habilitar las funcionalidades de protección propias del servicio para todo el tenant organizativo. - Asegurar que las directivas vayan acorde a las políticas.	MEDIA	
Configuración segura	- Asegurar la activación de la retención de información y la habilitación de las pistas de auditorías.	MEDIA	

Nota: Elaboración propia

Plataforma o Servicio	Directorio Activo	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	- El directorio activo se encuentra fuera de soporte de Microsoft con un nivel funcional que genera serias brechas de seguridad. - Los eventos y registros de auditorías no están siendo monitoreados por el CyberSOC ni integrados al SIEM. - Existen una política de contraseña débil.		
Control	Objetivo	Criticidad	Riesgo
Configuración de pistas de auditorías y monitoreo de eventos	- Asegurar la activación de los registros suficientes para alimentar los casos de uso y puedan alertas eventos de seguridad relaciones a amenazas como fuerza bruta, viajes imposibles y accesos no autorizados.	ALTA	
Control de accesos	- Asegurar la aplicación de una política de seguridad más robusta.	ALTA	
Configuración segura	- Desactivar funcionalidades y protocolos en desuso, limpieza de los objetos, elevación de lo nivel	ALTA	

	funcional así como actualizaciones y monitoreo para garantizar la continuidad,	
Contingencia	- Asegura la disponibilidad de los servicios contingencia con pruebas anuales.	ALTA

Nota: Elaboración propia

Plataforma o Servicio	WAF Imperva	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	- Los umbrales de protección contra ataques de denegación de servicios y bots para los sitios críticos no está afinados. - No se tiene habilitado sensores contra ataques Cross-Site-Scripting y SQL Injection.		
Control	Objetivo	Criticidad Riesgo	
Protección BOTS	- Asegurar que el sensor de detección de esta amenaza este en un valor que detecta estos intentos de penetración o denegación de servicios pero que no afecte la disponibilidad de los sitios protegidos.	ALTA	
Protección XSS y SQL Injection	- Asegurar el filtrado de peticiones sospechosas de estos ataques.	ALTA	
Control de parámetros y cookies	- Asegurar políticas de retención y parametrización de las aplicaciones para evitar manipulaciones.	ALTA	
Encriptación de tráfico	- Asegurar la protección y efectividad de los protocolos SSL/TLS de los sitios así como el mantenimiento de los certificados digitales válidos.	ALTA	

Nota: Elaboración propia

Plataforma o Servicio	Thales HSM Payshield 10K	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	- La plataforma HSM (caja criptográfica para PIN de tarjetas y servicios en línea) se encuentra obsoleta. - Las 3 cajas de los diferentes entornos no está homologadas. - No existe documentación para la administración, gestión de acceso y configuración de los equipos.		
Control	Objetivo	Criticidad Riesgo	
Actualización	- Asegurar un CAPEX para la compra de las 3 cajas criptográficas nuevas, actualizadas y puedan reemplazar los equipos obsoletos tanto en los ambientes DES/CAL. PROD y CONT con el menos impacto.	ALTA	
Configuración segura	- Asegurar que la configuración de las llaves y certificados se ejecuten sin afectar ningún servicio y con la recomendación de la marca.	ALTA	
Gestión de cambio	- Asegurar que todos los ambientes se encuentren homologados y los cambios se ejecuten bajo los procesos y lineamientos establecidos.	ALTA	

Nota: Elaboración propia

Plataforma o Servicio	Balanceador Citrix ADC	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	- Los equipos en modo ACTIVO-ACTIVO no estaban en su último nivel de parchado recomendado por la marca. - No se había definido una configuración de balanceo de tráfico eficiente que libere saturaciones en los enlaces de internet principal y contingencia - No se había habilitado configuraciones de seguridad como cifrado de tráfico, protección DDoS.		
Control	Objetivo	Criticidad Riesgo	
Actualización	- Asegurar que la plataforma se encuentre en su último nivel de actualización recomendado por la marca.	ALTA	

Protección DDoS, encriptación del tráfico.	- Asegurar la habilitación de las funcionalidades de seguridad como filtrado de tráfico por detección de firmas maliciosas, encriptación de tráfico y gestión de certificados digitales y parametrización para el balanceo de la carga de los enlaces de internet priorizando las aplicaciones y servicios críticos.	ALTA
Configuración segura	- Asegurar la integración de las pistas de auditoría con el SIEM, correcta gestión de accesos y parámetros de seguridad recomendado por marca.	ALTA

Nota: Elaboración propia

Plataforma o Servicio	CyberSOC + Gestión Plataforma	Criticidad	ALTA
Vulnerabilidades y/o Amenazas	- El servicio de las operaciones de seguridad está próximo a vencer y debe renovarse ampliando las capacidades contratadas		
Control	Objetivo	Criticidad Riesgo	
Contrato de servicios	- Asegurar que el contrato contenga todos los servicios actuales y con las nuevas capacidades requeridas para que lo siga operando un proveedor con la suficiente acreditación.	ALTA	
Gestión de eventos	- Asegurar que las capacidades de detección, contención y respuesta cubra las necesidades de seguridad.	ALTA	
Cacería de amenazas	- Asegurar un ejercicio anual de detección de vulnerabilidades ya sea por ethical hacking y servicios de escaneos por parte del proveedor.	ALTA	
Inteligencia de amenazas	- Asegurar que el proveedor tenga el suficiente contexto y conocimiento de las amenazas existentes, globales y tendencias coyunturales para responder oportunamente.	ALTA	
Monitoreo de las plataformas de seguridad	- Asegurar que la disponibilidad y respuesta oportuna ante incidentes propios de cada plataforma que administra.	ALTA	
Gestión de las plataformas de seguridad	- Asegurar que el proveedor ejecute los cambios de forma eficaz y eficiente en las plataformas que administra.	ALTA	
Mejora continua de los servicios	- Asegurar que el proveedor proponga mejoras o nuevas tecnologías que hagan más eficaces los controles.	ALTA	

Nota: Elaboración propia

3.2.5.3.2. Priorización de los controles

Los controles definidos se ejecutaron según el plan establecido durante la elaboración de PETI (Plan Estratégico de TI); y en ello, se determinaron los recursos como presupuesto, personal calificado, contratación y compra de equipos.

Según la evaluación realizada determinando los aspectos a mejorar bajo un enfoque más holístico de la ciberseguridad, se contrató a un proveedor para reforzar esta evaluación inicial, cuya conclusión coincidentemente en su mayor

parte, buscaban mejorar controles similares, pero también la parte de políticas y lineamientos que debía ser ejecutado por la unidad de Seguridad de la Información que pertenecía a la Vicepresidencia de Riesgos.

El Gráfico-11 sintetiza el resultado de la evaluación interna según el modelo de madurez de NIST y las capacidades que debían mejorarse en la primera línea de defensa.

Gráfico 11: Mapeo de las capacidades y responsabilidades de la primera línea de defensa

LÍNEA DE DEFENSA	GOBERNAR	IDENTIFICAR	PROTEGER	DETECTAR	RESPONDER	RECUPERAR
PRIMERA LÍNEA DE DEFENSA	Definir e implementar controles para el cumplimiento de políticas de SI/C (1.8)					
	Cultivar y desarrollar actitudes de SI/C (1.9)					
	Definir e implementar la arquitectura de SI/C del Banco (1.10)					
	Definir procedimientos, normas y líneas base de seguridad que operan con las políticas de SI/C (1.1)	Identifica y clasifica activos (prestando datos) (1.11)	Opera intrusiones y herramientas de SI/C (redes, administrativa, etc) (1.14)	Monitorea eventos e incidentes de SI/C (1.23) (*)	Define procedimientos para la respuesta a incidentes (1.30)	Ejecuta planes de continuidad de negocio (1.35)
	Define y ejecuta proyectos de Seguridad TI (1.2)	Identifica, analiza, evalúa y mide riesgos de ciberseguridad (1.12)	Realiza el (proceso de) datos, datos y resultados de la evaluación (1.13)	Monitorea y verifica el cumplimiento de las actividades de proveedores de servicios de seguridad TI (1.24)	Responde a incidentes de SI/C (1.31)	Clasifica y actualiza los planes de recuperación (1.36)
	Evalúa la efectividad de controles de SI/C (1.3)	Planifica en los procesos de certificaciones de herramientas de ciberseguridad (1.13)	Opera controles de seguridad de datos y LPOF (1.16)	Analiza eventos e incidentes recurrentes (1.25) (*)	Realiza el cumplimiento del marco de incidentes (1.32)	Coordina con los socios involucrados las actividades de recuperación ante un desastre (1.37)
	Genera KPI y reportes de control de seguridad TI (1.4)	Identifica y clasifica vulnerabilidades (1.14)	Evalúa el impacto de ataques (procesos de seguridad TI) (1.15)	Realiza pronósticos de incidentes e incidentes de SI/C de acuerdo a la información (1.26)	Reporta e informa a la unidad de ciberseguridad del Banco (1.33)	
	Monitorea e implementa los productos de seguridad TI (1.5)	Realiza el monitoreo y reporte de vulnerabilidades (1.15)	Realiza monitoreo y reporte de vulnerabilidades de los productos de seguridad TI (1.16)	Desarrolla, implementa y mantiene mecanismos de detección (1.28) (*)	Coordina actividades de respuesta de la unidad de SI/C de acuerdo a la información (1.34)	
	Gestiona los incidentes de SI/C (1.7)		Implementa el proceso de respuesta a incidentes de SI/C (1.17)	Realiza las pruebas para la identificación de vulnerabilidades de seguridad (1.29) (*)		

Fuente: Elaboración propia

El Gráfico-11 nos muestra los aspectos más urgentes a mejorar según la evaluación del proveedor quien determinó que la entidad de Microfinanzas se encontraba en un nivel inicial en donde debían implementarse controles con la mayor prioridad y celeridad.

Gráfico 12: Nivel de madurez bajo la metodología del consultor



Fuente: Assessment realizado por el consultor externo.

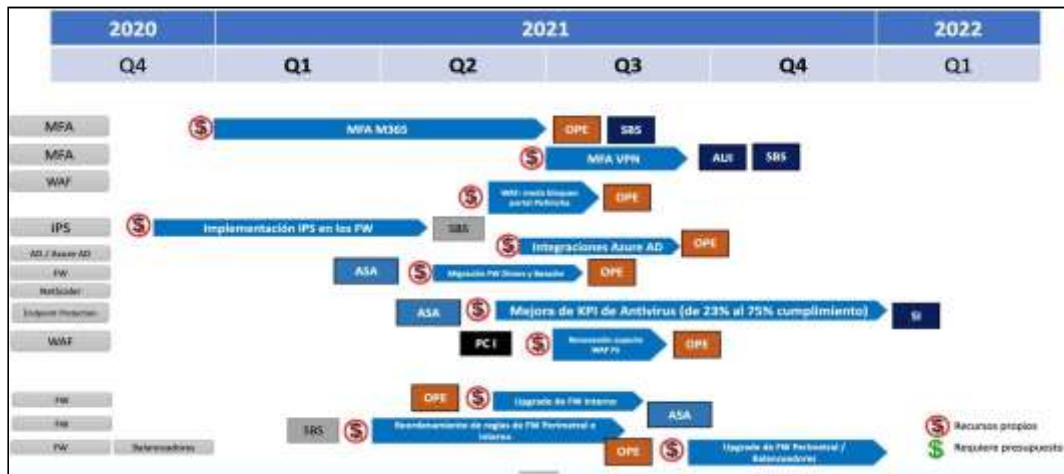
3.2.5.4. Etapa 4: Despliegue e implementación de los controles

3.2.5.4.1. Implementación de controles

En función a los niveles de riesgos y los informes presentados sumado a las priorizaciones regulatorias y vencimiento para el levantamiento de las observaciones de auditoría se determinó mediante el plan anual los controles a implementar.

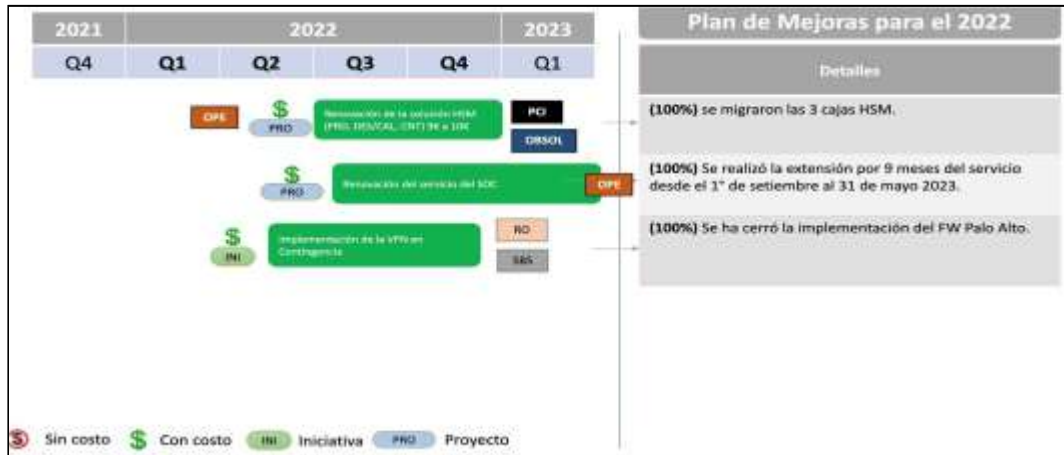
A continuación, se muestra un extracto de la presentación del PETI por año en donde se precisa la implementación de los controles definidos según las revisiones internas e informes de auditorías, así como los marcos regulatorios.

Gráfico 13: Extracto del plan estratégico de Seguridad TI 2021



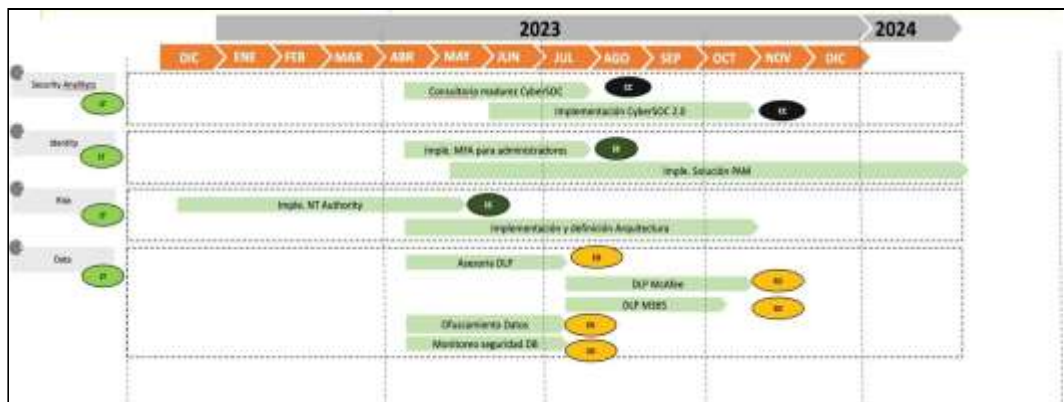
Fuente: Elaboración propia

Gráfico 14: Extracto del plan estratégico de Seguridad TI 2022



Fuente: Elaboración propia

Gráfico 15: Extracto del plan estratégico de Seguridad TI 2023



Fuente: Elaboración propia

TABLA 6

Plataformas y servicios de seguridad con las acciones ejecutadas para implementar o mejorar sus controles respectivos

Plataforma o Servicio	Firewall	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	
Actualizaciones	- Se elaboró un plan de parchado anual con las recomendaciones de las marca para que sea ejecutado siguiendo el proceso de cambio establecido.	IMPLEMENTADO	
Configuración base segura	- Se descargó la línea base de seguridad del portal de seguridad CIS (que en sus siglas en inglés “Center for Internet Security”) para luego aplicarlo en los FW Palo Alto de forma progresiva. - Se habilitó funcionalidades antimalware, antispoofing, IDS y IPS en los equipos en ambos equipos que están en alta disponibilidad.	IMPLEMENTADO	
Madurez de reglas	- Se hizo un trabajo progresivo para analizar todas las reglas creadas en el firewall, se depuraron las reglas sin tráfico y las reglas que generaban riesgos acotándolas en otros reglas con mejor control.	IMPLEMENTADO	

Nota: Elaboración propia

Plataforma o Servicio	Panorama Palo Alto	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	
Actualizaciones	- Se elaboró un plan de parchado anual con las recomendaciones de la marca para que sea ejecutado siguiendo el proceso de cambio establecido.	IMPLEMENTADO	
Configuración base segura	- Se integraron funcionalidades con el directorio activo para la gestión de usuarios en los grupos de navegación en las reglas de firewall y grupos VPN.	IMPLEMENTADO	
Control de acceso	- Se realizó elaboró un procedimiento para los accesos privilegiados para los administradores.	IMPLEMENTADO	

Nota: Elaboración propia

Plataforma o Servicio	VPN Palo Alto	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	
Políticas de firewall	- Se configuraron las reglas VPN en el firewall perimetral para que cuenten con controles antimalware, antispoofing, IDS e IPS.	IMPLEMENTADO	
Perfiles de seguridad	- Se gestionó una limpieza de los grupos de acceso VPN definido en el directorio activo y se elaboró un procedimiento con controles de revisión.	IMPLEMENTADO	
Doble factor de autenticación	- Se integró la autenticación VPN con el servicio de doble factor del M365	IMPLEMENTADO	
Configuración segura	- Se cambiaron los atributos de encriptación del tráfico por uno más robusto y se derivaron los logs al SIEM	IMPLEMENTADO	

Nota: Elaboración propia

Plataforma o Servicio	Filtro Web Trellix	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	
Actualizaciones	- Se elaboró un plan de parchado anual con las recomendaciones de la marca para que sea ejecutado siguiendo el proceso de cambio establecido..	IMPLEMENTADO	

Listas de control de acceso	- Se elaboró un procedimiento para la gestión de cuentas en los grupos de navegación según la política definida. - Se realizó una limpieza de las listas, listas negras, usuarios cesados, etc.	IMPLEMENTADO
Categorización de los sitios web	- Se revisaron las clasificaciones y reputaciones de las páginas por contenido.	IMPLEMENTADO
Filtrado de contenido	- Se afinaron las directivas de bloqueo con pruebas de efectividad.	IMPLEMENTADO
Configuración segura	- Se aseguró que los registros de auditoria estén integrados al SIEM	IMPLEMENTADO

Nota: Elaboración propia

Plataforma o Servicio	Consola AV ePO Trellex	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	
Actualizaciones	- Se elaboró un plan de parchado anual con las recomendaciones de la marca para que sea ejecutado siguiendo el proceso de cambio establecido.	IMPLEMENTADO	
Control de dispositivos	- Se ejecutaron limpiezas de los grupos y reglas en la consola ePO (que en sus siglas en inglés “ePolicy Orchestrator”). - Se elaboró un procedimiento para la gestión de objetos, directivas con controles e indicadores.	IMPLEMENTADO	
Gestión de amenazas	- Se afinaron las directivas de detección y eliminación de malware en todas las estaciones y servidores.	IMPLEMENTADO	
Políticas de seguridad	- Se aseguró la ejecución de la política para todo el inventario de estaciones y servidores .	IMPLEMENTADO	
Configuración segura	- Se aseguró que los registros de auditoria estén integrados al SIEM.	IMPLEMENTADO	

Nota: Elaboración propia

Plataforma o Servicio	EDR Trellex	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	
Detección y respuesta a los comportamientos anómalos	- Se configuraron directivas que detectan los síntomas cuando se trata de una infección masiva tipo ransomware.	IMPLEMENTADO	
Análisis en tiempo real sobre toda la red	- Se elaboró un tablero de control con SLA para la resolución de las alertas.	IMPLEMENTADO	
Configuración segura	- Se engacharon los registros de eventos y auditorías al SIEM.	IMPLEMENTADO	

Nota: Elaboración propia

Plataforma o Servicio	DLP Trellex	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	
Directivas DLP	- Se crearon directivas DLP, bloqueo de puertos y grupos específicos. - Se compraron más licencias DLP y de desplegaron progresivamente.	IMPLEMENTADO	
Inspección de contenido	- Se crearon casos de uso para detectar incumplimiento de la política DLP.	IMPLEMENTADO	
Configuración segura	- Se engacharon los registros de eventos y auditorías al SIEM..	IMPLEMENTADO	

Nota: Elaboración propia

Plataforma o Servicio	SIEM IBM QRadar	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	

Actualizaciones	- Se elaboró un plan de parchado anual con las recomendaciones de la marca para que sea ejecutado siguiendo el proceso de cambio establecido.	IMPLEMENTADO
Recopilación, normalización y correlación de eventos	- Se engacharon los registros de eventos y auditorías de los firewalls, balanceadores ADC, directorio activo, filtro web, servidores críticos, VPN, antivirus, DLP, EDR, LUMU y M365.	IMPLEMENTADO
Fuentes de amenazas	- Se configuró y actualizó componente de integración con las fuentes de ciberinteligencia del SIEM.	IMPLEMENTADO
Gestión de incidentes	- Se implementó un procedimiento junto con el proveedor de CyberSOC para el tratamiento de los eventos e incidentes con playbooks efectivos.	IMPLEMENTADO
Tablero de control	- Se desarrolló un tablero con los principales indicadores de detección en la plataforma del SIEM.	IMPLEMENTADO
Auditoría y cumplimiento	- Se crearon reportes personalizados para tener mejor trazabilidad del origen de un evento de ciberseguridad.	IMPLEMENTADO

Nota: Elaboración propia

Plataforma o Servicio	Seguridad O365	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	
Autenticación MFA	- Se implementó el MFA para todas las cuentas del tenant.	IMPLEMENTADO	
Políticas de contraseña	- Se sincronizaron las políticas de dominio con el Azure para desplegarlo de forma progresiva.	IMPLEMENTADO	
Funciones antimalware, antiphishing, antispam, DLP	- Se habilitaron las funcionalidades antimalware, antiphishing y antispam en el M365. - Se implementaron directivas DLP en el M365 para prevenir fuga de información.	IMPLEMENTADO	
Configuración segura	- Se engacharon los registros de eventos y auditorías al SIEM..	IMPLEMENTADO	

Nota: Elaboración propia

Plataforma o Servicio	Directorio Activo	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	
Configuración de pistas de auditorías y monitoreo de eventos	- Se activaron los eventos del AD para poder elaborar casos de usos en SIEM y prevenir vectores de ataque como fuerza bruta, escalamiento de privilegios, etc.	IMPLEMENTADO	
Control de accesos	- Se definió una política de contraseñas más robusta que de desplegó progresivamente a todo el dominio.	IMPLEMENTADO	
Configuración segura	- Se limpiaron del AD objetos en desuso, cuentas inactivas y se crearon directivas para el bloqueo de puertos, administración local de equipos, restricción de permisos “todos” en los directorios compartidos. - Se deshabilitaron protocolos inseguros	IMPLEMENTADO	
Contingencia	- Se implementó un directorio activo en el centro de datos de contingencia..	IMPLEMENTADO	

Nota: Elaboración propia

Plataforma o Servicio	WAF Imperva	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	
Protección BOTS	- Se realizaron pruebas para afinar las directivas que protegen los principales portales de ataques por bots, denegación de servicios, SQL Injection, entre otros.	IMPLEMENTADO	
Protección XSS y SQL Injection	- Se configuró el filtrado de peticiones sospechosas.	IMPLEMENTADO	

Encriptación de tráfico	- Se configuraron los protocolos TLS de los sitios con un procedimiento para la gestión de los mismo.	IMPLEMENTADO
-------------------------	---	--------------

Nota: Elaboración propia

Plataforma o Servicio	Thales HSM Payshield 10K	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	
Actualización	- Se elaboró un plan de actualización de las 3 cajas criptográficas mediante un proyecto de inversión.	IMPLEMENTADO	
Configuración segura	- Se realizaron pruebas de las llaves y certificados en entornos no productivos con las aplicaciones para luego ejecutarlo en producción.	IMPLEMENTADO	
Gestión de cambio	- Se estableció una política para asegurar la homologación de la configuración de las 3 cajas.	IMPLEMENTADO	

Nota: Elaboración propia

Plataforma o Servicio	Balanceador Citrix ADC	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	
Actualización	- Se elaboró un plan de parchado anual con las recomendaciones de la marca para que sea ejecutado siguiendo el proceso de cambio establecido.	IMPLEMENTADO	
Protección DDoS, encriptación del tráfico.	- Se establecieron configuraciones para detectar ataques tipo DDoS y se configuraron protocolos seguros para la entrada de tráfico crítico. - Se establecieron pesos para priorizar el tráfico crítico.	IMPLEMENTADO	
Configuración segura	- Se engancharon los registros de eventos y auditorías al SIEM...	IMPLEMENTADO	

Nota: Elaboración propia

Plataforma o Servicio	CyberSOC + Gestión Plataforma	Criticidad	ALTA
Control	Acciones ejecutadas	Estado	
Contrato de servicios	- Se diseñó un nuevo alcance de servicio bajo un contrato integral con las capacidades que una entidad financiera requiere.	IMPLEMENTADO	

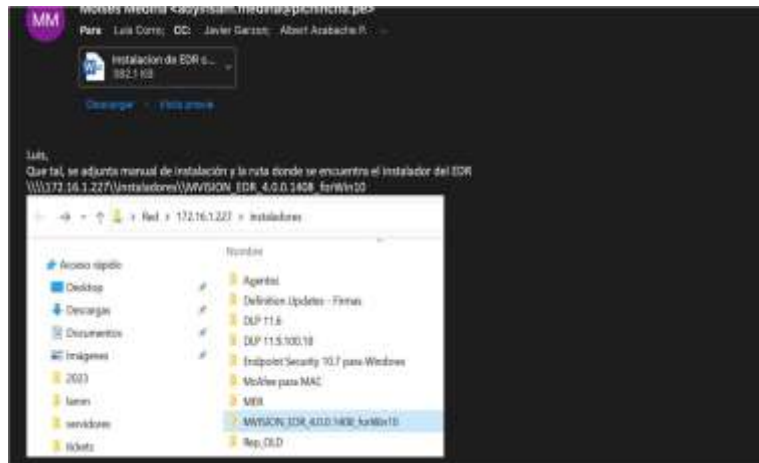
Nota: Elaboración propia

3.2.5.5. Etapa 5: Pruebas de efectividad de los controles

A medida que se iba cumpliendo con los objetivos, para implementar controles eficaces en las diferentes plataformas para contener las amenazas, se solicitaba a la unidad de Seguridad de la información pruebas en el control mismo para comprobar su correcto funcionamiento.

Estas pruebas muchas veces fueron coordinadas con las unidades de negocio, dado que se requería hacer pruebas en vivo como simular ataques de fuerza bruta o denegación de servicio sobre los canales de atención principales o los servicios críticos.

Gráfico 16: Correo informando el cierre de la implementación del control EDR



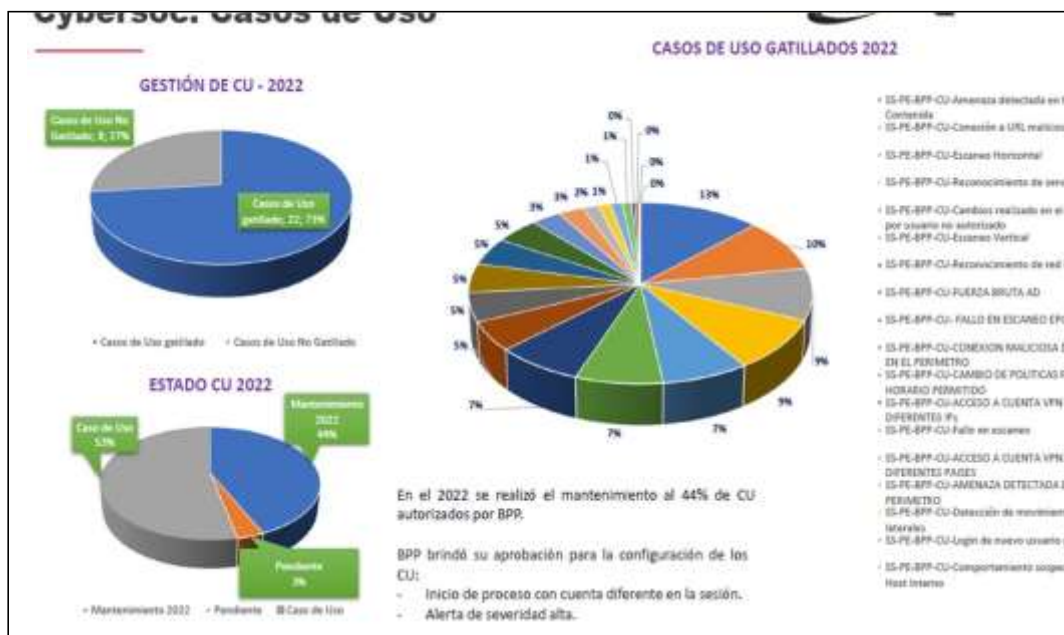
Fuente: Extracto del correo interno

Gráfico 17: Extracto del correo por la renovación del CyberSOC



Fuente: Extracto del correo interno

Gráfico 18: Resultados de la eficacia de los controles presentados por el proveedor



Fuente: Informe del proveedor de servicio

Gráfico 19: Extracto de la eficacia del control en el WAF

Para: Monitoreo SOC; Erick Alencar; Luis Corra; Centro de Control de Seguridad; Diego Rodríguez

CC: Servicedesk Electrodata; Centro de Control de Seguridad; Jorge Rojas

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

La presente es para comunicar la llegada de las siguientes alertas:

WAF Sessions

Client Type	Client App	URL	Method	Action
Unauthenticated	Bot	http://www.pichincha.pe/personas/solicitud-atraco	GET	Blocked
Unauthenticated	Bot	http://www.pichincha.pe/personas/solicitud-atraco	GET	Blocked
Unauthenticated	Bot	http://www.pichincha.pe/personas/solicitud-atraco	GET	Blocked
Unauthenticated	Bot	http://www.pichincha.pe/personas/solicitud-atraco	GET	Blocked
Unauthenticated	Bot	http://www.pichincha.pe/personas/solicitud-atraco	GET	Blocked

Fuente: Extracto del correo interno.

Gráfico 20: Extracto de correo de coordinación para las pruebas del control antiDoS en el WAF.

Para: Jose Alaga; Yair Omar Requena Camargo; Erick Alencar

CC: Luis Corra; Centro de Control de Seguridad; Lesly Jimenez; Servicedesk Electrodata; Luis Tovar Romero; Henry Flores; Rodolfo Vilchez Portillo; Arturo Simich; Arnold Arias; Jessica Cueto

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Comuniqué, Luis,

Intente comunicarme con su persona sin éxito.

¿Se tiene confirmada la ventana para el día viernes 12/11 a las 9:30 pm?

Saludos Cordiales

Grupo Secu [Redacted] Seguridad

Electrodata yrequena@electrodata.com.pe

Mobile: 99408588 / 940 [Redacted]

Lima - Perú

El vie, 5 nov 2021 a las 16:49, Erick Alencar (<erick.alencar@pichincha.pe>) escribió:

Hola Luis,

Gracias por la respuesta, en ese caso tendríamos que probar a las 09:30pm para no impactar la operativa del APP.

Hola Hernán,

Por favor nos confirmas si no hay problema con el horario.

Gracias, [Redacted]

Saludos,

Erick Alencar Ríos
Sub Gerente de Canales Alternativos
Vicepresidencia de Banca Personas

Fuente: Extracto del correo interno

Manual de la Política Corporativa

Security Analyst - (SOPT) Luis Correo, Jairo Morán, Carlos Cordero

El log generamos con el modo en que se muestra este mensaje, haga clic aquí para verlo en su navegador web.

Camión por usuarios activos de correo electrónico - 12 KB

Resumen de IP y firma en firewall generados por el - 107 KB

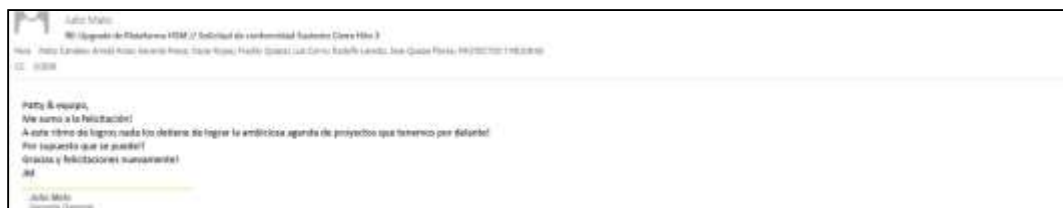
1. En el estado adjunto se encuentran los campos iniciales que buscamos para el reporte de cambios por usuarios administradores, también se encuentran los usuarios con el perfil de administrador.

2. Adjunto al correo que gestione con el SOPORT para el bloqueo de una IP o firma que ha detectado instrumentalmente (no alertada por el SOC). Por favor, envíelo para poder mejorar el caso de uso de amenazas por firma de administrador.

3. Ya se realizaron los trabajos para que las conexiones desde el exterior no se noten con la IP del balanceador 10.0.14.200, ya se puede visualizar la IP real de las conexiones, esto nos ayudará a determinar los falsos positivos de uso en implantación.

Source IP	Type	Source	From Zone	To Zone	Source address	Source user	Source Country	Destination address	Dynamic User	To Port	Application	Action	Severity
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal	10.0.0.14.200.20	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	10.0.0.14.200	Spain	10.0.14.200	10	10.0.14.200	10.0.14.200	10.0.14.200	10.0.14.200
10.0.0.14.200.20	normal												

Gráfico 22: Extracto del correo de felicitación del Gerente General por la migración de la plataforma HSM hacia una versión soportada



3.2.5.6. Etapa 6: Cierre de las observaciones de auditoria

A continuación, se muestra un extracto de la presentación del PETI por año en donde se precisa la implementación de los controles definidos según las revisiones internas e informes de auditorías, así como los marcos regulatorios.

3.3. EVALUACIÓN

3.3.1. EVALUACIÓN COSTO-BENEFICIO

La relación costo beneficio dentro de la implementación de los controles está relacionado a los factores de riesgos, por ejemplo:

- a. Materializar fuga de información o filtración de bancos de datos personales por una mala gestión en la custodia de los mismos, podría acarrear multas que pudieran ir desde las 5 unidades impositivas tributarias (UIT) hasta las 100 UIT's.
- b. La infección por ransomware podría indisponer los servicios financieros afectando canales transaccionales. Para la Entidad de Microfinanzas, la pérdida del servicio de Ventanilla y la Banca por Internet, además de un impacto reputacional y regulatorio, traería pérdidas financieras en la utilidad por un valor de 1.5 millones de soles por cada día.
- c. El presupuesto del gasto operativo para el año 2022 oscilaba entre los 4.4 millones de soles.
- d. El gasto de inversión en el mismo año fue de 1.2 millones de soles, acción efectuada para implementar controles.

En resumen, el costo por no implementar dependía del apetito y tolerancia del riesgo asumido por la Entidad de Microfinanzas; y, si los riesgos se materializaban, iba a significar una gran pérdida financiera.

CAPÍTULO IV. REFLEXIÓN CRÍTICA DE LA EXPERIENCIA

5.1. APOORTE / LECCIONES APRENDIDAS

- a. La principal lección aprendida fue lograr una coordinación sólida y efectiva durante la implementación de controles bajo el marco NIST garantizando una adopción de prácticas de ciberseguridad en la Entidad de Microfinanzas, contribuyendo a mejorar el nivel de madurez de ciberseguridad y a proteger los activos de información críticos contra las amenazas.
- b. La sinergia alcanzada entre directivos, ejecutivos, procesos de negocio y las unidades operativas fue crítica como factor clave de éxito, sumado a la capacidad de liderazgo gracias a la experiencia y conocimientos de ciberseguridad obtenidos en mi carrera profesional.
- c. La experiencia de implementar controles de seguridad bajo el marco NIST dependió de la necesidad de comprender con el mayor detalle los activos críticos y las vulnerabilidades específicas en la Entidad de Microfinanzas. Esto implicó realizar evaluaciones de riesgos detalladas para identificar amenazas potenciales y evaluar la probabilidad de su explotación, así como responder a las observaciones de auditoría.
- d. El nivel de conciencia sobre la importancia de la seguridad tecnológica se tornó evidente durante las diferentes fases de implementación. La capacitación del personal y la concientización sobre las prácticas seguras, fueron elementos fundamentales para cumplir con los objetivos estratégicos.
- e. Los controles técnicos, como el afinamiento de las reglas en los firewalls, cifrado de datos, detección de intrusos, entre otros, se convirtieron en parte integral de la infraestructura tecnológica de la Entidad de Microfinanzas. La implementación de políticas de acceso y el monitoreo constante reforzaron las barreras contra amenazas internas y externas.

No obstante, la experiencia de implementar controles de seguridad nos revela la necesidad de aplicar mejora continua en los procesos críticos de TI y del negocio permanentemente. Las amenazas de ciberseguridad evolucionan constantemente, y el marco NIST proporcionó un modelo flexible que permitió ajustar las estrategias de ciberseguridad.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.2. CONCLUSIONES

Las conclusiones obtenidas antes, durante y después de la implementación de los controles son:

- a. La implementación de los controles de seguridad en la Entidad de Microfinanzas bajo el marco NIST fue un gran logro más allá de la tecnología, permitiendo elevar la madurez organizativa y comprometer a las personas claves. Resulto imperativo un compromiso continuo con la evaluación en conjunto de los riesgos de tecnología, la adopción de mejores prácticas y la adaptación constante a un entorno de amenazas en evolución.
- b. La realización de una revisión periódica de los controles y garantizar la actualización de las políticas de seguridad en todos los dominios críticos, fue determinante para responder a las amenazas, vulnerabilidades detectadas y compromisos regulatorios vigentes.
- c. La priorización de la seguridad tecnológica con controles mucho más robustos, dio como consecuencia que la Entidad de Microfinanzas no solo protegió la información financiera, sino también fortaleció la confianza con el cliente en un mundo digital desafiante y cada vez más interconectado.
- d. La implementación de controles de seguridad en la Entidad de Microfinanzas, siguiendo el marco NIST, fue un proyecto complejo de vital importancia en la era digital actual, en donde fue necesario contar con personas altamente calificadas comprometidas con su crecimiento profesional al continuar desarrollando la pasión por la ciberseguridad. En adición, contribuyó a fortalecer las relaciones con los proveedores estratégicos de ciberseguridad.
- e. El desarrollo del proceso no solo implicó la aplicación de procedimientos técnicos, sino también la adopción de una mentalidad proactiva hacia la protección de la información, la mejora de la cultura organizacional y la sinergia de muchas unidades internas.

5.3. RECOMENDACIONES

Resulta relevante brindar algunas recomendaciones configuradas a razón de la experiencia obtenida a lo largo de mi desarrollo profesional y que todo líder de la ciberseguridad puede poner plasmar en su organización.

- a. Mantener la cohesión y sinergia de tu equipo de trabajo, quienes provienen de distintos dominios tecnológicos. Resulta imperativo una gran capacidad del líder de mantener la interacción en todos los niveles.
- b. Comunicar entre los actores claves de manera recurrente los objetivos de TI y del negocio, así como del amplio conocimiento de marcos, procedimientos y lineamientos regulatorios dirigidas a entidades financieras.
- c. Identificar prematuramente los puntos de dolor en cualquier etapa, para encontrar una rápida solución y no afectar la ruta crítica de cualquier proyecto.
- d. Reclutar personal altamente calificado y mantener un buen clima laboral resulta relevante en toda organización; así como, garantizar que todos los colaboradores tengan una buena base de prácticas de seguridad de forma holística.
- e. Exponer planteamientos claros a la Alta Dirección en aras de conseguir el apoyo financiero. Resulta imprescindible que se convierta en un valorado sponsor y que la organización pueda asumir riesgos durante las etapas.
- f. Mantener comunicación con sus pares de otras instituciones financieras y estar informado de las nuevas técnicas, herramientas y servicios ofrecidos por nuestros competidores. La actualización profesional es insoslayable.

5.4. FUENTES DE INFORMACIÓN

a. Libros:

CYBER SECURITY ESSENTIALS

Edited by James Graham, Richard Howard, Ryan Olson
2011 by Taylor and Francis Group, LLC

Cisco SAFE Implementation Student Guide

Version 2.0
2004, Cisco Systems, Inc.

b. Artículos

Cyber Assessment Framework V3.1

Version as of 11/04/2022
2022

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1
National Institute of Standards and Technology
April 16, 2018

Multi Source Analysis of the Top MITRE ATT&CK Techniques

Cyentia Institute.
2022

c. Sitios web de interés

<https://www.nist.gov/>

Portal oficial del marco de referencia NIST

<https://www.cisecurity.org/>

Portal del Centro de Seguridad de Internet.

<https://attack.mitre.org/>

Portal de la organización MITRE ATT&CK

5.4. GLOSARIO

ASA: Por sus siglas en inglés: Método Estándar Alternativo. Método para determinar el nivel de liquidez que una entidad financiera puede disponer para otorgar productos financieros en función al riesgo operacional.

Ciberseguridad: es la práctica de proteger dispositivos, redes, aplicaciones, sistemas críticos y datos de posibles amenazas tecnológicas.

CISO (Chief Information Security Office): persona que se encarga de dirigir, orientar y coordinar la estrategia de seguridad de una empresa.

Cloud: conjunto de servicios de computación en la nube diseñados para hacer frente a las necesidades del negocio.

Comités CAI y CAB: el primero por sus siglas Comité de Alto Impacto para revisar la criticidad e importancia de los proyectos o desarrollos dentro del marco estratégico y el segundo por sus siglas en inglés (Change Advisory Board o Comité Asesor de Cambios), comité que determina y aprueba los pases a producción.

CyberSOC: Centro de Operaciones de Ciberseguridad altamente especializado en la modalidad 24x7, conformado por infraestructura y profesionales expertos en ciberseguridad, procesos automatizados y tecnología con la capacidad de monitorear, detectar, contener y responder frente a eventos e incidentes de ciberseguridad.

DLP: del inglés Data Loss Prevention, prevención de pérdida de datos, sirve para garantizar que los usuarios no envíen información delicada o crítica fuera de la organización.

Firewall: sistema de seguridad de red que restringe el tráfico de Internet entrante, saliente o dentro de una red corporativa.

IDS/IPS: los Sistemas de Detección de Intrusos (IDS) como los Sistemas de Prevención de Intrusos (IPS) aumentan la seguridad de las redes vigilando el tráfico, y para ello examinan la red y los puertos, analizando paquetes de datos, para detectar patrones sospechosos.

ISO 27001: estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información.

ISO 27032: estándar cuyos objetivos principales son: Identificación de riesgos cibernéticos: La norma ayuda a las organizaciones a identificar los riesgos cibernéticos a los que podrían estar expuestas, tanto interna como externamente. Esto abarca desde amenazas de malware hasta ataques de ingeniería social.

ISO 31000: norma internacional para la gestión del riesgo. Al proporcionar principios integrales y directivas, esta norma ayuda a las organizaciones con su análisis y evaluación de riesgos

ITIL: El marco de ITIL está basado en un ciclo de vida del servicio y consiste de cinco etapas (estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio) que cuentan con su propia publicación de apoyo.

KPI: Sigla que proviene de la frase en inglés key performance indicator (indicador clave de rendimiento), es una métrica cuantitativa que muestra cómo tu equipo o empresa progresa hacia tus objetivos empresariales más importantes.

Ley 29733: ley de protección de datos personales que regula aquellos casos en los que se requiere solicitar autorización al titular de los datos personales para su tratamiento.

On-premise: en español “en las instalaciones propias” y se refiere a la utilización de servidores y entornos tecnológicos propios de la empresa.

Seguridad TI: denominado seguridad informática y se encarga de mantener la confidencialidad de los datos la Entidad de Microfinanzas y de recuperar el control mediante el uso de recursos de gestión de riesgos en el caso de que se haya producido algún incidente.

SIEM: información sobre seguridad y gestión de eventos o SIEM (Security Information and Event Management) es un sistema de seguridad que persigue proporcionar a las empresas una respuesta rápida y precisa para detectar y responder ante cualquier amenaza sobre sus sistemas informáticos.

SWIFT: Sociedad para las Comunicaciones Interbancarias y Financieras Mundiales.

Tecnologías de la Información (TI): aplicación de computadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos.

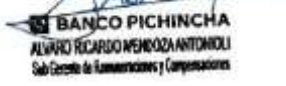
Thales HSM Payshield 10K: módulo de seguridad de hardware (HSM) certificado para realizar tareas tales como la validación y protección de PIN, procesamiento de transacciones, emisión de tarjetas móviles y de pago, y administración de claves.

VPN Palo Alto Global Protect: GlobalProtect Clientless VPN proporciona acceso remoto seguro a aplicaciones web empresariales comunes. Los usuarios tienen la ventaja de un acceso seguro desde navegadores web habilitados para SSL sin instalar el software GlobalProtect.

WAF: un Web Application Firewall (WAF) protege de múltiples ataques al servidor de aplicaciones web en el backend. La función del WAF es garantizar la seguridad del servidor web mediante el análisis de paquetes de petición HTTP / HTTPS y modelos de tráfico.

ANEXOS

1. CERTIFICACIONES

 BANCO PICHINCHA Se trata de ti.	Oficina Principal Av. Ricardo Palma 278, Miraflores T. (51) 612 2000 www.pichincha.pe  Banco Pichincha Perú
Miraflores, 11 de MAYO del 2023 CERTIFICADO DE TRABAJO A quien corresponda: Hacemos de conocimiento que el(la) Señor(a)(ita) LUIS FERNANDO CORRO QUISPE ha laborado en nuestra Institución desde el 28/05/2021 hasta el 11/05/2023 desempeñándose a la fecha de su retiro como JEFE DE SEGURIDAD TI. Atentamente,  	



IBM del Perú S.A.C.
av. Javier Prado N° 6230,
Lima 12 - Perú
Apartmento Postal 151 Lima 100

CERTIFICADO DE TRABAJO

El que suscribe, en representación de **IBM DEL PERU S.A.C.** con RUC N°
20100075009,

CERTIFICA

Que, el(la) Sr(a), **Luis Fernando Corro Quispe**, quien se identifica con DNI N°
40036211, ha laborado en nuestra empresa desde el **14 de setiembre de 2015**, en el
área de **Global Technology Services**, siendo su fecha de cese el **30 de abril de 2021**.

Se expide el presente documento, de acuerdo a Ley, para los fines que la parte
interesada crea conveniente.

Anabella Cordero de Castro
HR Manager Perú, Ecuador, Bolivia
IBM del Perú S.A.C.

Lima, 30 de abril de 2021

Certificado de Trabajo

Certificamos que el señor **Luis Fernando Corro Quispe** ha formado parte de nuestro personal desde 11 de julio de 2001 hasta el 31 de octubre de 2013, siendo su último puesto SUB GTE ADJ. GESTIÓN DE SERVICIOS DE TL.

El señor Corro Quispe, durante 12 año(s), 3 mes(es) y 20 día(s) de permanencia en nuestra Institución, desempeñó las labores encomendadas, demostrando responsabilidad, honestidad, espíritu de colaboración y eficiencia.



Gladys V. Alvarado
Asistente de Administración CDH
Gestión y Desarrollo Humano

Banco de Crédito BCP
División de Gestión y Desarrollo Humano



Maria Mendoza V.
Asistente de Administración CDH
Gestión y Desarrollo Humano

La Molina, 31 de octubre de 2013.

Mat: 0U17727

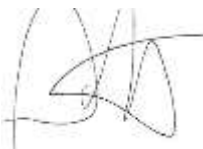
LIMA 8 DE ENERO DEL 2014

CERTIFICADO DE TRABAJO

El presente documento certifica que el señor Luis Fernando Corro Quispe, ha trabajado como Consultor Senior Independiente y Project Manager en nuestra representada para el Proyecto de Análisis para la Migración de un DATACENTER efectuado entre el mes de noviembre y diciembre del año 2013 para una entidad financiera local.

Su desempeño durante el presente servicio prestado fue profesional, ético y responsable.

Atentamente,



Dante Soto Velez De Villa
GERENTE GENERAL
WRSOFT S.A.C.

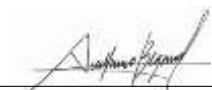
DANTE SOTO VELEZ DE VILLA
GERENTE GENERAL DE WRSOFT SAC

Certificado de Educación Profesional Continua

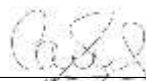
Otorgado a: **Luis Fernando Corro Quispe**

Por su participación en el Curso de Preparación para la Certificación Internacional "CISM" 01-2020 en modalidad virtual, organizado por ISACA Lima Chapter 146, los días 09, 16, 23 y 24 de mayo de 2020, con una duración de 28 horas lectivas. En cumplimiento de la Política de Educación Continua CISA, CISM, CGEIT y CRISC de ISACA Internacional, se le acredita 28 Horas CPE.

Lima, 30 de mayo de 2020



Guillermo Zegarra Cerna,
CRMA, CRISC, CICA, ISO 22301 LA, CobIT-F
Presidente ISACA Lima, Perú Chapter 146



José Carlos Vargas Medina,
MBA, CISA, CISM, CRISC, Comptia Security +, MCSA, MCSE
Vice Presidente - ISACA Lima, Perú Chapter 146

PECB



Professional Evaluation and Certification Board

hereby attests that

LUIS FERNANDO CORRO QUISPE

is awarded the title

PECB Certified ISO 31000 Lead Risk Manager

having met all the certification requirements, including all examination requirements, professional experience and adoption of the PECB Code of Ethics

Certificate Number: RMLM1057256-2020-03

Issue Date: 2020-03-20

This certificate is valid for three years for the purpose of PECB certification

A handwritten signature in black ink, appearing to read 'Carolina Cabezas'.

Carolina Cabezas, Compliance
Director

PECB

BEYOND
RECOGNITION

Attendance Record

This document confirms that

LUIS FERNANDO CORRO QUISPE

Has attended the training course

ISO/IEC 27001 Lead Implementer

This attendance record is valid for 31 Continuing Professional Development (CPD) credits

Held at: Lima, Peru
Course completion date: May 15th, 2020

PECB
6683 Jean Talon E, Suite 336
Montreal, QC
H1S 0A5 Canada
training@pecb.com



Tim Rama, Deputy CEO

PECB

BEYOND
RECOGNITION

Attendance Record

This document confirms that

LUIS FERNANDO CORRO QUISPE

Has attended the training course

ISO/IEC 27032 Lead Cybersecurity Manager

This attendance record is valid for 31 Continuing Professional Development (CPD) credits

Held at: Lima, Peru
Course completion date: March 19th, 2021

PECB
6683 Jean Talon E, Suite 336
Montreal, QC
H1S 0A5 Canada
training@pecb.com



Tim Rama, Deputy CEO



La Directora de Servicios Académicos y Registro de Postgrado de la Universidad del Pacífico, quien suscribe,

CERTIFICA

que don(ña) **LUIS FERNANDO CORRO QUISPE** estuvo matriculado(a) como alumno(a) regular en el **Curso Especializado para Ejecutivos Gestión de Riesgos de TI y Ciberseguridad**, desarrollado del 7 de marzo al 25 de abril de 2023, en un total de 21 horas, cursando la asignatura que se indica, con la calificación que se señala:

CURSO

Gestión de Riesgos de TI y Ciberseguridad	(21 horas)	Dieciséis y 00/100	(16.00)
---	------------	--------------------	---------

Nota: La nota mínima aprobatoria para el curso es once y 00/100 (.00)

Lima, 12 de junio de 2023

Olga Giselle de la Torre Delgado
Directora de Servicios Académicos y Registro
de Postgrado



Identificador I+Ti VcSp 0mMT VKMP rTNQ TCLI n7c=

Esta es una copia auténtica imprimible de un documento electrónico archivado por la Universidad del Pacífico, aplicando lo dispuesto por el artículo 25 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública - Decreto Supremo N° 072-2003-PCM, que fue incluido por el artículo 3 del Decreto Supremo N° 070-2013-PCM, y la Tercera Disposición Complementaria Final del Decreto Supremo N° 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web:
<https://universidadpacifico.administracionelectronica.net/SedeElectronica/verifyDocs.jsp>



UNIVERSIDAD ESAN

Confíete este certificado a

Luis Fernando Corro Quispe

por haber concluido y aprobado el curso de

Gerencia de Proyectos de Tecnologías de Información

desarrollado en 16 sesiones de clase de una hora y treinta minutos cada una, en el III Programa de Especialización para Ejecutivos 2006, en la ciudad de Lima, del 05 de junio al 11 de agosto de 2006.

ALBERTO ZAPATER C.
DECANO



III PROGRAMA DE ESPECIALIZACION PARA EJECUTIVOS 2006
(Del 05 de junio al 11 de agosto de 2006)

CERTIFICADO DE NOTAS

NOMBRE : Luis Fernando Corro Quispe
CURSO : Gerencia de Proyectos de Tecnologías de Información
NOTA : 15 (quince)

El curso se desarrolló en 16 sesiones de clase de una hora y treinta minutos cada una.

Nuestra escala de notas va de uno a veinte. Doce es el mínimo aprobatorio.

Lima, 08 de agosto de 2006


Patricia Reveggino Sosa
Jefe de Admisión y Registro





This is to certify that

Luis Fernando Corro

successfully completed and received a passing grade in

Big Data 10 1

(BD0101EN, provided by **Cognitive Class**)

an online course on **Cognitive Class**.

December 20, 2019

Authenticity of this certificate can be validated by going to:

<https://courses.cognitiveclass.ai/certificates/97a871de30d34a53b36b1a419efe2638>



This is to certify that

Luis Fernando Corro

successfully completed and received a passing grade in

Blockchain Essentials

(BC0101EN, provided by **developerWorks**)

an online course on **Cognitive Class**.

October 4, 2018

Authenticity of this certificate can be validated by going to:

[https:// courses.cognitiveclass.ai/ certificates/ 94a66149a91b464abe 0aa8bf0265d8b0](https://courses.cognitiveclass.ai/certificates/94a66149a91b464abe0aa8bf0265d8b0)

CERTIFICATE

This is to certify that

LUIS CORRO

has successfully demonstrated knowledge to
meet the requirements of the

**ITIL® VERSION 3 FOUNDATION
EXAMINATION**



Julia Chapelle
Director, Loyalist Certification Services
April 04, 2011

Candidate 914045

ITIL® is a Registered Trade Mark of the Office of Government
Commerce in the United Kingdom and other countries.



APM GROUP

OGC



00091216



IBM Learning Completion Certificate



This certificate is presented to

Luis Fernando Corro

for the completion of

Agile@IBM - A Taste of Agile

(AA-3469)

According to the Agile Academy system of record

Completion date: 11 Jul 2018

Learning hours: 2 hrs 3 mins




Completion Certificate




This certificate is presented to

Luis Fernando Corro

for the completion of

Agile@IBM - Operations Fundamentals

(AA-3563)

According to the Agile Academy system of record

Completion date: 11 Jul 2018

Learning hours: 1 hr 21 mins

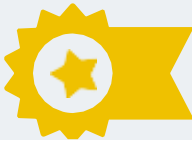
The next generation Your Learning experience is here! [Try it out](#) and tell us what you think.



Menu







This certificate is presented to
Luis Fernando Corro
for the completion of
DevOps Learning path for DevOps Essentials badge
(SMT_GBS-R728)
According to the SMARTERon IBM Cloud system of record

1 de 1

IBM Learning Completion Certificate



This certificate is presented to

Luis Fernando Corro

for the completion of

Blockchain

(ITA-BLOCKCHAIN)

According to the Think Academy system of record

Completion date: 03 Oct 2018

Learning hours: 30 mins

Your Learning • Certificate of Completion: ITA-BLOCKCHAIN

<https://yourlearning.ibm.com/#certificate/ITA-BLOCKCHAIN/IT...>

3/10/18 17:31