UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

ESCUELA DE POSGRADO
PROGRAMA DE MAESTRÍA EN DIRECCIÓN DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN

Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones

TESIS

Para optar el grado académico de Maestro en
Dirección de Sistemas y Tecnologías de la Información

AUTOR

Vilcarromero Zubiate, Ladi Lizeth (0000-0001-6628-3494)
Vilchez Linares, Evit (0000-0001-9628-4500)

ASESOR DE TESIS

Mejia Tarazona, Ronald (0000-0002-3232-3918)

Lima, 06 de agosto del 2018

Dedicado a:

A Dios por permitirme alcanzar esta meta tan importante y darme la fortaleza para continuar día a día, a mis hijas Angela y Valeria por ser el pilar de mi vida, darme su amor y apoyo incondicional, a mi esposo Carlos por estar a mi lado en todo momento incentivándome para cumplir con mis objetivos, a mis amigos quienes me han dado su mano cuando más lo necesitaba, compartiendo experiencias enriquecedoras tanto en lo profesional y personal.

A Dios, por haberme guiado hasta este punto y haberme dado voluntad para lograr mis objetivos.
A mi madre Delicia, por haberme apoyado en todo momento, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.
A mi padre Belisario, por el valor mostrado para salir adelante y por los ejemplos de paciencia y perseverancia que lo caracterizan y que me ha infundado siempre.
A mi hermana Fiorella, por estar conmigo compartiendo en todo momento y por estar dispuesta en ayudarme en cualquier momento, te quiero mucho.
A mi amiga Ladi, por haberme ayudado a realizar este trabajo y por compartir sus retos y consejos.
A mis familiares y amigos, aquellos que participaron directa o indirectamente en la elaboración de esta tesis.

Resumen

La seguridad nacional y económica de los países depende del funcionamiento confiable de su infraestructura crítica. Las amenazas de ciberseguridad explotan la creciente complejidad de dichos sistemas, colocando la economía, la seguridad pública y la salud en riesgo. Al igual que el riesgo financiero y de reputación, el riesgo de ciberseguridad afecta a los objetivos estratégicos de una empresa. Puede aumentar los costos y afectar los ingresos. Puede dañar la capacidad de una organización para Innovar, brindar servicios, ganar y mantener a los clientes.

Así mimo, la información se ha convertido en uno de los activos más importantes para cualquier organización, y el aseguramiento de la misma como un punto primordial para lograr ventajas competitivas y generación del valor, basando en el adecuado resguardo de la Confidencialidad, Disponibilidad e Integridad de la Información.

El propósito del presente trabajo es desarrollar y proponer un método que permita gestionar la ciberseguridad en empresas del sector telecomunicaciones sobre la base de una adecuada gestión del riesgo y la medición de controles según un nivel de madurez.

Este método propuesto se encuentra basado en el Cyber Security Framework (CSF) del National Institute of Standards and Technology (NIST) promulgada por el Presidente Obama mediante la Orden Ejecutiva (EO) 13636.

Palabras clave: Ciberseguridad, Infraestructuras Criticas, Telecomunicaciones, CSF, NIST.

Abstract

The national and economic security of the countries depends on the reliable operation of their critical infrastructure. Cybersecurity threats exploit the increasing complexity of these systems, putting the economy, public safety and health at risk. Like financial and reputation risk, cybersecurity risk affects the strategic objectives of a company. It can increase costs and affect income. It can damage the ability of an organization to innovate, provide services, earn and maintain customers.

Likewise, information has become one of the most important assets for any organization, and the assurance of it as a fundamental point to achieve competitive advantages and generation of value, based on the appropriate protection of Confidentiality, Availability and Integrity of the information.

The purpose of this paper is to develop and propose a method for managing cybersecurity in companies in the telecommunications sector on the basis of an adequate risk management and the measurement of controls according to a level of maturity.

This proposed method is based on the Cyber Security Framework (CSF) of the National Institute of Standards and Technology (NIST) promulgated by President Obama through Executive Order (EO) 13636.

Keywords: Cybersecurity, Critical Infrastructures, Telecommunications, CSF, NIST

Índice de Contenido

Índice de tablas

Índice de figuras

CAPÍTULO 1: MARCO TEORICO

Cuando se plantea la implementación de un nuevo modelo de Gestión de Ciberseguridad para el área de servicios de seguridad de una empresa Telco, se propone con la finalidad de alinear los objetivos estratégicos de la organización, definiendo: funciones, procesos, roles, y responsabilidades que aseguren las actividades del modelo con el fin de generar un valor agregado a la empresa.

La gestión de la ciberseguridad tiene recién pocos años de investigación, pero con una evolución exponencial, ya que la facilidad de acceso al internet y su fácil uso trae muchos beneficios y a la vez riesgos los cuales hay que estar preparados, en la actualidad existe aportes de investigadores donde realizan investigación de modelos de ciberseguridad que se pueden aplicar a la organización[1].

Como parte de las investigaciones ACM y AIS a fines de diciembre del 2017 se están desplegando una nueva carrera sobre Cybersecurity, la cual contempla las áreas de Seguridad de Datos, seguridad de Software, Seguridad de componentes, Seguridad de Conexión, Seguridad de Sistemas, Seguridad de personas, Seguridad Organizacional y Seguridad Social.[2]

A partir de las investigaciones realizadas en este capítulo se busca agrupar y categorizar los diversos conceptos del entorno de la ciberseguridad que nos ayudara para el planteamiento de nuestra propuesta de diseño.

1.1. Antecedentes

1.1.1. Antecedentes a nivel Internacional

En las regiones desarrolladas del mundo, las estrategias de ciberseguridad tienen un enfoque integral, que abarca aspectos económicos, sociales, educativos, jurídicos, de aplicación de la ley, técnicos, diplomáticos, militares y relacionados con la inteligencia[3]. Las consideraciones de soberanía en la formulación de políticas de ciberseguridad son cada vez más relevantes y se puede notar una mayor participación de los militares y de las ramas de inteligencia del gobierno. Sin embargo, cuando las estrategias de ciberseguridad se centran exclusivamente en asuntos militares y de inteligencia, es posible que no alcancen un equilibrio adecuado entre la seguridad y los derechos, tales como la privacidad y la libertad de expresión y de asociación.

Los ataques informáticos que fueron víctimas en el 2016: Yahoo!, Dropbox e incluso el Partido Demócrata de EE. UU., La OEA (Organización de los Estados Americanos) y el BID (Banco Interamericano de Desarrollo) Conscientes de estas amenazas publicaron el informe sobre Ciberseguridad en el 2016[4], donde se analizan la situación de 32 países de la región. Para el caso

[1] (Gestión, 2017)
[2] (CSEC2017, 2017)
[3] BID ONU
[4] (¿Estamos preparados en América Latina y el Caribe?, 2016)

de Perú, si bien se destaca la existencia de normas importantes, entre ellas, la Ley 30096 de delitos informáticos y la Ley 29733 de protección de datos personales, también hace mención "la ausencia de una estrategia y una cadena de mando clara la cual sigue impidiendo el fortalecimiento de la ciberseguridad en el país"[5].

Para la OEA y El BID, El C2M2 (Modelo de madurez de capacidad de ciberseguridad) fue identificado, organizado y documentado por expertos en la materia del sector energético de organizaciones públicas y privadas donde consideran a la ciberseguridad a través de cinco dimensiones: la Política y estrategia, Cultura y sociedad, Educación, Tecnologías y Marco Legales, donde las evalúa en cinco niveles de madurez (Inicial, Formativo, Establecido, Estratégico y Dinámico) de la capacidad de ciberseguridad se encuentra en cada país[6]. En este mismo informe hace mención que el estado situacional de la Ciberseguridad en América Latina contempla la interacción entre la ciberseguridad y los derechos fundamentales. Para este estudio se realizó la aplicación del Modelo de Madurez de Capacidad de Ciberseguridad (C2M2 - Cybersecurity Capability Maturity Model) patrocinado por el Departamento de Energía (DOE) quien desarrolló el Modelo de Madurez de Capacidad de Ciberseguridad (C2M2) del Modelo de Madurez de Capacidad de Ciberseguridad del Subsector de Electricidad (ES-C2M2) Versión 1.0 eliminando referencias y terminología específicas del sector. El ES-C2M2 es desarrollado con el apoyo de una iniciativa de la Casa Blanca dirigida por el DOE, en asociación con la Departamento de Seguridad Nacional (DHS), y en colaboración con el sector privado y público expertos[7]. El C2M2 es un proceso de evaluación voluntario que utiliza prácticas de ciberseguridad aceptadas por la industria que se puede usar para medir la madurez de las capacidades de ciberseguridad de una organización. El C2M2 está diseñado para medir tanto la sofisticación y el mantenimiento de un programa de ciberseguridad.

1.1.2. Ciberseguridad en el Perú y en Latinoamérica

La situación y el problema actual que el Perú presenta en materia de ciberseguridad nos indica que el ente encargado de los protocolos de seguridad de las tecnologías de la información del Estado es la Oficina Nacional de Gobierno Electrónico, y como tal se encarga de liderar los proyectos, la normatividad, y las diversas actividades que en materia de Gobierno Electrónico realiza el Estado. Según[8], el especialista Mario Sánchez Debernardi, refiere que en el Perú, la ciberseguridad en instituciones del estado se encuentra en una etapa inicial, y según[9] En lo que menos se ha avanzado es en aspectos de medidas de organización y capacitación, pues no se cuenta con una Agencia Nacional de Ciberseguridad, La Secretaría de Gobierno Digital (SeGDi) es el órgano de línea, con autoridad técnico normativa a nivel nacional, responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de Informática y Gobierno Electrónico. Asimismo, es el órgano rector del

[5] (Ley, 2016)
[6] (Desarrollo, 2016)
[7] ((C2M2), 2014)
[8] (Ciberseguridad en instituciones del Perú es aún incipiente, 2015)
[9] (Secretaría nacional de Seguridad y Defensa, 2015)

Sistema Nacional de Informática y brinda asistencia técnica en la implementación de los procesos de innovación tecnológica para la modernización del Estado en coordinación con la Secretaría de Gestión Pública[10], por la tanto se ve necesario establecer una política de protección tecnológica, y más aún cuando sabemos que existen instituciones encargadas del agua, luz, telecomunicaciones, etc., que pueden ser afectados por ciberataques, perjudicando a los consumidores. Además, se recalca que en el Perú desde el 2015, no existe una política nacional sobre ciberseguridad[11], y aunque no se han presentado problemas serios en esa materia, que también justifica el que las empresas no le toman una especial atención[12], es importante que se tomen previsiones del caso. Se afirma también que, en el Perú, las empresas solo destinan un 3.8 % de su presupuesto de tecnología a la ciberseguridad tanto para protección interna como para la de sus usuarios[13]. El especialista Claudio Caracciolo, Chief Security Ambassador de ElevenPaths reveló[14] "los mayores problemas que afectan hoy a las empresas están asociados a ataques de denegación de servicios, a los famosos y mediáticos ataques persistentes (APT), asaltos a bases de datos o de información confidencial, y robo de credenciales tanto a través de medios tradicionales o incluso a través de las plataformas móviles", paso con el portal del Ministerio de defensa, como también al portal del Estado Peruano, que fueron hackeados en el 2015. Digiware, empresa experta en seguridad informática, revela en su informe anual de seguridad informática 2015-2016, que el Perú es el quinto país que más recibe ataques cibernéticos a nivel de América Latina con un 11.22% y que, a nivel global, América percibe un 19% de ataques.[15] Perú es quinto país de la región que recibe más ataques cibernéticos y esto se debe a que la cantidad de usuarios que acceden a internet es mayor a la implementación de estrategias de ciberdefensa de usuarios y empresas, y por ello Perú se ubica en tal posición dentro de este Top. Es por esto de que el Perú debería tener una política de gobierno más robusta en cuestión de ciberataques, para ello hay que destinar mayor presupuesto en seguridad digital dentro de las entidades estatales a fin de propiciar una cultura cibernética más segura y de paso motivar a instituciones privadas a sumarse a este cambio. En el 2013, Perú tenía una penetración de internet del 38,2% de la población total[16] en comparación al actual que es de un 40% es decir 12 millones de personas.[17] Hoy Perú es un eje regional de actividad y comercio digital y, por lo tanto, corren riesgos de ciberseguridad. Se afirma que los incidentes cibernéticos aumentaron un 30% en 2013 y el país experimentó también un incremento de los ataques de malware durante la Copa Mundial de 2014, que se celebró en Brasil. El Equipo de Respuesta a Incidentes de Seguridad Informática del Perú, PeCERT, fue el encargado de responder con éxito a estos ataques. [18] Además de la respuesta a incidentes, el PeCERT también trabaja con la policía, las fuerzas militares y el sector privado, en lo que asuntos de seguridad se refiere. En el Perú figuran tres leyes que guían el marco legal para la

[10] (Digital, 2017)
[11] (ANDINA: Agencia Peruana de Noticias, 2015)
[12] (Mirando al futuro. José Callo. 2016 Año de la ciberseguridad., 2016)
[13] (Tecnología. Empresas destinan sólo 3.8% de su presupuesto de tecnología a la Ciberseguridad., 2015)
[14] (Diario Perú 21, 2015)
[15] (Perú, Common Digital Perú, 2015)
[16] (OEA & Symantec. , Junio, 2014)
[17] (OEA & BID Informe, 2016)
[18] (OEA & BID Informe, 2016)

ciberseguridad del Perú: la Ley 27309, que incluye la delincuencia cibernética en el código penal; la Ley 29733 de Protección de Datos; y la Ley 30096, que establece normas jurídicas en contra de la delincuencia cibernética.

La División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú (PNP) es la unidad máxima para el manejo de la delincuencia cibernética de esta nación. Equipada con capacidad de laboratorio forense, "La DIVINDAT descubrió una serie de recientes ataques cibernéticos dirigidos contra instituciones gubernamentales de alto nivel. Entre los constantes desafíos que se enfrentan, cabe citar su limitada capacidad técnica para el manejo de evidencia electrónica en los tribunales y la falta de una política de divulgación para el sector privado"[19].

El sector privado y los operadores de infraestructura crítica nacional han adoptado algunas normas de seguridad, incluyendo procesos de desarrollo de software. La ONGEI también proporciona directrices sobre la gestión de crisis; sin embargo, el alcance de denuncia responsable sigue siendo bajo, ya que las tecnologías de seguridad y la Infraestructura Crítica Nacional (ICN) son gestionadas de manera informal. Las entidades peruanas están discutiendo la posibilidad de contar con un seguro de delincuencia cibernética y otros mecanismos para proteger mejor la ICN.

Mientras que los servicios de gobierno electrónico y comercio electrónico continúan expandiéndose en el Perú, la conciencia social de la ciberseguridad es generalmente baja. La ONGEI nos ofrece literatura en línea sobre este tema, pero no hay una amplia campaña de sensibilización que esté actualmente vigente. Muchas universidades nacionales y empresas privadas ofrecen educación y capacitación en ciberseguridad. Sin embargo, suele carecerse de tecnología adecuada y personal educativo con experiencia.

El sector privado y operadores de Infraestructura crítica nacional han adoptado algunas normas de seguridad, que incluyen a procesos de desarrollo de software. Se afirma también, que la tecnología de seguridad e Infraestructura critica nacional (ICN) son gestionadas de manera informal, lo que ocasiona que el número de denuncias responsables siga siendo bajo. En la actualidad las entidades peruanas discuten la posibilidad de contar con un seguro de delincuencia cibernética y otros mecanismos para proteger mejor la ICN. "Se afirma que la conciencia social de la ciberseguridad es en general baja''[20].

1.1.3. Las Telecomunicaciones

En los últimos años el mercado de Telecomunicaciones Móviles ha experimentado cambios importantes pues todos los países tienen objetivos que se proponen alcanzar con respecto a las telecomunicaciones (expansión de infraestructura, cierre de brechas de cobertura, mercado competido, tarifas asequibles, calidad de servicio, usuarios informados y con disponibilidad de

[19] (SCRIBD, s.f.)
[20] (OEA & BID Informe, 2016)

opciones a elegir, seguridad de la información), cada país lleva a cabo su propia política regulatoria caracterizada por su marco institucional y legal[21].

En efecto, en unos países el marco institucional es tal que la autoridad encargada de la política sectorial es la misma que regula el sector, mientras en otros países ambas entidades están separadas, en el caso de Perú existe el Organismo Supervisor de la Inversión Privada en Telecomunicaciones (Osiptel) como organismo regulador y promotor de la competencia en telecomunicaciones, el cual depende de la Presidencia del Consejo de Ministros (PCM) —el regulador no forma parte del Ministerio de Transportes y Comunicaciones (MTC) que es la entidad encargada de la política sectorial, el marco legal la Ley General de Telecomunicaciones (Decreto Supremo Nº 013-93-TCC de 1993) no ha sido modificada, ya que muchas otras leyes tal como la de portabilidad numérica móvil (Ley Nº 28999 del 2007) no la modifican sino que son normas separadas.

Las principales instituciones que emiten normas vinculadas al quehacer de las telecomunicaciones son las seis que se muestran a continuación.

Tabla 1. Principales instituciones que emiten normas vinculadas al sector Telecom
Fuente: Elaboración propia en base a información de cada institución

Institución	Funciones	Sector
Ministerio de Transportes y Comunicaciones (MTC)	Responsable de la política de telecomunicaciones del país: - Otorga y revoca concesiones - Representa al Estado en las organizaciones Internacionales y en la negociación de tratados - Administra el uso del espectro radioeléctrico	Telecom
Fondo de inversión en Telecomunicaciones (FITEL)	Fondo destinado a la provisión de acceso universal, y se encuentra adscrito a MTC: - Formula los proyectos regionales en marco de la red dorsal nacional de fibra óptica (RDNFO)	Telecom
Organismo Supervisor de la Inversión Privada en Telecomunicaciones (OSIPTEL)	- Organismo regulador y promotor de la competencia adscrito a la Presidencia del Consejo de Ministros - Sus funciones supervisar, regular, normar, fiscalizar y sancionar, solucionar controversias y solucionar reclamos de usuarios	Telecom
Congreso de la República	- Se encarga de emitir las leyes, tanto por iniciativa legislativa, como del Poder Ejecutivo - La función legislativa comprende el debate y la aprobación de reformas de la	Multisectorial

[21] (Osiptel, s.f.)

Institución	Funciones	Sector
	constitución, de leyes y resoluciones legislativas, así como su interpretación, modificación y derogación	
Agencia de Promoción de la Inversión Privada (PROINVERSION)	- Promueve la incorporación de inversión privada en servicios públicos y obras públicas de infraestructura - Es el encargado del proceso de licitaciones de espectro y de los proyectos formulados por FITEL	Multisectorial
Instituto Nacional de Defensa de la competencia y de la Protección de la Propiedad Intelectual (INDECOPI)	- Tiene como funciones la promoción del mercado y la protección de los derechos de los consumidores (multisectorial). - Tiene la competencia exclusiva para investigar y sancionar los actos de competencia desleal desarrollados mediante la actividad publicitaria. - La Comisión de Eliminación de Barreras Burocráticas tiene como función velar por que las entidades del Estado no impongan barreras burocráticas	Multisectorial

El marco legal, para propósitos de exposición se estructura la normativa de telecomunicaciones en cinco grandes temas[22].

- Marco General: Ley general de telecomunicaciones, Política nacional de banda ancha, Marco institucional, Aportes de operadores (por regulación, canon, concesiones, etc.) Calidad regulatoria
- Infraestructura: Plan nacional de atribución de frecuencias, numeración y señalización, Licitaciones de espectro, Red dorsal nacional de fibra óptica (RDNFO) y proyectos regionales, Plan satelital, Televisión digital terrestre (TDT), Ley de antenas, Operador de infraestructura móvil rural (OIMR), Acceso y compartición de infraestructura, Sistema de Mensajería de Alerta Temprana de Emergencias (SISMATE)
- Competencia: Normas de interconexión, interoperabilidad y comercialización de tráfico, Determinación de proveedores importantes, Operador móvil virtual (OMV), Portabilidad numérica, Neutralidad de red, Represión de conductas anticompetitivas y competencia desleal, Solución de controversias, Usuarios
- Condiciones de uso: Registro de abonados e información de celulares robados, Reglamento de tarifas, Sistema de Información y Registro de Tarifas (SIRT), Calidad de servicio y atención, Reclamos de usuarios
- Fiscalización: Supervisiones y Sanciones[23]

[22] (Telesemana, 2017)
[23] (Javier Morales Fhon, 2017)

1.1.4. Tendencias de Ciber Ataque

La consiente importancia de desarrollar estrategias de Ciberseguridad está en aumento entre países de toda la región de América Latina y del Caribe (ALC). Algunos de ellos ya tienen una estrategia en operación, como Colombia, Jamaica, Panamá y Trinidad y Tobago. Otros países están en proceso de su desarrollo, como Costa Rica, República Dominica, Perú, Paraguay y Suriname. El nivel de madurez de estas estrategias varía, incluso en términos de proporcionar un marco para la cooperación entre los organismos gubernamentales y con actores externos[24].

La cooperación entre los países de ALC interesados es notable. Se puede encontrar, por ejemplo, en la creación de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), que se han generalizado en toda la región. La colaboración entre los CSIRT nacionales ha permitido el intercambio de conocimientos y buenas prácticas, lo que ha llevado a la creación de sistemas de comunicación más seguros y robustos. La mejora de las capacidades nacionales es importante para aumentar la confianza en los servicios digitales públicos y privados, que allanan el camino para una economía digital emergente y la gobernanza electrónica fiable. “Para los países de ALC se podrían avanzar hacia un nuevo concepto de Ciberseguridad que no deriva solamente de los dominios militares y de defensa, sino también de los derechos humanos”[25].

Otra regulación en la región de ALC es de la protección de la privacidad en línea y los datos personales. Después de las revelaciones de Snowden, en 2013[26], la conciencia de la intersección entre la Ciberseguridad y los datos personales ha quedado más clara, ya que se trataba de comunicaciones electrónicas diarias. A medida que Internet se ha vuelto esencial para el desarrollo socioeconómico de América Latina, las consecuencias de no protegerla pueden afectar la confianza de las actividades en línea, que tiene consecuencias potencialmente negativas para la economía de Internet y en la sociedad en su conjunto.

1.2. Definiciones y conceptos

1.2.1. Seguridad de la Información

Seguridad de la Información es el término más utilizado en los últimos tiempos ya que la información se considera como un activo que brinda valor al negocio; por lo que se necesita tener un adecuado manejo para protegerla frente a las amenazas y vulnerabilidades que está expuesta. La información puede adoptar distintas formas, de ahí surge la importancia de conocerlas para poder protegerla adecuadamente.

Según la norma ISO-IEC-27001-2013 la adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de seguridad de la información en una organización está influenciado por las necesidades y objetivos de la organización, los requisitos de seguridad,

[24] (community.icann.org, 2016)
[25] (Ciberseguridad, 2016)
[26] (Observatorio de la Ciberseguridad en America Latina y el Caribe, 2016)

los procesos organizativos utilizados y el tamaño y estructura de la organización. Se espera que todos estos factores influyentes cambien con el tiempo.

1.2.2. Ciberseguridad

El termino Ciberseguridad consiste en la protección de la información digital en los sistemas interconectados. La ciberseguridad se considera dentro de la seguridad de la información. Según Information Systems Audit and Control Association (ISACA), [27]la ciberseguridad es definida como "protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados". La ciberseguridad se enfoca principalmente a la información de tipo digital y los sistemas interconectados que lo procesan, almacenan o transmiten, por lo que tiene un mayor acercamiento con la seguridad informática.

1.3. Normas y marcos de trabajo de ciberseguridad.

1.3.1. ISO/IEC 27032

La ISO 27032, fue preparada por el Comité Técnico ISO/IEC JTC 1 encargados de la Tecnología de la Información, el Subcomité SC 27 mediante las Técnicas de Seguridad Informática, esta ISO contiene un estándar que garantiza directrices de seguridad que desde la organización han asegurado que "proporcionará una colaboración general entre las múltiples partes interesadas para reducir riesgos en Internet". Más concretamente, ISO/IEC 27032 proporciona un marco seguro para el intercambio de información, el manejo de incidentes y la coordinación para hacer más seguros los procesos[28].

La ISO 27032 proporciona un marco de orientación para mejorar el estado de la Ciberseguridad, usando para ello los aspectos estratégicos y técnicos relevantes para esa actividad, y sus dependencias con otros dominios de seguridad, en particular[29]:

- Seguridad de la información (considerando que la información es el activo más relevante de cualquier organización)
- Seguridad en redes
- Seguridad en el Internet
- La protección de infraestructuras críticas de información

"La norma (ISO/IEC 27032) facilita la colaboración segura y fiable para proteger la privacidad de las personas en todo el mundo. De esta manera, puede ayudar a prepararse, detectar, monitorizar y responder a los ataques"[30]. La organización espera que ISO/IEC 27032 permita luchar contra ataques de ingeniería social, hackers, malware, spyware y otros tipos de software no deseado.

[27] (welivesecurity.com, s.f.)
[28] (Computerworld, 2012)
[29] (Gianncarlo Gómez Morales, 2017)
[30] (García, 2012)

1.3.2. ISO 31000:2009 Gestión del Riesgo, principios y directrices

ISO 31000: 2009 proporciona principios y directrices sobre la gestión de riesgos, puede ser utilizado por cualquier empresa pública, privada o comunitaria, asociación, grupo o individuo. Por lo tanto, la norma ISO 31000: 2009 no es específica para cualquier industria o sector, esta norma internacional establece un conjunto de principios que se deben satisfacer para que la gestión del riesgo sea eficaz, además recomienda que las organizaciones desarrollen, implementen y mejoren de manera continuada un marco de trabajo cuyo objetivo sea integrar el proceso de gestión del riesgo en los procesos de gobierno, de estrategia de planificación, de gestión, y de elaboración de informes, así como en las políticas, los valores en la cultura de toda la organización.[31]

ISO 31000: 2009 se puede aplicar a lo largo de la vida de una organización, y para una amplia gama de actividades, incluidas las estrategias y decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos.

Esta norma está destinada a satisfacer las necesidades de un rango amplio de partes involucradas, incluyendo:

- Aquellos responsables del desarrollo de la política de gestión del riesgo dentro de la organización.
- Aquellos responsables de garantizar que el riesgo se gestiona eficazmente dentro de la organización como unidad o dentro de un área, proyecto o actividad específicos;
- Aquellos que necesitan evaluar la eficacia de una organización en cuanto a la gestión del riesgo.
- Aquellos que desarrollan normas, guías, procedimientos y códigos de práctica que, parcial o totalmente, establecen la manera de gestionar el riesgo dentro del contexto específico de estos documentos.

1.3.2.1. Análisis del riesgo

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, este último aspecto puede orientar la clasificación del riesgo, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este no se haya materializado.

Por Impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

[31] (Control, 2011)

Tabla 2. Probabilidad de Ocurrencia
Fuente: Elaboración propia

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 3 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 3 años.
3	Posible	El evento podría ocurrir en algún momento	Al menos de una vez en los últimos 2 años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de una vez en el último año.
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año.

Tabla 3. Nivel de impacto
Fuente: Elaboración propia

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Dañino	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Severo	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
	Critico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad

Tabla 4. Niveles de Madurez de los controles
Fuente: Elaboración propia

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Inexistente	Total, falta de un proceso reconocible. La organización ni siquiera ha reconocido que hay un problema que resolver.
2	Iniciado	Hay evidencia de que la organización ha reconocido que los problemas existen y que necesitan ser resueltos. Sin embargo, no hay procesos estandarizados, pero en cambio hay métodos ad hoc que tienden a ser aplicados en forma individual o caso por caso.

NIVEL	DESCRIPTOR	DESCRIPCIÓN
3	Definido	Los procedimientos han sido estandarizados y documentados, y comunicados a través de capacitación. Sin embargo, se ha dejado en manos de la persona el seguimiento de estos procesos, y es improbable que se detecten desviaciones.
4	Gestionado	Es posible monitorear y medir el cumplimiento de los procedimientos y emprender acción donde los procesos parecen no estar funcionando efectivamente. Los procesos están bajo constante mejoramiento y proveen buena práctica.
5	Optimizado	Los procesos han sido refinados hasta un nivel de la mejor práctica, basados en los resultados de mejoramiento continuo y diseño de la madurez con otras organizaciones. TI se usa en una forma integrada para automatizar el flujo de trabajo, suministrando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte con rapidez

1.3.2.2. Zonas de Riesgo y criterios de aceptación

Permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la empresa EP; de esta forma es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

A continuación, se presenta una matriz de calificación, evaluación y respuesta a los riesgos.

- Las categorías relacionadas con el impacto son: insignificante, menor, moderado, mayor y catastrófico.
- Las categorías relacionadas con la probabilidad son raro, improbable, posible, probable y casi seguro.

Tabla 5. Matriz de calificación, evaluación y respuesta a los riesgos
Fuente: Elaboración propia

PROBABILIDAD	IMPACTO				
	Insignificante [1]	Menor [2]	Dañino [3]	Severo [4]	Critico [5]
Raro [1]	B [1]	B [2]	M [3]	M [4]	M [5]
Improbable [2]	B [2]	M [4]	M [6]	M [8]	M [10]
Posible [3]	M [3]	M [6]	A [9]	A [12]	A [15]
Probable [4]	M [4]	M [8]	A [12]	A [16]	E [20]
Casi seguro [5]	M [5]	M [10]	A [15]	A [20]	E [25]

Tabla 6. Criterios de aceptación del Riesgo
Fuente: Elaboración propia

B	Zona de riesgo baja	Asumir el riesgo
M	Zona de riesgo moderada	Asumir el riesgo, evaluar reducir el riesgo
A	Zona de riesgo Alta	Reducir el riesgo, evitar, compartir o transferir
E	Zona de riesgo extrema	Reducir el riesgo, evitar, compartir o transferir

1.3.2.3. Tratamiento del riesgo

El tratamiento del riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica.

El tratamiento del riesgo implica un proceso cíclico de:

- Valoración del tratamiento del riesgo
- Decisión sobre si los niveles de riesgo residual son tolerables
- Si no son tolerables, generación de un nuevo tratamiento para el riesgo
- Valoración de la eficacia de dicho tratamiento

1.3.3. NIST

El NIST (National Institute of Standards and Technology) es una agencia del Departamento de Comercio de los Estados Unidos que promueve la aprobación de estándares sobre diversos productos y servicios relacionados con la tecnología. Entre todas sus publicaciones, son particularmente relevantes las pertenecientes a la serie SP 800, destinados a la Seguridad de la Información[32.] Marco de Ciberseguridad del NIST – Cybersecurity Framework CSF

El presidente (Obama) emitió la Orden Ejecutiva (EO) 13636, "Mejora de la Ciberseguridad de las Infraestructuras Críticas", el 12 de febrero de 2013, que establecía que "Es la política de los Estados Unidos mejorar la seguridad y la resiliencia de las Infraestructuras Criticas y mantener un entorno cibernético que fomente la eficiencia, la innovación y la prosperidad económica al mismo tiempo que promueve la seguridad, la confidencialidad comercial, la privacidad y las libertades civiles".

Como resultado de la creciente cantidad de ataques informáticos a sistemas de infraestructuras críticas y al impacto que dichos ataques pudieran tener en el contexto de la seguridad nacional de Estados Unidos, el 12 de febrero de 2013 el Presidente Barack Obama redactó la Orden Ejecutiva (EO) de Mejora de Ciberseguridad de Infraestructuras Críticas en donde se delegaba en el NIST (National Institute of Standards and Technology) el desarrollo de un marco de trabajo

[32] (NIST, s.f.)

para la reducción de riesgos asociados con este tipo de entornos, con el soporte del Gobierno, la industria y los usuarios.

1.3.3.1. Marco básico (Framework Core)

Es un conjunto de actividades de ciberseguridad. Resultados esperados y referencias aplicables que son comunes a los sectores de infraestructuras críticas, en términos de estándares de la industria, directrices y prácticas que permiten la comunicación de actividades de ciberseguridad y sus resultados a lo largo de la organización, desde el nivel ejecutivo hasta el nivel ejecutivo hasta el nivel de implementación/operación.

El framework Core consta de cinco funciones simultaneas y continuas:

- Identificar (Identify): Permite determinar los sistemas, activos, datos y competencias de la organización, su contexto de negocio, los recursos que soportan las funciones críticas y los riesgos de ciberseguridad que afectan este entorno.
- Proteger (Protect): Permite desarrollar e implementar las contramedidas y salvaguardas necesarias para limitar o contener el impacto de un evento potencial de ciberseguridad.
- Detectar (Detect): Permite desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad a través de la monitorización continua.
- Responder (Respond): Permite la definición y despliegue de actividades para reaccionar frente a un evento de ciberseguridad identificado y mitigar su impacto.
- Recuperar (Recover): Permite el despliegue de actividades para la gestión de resiliencia y el retorno a la operación normal después de un incidente.

1.3.3.2. Niveles de implementación del marco (Framework Implementation Tiers)

Los niveles de Implementación le permiten a la organización catalogarse en un umbral predefinido en función de las practicas actuales de gestión de riesgo, el entorno de amenazas, los requerimientos legales y regulatorios, los objetivos y misión del negocio y las restricciones de la propia empresa.

Tabla 7. Definiciones de Nivel de madurez
Fuente: Elaboración propia

N°	NIVEL	DESCRIPCION
1	Nivel 1: Parcial	Existen algunas iniciativas sobre ciberseguridad, aunque los esfuerzos se realizan en forma aislada. Se realizan implementaciones con enfoques ad-hoc y existe alta dependencia del personal que lleva a cabo las tareas que habitualmente no se encuentran documentadas. Existe una actitud reactiva ante incidentes de seguridad.
2	Nivel 2: Riesgo Informado	Se han establecido ciertos lineamientos o pautas para la ejecución de las tareas, pero aún existe dependencia del conocimiento individual. Se ha avanzado en el desarrollo de los procesos y existe cierta documentación para la realización de las tareas.
3	Nivel 3: Repetible	Se caracteriza por la formalización y documentación de políticas y procedimientos, así como implementaciones de alta complejidad y/o automatizaciones que otorgan centralización y permiten iniciativas de gobernanza. Las políticas y procedimientos son difundidos en el organismo,

N°	NIVEL	DESCRIPCION
		facilitan la gestión y otorgan la posibilidad de establecer controles y métricas. Los esfuerzos en ciberseguridad se enfocan en los procesos, las personas y la tecnología.
4	Nivel 4: Adaptativo	El Responsable de Seguridad de la Información (RSI) tiene un rol clave en el control y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) realizando o coordinando actividades de control interno para verificar cumplimientos y desvíos. Se desarrollan las lecciones aprendidas que junto con los controles determinan las acciones para la mejora continua. Las partes interesadas son informadas periódicamente lo cual permite alinear los esfuerzos, estrategias y tecnologías de ciberseguridad con los objetivos y estrategias del organismo.

1.3.3.3. Perfiles del Marco

Los perfiles se emplean para describir el estado actual (Current profile) de determinadas actividades de ciberseguridad. El análisis diferencial entre perfiles permite la identificación de brechas que deberían ser gestionadas para cumplir con los objetivos de gestión de riesgos.

De acuerdo con las descripciones anteriores, la arquitectura global del marco de trabajo de ciberseguridad quedaría de la siguiente manera:

Figura 1. Arquitectura del marco de trabajo de ciberseguridad del NIST (CSF)
Fuente: CSF del NIST, 2014

1.3.4. Método basado en el CSF del NIST

Las bases del CSF fueron establecidas directamente en la Orden Ejecutiva 13636:

- Identificar estándares de seguridad y guías aplicables de forma trasversal a todos los sectores de infraestructuras críticas
- Establecer un lenguaje común para gestionar riesgos de ciberseguridad
- Proveer un enfoque priorizado, flexible, repetible, neutral, basado en desempeño y efectivo en términos de coste-beneficio basado en las necesidades del negocio
- Ayudar a los responsables y operadores de infraestructuras críticas a identificar, inventariar y gestionar riesgos informáticos

- Establecer criterios para la definición de métricas para el control del desempeño en la implementación
- Establecer controles para proteger la propiedad intelectual, la privacidad de los individuos y las libertades civiles cuando se ejecuten actividades de ciberseguridad
- Identificar áreas de mejora que permitan ser gestionadas a través de colaboraciones futuras con sectores particulares y organizaciones orientadas al desarrollo de estándares
- No introducir nuevos estándares cuando existan iniciativas ya desarrolladas que cubran los objetivos de la orden ejecutiva.
- De acuerdo con el NIST: "El marco de trabajo es una guía voluntaria, basada en estándares, directrices y prácticas existentes para que las organizaciones de infraestructura crítica gestionen mejor y reduzcan el riesgo de ciberseguridad. Además, se diseñó para fomentar las comunicaciones de gestión del riesgo y la ciberseguridad entre los interesados internos y externos de la organización".

De acuerdo con lo anterior, los objetivos del marco de trabajo en su implementación en una organización se podrían catalogar en los siguientes puntos:

- Describir la postura actual de ciberseguridad
- Describir el estado objetivo de ciberseguridad
- Identificar y priorizar oportunidades de mejora en el contexto de un proceso continuo y repetible
- Evaluar el progreso hacia el estado objetivo
- Comunicación entre las partes interesadas internas y externas sobre el riesgo de ciberseguridad

Todo esto enmarcado en un enfoque orientado a la gestión del riesgo.

a) **NIST CSF PASO 1: Priorizar y determinar el alcance**

   El objetivo de este paso es comprender el enfoque actual de la gobernanza y la ciberseguridad en la empresa e identificar las partes interesadas clave, la misión de la organización, los roles y las responsabilidades.

b) **NIST CSF PASOS 2 Y 3: Oriente y cree un perfil actual**

   Ahora que las metas en cascada están completas, es hora de identificar amenazas y vulnerabilidades de esos sistemas y activos. El propósito de estos dos pasos es obtener una comprensión de los sistemas y activos de la empresa que permiten la misión descrita en el Paso 1.

   Aquí es donde los niveles de implementación del marco entran en la ecuación. Estos son niveles de implementación que pueden ayudar en la evaluación y planificación de actividades de ciberseguridad. Los niveles describen los atributos que se deben tener en cuenta al completar el perfil actual y crear un perfil objetivo más adelante, y describir la progresión de la implementación

   Este paso lleva a cabo una evaluación de estado actual utilizando el enfoque ISO 15504 para procesar la capacidad.

   Por lo tanto, un perfil actual también puede denominarse estado actual. Este es el resultado clave del paso 3. El NIST CSF proporciona una plantilla para esto.

c) NIST CSF PASOS 4 Y 5: Realizar una evaluación de riesgos y crear un perfil objetivo

El propósito de estos dos pasos es identificar las amenazas generales y las vulnerabilidades de los sistemas y activos identificados anteriormente, y determinar la probabilidad y el impacto de un ciber evento de seguridad. La finalización de estos pasos da como resultado un catálogo de posibles riesgos de seguridad y evaluación del impacto comercial, un nivel de capacidad objetivo y un perfil objetivo.

Los resultados clave de estos pasos incluyen la evaluación de riesgos de la empresa y el perfil del objetivo. El perfil de destino es similar a la plantilla de perfil actual y debe incluir la siguiente información:

- Función aplicable
- Categoría aplicable
- Subcategoría aplicable
- Referencia de COBIT 5 para identificar las prácticas requeridas para cumplir los objetivos de la subcategoría
- Calificación de logro (p. Ej., No alcanzada, parcialmente lograda, lograda en gran medida, totalmente lograda) basada en procedimientos existentes
- Prácticas, políticas y procedimientos identificados en la evaluación de riesgos
- Descripción de cómo se determinó la calificación de logro
- Acciones requeridas para alcanzar los objetivos del estado meta
- Recursos requeridos

d) NIST CSF PASO 6: Determinar, analizar y priorizar las brechas

En este paso, la empresa busca comprender y documentar las acciones necesarias para cerrar las brechas entre los entornos de estado actuales y de destino

La empresa registra las diferencias entre los estados actuales y los deseados y utiliza COBIT 5: procesos de habilitación para determinar las prácticas y actividades que deben mejorarse para cerrar las brechas. Además de las lagunas, uno debe comprender los recursos y capacidades que se requieren para llevar a cabo estos esfuerzos. Este plan de acción de actividades incluye hitos, responsabilidades y resultados deseados de acuerdo con las prioridades establecidas. Un plan de acción debe incluir lo siguiente:

- Identificación
- Prioridad
- Suposiciones y Restricciones
- Justificación
- Acciones específicas
- Recursos
- Horario / hitos
- Estado
- Prerrequisitos / dependencias
- Asignado a la acción

- Roles de los actores

e) NIST CSF PASO 7: Implementar el plan de acción

Una vez que se conocen las lagunas y se han determinado los planes para cerrar esas brechas, la empresa puede ejecutar el plan que aborda las prioridades para mejorar la seguridad y cumplir los objetivos de las partes interesadas. Este paso está alineado con el paso de implementación de COBIT 5 ¿Cómo llegamos allí? y el principio COBIT 5 Permitir un enfoque holístico.

La empresa debe considerar los desafíos, las causas y los factores de éxito de la Guía de implementación de COBIT 5, que incluyen:

- Pon a prueba el enfoque haciendo pequeñas mejoras inicialmente y para proporcionar algunas victorias rápidas
- Involucrar a todas las partes interesadas
- Mejore los procesos antes de intentar aplicar la automatización
- Establezca objetivos claros y mensurables y genere cuadros de mando que muestren cómo se mide el rendimiento
- Comunicarse en términos de impacto comercial

f) NIST CSF PASO 8: revisión del plan de acción de CSF

La empresa revisa la aplicación de las mejores prácticas de gestión y gestión, y confirma que el plan de acción entregó los beneficios esperados. Este paso está alineado con el paso de implementación de COBIT 5 ¿Llegamos allí? La empresa evalúa las actividades desde el paso de implementación para garantizar que las mejoras logren los objetivos previstos y los objetivos de gestión de riesgos. La empresa documenta las lecciones aprendidas e identifica cualquier necesidad específica de monitoreo continuo.

g) NIST CSF PASO 9: gestión del ciclo de vida del CSF

El propósito de este paso es proporcionar una revisión / evaluación continua del éxito general de la iniciativa, identificar.

CAPÍTULO 2: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

2.1. Descripción de la Empresa

Por razones de confidencialidad nos referiremos a la empresa de telecomunicaciones como la empresa EP.

EP es una empresa de telecomunicaciones, la empresa cuenta con varias líneas de negocio, las cuales son: telefonía fija local, telefonía pública y rural, larga distancia (nacional e internacional), telefonía móvil, Internet, televisión por suscripción, datos y tecnología de la información, entre otros. De éstas, las tres primeras son consideradas tradicionales, mientras que las restantes conforman la nueva oferta de servicios de la Empresa.

Adicionalmente a los servicios mencionados, EP también ofrece paquetes de servicios (Dúos y Tríos de Telefónica), los cuales están compuestos por: telefonía fija local, Internet y/o televisión por suscripción, cuyos precios, en conjunto, son menores a la suma de los precios individuales de cada uno de ellos.

2.2. Visión

La vida digital es la vida, y la tecnología forma parte esencial del ser humano. Queremos crear, proteger e impulsar las conexiones de la vida para que las personas, puedan elegir un mundo de posibilidades infinitas.

2.3. Misión

Ser una empresa OnLife Telco significa darle el poder a las personas para que ellas puedan usar los servicios digitales de telecomunicación como herramientas y elegir mejorar sus vidas.

Creemos que la tecnología forma parte de la vida de todos. Hoy, la conectividad no sirve sólo para relacionarnos, es esencial para nuestra vida personal y laboral. Nuestro papel es facilitarte el disfrute de la conexión, salvaguardando el uso de tus datos y dándote el control de tu vida digital.

2.4. Organigrama actual

El esquema organizacional de la empresa se basa en líneas de negocio los cuales están a cargo de un Gerente de Operación. La siguiente figura 2 muestra el organigrama actualizado de la empresa:

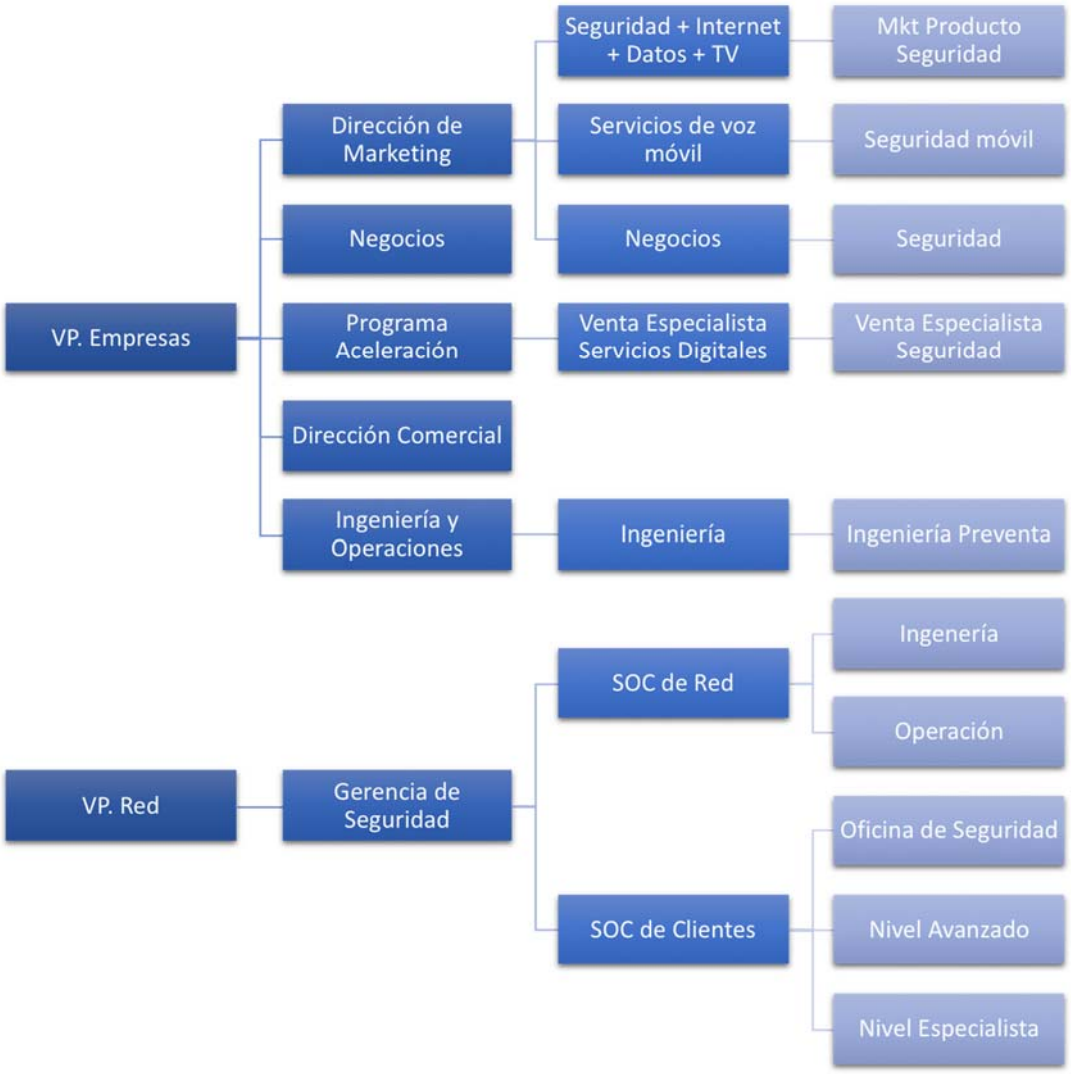


Figura 2. Organigrama actual del área en estudio
Fuente: Organizacional

2.5. SOC Clientes

La empresa EP cuenta con su SOC "Security Operation Center" sus siglas en inglés, es un Centro de Operaciones de Seguridad que tiene la función para ofrecer a sus clientes la mejor tecnología disponible al objeto de impulsar la innovación y la seguridad de sus servicios, agregando valor al negocio y maximizando las oportunidades de mejora en el ámbito de la Seguridad de la Información.

La Seguridad de la navegación y conectividad que las empresas realizan remotamente se realiza mediante el uso de Firewall que impiden el tráfico no deseado, la entrada de virus, códigos maliciosos y troyanos que constantemente amenazan las redes de clientes.

La creciente evolución de la tecnología y de las telecomunicaciones, como el masivo uso de Internet y de los negocios a través de las redes, hace a las empresas más vulnerables y más expuestas a los riesgos de Seguridad. En este sentido la productividad y la eficiencia de la

empresa dependen directamente de la rápida y correcta implementación de Tecnología, de las Políticas y los Procesos de Seguridad capaces de soportar su estrategia de Negocios.

En conclusión, la Seguridad de la Información en la actualidad es una necesidad de la empresa. Si ésta desea cuidar su imagen, mantener y mejorar su nivel de competitividad y garantizar la continuidad de sus negocios, debe realizar inversiones para incorporar la Seguridad en su Empresa.

Dado lo anterior el cliente enfrenta las siguientes problemáticas, al momento de evaluar la incorporación de Seguridad:

a) Elevados costos de inversión, operación y mantenimiento de infraestructura de seguridad.

b) Disponer de Personal que requiere una alta especialización.

c) Desconocimiento del origen de las amenazas y riesgos de seguridad.

d) Aumento de los ataques, riesgos y amenazas que cada vez son más frecuentes y de diversa naturaleza.

e) El cliente pierde foco en su giro principal de negocio y debe orientar recursos a resolver problemas derivados de los ataques e incidentes de seguridad.

2.5.1. Equipos de trabajo

2.5.1.1. Nivel Avanzado

Funciones del equipo de trabajo:

- Administrar, operar y mantener en óptimo funcionamiento los diversos equipos de seguridad localizados on-site y/o en la nube los 365 días del año.
- Mantener una constante monitorización de todas las plataformas y servicios de seguridad, con foco en eventos, recursos y disponibilidad.
- Mantener una comunicación profesional con el cliente y brindarle la máxima satisfacción a sus dudas y consultas del servicio de seguridad.
- Dar respuesta rápida y oportuna en caso de emergencias.
- Proveer la prevención, detección, corrección y mejora de eventos de seguridad.
- Monitoreo de la salud de los equipos de seguridad de nuestros clientes.
- Detectar, investigar, analizar y atender incidentes de phishing contra nuestros clientes.
- Atender y resolver incidentes de seguridad que afecten la operatividad y continuidad del servicio del cliente.
- Responder a amenazas de seguridad frente a intentos de intrusión, ataques dirigidos, malware, etc.
- Entregar los informes mensuales asociados a los servicios de seguridad contratados con Telefónica del Perú.
- Documentar de forma continua procedimientos e instructivos propios de la operación.
- Desplazarse a las ubicaciones del cliente ante incidencias críticas cuando se justifique.

2.5.1.2. Nivel Especialista

Funciones del equipo de trabajo:

- Resolución de escalamientos técnicos de clientes
- Administración de las diversas plataformas que soportan los servicios del área.
- Administración e implementación de nuevas plataformas que soportan la operativa.
- Sustentar y ejecutar propuestas mejoras en el diseño de la arquitectura.
- Participación directa en el despliegue de nuevos servicios.
- Automatización de procesos manuales que impacte en la operativa.
- Gestor de Problemas entre los fabricantes o proveedores.
- Implementación de la mejora continua en la post venta de los servicios
- Realizar el análisis y evaluación de riesgos de seguridad en las plataformas

2.5.1.3. Nivel Oficina de Seguridad

Funciones del equipo:

- Brindar una capa adicional de protección sobre los servicios tradicionales de conectividad
- Realizar el seguimiento de calidad a los proyectos implementados por nuestros proveedores, con el fin de asegurar el cumplimiento de las mejores prácticas en temas de seguridad.
- Realizar la mejora continua de los procesos de provisión y seguimiento a proveedores.
- Evaluación de Nuevas Plataformas

2.5.2. Cartera de servicios

2.5.2.1. Seguridad Gestionada

El servicio de Seguridad Gestionada permitirá al cliente final que la conexión a internet contratado y la navegación se realice con un alto nivel de seguridad y rendimiento. La infraestructura del servicio de Seguridad Gestionada comprende implementar una infraestructura en el perímetro de la red del Cliente permitiendo ofrecer las funcionalidades de seguridad perimetral y de contenidos que se definen como parte del alcance del servicio. Estas son principalmente firewall en red , IPS en red, Antivirus, Filtro Web, Control de Aplicaciones y VPN SSL.

Dentro del servicio de Seguridad Gestionada se realiza la siguientes funcionalidades:

- Protección de la Infraestructura del servicio y red del cliente frente a Internet, mediante una plataforma de seguridad implementada en el perímetro de la red del cliente.
- Protección contra Virus y códigos maliciosos: Antivirus de Navegación HTTP, FTP, SMTP.
- Filtrado de contenidos que permite limitar las capacidades de acceso a la Web de los usuarios, mediante la clasificación de contenidos y necesidades de los Clientes.
- Posibilidad de entregar diferentes perfiles de usuario para acceso a los sistemas de gestión.

- Aislamiento lógico total entre infraestructuras de distintos clientes, de forma independiente a la tecnología de acceso, con miras a ofrecer los niveles de privacidad requeridos para estos servicios.
- Consideración de los aspectos referentes a la posible coincidencia de direccionamiento IP entre distintos clientes.
- Informes de Uso y Consumo del servicio.
- Posibilidad de conexión a la intranet de los clientes, sin necesidad de instalación de ningún software de cliente.
- Capacidad de establecimiento de VPN sobre SSL, permitiendo la creación de túneles que permitirán el acceso a las redes privadas de los diferentes clientes.
- Niveles de acceso personalizables, según las siguientes posibilidades:
    - Autenticación, Radius, Directorio Activo, Certificado, etc.
    - Perfil personal de plantilla, personal ajeno, demo, etc.
    - Equipo, PC corporativo, PC doméstico, PDA, etc.

Los beneficios para los clientes y sus organizaciones son:

- Diseñamos e implementamos la seguridad perimetral con los productos idóneos y de prestigio en el mercado para su negocio.
- Contamos con personal especializado y certificado en los productos de seguridad, y cuentan con amplia experiencia para el desarrollo de proyectos.
- Ofrecemos productos de reconocida trayectoria en el mercado, fabricados bajo estándares internacionales.
- Contamos con acuerdos marco con los fabricantes a fin de optimizar los costos de los proyectos.
- Ofrecemos ser un único interlocutor de cara al cliente como único integrador.

2.5.2.2. Tráfico Seguro

El servicio de Tráfico Seguro permitirá al cliente final que la conexión a internet contratado y la navegación se realice con un alto nivel de seguridad y rendimiento. La infraestructura de Tráfico Seguro se encuentra alojado en la red de la empresa EP permitiendo ofrecer las funcionalidades de seguridad perimetral.

Dentro del servicio se realiza la siguientes funcionalidades:

- Permite al Cliente que la conexión y la navegación a Internet se realicen con un alto nivel de seguridad y rendimiento, permitiendo la escalabilidad de todos sus componentes.
- El Servicio está basado sobre una plataforma muy flexible y escalable a objeto que permita ofrecer servicios según las cambiantes necesidades de los clientes.
- Configuración de las prestaciones contratadas en el equipo de seguridad implementado en la red de la empresa EP: Firewall, IPS, Antivirus, Filtro Web/URL, Control de Aplicaciones, VPN IPSEC.
- Administración, Gestión y monitoreo de los equipos de seguridad 24x7x 365 días al año, durante el periodo del contrato.

El Servicio de Tráfico Seguro ofrece entre otros beneficios los siguientes:

- Mejora de la seguridad perimetral incorporando varios niveles de protección: Firewall, IPS, Antivirus, Filtro Web/URL, Control de Aplicaciones, VPN IPSEC.
- Mejora de la cobertura de la gestión de los incidentes de seguridad hasta un nivel de atención 24x7x 365 días al año, transfiriendo esta responsabilidad a una empresa especializada.
- No hay costos de inversión en equipos y licencias, ni costos de capacitación de personal de la compañía para labores operativos y especializados de seguridad.
- Posibilidad de obtener una gestión integral de las comunicaciones y seguridad perimetral a través de un único proveedor.

2.5.2.3. Correo Limpio

Este servicio engloba las funcionalidades principales de Antispam proporcionando protección frente a los envíos de correo electrónico no deseado, Antivirus para impedir la recepción de correo con contenido ejecutable malicioso tales como virus, troyanos, etc., Filtrado de Contenidos, para aplicar diferentes políticas de correo electrónico mediante reglas sobre los correos entrantes o salientes (contenidos inapropiados, confidenciales, etc.), y Archivo de larga duración de correo, sobre todo el correo electrónico entrante o saliente.

El servicio provee los siguientes beneficios para los clientes:

- Solución independiente de sus plataformas de correo y de fácil implantación
- Modelo de facturación "Pay-as-you-go" sin costes extra ni ocultos
- Informes on-line detallados y personalizados
- Solución transparente:
- No ralentiza la máquina del usuario.
- Sin instalación de software adicional.
- Como solución Cloud, el cliente no tiene que preocuparse ni de actualizaciones de la plataforma ni de la gestión de la misma.
- Servicio competitivo en calidad y cobertura

2.5.2.4. Seguridad Móvil

El servicio se trata Mobile Device Management (MDM) es una herramienta que permite gestionar dispositivos móviles (celulares o tablets) mediante la distribución de políticas o directivas de uso de estos dispositivos. Es una plataforma ofrecida en modalidad SaaS, se brinda desde la nube.

El alcance de este servicio incluye el manejo del producto desde la etapa de la Identificación de la Oportunidad hasta la Operación.

Las funcionalidades soportadas por el licenciamiento ofrecido son las siguientes:

- Eliminación remota de la información:
    - Envío de comando para el reseteo del equipo a modo fábrica.

- Administración y Monitoreo del Dispositivo:
    - Creación de grupos organizativos
    - Visualización del listado de las APPS instaladas en el dispositivo y su respectiva versión
    - Restricción del uso de la cámara
    - Distribución de aplicaciones
- Perfil de Uso de contraseñas:
    - Política de contraseñas con determinada complejidad configurable por el administrador
    - Resetear contraseña del equipo
    - Bloqueo de pantalla

En resumen en la siguiente figura 3 se muestra la cartera de servicios del SOC:

Figura 3. Cartera de servicios del SOC
Fuente: Elaboración propia

2.6. Mercado Actual

Con 16 años de experiencia en monitoreo e inteligencia de seguridad (el primer SOC de la empresa EP comenzó a proporcionar los servicios en el 2002), los equipos que ofrecen servicios personalizados para monitorear de forma continua, analizar y proteger mejor los activos de sus clientes, administrando permanentemente el proceso de protección contra las amenazas y

proporcionando a sus organizaciones la capacidad de responder rápida y eficazmente a las sofisticadas e impredecibles fuerzas maliciosas. Actualmente, la empresa EP gestiona un gran número de clientes en diferentes regiones; más de 1.000 clientes en Seguridad Gestionada, de los cuáles 640 en Latinoamérica, más de 7.000 dispositivos de seguridad gestionados, 3.500 en Latinoamérica.

2.6.1. Clientes Objetivos

El Servicio de Seguridad Gestionada está orientado al Segmento Empresas y Corporaciones de los distintos sectores del mercado: Banca y Finanzas, Entidades públicas y de Gobierno, Servicios, Educación, Industria, Telcos y Tecnología, Minas, Industria, retail entre otros, que poseen las siguientes características:

- Clientes del Segmento Empresas que tengan contratado con la empresa EP accesos dedicados a Internet.
- Empresas con necesidad de tercerizar la gestión, operación y monitoreo de la seguridad perimetral con una empresa competente en la realización de estas tareas.
- Empresas con necesidad de cobertura de una gestión, operación y monitoreo de 7x24x365 de los servicios de seguridad.
- Clientes que no deseen realizar inversiones en hardware o softwares de seguridad y consideran la alternativa de reemplazar el CAPEX por OPEX.

2.6.2. Competencia

Dentro de las empresas locales que tienen la capacidad de entregar a cliente ofertas con funcionalidades similares al servicio de Seguridad Gestionada se han identificado las siguientes:

Tabla 8. Empresas en el mercado peruano
Fuente: Elaboración Propia

Servicios	**Competidor**
Integradores	IBM
	NeoSecure
	Vilsol
	Bafing
	Electrodata
	Thinknetworks
Proveedores de Servicio de Internet	América Movil
	Level 3
	Optical Networks

2.7. Prioridades estratégicas

El área del SOC en conjunto con la dirección de marketing de la empresa EP definieron las prioridades estratégicas para el SOC con el fin de captar nuevos clientes e incluir nuevos servicios al catálogo de productos, como se detalla en la figura 4.

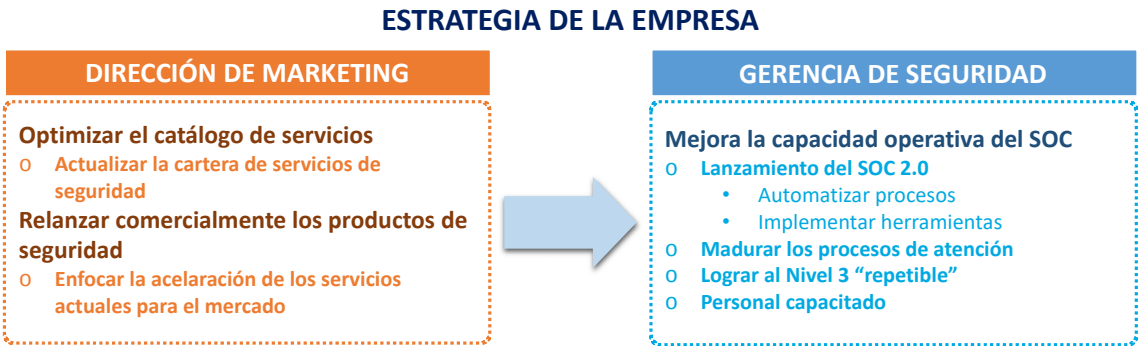


Figura 4. Estrategia de la empresa enfocado en seguridad
Fuente: Elaboración propia

Dentro de la proyección de crecimiento del negocio, la empresa cuenta con un roadmap alineado a las prioridades estratégicas como indica la figura 5.

Figura 5. Mapa de Servicios en PerúFuente: Área de Marketing de la empresa EP

2.8. Planteamiento del Problema

2.8.1. Análisis cuantitativo de los servicios del SOC

Actualmente el área del SOC de Clientes, gestiona los servicios de Seguridad Gestionada, Correo Limpio, Tráfico Seguro y Seguridad Móvil con **1218 clientes** distribuidos entre los diferentes servicios, con **atención 24x7**, de los cuales el **83%** de los clientes pertenece al servicio de "Seguridad Gestionada", como indica la figura 6.

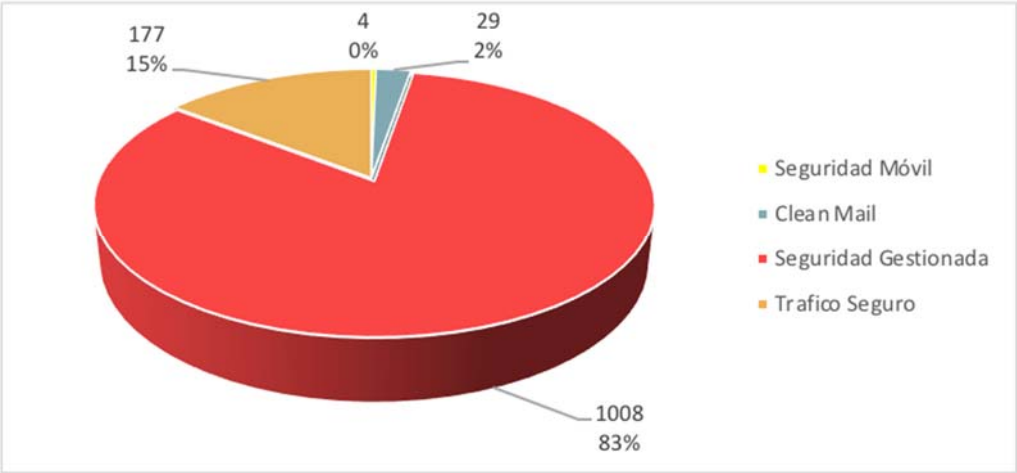


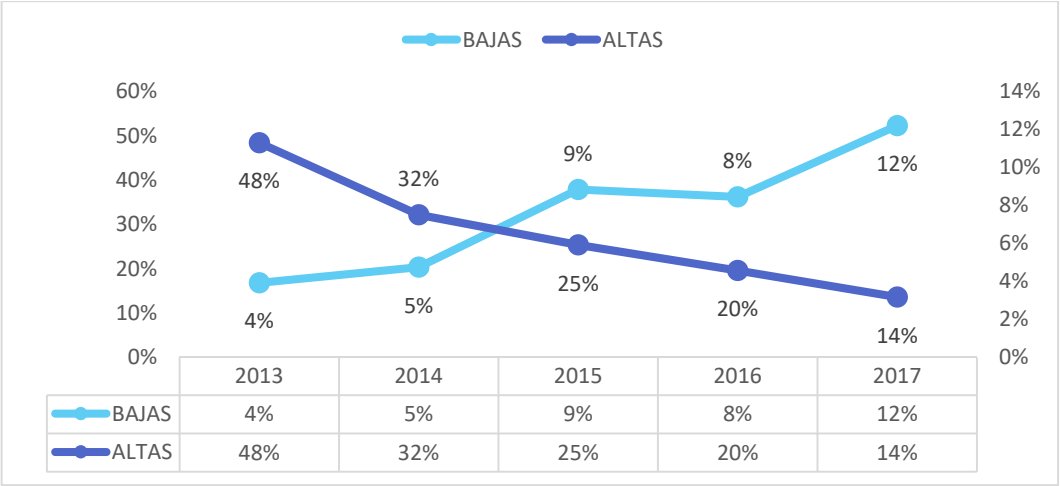
Figura 6. Distribución de servicios
Fuente: Elaboración Propia

El siguiente cuadro muestra los ingresos que tiene la empresa por los servicios que brindan en el área del SOC, mostrándose que en los últimos 5 años el servicio de seguridad gestionada es el 80% promedio de los ingresos anuales:

Tabla 9. Ingresos por servicios
Fuente: Elaboración propia

Servicio	2013	2014	2015	2016	2017
	Mil Soles	Mil Soles	Mil Soles	Mil Soles	Mil Soles
Correo Limpio	10,829 PEN	9,440 PEN	8,496 PEN	7,649 PEN	6,923 PEN
Seguridad Gestionada	179,578 PEN	156,553 PEN	140,898 PEN	126,854 PEN	114,803 PEN
Seguridad Móvil	10,829 PEN	795 PEN	716 PEN	644 PEN	583 PEN
Trafico Seguro	31,533 PEN	27,490 PEN	24,741 PEN	22,275 PEN	20,159 PEN
TOTAL DE INGRESOS	**232,769 PEN**	**194,278 PEN**	**174,851 PEN**	**157,422 PEN**	**142,468 PEN**

Se realizó un análisis del comportamiento evolutivo del servicio de Seguridad gestionada identificando las altas (clientes nuevos) y bajas (Clientes que no renuevan el servicio) de los últimos 5 años y se ha llegado a identificar que este servicio es el que ha sufrido el mayor impacto de pérdidas de clientes, mientras que cada año la proyección de altas de nuevos clientes ha ido decreciendo y las bajas de los clientes han ido aumentando considerablemente como se muestra en la siguiente figura 7.



	2013	2014	2015	2016	2017
BAJAS	4%	5%	9%	8%	12%
ALTAS	48%	32%	25%	20%	14%

Figura 7. Evolutivo de clientes del servicio Seguridad Gestionada
Fuente: Elaboración propia

Los contratos firmados con los clientes en el servicio de seguridad gestionada contemplan el cumplimiento de SLAs que se describen en la tabla 10 donde abarcan tiempos de respuesta de 4 a 24 horas dependiendo el tipo de incidente, al no cumplirse estos SLAs la empresa se viene obligada a pagar penalidades del 2% del pago mensual por el servicio.

Tabla 10. SLA del área
Fuente: contrato de servicios del SOC

Tipo de Incidente	Descripción del Incidente	Tiempo de Respuesta
Incidente Severidad 1	Falla de Hardware o software que involucre caída del servicio, causando impacto crítico en las operaciones vía internet del cliente.	04 horas
Incidente Severidad 2	Degradación en la calidad de servicio, impactando significativamente en las operaciones vía internet del cliente.	12 horas
Incidente Severidad 3	Problemas de menor impacto, consultas de tipo operativo, se incluye también cambios de configuración.	24 horas

Se realizó un análisis del total de tickets anuales atendidos por el área del SOC, identificando cuantos tickets porcentualmente no han cumplido con los SLAs especificados en la tabla 10, como muestra de este análisis en la figura 8, en el año 2016 y 2017 el 30% aproximado de las atenciones no han sido cumplidas.

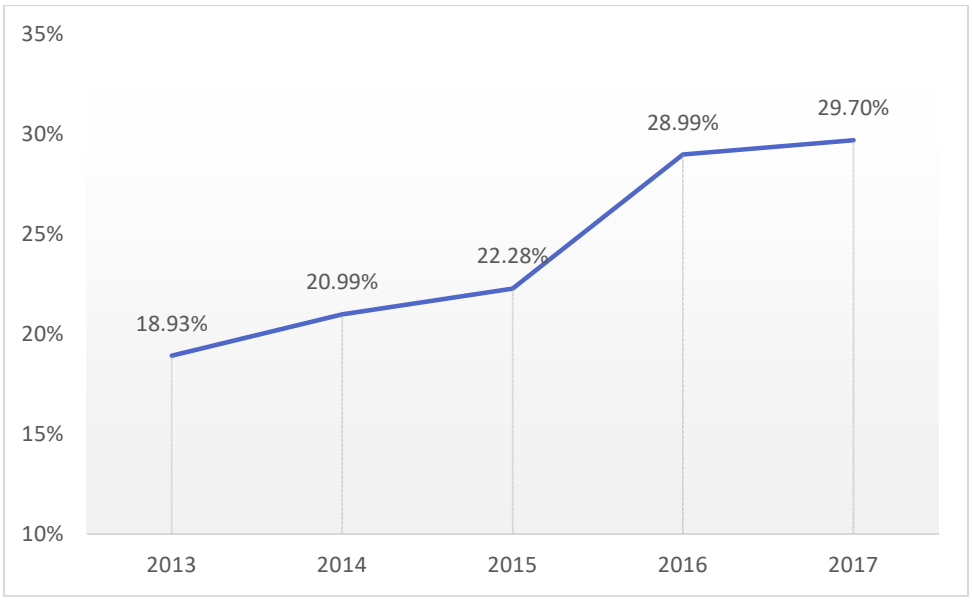
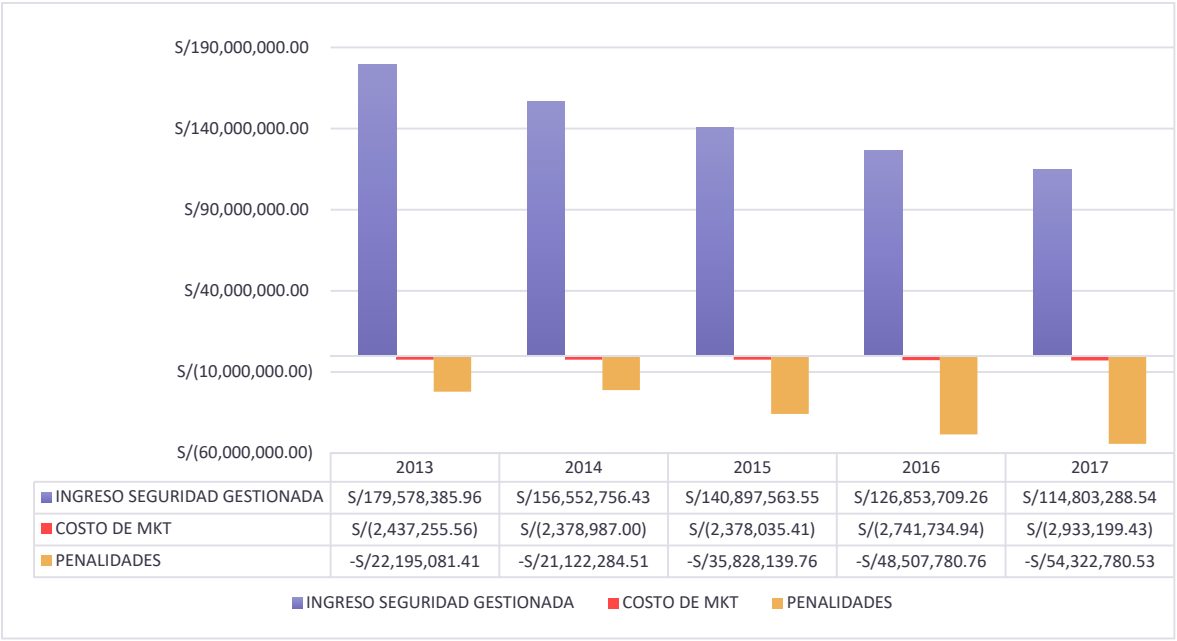


Figura 8. Evolutivo de ticket que incumple el SLA
Fuente: Elaboración propia

Estos tickets no atendidos han afectado al área de manera agresiva al tener que dejar de percibir los ingresos por las penalidades de estas atenciones al incumplimiento de los SLAs, en la figura 9 se detalla los ingresos en comparación de los egresos donde más del 30% se está dejando de percibir por las penalidades.



	2013	2014	2015	2016	2017
INGRESO SEGURIDAD GESTIONADA	S/179,578,385.96	S/156,552,756.43	S/140,897,563.55	S/126,853,709.26	S/114,803,288.54
COSTO DE MKT	S/(2,437,255.56)	S/(2,378,987.00)	S/(2,378,035.41)	S/(2,741,734.94)	S/(2,933,199.43)
PENALIDADES	-S/22,195,081.41	-S/21,122,284.51	-S/35,828,139.76	-S/48,507,780.76	-S/54,322,780.53

Figura 9. Evolutivo de Ingresos vs Egresos
Fuente: Elaboración propia

Conclusión:

- El servicio de Seguridad Gestionada es el que tiene más demanda dentro del área del SOC siendo este el core del negocio ya que del total de clientes de la cartera abarca el 83% como indica en la figura 6 y el 80.5 % de la facturación del total anual como se evidencia en la tabla 9.
- Existe una importante tendencia decreciente en la venta del servicio de Seguridad Gestionada, viendo la reducción a un 14% anual de la perdida de cartera de clientes.
- Se evidencia un problema operativo dado que en el 2017 se ha ascendido al 29% el nivel de cumplimiento de los acuerdos de servicio pactados con los clientes por ende se realiza un pago por penalidades superando el 30% en el último año.

2.8.2. Análisis operativo del servicio del SOC

Actualmente no se mantiene un marco de referencia que permita medir el grado de madurez y/o ausencia de controles de Ciberseguridad, por lo que el área del SOC maneja las Incidencias de ciberseguridad de manera reactiva ya que no existe un procedimiento normalizado de atención de incidencias donde los roles y los recursos sean los que controlen y ayuden a mitigar los riesgos del proceso de atención de ataques cibernéticos.

En los últimos 3 años el promedio de casos atendidos de manera proactiva ha sido del 30% aproximadamente, como se aprecia en la figura 10 se observa que en el año 2017 se reportaron 530 ataques de los cuáles el 71% han sido identificados de manera reactiva (Reportados por el cliente), según afirma Kaspersky: "Hay que ser proactivo en la prevención, detección y respuesta a los ataques, para minimizar su impacto y frecuencia. Se debe realizar un seguimiento y eliminar drásticamente los ataques lo antes posible. Cuanto antes se detecte una amenaza, menos daños provocará"[33] a ello nos concluye que las atenciones de incidencias de seguridad deben ser reportados de manera proactiva por un SOC, pero en la práctica el SOC de la empresa no cumple con las referencias del mercado.

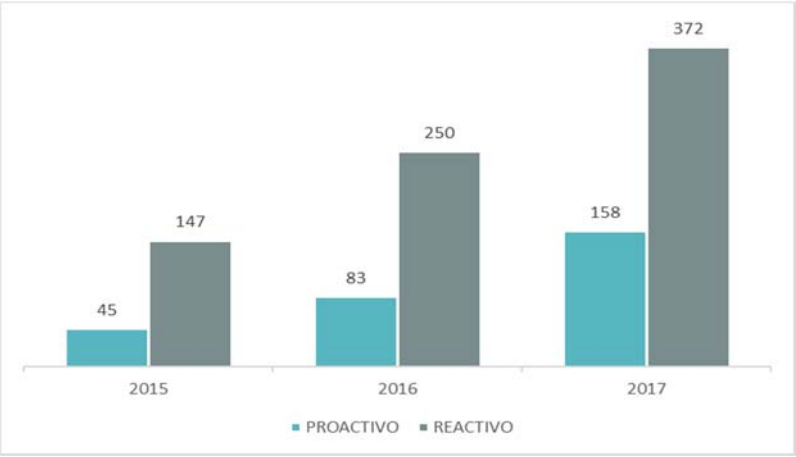


Figura 10. Evolutivo de incidencias reportadas
Fuente: Elaboración Propia

[33] (Informe SOC con tecnología de Kaspersky Lab, 2016)

Además, para contar con recursos de perfil adecuado a menudo puede tener un impacto alto en la operación del SOC, por ello se realizó una evaluación al personal basándose en categorías como conocimiento, desempeño, actitud, habilidades, experiencia, training y liderazgo que debe contar un analista de un SOC en referencia a lo planteado por Rick Howard, CSO de Palo Alto Networks[34] y el modelo de HP SOMM (Security operations maturity model)[35] se pudo establecer la siguiente matriz de evaluación que muestra el puntaje de capacidad y madurez de las personas que trabajan en el SOC a más detalle se puede apreciar en el anexo 1.

Tabla 11. Matriz de evaluación a personal del SOC
Fuente: Elaboración propio

CATEGORIA	SUBCATEGORIA	EVALUACION POR SUBCATEGORIA	EVALUACION POR CATEGORIA
Conocimiento	De la ciencia básica en computación	2.19	**1.56**
	De las operaciones de TI	1.95	
	De los conceptos de operaciones de seguridad	2.03	
	De la gestión de la vulnerabilidad	1.84	
	De códigos maliciosos	1.68	
	De las técnicas básicas de visualización; especialmente Big Data	0.46	
	De técnicas de inteligencia básica aplicada a la cibernética	1.03	
	De lenguas extranjeras	1.32	
Desempeño	Capacidad de delegar tareas	2.27	**2.51**
	Cumplimiento de los procedimientos existentes	2.41	
	Exactitud y calidad de trabajo	2.22	
	Productividad	3.30	
	Responsabilidad	2.38	
Actitud	Actitud hacia al área	2.70	**2.22**
	Actitud hacia superior/es	2.16	
	Actitud hacia los compañeros	2.19	
	Actitud hacia el cliente/usuario	1.81	
Habilidades	Iniciativa	2.32	**2.40**
	Respuesta bajo presión	2.43	
	Potencialidad - Capacidad de Aprendizaje	2.41	
	Coordinación	2.43	
Experiencia	En la industria de TI	2.11	**2.21**
	Entorno en sistemas	2.19	
	Rol en el SOC	2.32	
Training	Presupuesto	1.84	**1.76**
	Importancia	1.73	
	Efectividad	1.70	
Liderazgo	Visión	2.30	**1.88**
	Soporte de recursos humanos	1.43	
	Experiencia	2.38	
	Ámbito de control	1.41	

[34] (cioperu.pe, 2014)
[35] (State of Security Operations, HP, 2016)

Ante ello se realizó un comparativo sobre lo establecido por el SOMM de HP, indicando que el promedio del personal debe estar en un nivel 3.8 moderado, viéndose en la figura 11 que los recursos del SOC se encuentra lejos del promedio referencial.

Figura 11. Evaluación de personas
Fuente: Elaboración propia

Conclusión:

- El área cuenta con un déficit de atenciones proactivas como lo pide el mercado, sus atenciones abarcan el 71% de manera reactiva que es una cifra muy alta ya que debería alinearse a los estándares del mercado que es 90% de manera proactiva.
- La capacidad de los recursos del SOC se encuentran lejos del modelo de madurez operativo de un SOC según lo establecido por SOMM de HP.

2.8.3. Evaluación de estado de Ciberseguridad en el SOC

Para evaluar el estado de ciberseguridad se va utilizar el marco de ciberseguridad del NIST aplicando los 98 controles en el área, muestra de ello los resultados se encuentra a más detalles en el Anexo 2.

Luego de analizar los controles, nos da como resultado el siguiente análisis GAP que se muestra en la figura 12, donde se puede apreciar que el 66% de los controles están en el nivel parcial.

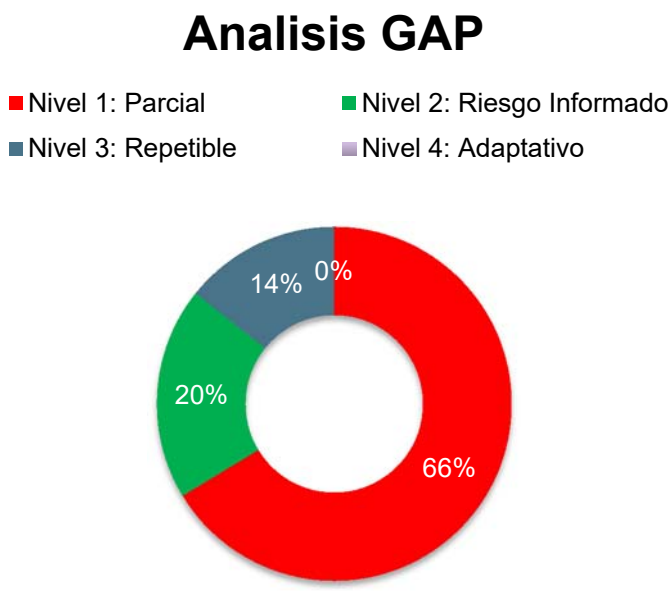


Figura 12. Resultados del nivel inicial
Fuente: Elaboración Propia

Según los resultados obtenidos, podemos determinar que el perfil actual de la empresa es **Nivel 1: Parcial.**

Respecto a los datos mostrados el área del SOC actualmente tiene ausencia de procedimientos alineados a buenas prácticas; ya que los recursos que están a cargo del servicio actúan de manera reactiva teniendo un bajo conocimiento de Ciberseguridad, y los impactos que esto implica.

Concluyendo que el principal problema es la falta de procedimientos para la atención del servicio de seguridad gestionada dentro del área de SOC, por lo que se requieren la implementación de un marco de referencia de Ciberseguridad para:

- La adopción de controles proporcionales a los riesgos percibidos.
- La documentación de políticas, procedimientos, controles y tratamiento de riegos.
- Identificación y asignación de responsabilidades al nivel adecuado.
- Formalización, seguimiento y revisión de los controles y riesgos, de forma sistemática (periódica) y metodológica.

CAPÍTULO 3: PROPUESTA DE IMPLEMENTACIÓN

3.1. Objetivos

3.1.1. Objetivo General

Proveer al área del SOC un marco de ciberseguridad para generar una solución que le permita implantar, operar, monitorear, revisar y mejorar los controles de Ciberseguridad, con el fin de ser un SOC de referencia y llegar a ser competitivo en el mercado.

3.1.2. Objetivos Específicos

- Diseñar un modelo de gestión de Ciberseguridad en el área del SOC que permita proporcionar las directrices y controles para la respuesta a incidentes cibernéticos.
- Desarrollar una política de Ciberseguridad utilizando el marco de ciberseguridad para alcanzar el perfil Nivel 3 Repetible.
- Implementar mejores prácticas que aseguren el uso de recursos y proceso de atención eficientes
- Desarrollar controles técnicos de Ciberseguridad para ejecutar eficientemente los nuevos servicios del SOC

3.2. Marco de Ciberseguridad

Todas las acciones que se debe realizar para implementar el marco de ciberseguridad se resume en la figura 13, deben ser implementadas dentro de un entorno de mejora continua, permitiendo que de forma continua la empresa EP optimice sus controles de seguridad y escale a niveles superiores dentro del marco de trabajo.

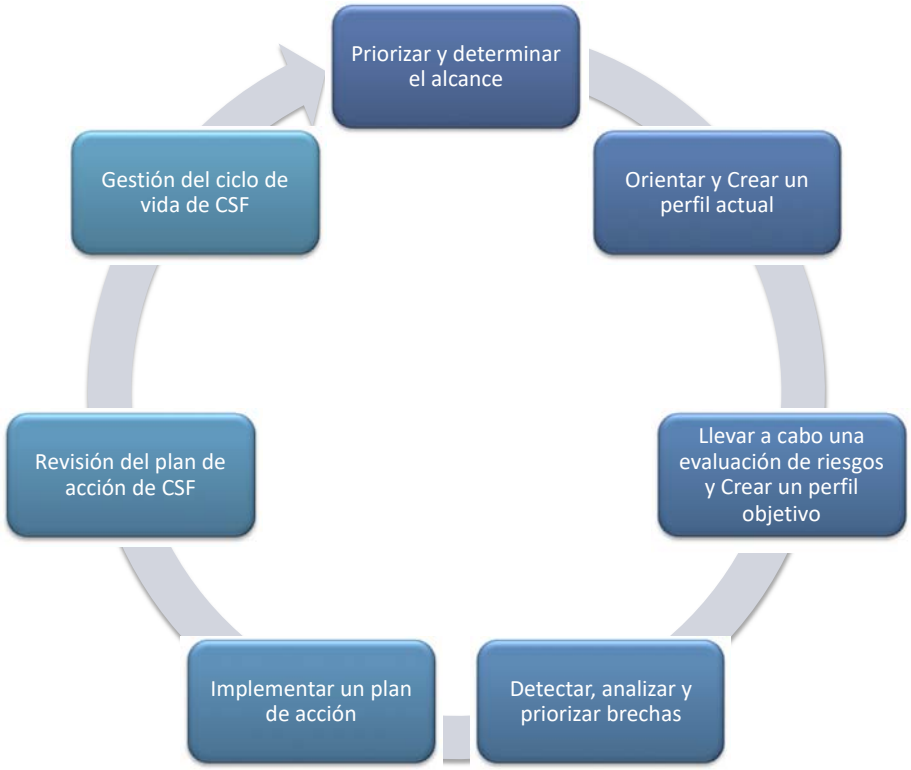


Figura 13 Método para la implementación del CSF del NIST
Fuente: (Elaboración propia, 2018)

3.3. Determinación del Alcance

El objetivo de este paso es comprender el enfoque actual de la gobernanza y la ciberseguridad del área del SOC de la empresa EP e identificar las partes interesadas claves como la misión de la organización, los roles y las responsabilidades complementando lo que se vio en el capítulo 2.

Para determinar el alcance se identificó los factores internos y externo que involucra la parte organizacional, infraestructura, principales funciones, procesos, tecnología y personal del área exponiendo las necesidades de cada una de ellas como se detalla en la tabla 12.

Tabla 12. Factores Internos y Externos
Fuente: Elaboración Propia

FACTORES INTERNOS Y EXTERNOS DE LA ORGANIZACION	
FACTORES EXTERNOS	**FACTORES INTERNOS**
ECONÓMICOS	**ORGANIZACIONAL**
• Asignación de presupuesto. • Ampliación del mercado de telecomunicaciones.	• Apoyo y compromiso de la alta dirección. • Presupuesto y Recursos Financieros. • Alineamiento de la empresa con las políticas nacionales y sectoriales.

FACTORES INTERNOS Y EXTERNOS DE LA ORGANIZACION	
FACTORES EXTERNOS	**FACTORES INTERNOS**
POLÍTICOS	**INFRAESTRUCTURA**
• Fomento de la inversión en el sector de Telecomunicaciones. • Legislación vigente de Telecomunicaciones.	• Sala de operación equipada para tratar casos de alta sensibilidad • Sala experimental para armar entornos no productivos (o maquetas) simulando un entorno real para pruebas de vulnerabilidad.
MERCADO DE TELECOMUNICACIONES	**PRINCIPALES FUNCIONES**
• Desarrollo del Mercado de Telecomunicaciones. • Ingreso de nuevas empresas operadoras.	• Respuesta a Incidentes de Seguridad
SOCIAL	**PROCESOS**
• Fundación social EP.	• Garantizar capacitación/certificación con fabricantes en función de la planta y mercado de equipamiento de Perú. • Especialización equipos SOC • Capacitación en herramientas • Creación manual de mejores prácticas
MEDIAMBIENTALES	**TECNOLOGIA**
• Desastres naturales.	• Plataforma Tecnológica de vanguardia.
TECNOLOGICOS	**PERSONAL**
• Incursión de nuevas tecnologías en el mercado de telecomunicaciones.	• Capacidad del personal. • Competencias.

Para determinar el alcance se consideran a las partes interesadas de los equipos de trabajo del SOC, clientes y Gobierno, siendo su principal expectativa las acciones basadas en las entradas y salidas de los siguientes procesos enfocados en Ciberseguridad como se detalla en la tabla 13.

Tabla 13. Procesos y requisitos de las partes interesada
Fuente: Elaboración propia

PARTE INTERESADA	PROCESOS	REQUISITO DE SEGURIDAD
Equipos de trabajo	• Respuesta a Incidentes de Seguridad	• Protección de la información personal y operatividad de la plataforma tecnológica que le aseguren un servicio seguro.

PARTE INTERESADA	PROCESOS	REQUISITO DE SEGURIDAD
Clientes	• Respuesta a Incidentes de Seguridad • Proceso de atención a usuarios.	• Protección de la información personal y operatividad de la plataforma tecnológica que le aseguren un servicio seguro. • Cumplimiento de los SLA.
Gobierno	• Respuesta a Incidentes de Seguridad	• Cumplimiento de la legislación y regulación en temas relacionados a seguridad de la información.

De lo expuesto en las tablas 12 y 13 considerando los factores internos y externo, las partes interesadas y sus expectativas para la Gestión de la Ciberseguridad se concluye el siguiente alcance:

"El proceso de Respuesta a Incidentes de Seguridad de la atención del servicio de seguridad gestionada del área del SOC de Clientes, según las funciones, categorías y subcategorías aplicables del CSF del NIST".

3.4. Perfil Actual

En el punto 2.8.3 se realizó la evaluación de los controles del marco de ciberseguridad donde los resultados obtenidos se determinó que el perfil actual se encuentra el Nivel 1: Parcial.

Tabla 14. Perfil Actual – Nivel 1: Parcial
Fuente: Elaboración propia

N°	NIVEL	DESCRIPCION
1	**Nivel 1: Parcial**	Existen algunas iniciativas sobre ciberseguridad, aunque los esfuerzos se realizan en forma aislada. Se realizan implementaciones con enfoques ad-hoc y existe alta dependencia del personal que lleva a cabo las tareas que habitualmente no se encuentran documentadas. Existe una actitud reactiva ante incidentes de seguridad.

3.5. Análisis y Gestión del Riesgo

3.5.1. Identificación del proceso

La identificación del riesgo se realiza determinando las causas asociadas al proceso de Respuesta a Incidentes de Seguridad que se detalla en la tabla 15.

Tabla 15. Descripción del proceso
Fuente: Elaboración propia

N°	PROCESO	DESCRIPCION
1	**Respuesta a Incidentes de Seguridad**	Este proceso abarca la atención y tratamiento de incidentes de seguridad en sus clientes que pueden iniciarse por 3 motivos: Incidencia reportada por el cliente, Monitoreo realizado por el equipo de Nivel Avanzado o Monitoreo a las plataformas realizado por el equipo de Nivel Especialista. Durante la atención del proceso de respuesta al incidente de seguridad toda la comunicación y resolución del incidente hacia el cliente e interesados es a través de la persona que cumple el rol de Relación con Clientes

3.5.2. Inventario de Activos

Para verificar el alineamiento de los activos que tiene el área de SOC, asociado al proceso de Respuesta a Incidentes de Seguridad, dentro de los 18 activos identificados se ha categorizado según la función que cumple dentro del área, como:

- Datos (D)
- Datos personales (DP)
- Hardware (HW)
- Software (S)
- Ubicaciones físicas (U)
- Comunicaciones (COM)

De tal manera que se realizó la identificación de cada activo alineado a la función, propietario que la gestiona y la descripción de cada activo como se detalla en la tabla 16.

Tabla 16. Inventario de Activos
Fuente: Elaboración propia

N°	CATEGORIA	ACTIVO	PROPIETARIO	DESCRIPCION
1	D	Información histórica de Clientes	Jefe del área	Información sensible como contratos, topologías, contactos del clientes.

N°	CATEGORIA	ACTIVO	PROPIETARIO	DESCRIPCION
2	DP	FileServer PRIM	Jefe del área	Servidor principal para custodiar la información de los clientes, del área y de los equipos de trabajo.
3	DP	FileServer SEC	Jefe del área	Servidor de backup para custodiar la información de los clientes, del área y de los equipos de trabajo.
4	U	Oficina de Seguridad	Jefe del área	Este equipo se encarga de realizar la provisión de servicios a los clientes nuevos.
5	U	Nivel Especialista	Jefe del área	Esta equipo se encarga de gestionar el mantenimiento y la operatividad de las plataformas del área.
6	U	Nivel Avanzado	Jefe del área	Este equipo se encarga de atender la postventa de los servicios que se brinda a los clientes en el área.
7	S	Telefonía	Jefe del área	Terminales telefónicos que funcionan en las redes de telecomunicaciones: terminales telefónicos fijos, con tecnología analógica o digital, terminales telefónicos móviles, con diverso tipo de tecnologías, terminales de software (“softphones”), terminales para uso corporativo.
8	S	Correo electrónico	Jefe del área	Servicio en el que se puede enviar y recibir mensajes de manera rápida por medio de un canal electrónico o informático. Servicio de red que ofrece a los usuarios, comunicación entre ellos a través de mensajes, utilizando una computadora o dispositivo móvil.
9	S	Internet	Jefe del área	Unión de todas las redes y computadoras distribuidas por todo el mundo, red global donde se juntan todas las redes que utilizan protocolos TCP/IP y que son compatibles entre sí.
10	COM	Red de Datos	Jefe del área	Red de telecomunicaciones que permite a los equipos de cómputo intercambiar datos. Las conexiones (enlaces de red) entre los nodos establecidos mediante medios de comunicación, ya sea por cable o medios inalámbricos.
11	HW	FAZ_SIS	Jefe del área	Equipo primario que se encarga de recolectar los logs de los firewalls instalados en los clientes y crear reportes del servicio Seguridad Gestionada.
12	HW	FAZ_WASH	Jefe del área	Equipo secundario que se encarga de recolectar los logs de los firewalls instalados en los clientes y crear reportes del servicio Seguridad Gestionada.

N°	CATEGORIA	ACTIVO	PROPIETARIO	DESCRIPCION
13	HW	FW_SOC_SEC	Jefe del área	Firewall configurado en alta redundancia (HA) del área que brinda la seguridad perimetral.
14	HW	FW_SOC_PRIM	Jefe del área	Firewall del área que brinda la seguridad perimetral.
15	HW	PE-LIM-DLP-SOC	Jefe del área	Servidor DLP.
16	HW	PE-LIM-RMDY-BD1	Jefe del área	Servidores Remedy -Base de Datos original.
17	HW	PE-LIM-RMDY-BD2	Jefe del área	Servidores Remedy -Base de datos replicados.
18	SW	OPSVIEW	Jefe del área	Monitorea la salud de los equipos instalados en el local del cliente.

Este análisis nos arrojó como los activos están relacionados a la custodia y protección de los datos del negocio.

3.5.3. Valuación de Activos

Se ha considerado para evaluar los activos lo siguientes criterios:

- Crítico: Muy Importante para la operación
- Dañino: Medianamente importante para la operación
- Insignificante: No importante para la operación

Según muestra en la tabla 17, la valoración de cada activo por los criterios descritos:

Tabla 17. Valuación de Activos
Fuente: Elaboración propia

N°	CATEGORIA	PROPIETARIO	ACTIVO	C	D	I	TOTAL
1	D	Jefe del área	Información histórica de Clientes	5	5	5	5
2	DP	Jefe del área	FileServer PRIM	5	5	5	5
3	DP	Jefe del área	FileServer SEC	5	5	5	5
4	U	Jefe del área	Nivel Avanzado	4	5	5	5
5	S	Jefe del área	Correo electrónico	4	5	5	5
6	S	Jefe del área	Internet	5	5	5	5
7	COM	Jefe del área	Red de Datos	5	5	5	5
8	HW	Jefe del área	FAZ_SIS	5	5	5	5
9	HW	Jefe del área	PE-LIM-DLP-SOC	5	5	5	5
10	HW	Jefe del área	PE-LIM-RMDY-BD1	4	5	5	5
11	U	Jefe del área	Oficina de Seguridad	4	4	4	4

N°	CATEGORIA	PROPIETARIO	ACTIVO	C	D	I	TOTAL
12	U	Jefe del área	Nivel Especialista	4	4	4	4
13	S	Jefe del área	Telefonía	3	4	4	4
14	HW	Jefe del área	FAZ_WASH	5	4	4	4
15	HW	Jefe del área	FW_SOC_SEC	5	4	4	4
16	HW	Jefe del área	FW_SOC_PRIM	5	3	5	4
17	HW	Jefe del área	PE-LIM-RMDY-BD2	4	4	4	4
18	SW	Jefe del área	OPSVIEW	4	4	4	4

3.5.4. Resultados del Análisis de Riesgo

Este análisis busca conocer que es lo que se desea proteger, conociendo sus vulnerabilidades y las amenazas a las que está expuesto los activos del SOC, para revelar el grado de riesgo según se muestra en el Anexo 3, donde permitió identificar los activos con riesgo alto (A) y extremo (E) considerado su criticidad y vulnerabilidad e impacto en el negocio.

3.5.5. Plan de tratamiento de Riesgo

Este plan busca analizar y evaluar el funcionamiento y efectividad de las medidas a realizar para la mitigación del riesgo, con el fin de mejorar las medidas que son ineficientes, en caso de disconformidades. Además, se busca registrar y aprender de las lecciones de dicha implementación como se muestra en el Anexo 4.

Además, se agregó a la relación de riesgos que impactan a los activos una salvaguarda que permite mitigar el riesgo, a ello se relaciona un control propuesto en base a las categorías del marco de ciberseguridad; es decir si para mitigar un riesgo de robo de información se implementa un DLP la cual está alineada a la categoría Seguridad de datos (PR.DS) del marco de ciberseguridad.

Se ha considerado dentro de las medidas a realizar los riesgos asociados a los activos y a la vez se ha alineado a los objetivos del negocio como se muestra en el análisis de un activo en la siguiente tabla 18:

Tabla 18. Tratamiento de riesgo de un activo
Fuente: Elaboración propia

AMENAZA	ACTIVO	ZONA DE RIESGO	DUEÑO RIESGO	SALVAGUARDAS	CATEGORIAS CSF	MEDIDAS A REALIZAR	OBJETIVOS ESTRATEGICOS
Robo	Información histórica de Clientes	E	Jefe del SOC	Implementacion de un DLP	Tecnología de Protección (PR.PT) Seguridad de datos (PR.DS) Procedimientos de protección de la información (PR.IP)	Establecer lineamientos para ejecución de auditorias de sistemas de información considerando requisitos de auditoría para acceso a sistemas y a datos	Lanzamiento del SOC 2.0 Automatizar procesos Implementar herramientas

3.6. Política de Ciberseguridad

Determinando el alcance, el perfil actual y analizando los riesgos se ha determinado la siguiente política de Ciberseguridad para el SOC de la empresa EP.

"La empresa EP considera a la información y sus activos críticos de vital importancia y el aseguramiento de la confidencialidad, disponibilidad e integridad como primordial para realizar con normalidad sus operaciones y actividades institucionales. Por tanto, establece los mecanismos para su protección en los medios de soporte, comunicación y tratamiento de todo tipo de amenazas, sean internas o externas, deliberadas o accidentales.

La Política de Ciberseguridad está orientada a gestionar eficazmente la seguridad de la información tratada por los sistemas informáticos de la empresa EP, la información de nuestros clientes, así como los activos que participan en nuestros procesos.

La empresa EP garantiza el apoyo al proceso de planificación, implementación, revisión y mejora del Sistema de Gestión de Ciberseguridad, asumiendo con ello, el compromiso de proteger los recursos de información."

3.7. Determinar Perfil Objetivo

Según la política establecida para la mejora de los controles de ciberseguridad de la empresa EP, se determina el perfil objetivo en "Nivel 03: Repetible" donde los beneficios se detalla en la tabla 19.

Tabla 19. Perfil Objetivo – Nivel 3: Repetible
Fuente: Elaboración propia

N°	NIVEL	DESCRIPCION
1	Nivel 3: Repetible	En este nivel las prácticas formales de gestión de riesgo son actualizadas regularmente como parte de la aplicación de análisis en cambios en requerimientos de negocio, amenazas o tecnologías. Se ha establecido un marco de colaboración formal con terceros según lo expuesto alineado a unos de los objetivos específicos que requiere el SOC de la empresa EP.

3.8. Propuesta de Plan de Acción

Para llegar al Nivel 3: Repetible objetivo, se debe implementar el plan de acción propuesto alineado a los controles identificados en el Nivel 1: Parcial y Nivel 2: Riesgo informado, que se vio en el punto 2.8.3 los cuáles están basados en las categorías y subcategorías del marco de ciberseguridad.

Tabla 20. Plan de Acción
Fuente: Elaboración propia basado en el CSF del NIST

Entorno Empresarial (ID.BE)		Responsable
ID.BE-3	Desarrollar procedimiento que contemple las actividades a considerar en la inducción a personal	Oficina de Seguridad
ID.BE-1	Definir roles y funciones orientados a Ciberseguridad que debe tener el personal que atiende el servicio del SOC	Oficina de Seguridad
ID.BE-2	Desarrollar procedimientos e instructivos de Monitoreo de infraestructura	Nivel Especialista
ID.BE-4	Realizar mapeo de dependencias y funciones de cada área del SOC Desarrollar procedimientos de comunicación entre el área del SOC y otras dependencias	Nivel Especialista
ID.BE-5	Crear una lista de acciones proactivas identificadas. Desarrollar procedimiento para la atención de situaciones críticas identificadas.	Nivel Especialista
Estrategia de Gestión de Riesgos (ID.RM)		Responsable
ID.RM-1	Desarrollar procedimiento para respuesta a los riesgos	Oficina de Seguridad
Evaluación de riesgos (ID.RA)		Responsable
ID.RA-1	Establecer directrices para vulnerabilidades técnicas Definir los recursos de información que se usarán para identificar las vulnerabilidades técnicas Establecer una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes potencialmente	Oficina de Seguridad
ID.RA-1	Desarrollar instructivo que contenga los pasos de recopilación de fuentes de información sobre amenazas Desarrollar procedimiento de notificación de amenazas de seguridad a los clientes del SOC.	Oficina de Seguridad
ID.RA-5	Desarrollar procedimiento de registro e identificación de amenazas cibernéticas que afecten a los activos del SOC. Crear formatos de informes asociados al procedimiento para que estos sean documentados y guardados en el FS del SOC.	Oficina de Seguridad
ID.RA-5	Identificar y listar los impactos y probabilidades de ataques que sean causa de riesgos en la ejecución de la operación del SOC.	Oficina de Seguridad
Gestión de activos (ID.AM)		Responsable
ID.AM-1	Desarrollar procedimiento de uso de dispositivos físicos del área en el Remedy	Nivel Especialista
ID.AM-2	Desarrollar procedimiento de registro de plataformas, software y aplicaciones del área en el Remedy.	Nivel Especialista

ID.AM-4	Desarrollar procedimiento que contenga el registro en el remedy para catalogar los sistemas. Definir directrices para proteger los equipos fuera de las instalaciones	Nivel Especialista
ID.AM-5	Definir los niveles de priorización de los recursos por clasificación, criticidad y valor comercial	Nivel Especialista
ID.AM-6	Desarrollar MOF para cada área del SOC.	Nivel Especialista
Gobernabilidad (ID.GV)		Responsable
ID.GV-1	Establecer, documentar y desplegar una política de seguridad con base en los requisitos del negocio y de seguridad de la información.	Nivel Especialista
ID.GV-3	Listar los requisitos legales y reglamentarios relativos a la ciberseguridad para ser implementados dentro del área del SOC. Se debe fomentar charlas de manera periódica.	Oficina de Seguridad
ID.GV-4	Establecer un procedimiento que apoye en la gestión de riesgos.	Oficina de Seguridad

Mantenimiento (PR.MA)		Responsable
PR.MA-1	Desarrollar procedimiento para el retiro de activos del área del SOC	Nivel Especialista
PR.MA-2	Desarrollar procedimiento de mantenimiento remoto incluyendo las actividades relacionadas.	Nivel Especialista
Procesos y procedimientos de protección de la información (PR.IP)		Responsable
PR.IP-1	Desarrollar procedimiento para la gestión de configuración y mantenimiento de los sistemas que soportan la operación del SOC.	Nivel Especialista
PR.IP-2	Desarrollar procedimiento para la gestión de seguridad del ambiente de desarrollo	Nivel Especialista
PR.IP-3	Desarrollar directrices y procedimientos de control de configuración	Nivel Especialista
PR.IP-5	Definir control de seguimiento de cumplimiento de políticas	Nivel Especialista
PR.IP-6 PR.DS-3	Desarrollar procedimiento de administración de activos en caso de remoción, transferencia y/o disposición	Nivel Especialista
PR.IP-7	Desarrollar procedimientos de mejora continua para la protección de datos	Nivel Especialista
PR.IP-8	Desarrollar procedimiento para compartir la eficacia de las tecnologías de protección.	Nivel Especialista
PR.IP-9	Identificar elementos de resiliencia para soportar la entrega de los servicios críticos de la entidad.	Nivel Especialista
PR.IP-10 RS.CO-1 RS.CO-3	Desarrollar procedimientos para controlar los planes de respuesta y planes de recuperación	Nivel Especialista
PR.IP-11 ID.BE-1	Definir roles y funciones orientados a Ciberseguridad alineado al personal que atiende el servicio del SOC	Nivel Especialista

PR.IP-12 DE.CM-8 RS.MI-3 ID.RA-1 ID.RA-5	Crear directrices para proteger vulnerabilidades técnicas	Nivel Especialista
Seguridad de datos (PR.DS)		Responsable
PR.DS-2	Desarrollar procedimiento que conecta las actividades de protección de datos en reposo.	Nivel Especialista
PR.DS-3	Desarrollar procedimiento para identificar datos en tránsito	Nivel Especialista
PR.DS-6	Crear instructivo que contenga las funciones de la herramienta de cumplimiento parta verificar el software, el firmware y la integridad de la información.	Nivel Especialista
Sensibilización y Capacitación (PR.AT)		Responsable
PR.AT-1 RS.CO-4	Definir funciones del rol que se encargue de la coordinación y validación de información.	Oficina de Seguridad
PR.AT-5	Crear plan de eventos de ciberseguridad donde los altos ejecutivos sean los principales sponsor en la comunicación de Ciberseguridad.	Nivel Especialista
Tecnología de Protección (PR.PT)		Responsable
PR.PT-1	Desarrollar lineamientos para ejecución de auditorías de sistemas de información	Nivel Especialista
PR.PT-2	Crear un instructivo de uso de la herramienta de DLP	Nivel Especialista
PR.PT-3	Desarrollar procedimiento de protección para todos los colaboradores del área con la herramienta DLP.	Nivel Especialista
Anomalías y Eventos (DE.AE)		Responsable
DE.AE-1	Listar las operaciones realizadas en el SOC, considerando la actualización y creación de flujos de atención y/o operación.	Nivel Especialista
DE.AE-2	Desarrollar procedimiento que cuente con métodos para la identificación de anomalías y eventos de seguridad, que incluya las actividades de análisis de los ataques.	Nivel Especialista
DE.AE-3	Analizar e implementar herramientas existentes en el mercado que apoyen el análisis de eventos con un SIEM.	Nivel Especialista
DE.AE-4	Crear lista de los impactos que causan eventos de ciberseguridad en los activos del SOC.	Nivel Especialista
DE.AE-5	Listar los umbrales de alertas por cada tipo de activo.	Nivel Especialista
Monitoreo Continuo de Seguridad (DE.CM)		Responsable
DE.CM-1	Desarrollar procedimiento de monitoreo que incluya eventos de ciberseguridad asociados a los activos del SOC.	Nivel Especialista
DE.CM-2	Desarrollar procedimiento de monitoreo continuo de ciberseguridad que incluya actividades, responsabilidades dentro del SOC.	Nivel Especialista
DE.CM-3	Definir controles de seguridad para el personal que labora en el SOC.	Nivel Especialista

DE.CM-4 RS.MI-2	Implementar un Sandbox en la red del SOC para detectar código malicioso.	Nivel Especialista
DE.CM-5	Crear políticas de ciberseguridad con el fin de evitar la ejecución de códigos móviles no autorizados.	Nivel Especialista
DE.CM-6	Desarrollar procedimiento directrices de desarrollo externos del SOC.	Nivel Especialista
DE.CM-7	Desarrollar procedimiento para registro de eventos de monitoreo en el Check MK que se utiliza en el SOC.	Nivel Especialista
Procesos de Detección (DE.DP)		Responsable
DE.DP-1	Revisar restricciones y las reglas para la instalación de software por parte de los usuarios.	Nivel Especialista
DE.DP-2	Desarrollar procedimiento de detección con alcance para el SOC.	Nivel Especialista
DE.DP-3	Desarrollar procedimiento de pases a producción a los desarrollos para asegurar pruebas de seguridad.	Nivel Especialista
DE.DP-4	Crear directrices de reporte de eventos de seguridad de la información	Nivel Especialista
DE.DP-5 RS.AN-2	Analizar y establecer procedimiento de detección de incidente detectados	Nivel Especialista

Análisis (RS.AN)		Responsable
RS.AN-1	Crear directrices para recolección de evidencia	Nivel Especialista
RS.AN-2	Determinar eventos de los sistemas de Información.	Nivel Especialista
RS.AN-3	Crear plan de acción ante incidentes de seguridad	Nivel Especialista
RS.AN-4	Analizar y establecer impacto de los incidente detectados para el registro de lecciones aprendidas	Nivel Especialista
Comunicaciones (RS.CO)		Responsable
RC.CO-1	Diseñar un flujo de comunicación con el CSIRT de la empresa.	Nivel Especialista
RC.CO-2	Desarrollar un proceso de comunicación luego de ser mitigado un evento de ciberseguridad	Nivel Especialista
RS.CO-3	Desarrollar procedimientos para comunicar los planes de respuesta y planes de recuperación	Nivel Especialista
RS.CO-5	Identificar los actores externos del SOC.	Oficina de Seguridad
Mejoras (RS.IM)		Responsable
RS.MI-1	Revisar el impacto de los incidente detectados para registrar las lecciones aprendidas y asociarla al plan de respuesta a los incidentes del SOC.	Nivel Especialista
Planificación de Respuesta (RS.RP)		Responsable
RS.RP-1 RS.AN-1 RS.MI-1 RC.RP-1	Desarrollar procedimiento para ejecutar actividades de respuesta durante los eventos de seguridad.	Nivel Especialista

Comunicaciones (RC.CO)		Responsable
RS.CO-4	Crear flujo de comunicación con el CSIRT de la empresa.	Oficina de Seguridad
RS.CO-5	Desarrollar proceso de comunicación luego de ser mitigado un evento de ciberseguridad	Oficina de Seguridad
Mejoras (RC.IM)		Responsable
RC.IM-1	Revisar el impacto de los incidente detectados para detectar mejoras en el servicio	Nivel Especialista
Planificación de la recuperación (RC.RP)		Responsable
RC.RP-1	Desarrollar procedimiento para ejecutar actividades de recuperación durante los eventos de seguridad.	Nivel Especialista

3.9. Plan de Proyecto

El plan de proyecto formulado contiene los planes de alto nivel, siguiendo un esquema metodológico basado en la guía del PMBOK.

Tabla 21. Plan de Proyecto
Fuente: Elaboración propia

Tipo de Proyecto	Proyecto Estratégico
Descripción	Implementación de un modelo de gestión de ciberseguridad para el SOC
Patrocinador	Dirección de marketing
Área Responsable	Gerencia de Seguridad

El objetivo del proyecto es poder contar con la información oportuna para la toma de decisiones asociada a la implementación del modelo en el SOC.

3.10. Plan de Participantes

El la figura 14 se establece la organización del equipo del proyecto, a fin de asegurar su gestión efectiva del para lograr el éxito del plan de acción

Figura 14. Organización del Equipo de Trabajo
Fuente: Elaboración propia

En la tabla 22 se establece el registro de los roles, responsabilidades y objetivos por cada participante del equipo del proyecto.

Tabla 22. Roles y Responsabilidades
Fuente: Elaboración propia

Rol	Responsabilidades	Objetivos
Sponsor	Patrocinador y toma de decisiones.	Brindar respaldo y prioridad al proyecto.
Dirección	Patrocinador y toma de decisiones.	Asegurar la correcta implementación desde el punto de vista técnico.
Gerente de Proyecto	Liderazgo del proyecto. Responsable de la gestión y monitoreo del proyecto y de la definición de estándares (PMO).	Resolver principales problemas y riesgos que se presenten en el proyecto.
Líder de Proyecto	Responsable del diseño, ejecución y monitoreo de las iniciativas comprendidas del proyecto.	Llevar a cabo el proyecto con éxito, asegurando su culminación con el alcance, tiempo, costo y calidad requeridos.
Analista de Procesos	Encargado del análisis y mejoramiento de los procesos involucrados, genera y monitorea indicadores de gestión e identifica la optimización de los procesos.	Ejecutar la gestión del proyecto.

Rol	Responsabilidades	Objetivos
Usuarios del Proceso	Responsable de brindar. Facilidades para generar información.	Que sus necesidades puedan ser atendidas de forma ágil y sencilla.
Referente de Ciberseguridad	Resolver principales problemas y riesgos que se presenten en el proyecto.	Asegurar la correcta implementación desde el punto de vista técnico.

3.11. Plan de Costos

En la tabla 23 muestra un resumen del presupuesto del equipo de trabajo encargado de ejecutar la implementación con el apoyo de consultores y provisión de personal parte del equipo del SOC.

Tabla 23. Presupuesto del Equipo de Trabajo
Fuente: Elaboración propia

Recursos	Valor estimado
Jefe de Proyecto (14 meses)	S/ 87,010.00
Equipo SOC (1 recurso por 14 meses)	S/ 43,505.00
Consultoría de referente de Ciberseguridad	S/ 32,000.00
Gastos Administrativos	S/ 10,000.00
Reservas de Contingencia	S/ 5,000.00
Total	**S/ 177,515.00**

3.12. Plan de Comunicación

En la tabla 24 se establece los mecanismos de comunicación que debe ser ejecutado por el equipo de trabajo en el tiempo de duración del proyecto de implementación.

Tabla 24. Plan de Comunicación
Fuente: Elaboración Propia

Interesado(s)	Acción de Comunicación	Objetivo	Responsable	Frecuencia	Canal de comunicación
Equipo de proyecto	Coordinaciones del avance de actividades.	Mantener informados para el cumplimiento de las actividades en fechas comprometidas.	Jefe de Proyecto	Semanal	Correo electrónico, SharePoint
Gerencia de Seguridad	Informe de Riesgos	Informar el avance del proyecto.	Jefe de Proyecto	Quincenal	Correo electrónico, SharePoint
Dirección de Marketing	Informe de Gestión	Informar los riesgos y problemas del proyecto.	Jefe de Proyecto	Mensual	Correo electrónico, SharePoint

3.13. Cronograma de implementación

Tabla 25. Cronograma de implementación
Fuente: Elaboración propia

ACTIVIDADES	JEFE DEL ÁREA	NIVEL ESPECIALISTA	OFICINA DE SEGURIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6	MES 7	MES 8	MES 9	MES 10
IMPLEMENTACION DE MARCO DE CIBERSEGURIDAD BASADO EN NIST NIVEL 3													
GESTION DE PROYECTO	x												
Plan de Gestión de proyecto	x												
Registro de partes intersados	x												
Informe de Gestión	x												
Registro de riesgos y problemas	x												
Implementación alineados a las funciones y categorías													
IDENTIFICAR													
Entorno Empresarial (ID.BE)		x	x										
Estrategia de Gestión de Riesgos (ID.RM)			x										
Evaluación de riesgos (ID.RA)			x										
Gestión de activos (ID.AM)		x											
Gobernabilidad (ID.GV)		x	x										
PROTEGER													
Mantenimiento (PR.MA)		x											
Procesos y procedimientos de protección de la información (PR.IP)		x											
Seguridad de datos (PR.DS)		x											
Sensibilización y Capacitación (PR.AT)		x	x										
Tecnología de Protección (PR.PT)		x											
DETECTAR													

ACTIVIDADES	JEFE DEL ÁREA	NIVEL ESPECIALISTA	OFICINA DE SEGURIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6	MES 7	MES 8	MES 9	MES 10
Anomalías y Eventos (DE.AE)		x											
Monitoreo Continuo de Seguridad (DE.CM)		x											
Procesos de Detección (DE.DP)		x											
RESPONDER													
Análisis (RS.AN)		x											
Comunicaciones (RS.CO)		x	x										
Mejoras (RS.IM)		x											
Planificación de Respuesta (RS.RP)		x											
RECUPERAR													
Comunicaciones (RC.CO)			x										
Mejoras (RC.IM)		x											
Planificación de la recuperación (RC.RP)		x											
DESPLIEGUE DEL MARCO DE CIBERSEGURIDAD													
Lanzamiento del marco	x												
Entrenamiento y soporte	x												
Mantenimiento de las mejoras	x												

CAPÍTULO 4: ANÁLISIS FINANCIERO

Este capítulo contiene el análisis financiero alineado a la implementación del plan de acción propuesto que contempla los recursos y equipamiento a adquirir.

4.1. Análisis de Beneficios

El análisis de los beneficios del plan de acción se enfoca en detallar los costos que genera el área y como estos disminuirían con la implementación de equipos que automaticen la carga manual que está expuesta a error y reducir costos de recursos además de reducir las penalidades como se indicó en la figura 9.

Actualmente en el área se contrata servicios de terceros en un total de 37 recursos divididos en 3 niveles; N1 Requerimientos, N2 Incidencias y N3 Especialistas que incurre en gastos anuales de S/ 3,255,670.56 como indica la tabla 26.

Tabla 26. Costos de Terceros
Fuente: Elaboración propia

Cantidad	Niveles	Número de meses	Costo Mensual	Total
18	N1 Requerimientos	12	S/ 6,215.44	S/ 1,342,535.04
13	N2 Incidencias	12	S/ 7,652.92	S/ 1,193,855.52
6	N3 Especialistas	12	S/ 9,990.00	S/ 719,280.00
Total general				**S/ 3,255,670.56**

Se debe enfocar que la implementación de herramientas apunta a una reducción sustancial de esta inversión lo cual beneficia a la empresa en sinergia de costos.

4.2. Análisis de Inversión

Dentro de las necesidades de implementar el equipamiento en CAPEX se proyecta invertir el monto de S/ 3,790,663.40.

Tabla 27. Inversión de herramientas
Fuente: Elaboración propia

Proyecto	Descripción	Fabricante	Costo
Herramienta Administración de eventos	Colecta los logs, genera metadatos de estos logs los indexa a un mismo formato para generar eventos de seguridad.	Abierto	S/ 1,926,664.40
Herramienta de compliace	Identificar automáticamente brechas en el cumplimiento, remediarlas y poder cumplir con las diferentes auditorias.	Abierto	S/ 850,000.00

Proyecto	Descripción	Fabricante	Costo
Herramientas de monitoreo	Análisis del funcionamiento de los equipos de seguridad con la finalidad de evitar fallos en la red.	Abierto	S/ 510,000.00
Herramienta DLP	Implementación de DLP en la red para evidenciar las fallas de seguridad e implementar la mejoras.	Abierto	S/ 204,000.00
Herramienta de Análisis Forense	Herramienta para análisis forense a activos de la red de servicios para encontrar evidencia y por donde ingresa el ataque.	Abierto	S/ 299,999.00
Total general			**S/ 3,790,663.40**

De los cuáles al implementar herramientas como administración de eventos, monitoreo, instalación de un DLP entre otras como se detalla en la tabla 27, en este sentido se reemplazaría tareas manuales que realizan los recursos por tareas automáticas reduciendo el personal de 37 a 24 y 32 recursos en segundo y tercer año respectivamente, se detalla los montos en la tabla 28 y 29.

Tabla 28. Costos de Terceros por 32 recursos
Fuente: Elaboración propia

Cantidad	Niveles	Número de meses	Costo Mensual	Total
16	N1 Requerimientos	12	S/6,215.44	S/1,193,364.48
10	N2 Incidencias	12	S/7,652.92	S/918,350.40
6	N3 Especialistas	12	S/9,990.00	S/719,280.00
Total general				**S/2,830,994.88**

Tabla 29. Costos de Terceros por 24 recursos
Fuente: Elaboración propia

Cantidad	Niveles	Número de meses	Costo Mensual	Total
14	N1 Requerimientos	12	S/6,215.44	S/1,044,193.92
6	N2 Incidencias	12	S/ 7,652.92	S/ 551,010.24
4	N3 Especialistas	12	S/9,990.00	S/479,520.00
Total general				**S/ 2,074,724.16**

4.3. Análisis financiero

Se procedió en realizar el flujo de caja para poder definir si la inversión es viable, además se analizó la inversión por 3 años como se muestra en la tabla 30.

Tabla 30. Flujo de caja
Fuente: Elaboración propia

	AÑO 0	AÑO 1	AÑO 2	AÑO 3
Gastos Totales del Proyecto				
Inversión				
Herramienta Administración de eventos	(S/.1,926,664)			
Herramienta de compliace	(S/.850,000)			
Herramientas de monitoreo	(S/.510,000)			
Herramienta DLP	(S/.204,000)			
Herramienta de Análisis Forense	(S/.299,999)			
Capacitación de personal	(S/.33,410)			
Proyecto implementación de marco	(S/.177,515)			
Recurrentes				
Soporte Herramienta Administración de eventos		(S/.167,116)	(S/.167,116)	(S/.167,116)

	AÑO 0	AÑO 1	AÑO 2	AÑO 3
Soporte Herramienta de compliace		(S/.25,477)	(S/.25,477)	(S/.25,477)
Soporte Herramientas de monitoreo		(S/.55,135)	(S/.55,135)	(S/.55,135)
Soporte Herramientas DLP		(S/.22,054)	(S/.22,054)	(S/.22,054)
Soporte Herramienta de Análisis Forense		(S/.36,000)	(S/.36,000)	(S/.36,000)
Soporte de terceros	(S/.3,255,671)	(S/.3,255,671)	(S/.2,830,995)	(S/.2,074,724)
Beneficios Tangibles				
Ahorra de penalidades		S/.0	S/.7,165,628	S/.10,748,442
Ahorro por eficiencia operativa		S/.0	S/.424,676	S/.1,180,946
Flujo de Caja Bruto	**(S/.7,257,259)**	**(S/.3,765,307)**	**S/.4,249,673**	**S/.9,345,028**
Factor de Descuento:				
10%	1.0000	0.9091	0.8264	0.7513
Flujo de Caja Neto Descontado	**(S/.7,223,849)**	**(S/.3,237,716)**	**S/.3,680,395**	**S/.7,174,075**

Tabla 31. Indicadores financieros
Fuente: Elaboración propia

Indicador	Valor
VAN - Valor Presente Neto	S/ 392,905.16
TIR- Tasa Interna de Retorno	11.740%
Periodo Recuperación Descontada	**2.95**

Por los valores calculados, se observa que el proyecto es viable en el ámbito financiero por lo siguiente:

- El VPN (Valor Presente Neto) es positivo con un valor de **S/ 392,905.16** que nos indica un beneficio para la empresa EP.
- El TIR (Tasa Interna de Retorno) supera a la tasa de descuento que utiliza la empresa con un valor del **11.74%** lo cual aporta para que el proyecto sea viable.
- Además, el periodo de recuperación es de 2.95 años es decir 36 meses aproximadamente, lo cual nos indica que se cuenta con un tiempo razonable para recuperar la inversión del equipamiento de herramientas.

CONCLUSIONES

1. Con la perspectiva de ciberseguridad y/o riesgo, adoptando el Marco del NIST para mejorar la ciberseguridad de las infraestructuras críticas, es un factor importante en la creación de valor para las empresas. La metodología de adopción para ejecutar el marco debe tener un enfoque de gobernanza coherente para adoptar una buena decisión. Este marco es un modelo flexible que se pueden modificar para satisfacer las necesidades de la empresa y permite que cualquier organización tenga un marco central probado y repetible.

2. El Marco del NIST elaborado en esta propuesta, aporta en la creación de estrategias de ciberseguridad para una empresa del sector Telecomunicaciones, tomando este tema como prioritario sobre la base del análisis de experiencias y publicaciones reconocidas en la materia y ayudando a identificar servicios críticos.

3. El modelo desarrollado representa el primer paso para proteger los servicios críticos de del área de servicios de seguridad, su aplicación debe integrar múltiples miradas e identificar las interdependencias entre sectores para determinar los impactos directos e indirectos. Como queda evidenciado, en la actualidad, ante un incidente de ciberseguridad que afecte un servicio crítico, la mayoría de las empresas no cuenta con protocolos de respuesta para saber cómo proceder.

4. La Ciberseguridad gestionada en el área de servicios de seguridad es un compromiso compartido de todos los niveles jerárquicos dentro de la empresa, para ello se debe elaborar un plan adecuado de implantación de esquemas de Ciberseguridad con la adecuada coordinación de todas las áreas de la empresa.

5. Los resultados de la encuesta al personal del área de servicios de seguridad informática nos permitieron conocer la falta de conocimiento de ciberseguridad, dejando así al área vulnerable a todos los riesgos cibernéticos de información vital y privada de la misma, por lo que es necesario implantar una cultura de ciberseguridad en el área.

6. El análisis de este trabajo permitió evaluar al área de servicios de seguridad en tomar en cuenta la importancia que se debe considerar la ciberseguridad en la gestión del área y con la realización de este trabajo se desea promover y motivar a las empresas en temas de ciberseguridad y a la vez que los colaboradores tomen conciencia de como utilizan la tecnología en sus labores diarias.

7. Finalmente, con el análisis financiero se concluye que es viable para la empresa, obteniendo un VPN positivo de S/ 392,905.16, lo cual apalanca a los beneficios de la empresa, con un TIR que supera al que usa la empresa de 10% a 11.74% y por concluir en un tiempo de 36 meses el cuál es bastante razonable para la implementación del marco de seguridad en el área.

RECOMENDACIONES

1. El Marco del Nist permite que tanto la alta dirección como los ingenieros y demás personal de TI comprendan fácilmente qué se debe implementar y dónde están las vulnerabilidades por lo que se debe incluir dentro de las funciones de la alta dirección identificar con visión proactiva las mejoras de ciberseguridad.

2. El Marco del NIST está enfocada a planificar e implementar la seguridad cibernética, pero sin una medición constante, revisión, auditoría, acciones correctivas y mejoras, dicho sistema se deteriorará gradualmente y finalmente pierde su propósito por lo que se requiere una constante revisión de las áreas competentes.

3. La ciberseguridad de una organización depende de muchos factores tanto tecnológicos como humanos y las normas que la regulan, es muy importante el diseño de una política de ciberseguridad para el área de servicios de seguridad, con la finalidad de asegurar el compromiso de toda la organización, desde la dirección hasta cualquier empleado.

4. Establecer estrategias de formación y de capacitación permanente en materia de ciberseguridad y de carácter obligatorio a todos los trabajadores que conozcan las prácticas indispensables en esta materia ya que son un filtro importante de información cibernética de la empresa la cual debe ser protegida y resguardada.

5. El área de servicios de seguridad debe trabajar con políticas de seguridad e instalar todas las medidas tecnológicas que están a su alcance como el uso de firewalls, routers, end points, de marcas reconocidas y comprometerse en la actualización inmediata de parches de seguridad frente a nuevas vulnerabilidades detectadas en el diseño del código de desarrollo utilizado. El uso de antivirus, antimalware es fundamental para que el SOC (Security Operations Center) propio, pueda actuar en un servicio 24x7x365 días y actuar sobre la infraestructura en caso de ataque o, lo más importante, prevenir amenazas ante ataques posibles que se estén realizando a otros usuarios en cualquier lugar del mundo.

6. Establecer control de uso de claves seguras, suficientemente largas y robustas dentro de la política de seguridad, donde los usuarios tengan acceso a entornos seguros, inhabilitar la navegación por páginas que estén incluidas en listas negras, además implantar la utilización sistemática programada de copias de seguridad ante un ataque de ransomware, ya que permite borrar la maquina infectada y actualizarla con la copia de seguridad más reciente. Con eso se evitará: traumas, crisis y, sobre todo, no se alimentará la cibercriminalidad.

GLOSARIO DE TERMINOS

B

BIA (del inglés Business Impact Analysis)

C

Categoría

La subdivisión de una función en grupos de resultados de ciberseguridad, estrechamente ligada a necesidades programáticas y actividades particulares. Ejemplos de categorías incluyen "Gestión de activos", "Control de acceso" y "Procesos de detección".

Cartera

Un grupo de programas, proyectos, servicios o activos seleccionados, gestionados y monitoreados para optimizar el rendimiento del negocio.

Ciberseguridad

El proceso de proteger la información mediante la prevención, detección y respuesta a los ataques.

Código Móvil

Un programa (por ejemplo, script, macro u otra instrucción portátil) que se puede enviar sin cambios a una colección heterogénea de plataformas y ejecutarse con semántica idéntica.

D

Detectar (Función)

Desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.

E

Evento de seguridad informática

Es una ocurrencia identificada de un estado de un sistema, servicio o red que indica que una posible violación de la política de seguridad de la información, la falla de medidas de seguridad o una situación previamente desconocida, que pueda ser relevante para la seguridad. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones]

F

Framework (Marco)

Un enfoque basado en el riesgo para reducir el riesgo de la ciberseguridad, compuesto de tres partes: el Marco básico (Framework Core), el perfil marco y los Niveles de implementación del marco (Framework Implementation Tiers) (Framework Implementation Tiers). También conocido como el "Marco de Ciberseguridad".

Framework Core básico (Marco básico (Framework Core))

Un conjunto de actividades y referencias de ciberseguridad que son comunes en los sectores de infraestructura crítica y se organizan en torno a determinados resultados. El Framework Core comprende cuatro tipos de elementos: Funciones, Categorías, Subcategorías y Referencias Informativas.

Función

Uno de los principales componentes del Marco. Las funciones proporcionan el nivel más alto de estructura para organizar las actividades básicas de ciberseguridad en categorías y subcategorías. Las cinco funciones son Identificar, Proteger, Detectar, Responder y Recuperar.

G

Gestión de riesgos

El proceso de identificación, evaluación y respuesta al riesgo.

I

Identificar (función)

Desarrollar el entendimiento organizacional para manejar el riesgo de ciberseguridad a sistemas, activos, datos y capacidades.

Incidente de ciberseguridad

Un cambio de ciberseguridad que puede tener un impacto en las operaciones de la organización (incluida la misión, las capacidades o la reputación).

Incidente de seguridad informática

Es una violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que compromete la seguridad de un sistema (confidencialidad, integridad o disponibilidad). [Decreto N° 451/009 de 28 de Setiembre 2009-Art.3 Definiciones]

Incidente de seguridad de la información

Un incidente de seguridad de la información es indicado por un único o una serie de eventos indeseados o inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información. [ISO/IEC 27035:2011]

Infraestructura Critica

Sistemas y activos físicos o virtuales tan vitales para los Estados Unidos que la incapacidad o destrucción de tales sistemas y activos tendría un impacto debilitante en la ciberseguridad, la seguridad económica nacional, la salud pública nacional o la seguridad, o cualquier combinación de estos asuntos.

L

Línea base

Una especificación o producto que se ha revisado formalmente y sobre los que se ha llegado a un acuerdo, y que de ahí en adelante sirve como base para un desarrollo posterior y que puede cambiarse solamente a través de procedimientos formales de control de cambios. [IEEE 610.12/1990]

Nivel de implementación del marco

Una lente a través de la cual ver las características del enfoque de riesgo de una organización - cómo una organización ve el riesgo de ciberseguridad y los procesos en marcha para manejar ese riesgo.

P

Perfil del marco Función

Una representación de los resultados que un sistema u organización particular ha seleccionado de las categorías de marco y subcategorías.

Plan de respuesta a incidentes

Este documento contiene, además del procedimiento de respuesta a incidentes, la planificación de la respuesta, por ejemplo: introducción, roles y responsabilidades, metodología, fases de las respuestas a incidentes, plan de comunicación, documentación, etc.

Propietario de activos

El término propietario identifica un individuo o entidad que ha probado habilidades de gestión para controlar la producción, desarrollo, mantenimiento, uso y seguridad de un activo. El término propietario no significa que la persona tiene efectivamente derechos de propiedad sobre el activo. [AGESIC (políticas marco, políticas del SGSI, políticas de Presidencia – Manual de Polític

Proteger (función)

Desarrollar e implementar las salvaguardias apropiadas para asegurar la provisión de servicios de infraestructura crítica.

R

Referencia informativa

Una sección específica de normas, directrices y prácticas comunes entre los sectores de infraestructura crítica que ilustra un método para lograr los resultados asociados con cada subcategoría. Un ejemplo de referencia informativa es el control ISO/IEC 27001 A.10.8.3, que soporta la subcategoría "Protección de Datos en tránsito" de la categoría "Seguridad de datos" en la función "Proteger".

Recuperar (función)

Desarrollar e implementar las actividades apropiadas para mantener los planes de resiliencia y restaurar las capacidades o servicios que fueron deteriorados debido a un evento de ciberseguridad.

Responder (función)

Desarrollar e implementar las actividades apropiadas para tomar medidas con respecto a un evento de ciberseguridad detectado.

Riesgo

S

SLA (del ingles Service Level Agreement)

Acuerdo negociado entre dos partes, una cliente y otra proveedora, donde se definen puntos comunes de entendimiento sobre servicios, prioridades, responsabilidades y garantías. Incluye elementos tales como definición de los servicios, garantías y finalización del acuerdo, medición del rendimiento, gestión de problemas, obligaciones de las partes, entre otros.

Software de aplicación

Programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos.

Software de base

Software que sirve para controlar e interactuar con el sistema operativo, proporcionando control sobre el hardware y dando soporte a otros programas, incluyendo el propio sistema operativo.

Subcategoría

La subdivisión de una Categoría en resultados específicos de actividades técnicas y/o de gestión. Los ejemplos de subcategorías incluyen "Los sistemas de información externos están catalogados", "Los datos en reposo están protegidos" y "Se investigan las notificaciones de los sistemas de detección".

U

Usuario privilegiado

Un usuario autorizado (y, por lo tanto, de confianza) para realizar funciones de seguridad que los usuarios comunes no están autorizados a realizar

V

Valor

El(los) resultado(s) final(es) esperado(s) de una inversión de negocio posibilitada porTI

W

WAF (del ingles Web Application Firewall)

Un Firewall de Aplicaciones Web es un dispositivo de hardware o software que permite proteger los servidores de aplicaciones web de determinados ataques específicos en Internet.

BIBLIOGRAFIA

[1] Expansión. (2018). *17 datos sobre internet en su día mundial. [Online] Available at*: https://expansion.mx/empresas/2018/05/17/17-datos-sobre-internet-en-su-dia-mundial

[2] (INEGI), I. (2018). *TIC's en hogares. [Online] Beta.inegi.org.mx. Available at*: http://www.beta.inegi.org.mx/temas/ticshogares/

[3] Cisco. (2018). *Cybersecurity Essentials. [Online] Available at:* https://static-course-assets.s3.amazonaws.com/CyberEss/es/index.html#2.2.2.1

[4] Avast.com. (2018). *¿Qué es el malware y cómo eliminarlo? | Antimalware. [Online] Available at:* https://www.avast.com/es-es/c-malware

[5] Cisco. (2018). *Informe de ciberseguridad anual de 2018 de Cisco - [Online] Cisco. Available at:* https://www.cisco.com/c/es_mx/products/security/security-reports.html

[6] CIO PERU (2014). *5 habilidades necesarias para un analista de SOC - CIO Perú 13/06/2014 Available at:* https://cioperu.pe/articulo/16145/5-habilidades-necesarias-para-un-analista-de-soc/

[7] Hewlett Packard (2016). *State of security operations Available at:*

https://www.thehaguesecuritydelta.com/media/com_hsd/report/55/document/State-of-SOC-operations-2016--2-.pdf

[8] Micro Focus (2018) *Consultoría de operaciones e inteligencia de seguridad Available at: :* https://software.microfocus.com/es-es/services/security-operations-center?jumpid=va_d1842km6bu

[9] Kaspersky lab (2016). *SOC con tecnología de Kaspersky Lab Available at:* https://media.kaspersky.com/es/business-security/enterprise/2017_%20Brochure_SOC_powered_by_KL.pdf

[10] Draft of the Preliminary Cybersecurity Framework (28/08/2013). *Discussion Draft of the Preliminary Cybersecurity Framework:* http://www.isaca.org/Knowledge-Center/Research/Documents/US-preliminary-cybersecurity-framework_res_eng_0913.pdf

ANEXOS

Anexo 1 Evaluación del personal del SOC

	Conocimiento								Desempeño					Actitud				Habilidades				Experiencia			Training			Liderazgo			
NOMBRE	De la ciencia básica en	De las operaciones de TI	De los conceptos de	De la gestión de la	De códigos maliciosos	De las técnicas básicas de	De técnicas de inteligencia	De lenguas extranjeras	Capacidad de delegar tareas	Cumplimiento de los	Exactitud y calidad de trabajo	Productividad	Responsabilidad	Actitud hacia al área	Actitud hacia superior/es	Actitud hacia los compañeros	Actitud hacia el	Iniciativa	Respuesta bajo presión	Potencialidad - Capacidad de	Coordinación	En la industria de TI	Entorno en sistemas	Rol en el SOC	Presupuesto	Importancia	Efectividad	Visión	Soporte de recursos humanos	Experiencia	Ámbito de control
Jimmy Cabrejos	1	2	3	2	2	0	0	1	3	4	2	3	4	4	1	1	2	4	0	3	0	0	3	0	2	1	0	3	2	3	1
Marlon Torrres	2	3	0	2	0	0	0	1	1	0	0	2	2	4	0	1	1	4	3	3	1	2	2	2	1	2	2	2	1	0	2
Marilu Intuscca	1	1	1	1	1	0	0	1	3	2	3	3	1	1	2	3	1	3	2	3	1	1	3	2	3	0	1	0	0	1	1
Giovani Catacora	1	1	4	3	2	1	0	1	1	3	2	5	3	5	2	1	2	4	1	4	5	1	2	5	2	3	2	4	3	3	3
Henry Falconi	1	1	1	1	3	1	1	1	2	5	3	4	3	2	5	1	1	4	1	4	1	1	4	3	2	2	2	3	2	3	1
Hugo Cabrera	3	2	2	1	1	0	0	1	1	2	3	2	3	2	4	4	2	1	3	3	2	1	0	1	0	1	2	3	2	0	1
Julio Roque	3	2	1	1	1	0	0	1	1	4	3	4	1	3	3	4	2	4	4	0	4	3	4	3	2	0	1	2	1	3	2
Miguel Miyahira	3	3	3	2	3	3	3	3	5	3	2	4	3	3	3	2	3	3	4	5	5	3	2	5	3	3	3	3	2	3	1
Miguel Soriano	3	1	1	3	2	1	1	1	5	3	3	5	3	4	1	4	2	5	5	4	2	3	4	4	3	3	3	3	2	3	3
Jean Piere Herrera	3	1	3	2	0	0	0	2	1	2	2	2	3	2	1	1	1	3	3	1	2	0	1	3	1	2	1	2	1	0	0
Diego Humari	3	1	0	0	0	0	0	4	1	2	2	2	2	1	4	2	0	2	0	3	0	0	0	2	1	2	1	3	2	0	1
Diego Zuñiga	2	3	4	3	3	1	2	1	5	1	4	4	1	5	4	1	2	1	5	5	2	2	5	5	3	2	2	2	1	2	3

	Conocimiento								Desempeño					Actitud				Habilidades				Experiencia			Training			Liderazgo			
NOMBRE	De la ciencia básica en	De las operaciones de TI	De los conceptos de	De la gestión de la	De códigos maliciosos	De las técnicas básicas de	De técnicas de inteligencia	De lenguas extranjeras	Capacidad de delegar tareas	Cumplimiento de los	Exactitud y calidad de trabajo	Productividad	Responsabilidad	Actitud hacia al área	Actitud hacia superior/es	Actitud hacia los compañeros	Actitud hacia el	Iniciativa	Respuesta bajo presión	Potencialidad - Capacidad de	Coordinación	En la industria de TI	Entorno en sistemas	Rol en el SOC	Presupuesto	Importancia	Efectividad	Visión	Soporte de recursos humanos	Experiencia	Ámbito de control
Jorge Chavez	3	2	4	1	1	0	0	1	0	0	0	3	1	3	1	3	3	3	2	3	4	4	0	1	1	1	1	3	2	2	1
William Soto	3	2	2	1	1	0	0	1	1	2	3	2	3	2	4	4	2	1	3	4	4	1	0	1	0	1	3	3	2	0	1
Aldo Lopez	4	3	3	3	4	3	3	3	4	2	2	5	4	2	2	3	2	3	3	3	3	5	2	2	3	3	3	3	2	4	2
Marco Coronado	2	2	3	1	3	0	3	3	5	4	5	3	1	4	4	5	5	1	1	5	4	3	3	1	2	1	2	3	2	4	2
Frank Alvarado	1	1	0	2	1	0	0	1	2	2	2	3	1	3	1	3	1	0	3	2	0	1	4	1	1	1	2	3	2	0	1
Solange Carrillo	1	2	3	1	1	0	0	2	3	2	1	3	4	3	1	1	0	4	4	0	3	3	3	4	1	1	0	2	1	4	3
Marco Ramos	1	1	2	1	1	0	0	1	3	2	4	3	1	3	1	3	2	3	2	1	3	4	2	2	2	3	0	2	1	4	1
Jefferson Aguilar	3	1	3	1	1	0	0	1	2	3	0	1	4	2	0	3	0	0	0	0	1	4	3	4	2	1	1	3	2	1	1
Carlos Ordinola	2	3	3	1	1	0	0	1	0	3	1	3	4	2	0	0	0	0	3	2	2	1	2	3	0	2	1	3	2	4	3
Fredy Pacori	3	1	0	2	2	0	1	1	1	0	1	3	2	2	2	3	1	2	3	0	2	1	4	0	3	1	3	0	0	1	0
Alejandro Zarate	3	3	1	2	3	0	0	1	0	2	2	4	4	4	4	2	1	4	4	4	4	4	0	2	3	1	2	1	0	1	0
Consuelo Torres	1	3	2	1	2	0	1	1	2	3	3	4	4	2	1	5	4	1	5	5	3	2	5	4	3	3	1	3	2	4	1
Jorge Bellon	4	3	3	3	2	1	1	1	3	5	2	5	2	2	2	3	3	3	5	4	4	1	5	5	2	2	1	3	2	5	2
Juan Vilca	1	3	2	4	0	1	3	1	4	0	3	4	4	1	2	0	3	0	0	1	1	4	2	0	1	1	2	1	0	4	2
Luis Lumba	1	2	0	2	1	0	0	1	1	4	2	4	1	1	2	1	1	2	2	3	1	2	0	1	3	1	3	1	0	3	1
Luis Aragon	2	2	1	3	1	1	0	1	2	3	5	4	1	5	2	3	5	3	3	1	3	3	4	5	3	2	2	2	1	2	1
Luis Nuñez	1	2	3	3	3	1	0	2	2	4	1	5	4	2	2	3	3	3	0	0	2	3	4	4	3	3	3	0	0	2	0

	Conocimiento								Desempeño					Actitud				Habilidades				Experiencia			Training			Liderazgo			
NOMBRE	De la ciencia básica en	De las operaciones de TI	De los conceptos de	De la gestión de la	De códigos maliciosos	De las técnicas básicas de	De técnicas de inteligencia	De lenguas extranjeras	Capacidad de delegar tareas	Cumplimiento de los	Exactitud y calidad de trabajo	Productividad	Responsabilidad	Actitud hacia al área	Actitud hacia superior/es	Actitud hacia los compañeros	Actitud hacia el	Iniciativa	Respuesta bajo presión	Potencialidad - Capacidad de	Coordinación	En la industria de TI	Entorno en sistemas	Rol en el SOC	Presupuesto	Importancia	Efectividad	Visión	Soporte de recursos humanos	Experiencia	Ámbito de control
Bruce Ramos	1	2	3	1	3	1	2	1	1	3	1	1	1	2	2	0	1	1	3	0	3	0	2	1	3	2	3	3	2	3	0
Elvis Apaza	4	2	4	3	0	1	2	1	4	4	2	4	4	1	0	0	3	4	1	1	2	2	4	3	2	3	1	3	2	4	1
Erika Changano	1	1	2	2	2	0	1	1	2	0	0	3	1	3	4	1	3	1	2	4	4	3	0	3	1	3	3	3	2	3	2
Jose Foronda	4	2	3	1	3	0	4	1	4	0	4	3	1	4	3	1	1	1	4	2	1	4	0	1	2	2	3	3	2	1	2
Juan Ccanccapa	1	1	2	2	1	0	3	1	3	1	2	4	1	1	3	1	0	1	0	4	4	2	0	0	2	1	1	0	0	2	1
Liliana Sanchez	1	1	1	1	1	0	1	1	3	4	2	3	2	3	4	3	0	2	1	1	3	0	0	3	0	3	0	4	3	4	3
Luis Juarez	3	3	2	1	2	0	2	1	1	1	1	2	1	4	0	1	0	1	1	0	2	2	1	0	1	1	0	3	2	3	1
Tito Choque	4	3	0	4	4	1	4	1	2	4	4	3	3	3	3	4	4	4	4	1	2	2	1	0	1	0	2	0	0	2	1

Anexo 2 Análisis del Perfil actual

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
1	IDENTIFICAR (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar objetivos de negocio se identifican y gestionan de acuerdo con su importancia relativa para los objetivos de negocio y la estrategia de riesgo de la organización.	**ID.AM-1:** Los dispositivos físicos y los sistemas dentro de la organización son inventariados	Nivel 2: Riesgo Informado	Actualmente se realiza el registro de los dispositivos físicos, sistemas en la herramienta de ticketing "remedy" el cual el registro está a cargo del área de Oficina de Seguridad como indica en el instructivo "Registro de Alta de Clientes en Remedy".
2			**ID.AM-2:** Las plataformas de software y las aplicaciones dentro de la organización son inventariadas	Nivel 2: Riesgo Informado	Actualmente se realiza el inventario de las aplicaciones dispositivos físico y plataformas en la herramienta de ticketing "remedy" el cual el registro está a cargo del área de Nivel de Especialista, como indica su flujo de atenciones.
3			**ID.AM-3:** La comunicación organizacional y los flujos de datos están mapeados	Nivel 3: Repetible	Actualmente se encuentra registrado los flujos de atención de los clientes hacia el área como indica la figura de flujo de atención.
4			**ID.AM-4:** Se catalogan los sistemas de información externos	Nivel 1: Parcial	Actualmente no se encuentra sistemas de información expuesto a nivel público, se cuenta con información netamente confidencial que está alojado en un file server en la red interna del área.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
5			**ID.AM-5:** Los recursos (por ejemplo, hardware, dispositivos, datos y software) se priorizan en función de su clasificación, criticidad y valor comercial	Nivel 1: Parcial	Actualmente los recursos se encuentran priorizados.
6			**ID.AM-6:** Se establecen las funciones y responsabilidades de la ciberseguridad para toda la fuerza de trabajo y las partes interesadas de terceros (por ejemplo, proveedores, clientes, socios)	Nivel 1: Parcial	Actualmente no se han establecidos las funciones, responsabilidades de ciberseguridad.
7		**Entorno Empresarial (ID.BE):** Se entiende y prioriza la misión, los objetivos, las partes interesadas y las actividades de la organización; Esta información se utiliza para informar las funciones de ciberseguridad, las responsabilidades y las decisiones de gestión de riesgos.	**ID.BE-1:** El rol de la organización en la cadena de suministro es identificado y comunicado	Nivel 2: Riesgo Informado	Se tiene identificado 3 sub área en el SOC como Nivel Avanzado, Nivel Especialista y Oficina de seguridad, así como las funciones respectivas.
8			**ID.BE-2:** El lugar de la organización en la infraestructura crítica y su sector industrial se identifica y se comunica	Nivel 2: Riesgo Informado	El área comunica a sus clientes cuando se identifica la criticidad de los equipos que se gestiona a través de un informe de Incidencias realizado por unos de los equipos de Nivel Avanzado o Nivel Especialista.
9			**ID.BE-3:** Se establecen y se comunican las prioridades de la	Nivel 1: Parcial	Actualmente no se está estableciendo, ni comunicando al equipo.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
			misión, los objetivos y las actividades de la organización		
10			**ID.BE-4:** Se establecen dependencias y funciones críticas para la prestación de servicios críticos	Nivel 2: Riesgo Informado	Se encuentra establecidas y asociadas a los equipos de trabajo Nivel Avanzado y Nivel Especialista de las cuales están definidas sus funciones respectivamente.
11			**ID.BE-5:** Los requisitos de resistencia para apoyar la prestación de servicios críticos se establecen	Nivel 1: Parcial	Se encuentre establecidos de manera proactiva, no se encuentra definidos en un instructivo con su alcance hasta donde prestar el apoyo.
12		**Gobernabilidad (ID. GV):** Las políticas, procedimientos y procesos para administrar y monitorear los requerimientos regulatorios, legales, de riesgo, ambientales y operativos de la organización son entendidos e informar a la gerencia del riesgo de ciberseguridad.	**ID. GV-1:** Se establece la política de seguridad de la información organizacional	Nivel 1: Parcial	Actualmente se cuenta con un procedimiento de obligaciones y recomendaciones de Seguridad que está establecida para toda la Dirección de Ingeniería y Gestión de Core y Plataformas, que repercuta en el área de SOC de Clientes ya que se encuentra en esta dirección.
13			**ID. GV-2:** Las funciones y responsabilidades de seguridad de la información están coordinadas y alineadas con las funciones internas y los socios externos	Nivel 3: Repetible	En la oferta técnica que es derivada al área del SOC cuando se realiza el alta de un nuevo cliente, están definidas las responsabilidades y las coordinaciones que se debe tener con los socios externos.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
14			**ID. GV-3:** Los requisitos legales y reglamentarios relativos a la ciberseguridad, incluidas las obligaciones en materia de privacidad y libertades civiles, se entienden y se gestionan	Nivel 1: Parcial	Actualmente no se cuenta establecido.
15			**ID. GV-4:** Los procesos de gobernanza y gestión de riesgos abordan los riesgos de la ciberseguridad	Nivel 1: Parcial	Actualmente no se está considerando los riesgos en ciberseguridad.
16		**Evaluación de riesgos (ID.RA):** La organización entiende el riesgo de ciberseguridad para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y los individuos.	**ID.RA-1:** Se identifican y documentan las vulnerabilidades de activos	Nivel 1: Parcial	Actualmente se llega a identificar las vulnerabilidades de activos cuando se pública los CVE (Common Vulnerabilities and Exposures) que son expuestos de manera pública y afecten a los activos, pero no se realiza la documentación del impacto y/o mitigación del mismo.
17			**ID.RA-2:** La información sobre amenazas y vulnerabilidades se recibe de los foros y fuentes de intercambio de información	Nivel 2: Riesgo Informado	Actualmente se recibe información de las vulnerabilidades y amenazas que afecte los activos del servicio de Vigilancia Digital de Telefónica España.
18			**ID.RA-3:** Las amenazas, tanto internas como externas, son identificadas y documentadas	Nivel 1: Parcial	Actualmente solo se identifica, pero no se documenta.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
19			**ID.RA-4:** Se identifican los posibles impactos y probabilidades de los negocios	Nivel 1: Parcial	Actualmente no se realiza el impacto que pueda afectar al negocio todos estos ataques.
20			**ID.RA-5:** Se usan amenazas, vulnerabilidades, probabilidades e impactos para determinar el riesgo	Nivel 1: Parcial	Actualmente no se realiza.
21			**ID.RA-6:** Las respuestas al riesgo son identificadas y priorizadas	Nivel 1: Parcial	Las respuestas son de manera proactiva por el equipo de Nivel Avanzado, de acuerdo como este afecte en una incidencia, pero no se cuenta con respuestas asociadas a un riesgo ya identificado.
22		**Estrategia de Gestión de Riesgos (ID.RM):** Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y utilizan para apoyar las decisiones de riesgo operacional.	**ID.RM-1:** Los procesos de gestión de riesgos son establecidos, gestionados y acordados por las partes interesadas de la organización	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
23			**ID.RM-2:** La tolerancia al riesgo organizacional se determina y se expresa claramente	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
24			**ID.RM-3:** La determinación de la organización de la tolerancia al riesgo se basa en su papel en la infraestructura crítica y en el	Nivel 1: Parcial	Actualmente no se encuentra establecidos.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
			análisis de riesgos específicos de cada sector		
25	PROTEGER (PR)	**Control de acceso (PR.AC):** El acceso a los activos e instalaciones asociadas está limitado a usuarios, procesos o dispositivos autorizados, ya las actividades y transacciones autorizadas.	**PR.AC-1:** Las identidades y credenciales se administran para dispositivos y usuarios autorizados	Nivel 3: Repetible	Las identidades y credenciales están administradas por el equipo de Nivel Especialista y son desplegada solo a usuarios autorizados.
26			**PR.AC-2:** El acceso físico a los activos se gestiona y protege	Nivel 3: Repetible	Actualmente los activos físicos están siendo gestionados por el equipo de Nivel Especialista su función de ellos es gestionar estos activos y protegerlos de manera física y digital.
27			**PR.AC-3:** El acceso remoto se gestiona	Nivel 3: Repetible	Actualmente el equipo de Nivel Especialista son los que gestionan los accesos remotos.
28			**PR.AC-4:** Los permisos de acceso se gestionan, incorporando los principios del privilegio mínimo y la separación de funciones	Nivel 3: Repetible	Actualmente el encargado de definir la clasificación de los usuarios es el equipo de Nivel Especialista, ellos definen los niveles de la siguiente manera: usuario de lectura, usuario de escritura básico, usuario Admin (máximo privilegio).

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
29			**PR.AC-5:** La integridad de la red está protegida, incorporando la segregación de red cuando sea apropiado	Nivel 3: Repetible	Actualmente el encargado de proteger la red es el equipo de Nivel Especialista.
30		**Sensibilización y Capacitación (PR.AT):** El personal y los socios de la organización reciben educación para la concienciación en ciberseguridad y están adecuadamente capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad de la información, de acuerdo con las políticas, procedimientos y acuerdos relacionados.	**PR.AT-1:** Todos los usuarios están informados y capacitados	Nivel 2: Riesgo Informado	Actualmente todos los usuarios están informados de los servicios y de las funciones correspondientes y de los equipos que se gestionan, en este caso lo que afecta las capacitaciones es la alta rotación del personal de terceros.
31			**PR.AT-2:** Los usuarios privilegiados entienden las funciones y responsabilidades	Nivel 3: Repetible	Actualmente al brindar un usuario privilegiado se entrega una ficha donde se indica al usuario las funciones y responsabilidades que competen.
32			**PR.AT-3:** Terceros interesados (por ejemplo, proveedores, clientes, socios) entienden las funciones y responsabilidades	Nivel 3: Repetible	Actualmente el equipo de Oficina de Seguridad son los encargados de transmitir las funciones y responsabilidades los terceros al realizar altas nuevas con los clientes ya sea de un servicio o en el caso de instalación de un equipo con proveedores o socios.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
33			**PR.AT-4:** Los altos ejecutivos entienden roles y responsabilidades	Nivel 2: Riesgo Informado	Actualmente se tiene definido los roles y responsabilidades, pero por la premura de las atenciones del servicio no se cumple siempre.
34			**PR.AT-5:** El personal de seguridad física y de la información entiende las funciones y responsabilidades.	Nivel 1: Parcial	Actualmente no se cuenta con una persona de seguridad física y de información.
35		**Seguridad de datos (PR.DS):** La información y los registros (datos) se manejan de acuerdo con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-1:** Los datos en reposo están protegidos	Nivel 2: Riesgo Informado	Actualmente se cuenta con pocos datos de reposo los cuales están siendo protegidos en un almacén
36			**PR.DS-2:** Los datos en tránsito están protegidos	Nivel 1: Parcial	Actualmente el área no gestiona los datos en tránsito de la empresa
37			**PR.DS-3:** Los activos se administran formalmente durante la remoción, las transferencias y la disposición	Nivel 1: Parcial	Actualmente los activos siempre son administrados por el equipo de Nivel Especialista durante remoción, transferencia.
38			**PR.DS-4:** Se mantiene la capacidad adecuada para garantizar la disponibilidad	Nivel 3: Repetible	Actualmente se garantiza la disponibilidad con equipos en redundancia en sedes diferentes.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
39			**PR.DS-5:** Las protecciones contra fugas de datos se implementan	Nivel 3: Repetible	Actualmente se cuenta instalado en las PC de los terceros la herramienta DLP de McAffe que es gestionada por el equipo de Nivel Especialista que controlan los permisos correspondientes por usuarios.
40			**PR.DS-6:** Los mecanismos de verificación de integridad se utilizan para verificar el software, el firmware y la integridad de la información	Nivel 1: Parcial	Actualmente se está implementando en los equipos que tiene el área una herramienta de cumplimiento de políticas de seguridad de la marca FireMon.
41			**PR.DS-7:** Los entornos de desarrollo y prueba están separados del entorno de producción	Nivel 3: Repetible	Actualmente estos ambientes para pruebas lo gestionan el equipo de Nivel Especialista que controla
42		**Procesos y procedimientos de protección de la información (PR.IP):** Se mantienen y utilizan las políticas de seguridad (que abordan el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la administración y la coordinación entre las entidades organizacionales), procesos y procedimientos	**PR.IP-1:** Se crea y mantiene una configuración de línea de base de los sistemas de tecnología de la información / control industrial	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
43			**PR.IP-2:** Se implementa un ciclo de vida de desarrollo de sistemas para gestionar sistemas	Nivel 1: Parcial	Actualmente no se encuentra establecidos.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
44		para administrar la protección de los sistemas y activos de información.	**PR.IP-3:** Los procesos de control de cambio de configuración están en su lugar	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
45			**PR.IP-4:** Las copias de seguridad de la información se realizan, se mantienen y se prueban periódicamente	Nivel 3: Repetible	Actualmente contamos con un sistema que almacena las configuraciones diarias de los equipos.
46			**PR.IP-5:** Se cumplen las políticas y reglamentos relativos al entorno físico de funcionamiento de los activos de la organización	Nivel 2: Riesgo Informado	Actualmente se cumple las políticas y los reglamentos, se cuenta con un instructivo.
47			**PR.IP-6:** Los datos se destruyen según la política	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
48			**PR.IP-7:** Mejora continua de los procesos de protección	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
49			**PR.IP-8:** La eficacia de las tecnologías de protección se comparte con las partes apropiadas	Nivel 2: Riesgo Informado	Actualmente se cuenta con un responsable por cada equipo encargadas para compartir con las partes apropiadas
50			**PR.IP-9:** Planes de respuesta (Respuesta a Incidentes y Continuidad de Negocio) y planes de recuperación (Recuperación de	Nivel 1: Parcial	Actualmente no se encuentra establecidos.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
			Incidentes y Recuperación de Desastres)		
51			**PR.IP-10:** Se analizan los planes de respuesta y recuperación	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
52			**PR.IP-11:** La ciberseguridad se incluye en las prácticas de recursos humanos (por ejemplo, desprovisionamiento, selección de personal)	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
53			**PR.IP-12:** Se desarrolla e implementar un plan de gestión de la vulnerabilidad	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
54		**Mantenimiento (PR.MA):** El mantenimiento y las reparaciones de los componentes del control industrial y del sistema de información se realizan de acuerdo con las políticas y procedimientos.	**PR.MA-1:** El mantenimiento y la reparación de los activos de la organización se realizan y registran de manera oportuna, con herramientas aprobadas y controladas.	Nivel 2: Riesgo Informado	Actualmente el equipo de Nivel Especialista está encargado del mantenimiento de las herramientas.
55			**PR.MA-2:** El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de una manera que evita el acceso no autorizado	Nivel 2: Riesgo Informado	Actualmente el equipo de Nivel Especialista está encargado del mantenimiento de los activos para conexiones remotas y gestionan el control de los accesos.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
56		**Tecnología de Protección (PR.PT):** Las soluciones de seguridad técnica se gestionan para garantizar la seguridad y la resiliencia de los sistemas y activos, de acuerdo con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-1:** Los registros de auditoría / registro son determinados, documentados, implementados y revisados de acuerdo con la política	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
57			**PR.PT-2:** Los medios extraíbles están protegidos y su uso está restringido según la política	Nivel 2: Riesgo Informado	Actualmente está protegido y restringido solo para el personal de los terceros en supervisión del equipo de Nivel Especialista.
58			**PR.PT-3:** Se controla el acceso a sistemas y activos, incorporando el principio de menor funcionalidad	Nivel 2: Riesgo Informado	Actualmente el control está a cargo del Nivel de Especialista.
59			**PR.PT-4:** Las redes de comunicaciones y control están protegidas	Nivel 3: Repetible	Actualmente se cuenta controladas a través de un equipo de seguridad perimetral de la marca Fortinet.
60	**DETECTAR (DE)**	**Anomalías y Eventos (DE.AE):** La actividad anómala se detecta de manera oportuna y se entiende el impacto potencial de los eventos.	**DE.AE-1:** Se establece y gestiona una línea base de operaciones de red y flujos de datos esperados para usuarios y sistemas	Nivel 1: Parcial	Actualmente solo se cuenta con flujos de operación para requerimientos e incidencias de los activos que se gestiona de los clientes.
61			**DE.AE-2:** Los eventos detectados se analizan para comprender objetivos y métodos de ataque	Nivel 2: Riesgo Informado	Actualmente se cuenta con log de los equipos, pero no se realiza el análisis de manera establecido solo en casos que sean solicitados por los clientes de los servicios.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
62			**DE.AE-3:** Los datos de eventos se agregan y se correlacionan de múltiples fuentes y sensores	Nivel 1: Parcial	Actualmente la data no se cuenta correlacionada.
63			**DE.AE-4:** El impacto de los eventos se determina	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
64			**DE.AE-5:** Se establecen los umbrales de alerta de incidentes	Nivel 1: Parcial	Actualmente el umbral la única alerta de incidentes es cuando se detecta que los equipos se han desconecta o apagado.
65		**Monitoreo Continuo de Seguridad (DE.CM):** El sistema de información y los activos son monitoreados a intervalos discretos para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de protección.	**DE.CM-1:** Se supervisa la red para detectar posibles eventos de ciberseguridad	Nivel 1: Parcial	Actualmente se cuenta con un reportador donde se almacena los eventos de seguridad
66			**DE.CM-2:** El entorno físico es monitoreado para detectar posibles eventos de ciberseguridad	Nivel 1: Parcial	Actualmente se realiza de forma proactiva por un personal de tercero.
67			**DE.CM-3:** Se monitorea la actividad de personal para detectar posibles eventos de ciberseguridad	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
68			**DE.CM-4:** Se ha detectado código malicioso	Nivel 1: Parcial	Actualmente no se encuentra establecidos, solo en caso haya sido reportado por un cliente.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
69			**DE.CM-5:** Se detecta código móvil no autorizado	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
70			**DE.CM-6:** Se supervisa la actividad del proveedor de servicios externos para detectar posibles eventos de ciberseguridad	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
71			**DE.CM-7:** Se realiza el monitoreo de personal no autorizado, conexiones, dispositivos y software	Nivel 2: Riesgo Informado	Actualmente no se encuentra establecidos, pero se puede realizar solo en caso sea solicitado.
72			**DE.CM-8:** Se realizan escaneos de vulnerabilidad	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
73		**Procesos de Detección (DE.DP):** Los procesos y procedimientos de detección son mantenidos y probados para asegurar una conciencia oportuna y adecuada de eventos anómalos.	**DE.DP-1:** Los roles y responsabilidades para la detección están bien definidos para garantizar la rendición de cuentas	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
74			**DE.DP-2:** Las actividades de detección cumplen con todos los requisitos aplicables	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
75			**DE.DP-3:** Los procesos de detección son probados	Nivel 1: Parcial	Actualmente no se encuentra establecidos.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
76			**DE.DP-4:** La información de detección de eventos se comunica a las partes apropiadas	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
77			**DE.DP-5:** Los procesos de detección se mejoran continuamente	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
78	RESPONDER (RS)	**Planificación de Respuesta (RS.RP):** Los procesos y procedimientos de respuesta se ejecutan y mantienen para asegurar la respuesta oportuna a eventos de ciberseguridad detectados.	**RS.RP-1:** El plan de respuesta se ejecuta durante o después de un evento	Nivel 2: Riesgo Informado	Actualmente solo se realiza un plan de respuestas solo para fechas festivas.
79		**Comunicaciones (RS.CO):** Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según corresponda, para incluir el apoyo externo de los organismos encargados de hacer cumplir la ley.	**RS.CO-1:** El personal conoce sus funciones y el orden de las operaciones cuando se necesita una respuesta	Nivel 1: Parcial	Actualmente no hay una capacitación una información constante del personal, ya que se cuenta con personal altamente rotativo.
80			**RS.CO-2:** Los eventos se reportan de acuerdo con los criterios establecidos	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
81			**RS.CO-3:** La información se comparte con los planes de respuesta	Nivel 2: Riesgo Informado	Actualmente solo se comparte para fechas festivas.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
82			**RS.CO-4:** La coordinación con las partes interesadas es coherente con los planes de respuesta	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
83			**RS.CO-5:** El intercambio voluntario de información se da con los actores externos para lograr una mayor conciencia de la situación cibernética	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
84		**Análisis (RS.AN):** Se realiza un análisis para asegurar una respuesta adecuada y apoyar las actividades de recuperación.	**RS.AN-1:** Se investigan las notificaciones de los sistemas de detección	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
85			**RS.AN-2:** Se entiende el impacto del incidente	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
86			**RS.AN-3:** Forensics se realizan	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
87			**RS.AN-4:** Los incidentes se clasifican de acuerdo con los planes de respuesta	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
88		**Mitigación (RS.MI):** Se realizan actividades para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente.	**RS.MI-1:** Los incidentes están contenidos	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
89			**RS.MI-2:** Los incidentes son mitigados	Nivel 1: Parcial	Actualmente no se encuentra establecidos.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
90			**RS.MI-3:** Las vulnerabilidades recientemente identificadas se mitigan o documentan como riesgos aceptados	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
91		**Mejoras (RS.IM):** Las actividades de respuesta organizacional se mejoran incorporando las lecciones aprendidas de las actividades actuales y anteriores de detección / respuesta.	**RS.IM-1:** Los planes de respuesta incorporan las lecciones aprendidas	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
92			**RS.IM-2:** Estrategias de respuesta actualizadas	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
93	RECUPERAR (RC)	**Planificación de la recuperación (RC.RP):** Los procesos y procedimientos de recuperación se ejecutan y se mantienen para asegurar la restauración oportuna de sistemas o activos afectados por eventos de ciberseguridad.	**RC.RP-1:** El plan de recuperación se ejecuta durante o después de un evento	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
94		**Mejoras (RC.IM):** La planificación y los procesos de recuperación se mejoran incorporando las lecciones aprendidas en las actividades futuras.	**RC.IM-1:** Los planes de recuperación incorporan las lecciones aprendidas	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
95			**RC.IM-2:** Las estrategias de recuperación se actualizan	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
96		**Comunicaciones (RC.CO):** Las actividades de restauración se coordinan con las partes	**RC.CO-1:** Gestión de relaciones públicas	Nivel 1: Parcial	Actualmente no se encuentra establecidos.

N°	Función	Categoría	Subcategoría	Nivel de Madurez	Justificación
97		internas y externas, tales como centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores.	**RC.CO-2:** Reputación después de un evento se repara	Nivel 1: Parcial	Actualmente no se encuentra establecidos.
98			**RC.CO-3:** Las actividades de recuperación se comunican a las partes interesadas internas ya los equipos ejecutivos y de gestión	Nivel 1: Parcial	Actualmente no se encuentra establecido.

Anexo 3 Análisis del Riesgo

				AMENAZA		OCURRENCIA		MEDICION DEL RIESGO	
N°	PROPIETARIO	ACTIVO	AMENAZA	IMPACTO DE AMENAZA	VALOR	PROBABILIDAD DE OCURRENCIA	VALOR	TOTAL	ZONA DE RIESGO
1	Jefe del área	**Información histórica de Clientes**	Acceso no autorizado	Severo	4	Posible	3	12	A
			Corrupción o destrucción de la información	Critico	5	Posible	3	15	A
			Divulgación de información	Severo	4	Probable	4	16	A
			Robo	Critico	5	Probable	4	20	E
			Desastres Naturales	Menor	2	Improbable	2	4	M
2	Jefe del área	**FileServer PRIM**	Acceso no autorizado	Critico	5	Probable	4	20	E
			Corrupción o destrucción de la información	Critico	5	Posible	3	15	A
			Divulgación de información	Critico	5	Posible	3	15	A
			Robo	Critico	5	Probable	4	20	E
			Desastres Naturales	Dañino	3	Posible	3	9	A
3	Jefe del área	**FileServer SEC**	Acceso no autorizado	Dañino	3	Probable	4	12	A
			Corrupción o destrucción de la información	Dañino	3	Posible	3	9	A
			Divulgación de información	Dañino	3	Improbable	2	6	M
			Robo	Dañino	3	Probable	4	12	A
			Desastres Naturales	Dañino	3	Posible	3	9	A
4	Jefe del área	**Oficina de Seguridad**	Acceso no autorizado	Severo	4	Posible	3	12	A
			Corrupción o destrucción de la información	Severo	4	Posible	3	12	A
			Divulgación de información	Dañino	3	Posible	3	9	A
			Robo	Severo	4	Posible	3	12	A
5	Jefe del área	**Nivel Especialista**	Acceso no autorizado	Severo	4	Posible	3	12	A
			Corrupción o destrucción de la información	Severo	4	Posible	3	12	A
			Divulgación de información	Dañino	3	Posible	3	9	A
			Robo	Severo	4	Posible	3	12	A

				AMENAZA		OCURRENCIA		MEDICION DEL RIESGO	
N°	PROPIETARIO	ACTIVO	AMENAZA	IMPACTO DE AMENAZA	VALOR	PROBABILIDAD DE OCURRENCIA	VALOR	TOTAL	ZONA DE RIESGO
6	Jefe del área	Nivel Avanzado	Acceso no autorizado	Critico	5	Posible	3	15	A
			Corrupción o destrucción de la información	Severo	4	Posible	3	12	A
			Divulgación de información	Critico	5	Probable	4	20	E
			Robo	Critico	5	Probable	4	20	E
7	Jefe del área	Telefonía	Avería de origen físico o lógico	Dañino	3	Posible	3	9	A
			Desastres Naturales	Severo	4	Posible	3	12	A
			Robo	Dañino	3	Improbable	2	6	M
			Corte del suministro eléctrico	Dañino	3	Raro	1	3	M
8	Jefe del área	Correo electrónico	Acceso no autorizado	Severo	4	Posible	3	12	A
			Desastres Naturales	Critico	5	Improbable	2	10	M
			Robo	Severo	4	Posible	3	12	A
			Corte del suministro eléctrico	Severo	4	Posible	3	12	A
9	Jefe del área	Internet	Acceso no autorizado	Severo	4	Posible	3	12	A
			Desastres Naturales	Critico	5	Improbable	2	10	M
			Robo	Severo	4	Posible	3	12	A
			Desastres debidos a la actividad humana	Severo	4	Probable	4	16	A
			Corte del suministro eléctrico	Severo	4	Posible	3	12	A
10	Jefe del área	Red de Datos	Avería de origen físico o lógico	Dañino	3	Posible	3	9	A
			Caída del sistema por agotamiento de recursos	Dañino	3	Probable	4	12	A
			Errores de mantenimiento / actualización de equipos	Severo	4	Probable	4	16	A
			Errores en servicios contratados externamente	Critico	5	Improbable	2	10	M
11	Jefe del área	FAZ_SIS	Avería de origen físico o lógico	Dañino	3	Probable	4	12	A
			Caída del sistema por agotamiento de recursos	Dañino	3	Probable	4	12	A
			Errores de mantenimiento / actualización de equipos	Dañino	3	Posible	3	9	A
			Errores en servicios contratados externamente	Dañino	3	Improbable	2	6	M

				AMENAZA		OCURRENCIA		MEDICION DEL RIESGO	
N°	PROPIETARIO	ACTIVO	AMENAZA	IMPACTO DE AMENAZA	VALOR	PROBABILIDAD DE OCURRENCIA	VALOR	TOTAL	ZONA DE RIESGO
12	Jefe del área	FAZ_WASH	Avería de origen físico o lógico	Critico	5	Probable	4	20	E
			Caída del sistema por agotamiento de recursos	Critico	5	Posible	3	15	A
			Corte del suministro eléctrico	Severo	4	Posible	3	12	A
			Errores de mantenimiento / actualización de equipos	Severo	4	Improbable	2	8	M
13	Jefe del área	FW_SOC_SEC	Avería de origen físico o lógico	Severo	4	Posible	3	12	A
			Caída del sistema por agotamiento de recursos	Critico	5	Posible	3	15	A
			Errores de mantenimiento / actualización de equipos	Severo	4	Probable	4	16	A
			Errores en servicios contratados externamente	Dañino	3	Improbable	2	6	M
14	Jefe del área	FW_SOC_PRIM	Avería de origen físico o lógico	Dañino	3	Probable	4	12	A
			Caída del sistema por agotamiento de recursos	Severo	4	Probable	4	16	A
			Errores de mantenimiento / actualización de equipos	Dañino	3	Posible	3	9	A
			Errores en servicios contratados externamente	Dañino	3	Improbable	2	6	M
15	Jefe del área	PE-LIM-DLP-SOC	Avería de origen físico o lógico	Dañino	3	Probable	4	12	A
			Caída del sistema por agotamiento de recursos	Dañino	3	Improbable	2	6	M
			Errores de mantenimiento / actualización de equipos	Dañino	3	Probable	4	12	A
			Errores en el servicio de comunicaciones	Severo	4	Probable	4	16	A
16	Jefe del área	PE-LIM-RMDY-BD1	Avería de origen físico o lógico	Dañino	3	Casi Seguro	5	15	A
			Caída del sistema por agotamiento de recursos	Severo	4	Probable	4	16	A
			Errores de mantenimiento y/o Actualización de equipos	Severo	4	Posible	3	12	A
			Errores de los usuarios	Menor	2	Casi Seguro	5	10	M
			Indisponibilidad del personal	Menor	2	Posible	3	6	M
17	Jefe del área	PE-LIM-RMDY-BD2	Avería de origen físico o lógico	Dañino	3	Probable	4	12	A
			Caída del sistema por agotamiento de recursos	Severo	4	Probable	4	16	A
			Errores de mantenimiento y/o Actualización de equipos	Severo	4	Posible	3	12	A
			Errores de los usuarios	Menor	2	Casi Seguro	5	10	M

				AMENAZA		OCURRENCIA		MEDICION DEL RIESGO	
N°	PROPIETARIO	ACTIVO	AMENAZA	IMPACTO DE AMENAZA	VALOR	PROBABILIDAD DE OCURRENCIA	VALOR	TOTAL	ZONA DE RIESGO
			Indisponibilidad del personal	Severo	4	Posible	3	12	A
18	Jefe del área	OPSVIEW	Errores en servicios contratados externamente	Severo	4	Posible	3	12	A
			Caída del sistema por agotamiento de recursos	Severo	4	Posible	3	12	A
			Cambios de Software no autorizados	Dañino	3	Improbable	2	6	M
			Difusión de software dañino	Critico	5	Improbable	2	10	M
			Errores de mantenimiento y/o Actualización de equipos	Dañino	3	Probable	4	12	A

Anexo 4 Plan de Tratamiento de Riesgo alineado a los Objetivos estratégicos del negocio

AMENAZA	ACTIVO	ZONA DE RIESGO	DUEÑO RIESGO	SALVAGUARDAS	CATEGORIA CSF	MEDIDAS A REALIZAR
Acceso no autorizado	Información histórica de Clientes	A	Jefe del SOC	Cámaras de Videovigilancia Acceso biométrico en oficinas Next Generation firewall	PR.PT	Establecer lineamientos para ejecución de auditorías de sistemas de información considerando requisitos de auditoría para acceso a sistemas y a datos estos deben ser acordados con la dirección apropiada; definir el alcance de las pruebas técnicas de auditoría se debe acordar y controlar; establecer las pruebas de auditoría donde se debe limitar a acceso a software y datos únicamente para lectura; definir el acceso diferente al de solo lectura solamente se debe preveer para copias aisladas de los archivos del sistema, que se deben borrar una vez que la auditoría haya finalizado, o se debe proporcionar información apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría; definir los requisitos para procesos especiales y adicionales estos deben ser identificados y acordados; establecer las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales; realizar seguimiento de todos los accesos y logged para producir un rastro de referencia.
	FileServer PRIM	E				
	FileServer SEC	A				
	Oficina de Seguridad	A				
	Nivel Especialista	A				
	Nivel Avanzado	A				
	Correo electrónico	A				
	Internet	A				
Avería de origen físico o lógico	Telefonía	A	Jefe del SOC	Mantenimiento preventivo	PR.MA	Establecer un procedimiento que contenga las directrices para el retiro de activos: a) identificar a los empleados y usuarios de partes externas que tienen autoridad para permitir el retiro de activos del sitio; b) establecer los límites de tiempo para el retiro de activos y verificar que se cumplen las devoluciones; c) definir cuando sea necesario y apropiado, registrar los activos se retiran del sitio y cuando se hace su devolución; d) documentar la identidad, el rol y la filiación de cualquiera que maneje o
	Red de Datos	A				
	FAZ_SIS	A				
	FAZ_WASH	E				
	FW_SOC_SEC	A				

AMENAZA	ACTIVO	ZONA DE RIESGO	DUEÑO RIESGO	SALVAGUARDAS	CATEGORIA CSF	MEDIDAS A REALIZAR
	FW_SOC_PRIM	A				use activos, y devolver esta documentación con el equipo, la información y el software. Información adicional Establecer el procedimiento de mantenimiento remoto incluyendo las actividades relacionadas.
	PE-LIM-DLP-SOC	A				
	PE-LIM-RMDY-BD1	A				
	PE-LIM-RMDY-BD2	A				
Caída del sistema por agotamiento de recursos	Red de Datos	A	Jefe del SOC	Gestion de la capacidad	RC.RP	Se debe realizar procedimiento indicando plan de respuesta para que sea ejecutado durante los eventos de seguridad. Revisar las siguientes directrices para respuesta a incidentes de seguridad de la información: a) Los incidentes son contenidos y la probabilidad de que vuelvan a ocurrir mitigada. b) Se debe contar con un plan de recuperación de incidentes durante o después del mismo. b) recolectar evidencia lo más pronto posible después de que ocurra el incidente; c) llevar a cabo análisis forense de seguridad de la información, según se requiera d) llevar el asunto a una instancia superior, según se requiera; e) asegurar que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior; f) comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo; g) tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente; g) establecer que una vez que el incidente se haya tratado lo suficiente,
	FAZ_SIS	A				
	FAZ_WASH	A				
	FW_SOC_SEC	A				
	FW_SOC_PRIM	A				
	PE-LIM-RMDY-BD1	A				

AMENAZA	ACTIVO	ZONA DE RIESGO	DUEÑO RIESGO	SALVAGUARDAS	CATEGORIA CSF	MEDIDAS A REALIZAR
	PE-LIM-RMDY-BD2	A				cerrarlo formalmente y hacer un registro de esto. h) de acuerdo a la NIST se deben investigar las notificaciones de los sistemas de detección.
	OPSVIEW	A				
Corrupción o destrucción de la información	Información histórica de Clientes	A	Jefe del SOC	Copias de Respaldo	PR.DS PR.IP	Desarrollar procedimiento que contecta las actividades de proteción de datos en reposo. Desarrollar procedimiento para identificar datos en tránsito Crear instructivo que contenga las funciones de la herramienta de cumplimiento parta verificar el software, el firware y la integridad de la información.
	FileServer PRIM	A				
	FileServer SEC	A				
	Oficina de Seguridad	A				
	Nivel Especialista	A				
	Nivel Avanzado	A				
Corte del suministro eléctrico	Correo electrónico	A	Jefe del SOC	Redundancia electrica	RC.RP	Se debe realizar procedimiento indicando plan de respuesta para que sea ejecutado durante los eventos de seguridad. Revisar las siguientes directrices para respuesta a incidentes de seguridad de la información: a) Los incidentes son contenidos y la probabilidad de que vuelvan a ocurrir mitigada. b) Se debe contar con un plan de recuperación de incidentes durante o después del mismo.

AMENAZA	ACTIVO	ZONA DE RIESGO	DUEÑO RIESGO	SALVAGUARDAS	CATEGORIA CSF	MEDIDAS A REALIZAR
	Internet	A				b) recolectar evidencia lo más pronto posible después de que ocurra el incidente; c) llevar a cabo análisis forense de seguridad de la información, según se requiera d) llevar el asunto a una instancia superior, según se requiera; e) asegurar que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior; f) comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo; g) tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente; g) establecer que una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto. h) de acuerdo a la NIST se deben investigar las notificaciones de los sistemas de detección.
	FAZ_WASH	A				
Desastres debidos a la actividad humana	Internet	A	Jefe del SOC	Procedimientos documentados	PR.AT RS.CO	Establecer un plan de eventos de ciberseguridad donde los altos ejecutivos sean los principales sponsor.

AMENAZA	ACTIVO	ZONA DE RIESGO	DUEÑO RIESGO	SALVAGUARDAS	CATEGORIA CSF	MEDIDAS A REALIZAR
Desastres Naturales	FileServer PRIM	A	Jefe del SOC	Site de contingencia en España	RC.RP	Se debe realizar procedimiento indicando plan de respuesta para que sea ejecutado durante los eventos de seguridad. Revisar las siguientes directrices para respuesta a incidentes de seguridad de la información: a) Los incidentes son contenidos y la probabilidad de que vuelvan a ocurrir mitigada. b) Se debe contar con un plan de recuperación de incidentes durante o después del mismo. b) recolectar evidencia lo más pronto posible después de que ocurra el incidente; c) llevar a cabo análisis forense de seguridad de la información, según se requiera d) llevar el asunto a una instancia superior, según se requiera; e) asegurar que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior; f) comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo; g) tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente; g) establecer que una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto. h) de acuerdo a la NIST se deben investigar las notificaciones de los sistemas de detección.
	FileServer SEC	A				

AMENAZA	ACTIVO	ZONA DE RIESGO	DUEÑO RIESGO	SALVAGUARDAS	CATEGORIA CSF	MEDIDAS A REALIZAR
	Telefonía	A				Tenga en cuenta para la calificación: 1) Si los planes de respuesta a incidentes incluyen algunas áreas de la entidad y si se evalúa la efectividad los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro es 60 2) Se incluyen todas las áreas de la Entidad, en los planes de respuesta de incidentes es 80
Divulgación de información	Información histórica de Clientes	A	Jefe del SOC	Implementacion de un DLP	PR.DS PR.IP	Desarrollar procedimiento que contecta las actividades de proteción de datos en reposo. Desarrollar procedimiento para identificar datos en tránsito Crear instructivo que contenga las funciones de la herramienta de cumplimiento parta verificar el software, el firware y la integridad de la información.
	FileServer PRIM	A				
	Oficina de Seguridad	A				
	Nivel Especialista	A				
	Nivel Especialista	A				
	Nivel Avanzado	E				
Errores de mantenimiento / actualización de equipos	Red de Datos	A	Jefe del SOC	Procedimientos documentados	PR.AT	Establecer un plan de eventos de ciberseguridad donde los altos ejecutivos sean los principales sponsor.
	FAZ_SIS	A				
	FW_SOC_SEC	A				
	FW_SOC_PRIM	A				
	PE-LIM-DLP-SOC	A				
Errores de mantenimiento y/o	PE-LIM-RMDY-BD1	A		Procedimientos documentados	PR.AT	Establecer un plan de eventos de ciberseguridad donde los altos ejecutivos sean los principales sponsor.

AMENAZA	ACTIVO	ZONA DE RIESGO	DUEÑO RIESGO	SALVAGUARDAS	CATEGORIA CSF	MEDIDAS A REALIZAR
Actualización de equipos	PE-LIM-RMDY-BD2	A	Jefe del SOC			
	OPSVIEW	A				
Errores en el servicio de comunicaciones	PE-LIM-DLP-SOC	A	Jefe del SOC	Procedimientos documentados	PR.AT	Establecer un plan de eventos de ciberseguridad donde los altos ejecutivos sean los principales sponsor.
Errores en servicios contratados externamente	OPSVIEW	A	Jefe del SOC	Revision de contratos	ID.GV	Establecer un procedimiento que apoye en la gestión de riesgos.
Indisponibilidad del personal	PE-LIM-RMDY-BD2	A	Jefe del SOC	Politica de sucesion de personal	PR.IP	Establecer un control de seguimiento de cumplimiento de políticas, a travez del registro del formato de cumplimiento de políticas. Establecer un procedimiento que contemple las actividades y responsabilidades de los lineamientos de compartir la eficiacia de las tecnologías de protección.
Robo	Información histórica de Clientes	E	Jefe del SOC	Implementacion de un DLP	PR.IP	Establecer lineamientos para ejecución de auditorias de sistemas de información considerando requisitos de auditoría para acceso a sistemas y a datos estos deben ser acordados con la dirección apropiada; definir el alcance de las pruebas técnicas de auditoría se debe acordar y controlar; establecer las pruebas de auditoría donde se debe limitar a acceso a software y datos únicamente para lectura; definir el acceso diferente al de solo lectura solamente se debe preveer para copias aisladas de los archivos del sistema, que se deben borrar una vez que la auditoría haya finalizado, o se debe proporcionar información apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría; definir los requisitos para procesos especiales y adicionales estos deben ser identificados y acordados; establecer las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales;
	FileServer PRIM	E				
	FileServer SEC	A				
	Oficina de Seguridad	A				
	Nivel Especialista	A				
	Nivel Avanzado	E				

AMENAZA	ACTIVO	ZONA DE RIESGO	DUEÑO RIESGO	SALVAGUARDAS	CATEGORIA CSF	MEDIDAS A REALIZAR
	Correo electrónico	A				realizar seguimiento de todos los accesos y logged para producir un rastro de referencia.
	Internet	A				

Fuente: Elaboración propia