UPN
UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POSGRADO Y ESTUDIOS CONTINUOS

MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

Tesis para optar el grado de **MAESTRO** en:

INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE SISTEMAS DE INFORMACIÓN

Autor:

Alan Pierre Salinas Tomapasca

Asesor:

Dr. Alberto Carlos Mendoza de los Santos

Trujillo – Perú

2020

Resumen

Los modelos de ciberseguridad, ayudan a controlar y medir los riesgos a los que se ven expuestos toda organización; a través de diferentes controles, procedimientos y estrategias. Así mismo, permite proteger los activos de información y los servicios de negocio que brinda la empresa y que constantemente se ven amenazadas por la ciberdelincuencia y los ciberataques. La evolución de los clientes bancarios y su decidida incorporación al mundo digital, hacen que la transformación digital, sea uno de los más grandes retos estructurales que afecta el sector financiero; y sin duda, el más trascendental para el futuro de estas entidades; lo cual obliga también a la evolución de sus modelos de ciberseguridad. La pandemia del covid-19, ha puesto de manifiesto la necesidad que tienen las empresas en acelerar sus procesos de transformación digital.

El objetivo del presente estudio fue elaborar la propuesta para un modelo de ciberseguridad con nuevo enfoque para cajas municipales, en tiempo de transformación digital, que incluya características de integridad, confidencialidad y disponibilidad, y que pueda servir para adaptarse a las exigencias actuales de la transformación digital y hacerle frente a los nuevos tipos de amenaza y ataques informáticos que evolucionan constantemente. Dentro de los resultados, se desarrolló la propuesta, utilizando el modelo de ciberseguridad “Zero Trust”, basado en el marco de gestión de ciberseguridad NIST. Así mismo, se diseñó un modelo organizacional basado en un esquema de niveles Estratégicos, Operacionales y Tácticos en forma de pirámide, que permitirá una mejor gestión de ciberseguridad y una comunicación constante entre todos los departamentos de la organización. Se modificó el organigrama del departamento de seguridad de la información; así como también, se elaboró la estructura de una nueva sección dentro del departamento de Tecnologías de Información llamado “Seguridad informática”; ambas, con sus respectivas macro funciones. Se elaboró el diseño de arquitectura de seguridad que protege y monitorea tanto el perímetro como lo que se encuentra fuera de él (internet). Se diseñó una matriz para el uso de 20 controles de seguridad CIS y acciones para crear una cultura robusta en ciberseguridad en toda la organización. Como conclusión, se logró identificar los modelos de ciberseguridad: “Defensa en Profundidad”, “Modelo Perimetral”, Modelo Zero Trust” y “Modelo Thin Security” a través de una matriz de priorización validada por expertos en ciberseguridad. Así mismo, se evaluaron estos modelos a través de una matriz de comparación de características; se determinaron las características que debe utilizar el modelo y fueron validadas a través de una lista de cotejo de usuarios potenciales. En base a lo anterior, se elaboró la

propuesta utilizando el modelo de ciberseguridad Zero Trust basado en el marco NIST, el diseño de una nueva estructura organizacional de seguridad, la creación de una matriz de soporte de controles de seguridad CIS, el diseño de una arquitectura de ciberseguridad y los pasos para la creación de cultura en ciberseguridad en la organización. Finalmente, se validó la pertinencia, relevancia y claridad de la propuesta a través de una evaluación de Juicio de Expertos realizada a los usuarios potenciales.

Abstract

Cybersecurity models help to control and measure the risks to which every organization is exposed; through different controls, procedures and strategies. Likewise, it allows to protect the information assets and the business services that the company provides and that are constantly threatened by cybercrime and cyberattacks. The evolution of banking clients and their determined incorporation into the digital world make digital transformation one of the greatest structural challenges affecting the financial sector; and without a doubt, the most important for the future of these entities; which also forces the evolution of their cybersecurity models. The covid-19 pandemic has highlighted the need for companies to accelerate their digital transformation processes.

The objective of this study was to develop the proposal for a cybersecurity model with a new approach for municipal savings banks, in times of digital transformation, that includes integrity, confidentiality and availability characteristics, and that can be used to adapt to the current demands of transformation and tackle new types of cyber threats and attacks that are constantly evolving. Among the results, the proposal was developed, using the “Zero Trust” cybersecurity model, based on the NIST cybersecurity management framework. Likewise, an organizational model was designed based on a scheme of Strategic, Operational and Tactical levels in the form of a pyramid, which will allow better cybersecurity management and constant communication between all the departments of the organization. The organization chart of the information security department was modified; as well as, the structure of a new section within the Information Technologies department called "Computer Security" was elaborated; both, with their respective macro functions. The security architecture design was developed that protects and monitors both the perimeter and what is outside it (internet). A matrix was designed for the use of 20 CIS security controls and actions to create a robust culture in cybersecurity throughout the organization. As a conclusion, it was possible to identify the cybersecurity models: "Defense in Depth", "Perimeter Model", Zero Trust Model "and" Thin Security Model "through a prioritization matrix validated by cybersecurity experts. Likewise, these models were evaluated through a characteristic comparison matrix; The characteristics that the model should use were determined and validated through a checklist of potential users. Based on the above, the proposal was prepared using the Zero Trust cybersecurity model based on the NIST framework, the design of a new organizational security structure, the creation of a CIS security controls support matrix, the design of a cybersecurity architecture and the steps for creating a cybersecurity culture in the organization. Finally, the relevance, relevance and clarity of the proposal was validated through an Expert Judgment evaluation carried out on potential users.

Dedicatoria y Agradecimientos

A Dios, por permitirme llegar a este momento tan especial de mi vida, por iluminar mi camino y ayudarme en todo momento.

A mis padres y hermano, por su apoyo incondicional y sus consejos para hacer de mi una mejor persona.

A mi esposa, por su cariño y apoyo incondicional.
A mis hijos, Santiago y Sofía, que son la razón de mi vida y el motivo de mi sacrificio a diario.

A mis profesores, por su tiempo y apoyo incondicional; y por la sabiduría que me transmitieron durante todo el desarrollo de mi formación profesional.

Tabla de contenido

Índice de figuras

Índice de tablas

I. INTRODUCCIÓN

I.1. Realidad problemática

Las empresas hoy en día enfrentan nuevos retos para hacer crecer sus negocios y ser competitivos. Uno de los más importantes es lograr la transformación digital a través del uso de nuevas y modernas tecnologías; sin embargo, ser digital conlleva un riesgo nuevo: los ciberataques. En ese contexto, la ciberseguridad y el uso de un adecuado modelo y estrategia juegan un papel muy importante para hacerle frente a este nuevo riesgo.

Los problemas fundamentales con la ciberseguridad hoy en día es que está tratando de resolver el problema incorrecto. Por lo menos, es un problema desactualizado. La industria en su conjunto se ha construido sobre, y todavía está impulsada principalmente, por soluciones puntuales diseñadas para “mantener a las personas alejadas”. Es un modelo que supone que hay un “nosotros” y un “ellos”, un “adentro” y un “Fuera”, y luego se esfuerza por garantizar que los actores maliciosos de los grupos “ellos” y “fuera” puedan ser detectados y bloqueados antes de que puedan comprometer los sistemas y los datos.

La historia, o los titulares de cualquier semana, ilustran que este modelo es disfuncional en el mejor de los casos. Las herramientas centrales de ciberseguridad, como los firewalls y las defensas antimalware, siguen siendo necesarias, pero no necesariamente algo en lo que gastar demasiado dinero. Son “apuestas en la mesa” de seguridad cibernética y tienen el propósito de identificar y bloquear la mayoría de las amenazas conocidas, por lo que aún tienen valor. Sin embargo, claramente no son suficientes por sí solos.

El nuevo modelo de ciberseguridad gira en torno a tecnologías como la autenticación multifactorial, el análisis de comportamiento y la tecnología de engaño.

Diferentes países en el mundo, están tomando como prioridad tener una adecuada estrategia y modelos de ciberseguridad que soporten la creciente, sofisticada y rápida evolución de los ciberataques; además de las diferentes relaciones y convenios internacionales para apoyarse mutuamente.

Según el Global Cybersecurity Index (GCI) de 2018, España ocupa el séptimo puesto a nivel mundial en su compromiso con la ciberseguridad, superada en este orden por Reino Unido, Estados Unidos, Francia, Lituania, Estonia y Singapur. En la edición de 2018 han participado un total de 155 países, siendo la edición que más participantes acumulo.

La unión europea utiliza una estrategia en ciberseguridad, la cual se basa en cinco principios fundamentales: los valores esenciales de la Unión Europea se deben aplicar “tanto en el mundo digital como en el físico”, la protección de derechos fundamentales, libertad de expresión, datos personales y privacidad, acceso para todos, gobierno eficiente y democrático de los grupos de interés y, la responsabilidad compartida.

En el Perú, la ciberseguridad viene avanzando de a pocos y convirtiéndose en un tema de prioridad e importancia, sobre todo, desde que se conoce que es el país que más ataques de malware ha sufrido en Latinoamérica, solo detrás de Brasil y México. En todo el mundo, ocupa la posición 24, según el mapa interactivo de kaspersky, que muestra los efectos de la amenaza en tiempo real.

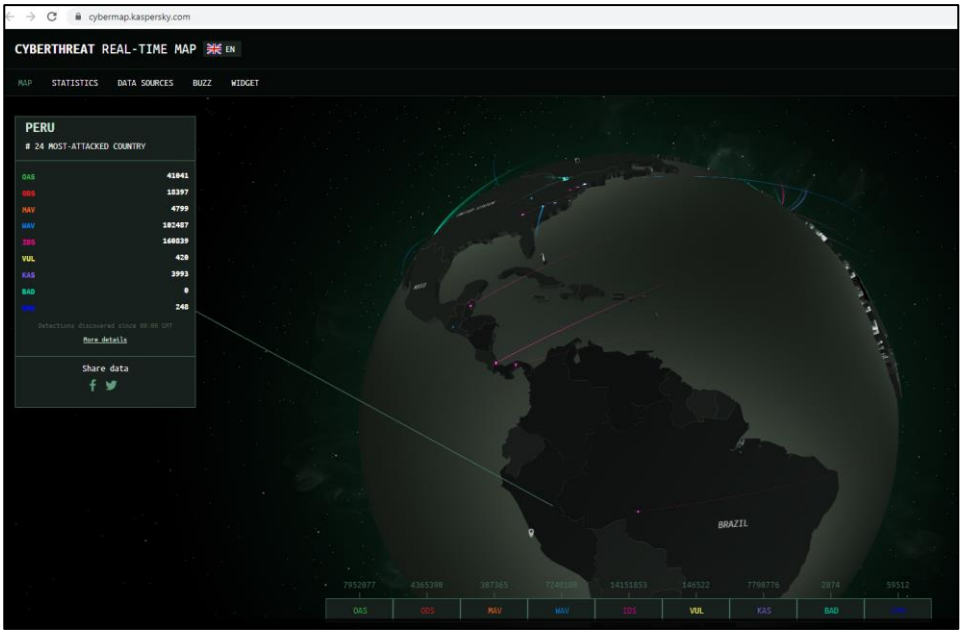


Figura 1: Ciberataques por país

Tal y como se recoge en el informe de 2016 del Banco Interamericano de Desarrollo, “mientras que los servicios de gobierno electrónico y comercio electrónico continúan expandiéndose en Perú, la conciencia social es generalmente baja en lo que respecta a ciberseguridad”.

Afortunadamente, se observan avances legislativos y ejecutivos en lo que respecta a la gestión de la ciberseguridad en Perú, como:

- Proyectos de ley de Ciberdefensa (Proyecto de Ley No. 4228) y de ciberseguridad (Proyectos de Ley No. 4237 y 4352).
- Ley N ° 30.171 que amplía el Código Penal incluyendo los delitos informáticos o la Ley N ° 29.733, la Ley de Protección de Datos Personales (PDPA).
- Se ha propuesto crear un Viceministerio de Tecnología de la Información y la Comunicación, que permitiría establecer iniciativas sobre el desarrollo de la tecnología, y se centraría en las normas de seguridad cibernética.

- Existe una División de Delitos de Alta Tecnología como parte de la Policía Nacional, cuyos miembros están capacitados para llevar a cabo patrullas virtuales.

Las entidades financieras en el Perú, también realizan denodados esfuerzos por hacerle frente al cibercrimen; más aun siendo uno de los sectores más afectados por este tipo de ataques; tanto es así, que la Superintendencia de Banca, Seguros y AFP (SBS), estarían proyecto contar con un programa de ciberseguridad, como parte de la actualización regulatoria que trabajan a fin de encarar este riesgo.

"La actualización regulatoria que estamos trabajando tiene previsto incorporar la exigencia de un programa de ciberseguridad en las entidades financieras, el mismo que debería priorizarse", dijo el intendente de Supervisión de Sistemas de Información y Tecnología de la SBS, Magno Condori.

Esta actualización regulatoria también precisará las medidas que deben acompañar los servicios de la nube, sostuvo: "Se debe definir las responsabilidades entre proveedor y las entidades financieras y quien tendrá que mantener la obligación de supervisar ese servicio (de nube) son las entidades financieras", señaló.

Además se tiene por finalidad incorporar en esta actualización regulatoria los requisitos mínimos de autenticación, refirió. Sostuvo que se prevé realizar un ejercicio sectorial el próximo año enfocado en esfuerzos para enfrentar un escenario de ciberataque.

A su turno, el superintendente adjunto de Riesgos de la SBS, Alejandro Medina, consideró que uno de los principales riesgos que amenazan a las empresas del sistema financiero son los riesgos operacionales. En ese contexto, muchas de las preocupaciones están relacionadas a fallas en la información en el ámbito tecnológico, pudiendo ser problemas internos, y no solo ciberataques, refirió.

Por su parte, el presidente del Comité de Riesgo Operacional de la Asociación de Bancos del Perú (Asbanc), César Caballero, comentó que en un sistema de pagos las entidades financieras están interconectadas vía el Banco Central de Reserva (BCR) y alguna intrusión podría ingresar al sistema financiero mediante una institución con una protección débil, afectándolo. "Por eso es relevante que cada entidad financiera maneje el riesgo de ciberseguridad", dijo.

Estas declaraciones las brindaron en el VI Seminario Internacional de Prevención de Fraudes y 8° Seminario Internacional de Riesgo Operacional, organizado por Asbanc.

Los bancos por ejemplo, tienen departamentos dedicados al tema de ciberseguridad, los cuales operan bajo un modelo marco estratégico, operacional y técnico que les permite reforzar y proteger vectores vulnerables, además de contar con visibilidad de todas sus redes. Así mismo, a nivel organizacional, los departamentos relacionados a la ciberseguridad tienen un buen sitial.

Uno de los sectores que más ha crecido en el mercado financiero en los últimos 40 años son las Cajas Municipales de ahorro y créditos; logrando extenderse por todo el territorio nacional; tanto es así, que hoy en día, las Cajas Municipales representan la segunda fuerza financiera del país, después de la banca múltiple.

Existen 11 Cajas Municipales de Ahorro y Créditos en nuestro país, todas ellas representadas por la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC); las cuales, vienen trabajando por la inclusión financiera en el país, atendiendo muy de cerca las necesidades financieras de la población más vulnerable; lo que les ha permitido desarrollar y consolidar un mercado de micro finanzas principalmente con la micro y pequeña empresa; es decir, un eficiente y adecuado modelo de finanzas con características y estrategias similares en cada una de ellas; sin embargo, aún no se logra lo mismo respecto a la ciberseguridad.

El modelo organizacional de las cajas municipales es muy parecido. Todas ellas cuentan con un directorio y 3 gerencias centrales (Administración, negocios y finanzas); sin embargo, respecto a los departamentos que tienen que ver directamente con temas de ciberseguridad, hay ciertas diferencias.

El departamento de seguridad de la información, en algunas cajas municipales, depende directamente de la gerencia de riesgos; en otras en cambio, se encuentran en un nivel superior reportando directamente a las gerencias centrales. El equipo de seguridad de la información (que en muchos casos no cuenta con el recurso humano especializado y con la cantidad de personal necesario), carece de una estructura definida y específica para tratar los temas objetivos como son la integridad, disponibilidad y confidencialidad de la información. Los mayores esfuerzos se encuentran relacionados al aspecto legal y normativo. Los esfuerzos por abordar temas específicos de la ciberseguridad no son cubiertos, aunque se hace el esfuerzo.

Del lado del departamento de tecnologías de información (T.I), si bien es cierto, la sección de infraestructura se encarga también de ver temas relacionados a la seguridad del perímetro, entre otras; no existe una sección exclusivamente dedicada a ver temas de ciberseguridad como si las hay en entidades financieras como los bancos por ejemplo (que inclusive, no pertenecen al departamento de TI si no reportan directamente a la gerencia central); y se mezclan mucho actividades operativas y de seguridad, por lo que no se cubre todo los aspectos requeridos para la protección de la información y del perímetro. Las cajas municipales, cada vez crecen más, se expanden por todo el territorio nacional y publican muchos servicios en internet; así como también, se encuentran migrando ya algunos servicios a la nube; por lo que hace necesario tener personal dedicado al monitoreo de ese tráfico.

Las gerencias ya no pueden asumir que la ciberseguridad es responsabilidad exclusiva del departamento de seguridad de la información

o del departamento de TI. Las cajas municipales deben hacer de la ciberseguridad una parte central de la estrategia y cultura empresarial, al hacerlo, pueden permitir a toda la organización comprender los riesgos que enfrentan, abrazar la innovación necesaria para contrarrestar esos riesgos, ya que no existe una visión de ciberseguridad holística e integrada, que reúna las diversas funciones y dependencias con otras partes de la organización, con partes interesadas clave y con proveedores externos.

Los departamentos de seguridad de la información y tecnologías de la información, deben romper el paradigma de la competencia interna que por años mantienen, y deben dejar de verse como enemigos privados y empezar a crear una sinergia entre ellos que permita cumplir con el principal objetivo para los dos y para la organización: La protección de la información, de los servicios publicados y de los clientes.

No todas las cajas municipales basan su modelo de ciberseguridad (algunas no lo tienen) en estándares globales y marcos de ciberseguridad ya existentes. Muchas de las cajas municipales aún mantienen el enfoque de seguridad tradicional y reactivo; el cual, ya no es útil en estos tiempos. Hay que dejar de pensar solo en la protección del perímetro (sin descuidarlo) y pensar en servicios en la nube; pensar en que ya no solo protegemos usuarios dentro de la red si no también fuera de ella; y que necesitamos tener una visibilidad completa de lo que pasa por nuestra red.

La exigencia para el personal de seguridad no guarda relación con las capacitaciones que este debe recibir. El personal que tiene que ver con temas de ciberseguridad debe ser constantemente capacitado; ya que los ataques y las amenazas evolucionan constantemente y nos llevan una gran delantera.

Un problema que también se encuentra comúnmente, es que las diferentes tecnologías de seguridad que se adquieren, no cuentan con una configuración adecuada; y lo que es peor, muchas de ellas no se integran con otras soluciones ya implementadas en la institución. Todo eso genera que la visión de nuestra red no sea tan clara y que se tenga que revisar

diferentes consolas para hacer la tranza de un incidente y revisar numerosos logs.

El presupuesto para tecnologías es muy bajo; y solo el 3.8% de ese presupuesto se invierte en ciberseguridad; y peor aún, en tiempos de transformación digital, el porcentaje de inversión en el endpoint es muy bajo.

El endpoint se ha convertido en el objetivo de un ataque; sin embargo, solo recibe entre 3-4 % del presupuesto de seguridad.

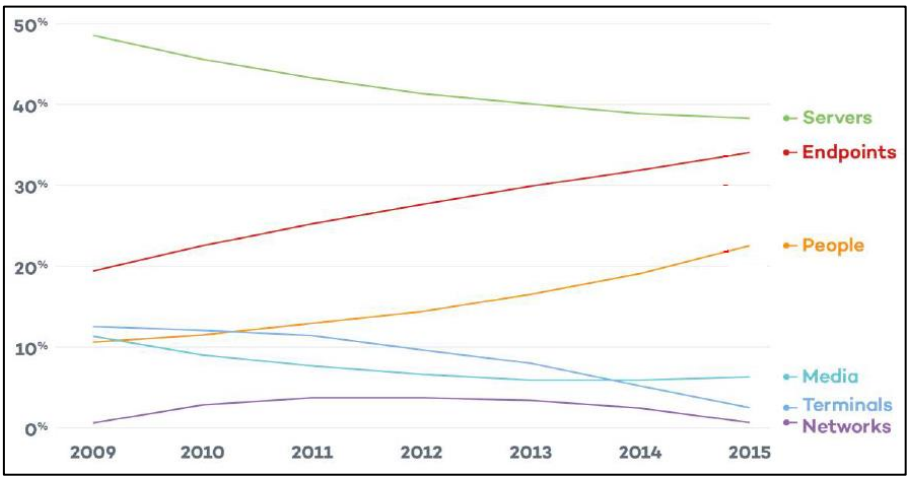


Figura 2: Incidencias por objetivo de ataque

Sumado a esto, los ataques también han evolucionado. Son más sofisticados y dirigidos de manera específica. Se maneja malware y ransomware como servicio; así como también, se evidencia un aumento en el cómputo y en los procesos. Se utilizan técnicas de evasión de equipos y políticas de seguridad, utilizan IA.

Así mismo, se ha incrementado considerablemente las alertas a investigar que ofrecen los equipos de seguridad; es decir, si no se cuenta con una configuración adecuada y granular respecto a las alertas que si se deben analizar; y peor aún, si no se tiene los recursos necesarios para poder analizarlas, perdemos completa visibilidad de lo que está pasando en nuestra red.

La arquitectura y los modelos de ciberseguridad como los conocíamos ya no satisfacen los nuevos requerimientos, deben adaptarse, deben evolucionar para poder controlar el riesgo y ser una garantía de éxito para los procesos de negocio. Prácticamente por cualquier medida objetiva, el modelo tradicional de ciberseguridad ha fallado. No tiene ningún sentido simplemente seguir invirtiendo dinero en la siguiente solución puntual y esperar que las cosas salgan de otra manera. Es hora de que las organizaciones reconozcan que el ecosistema tecnológico y el panorama de amenazas han evolucionado, y que es necesario un nuevo enfoque para una ciberseguridad más efectiva.

I.2. Pregunta de investigación

¿Qué características debe tener un modelo de ciberseguridad con nuevo enfoque para cajas municipales en tiempos de transformación digital?

I.3. Objetivos de la investigación

I.3.1. Objetivo General

Elaborar la propuesta para un modelo de ciberseguridad con nuevo enfoque para cajas municipales, en tiempo de transformación digital, que incluya características de integridad, confidencialidad y disponibilidad.

I.3.1. Objetivos Específicos

- Identificar modelos de ciberseguridad.
- Comparar modelos de ciberseguridad.
- Proponer características aplicables para un modelo de ciberseguridad con nuevo enfoque.
- Presentar la propuesta para un modelo de ciberseguridad con nuevo enfoque.

I.4. Justificación de la investigación

En estos tiempos de pandemia, las entidades financieras deben salir al mercado con campañas crediticias más agresivas y servicios que permitan a sus clientes realizar sus operaciones desde la comodidad de su casa; lo cual obligara a flexibilizar controles en aras de la agilidad.

Así mismo, los empleados de la organización, tienen la necesidad, y en muchas casos, la urgencia de poder realizar su trabajo de manera remota; es decir, se necesitan habilitar accesos a nuestra red desde sus hogares; lo cual significa, que nuestro endpoint (pc del usuario) que antes

lo protegíamos de tras del perímetro, ahora tendremos que protegerlo estando fuera de él.

Este desafío, recae en las áreas de Seguridad de la Información y Tecnologías de la Información; quienes tienen que lidiar con la flexibilidad sin sacrificar la ciberseguridad.

La situación causada por la pandemia ha forzado la adaptación en el corto plazo, pero debe verse como un paso o un salto hacia la transformación digital, ofreciendo más flexibilidad a los clientes y empleados y potencialmente abriendo nuevas oportunidades de ingresos.

Nuestra investigación se justifica porque permite tener una mejor gestión de los controles de ciberseguridad que ayudan a reducir el riesgo de ataques cibernéticos; y de esa manera, poder proteger los activos de la empresa y la información relevante de sus clientes; ya que hoy en día, los ataques informáticos incrementan de manera significativa y evolucionan constantemente, afectando principalmente a las entidades financieras. Así mismo, se puede tener una visibilidad completa de lo que pasa en nuestra red, tanto de los usuarios que se encuentran detrás del perímetro, como los que se encuentran fuera de él; lo que nos permite identificar nuevos vectores de ataque y poder coordinar también, campañas de sensibilización y capacitación para todos nuestros usuarios y clientes, con el fin de minimizar el riesgo de ser engañados y entregar datos sensibles a través de los diferentes ataques realizados.

La justificación práctica se basa principalmente en la innovación de los modelos de ciberseguridad tradicionales que utilizan la mayoría de cajas municipales y que no se adaptan a los cambios originados por la transformación digital, con un nuevo modelo que permita satisfacer todas esas necesidades. Esta adaptación o innovación, permite brindar valor agregado a los procesos del negocio sin tener que sacrificar aspectos importantes de ciberseguridad.

La justificación teórica se base en que nuestro modelo de ciberseguridad combina estrategias del marco de ciberseguridad NIST y la norma ISO 27032 sobre gestión de la ciberseguridad. Estos modelos, permiten tener una base sólida en la cual soportaremos los diferentes procesos y actividades del ciclo del modelo. Así mismo, utilizar marcos ya reconocidos y aprobados internacionalmente, brinda un valor agregado en la imagen corporativa y te da la posibilidad de obtener una certificación en algunos procesos de negocio.

I.5. Alcance de la investigación

Ante la realidad problemática descrita anteriormente, el presente trabajo de investigación tiene como alcance, la elaboración de la propuesta de un modelo de ciberseguridad con nuevo enfoque; que servirá como soporte para que las Cajas Municipales de Ahorro y créditos, se adapten y respondan de manera exitosa a los nuevos retos y desafíos que trae consigo la transformación digital.

El alcance de esta propuesta tiene una relevancia social en 03 puntos importantes:

- Ayuda a fortalecer la ciberseguridad en todos los niveles de la organización; y le permite mejorar su competitividad en medio de una constante transformación digital. Así mismo, permite tener una visión de ciberseguridad integrada, uniendo a todas las partes de la organización para lograr un objetivo común.

- Refuerza la confianza en la protección de datos personales y cuentas bancarias de sus clientes. Así mismo, permite brindarles una capacitación constante respecto a las nuevas vulnerabilidades o vectores de ataque a través del rápido análisis que permite un modelo moderno de ciberseguridad.

- Refuerza las capacidades y la cultura en ciberseguridad en el aun eslabón más débil de la ciberseguridad: “los usuarios,” y permite proteger sus espacios de trabajo ya sean presenciales o remotos.

La presente investigación no pretende desvirtuar la aplicación de los modelos existentes si no encontrar la aplicabilidad e idoneidad de los modelos con mayor aplicabilidad en tiempos de transformación digital.

II. MARCO TEÓRICO

II.1. Antecedentes

Lara (2019). Ecuador. “*Diseño de un modelo de seguridad de la información, basado en osstmmv3, nist sp 800-30 e iso 27001, para centros de educación: caso de estudio universidad regional autónoma de los andes, extensión Tulcán”.* Esta investigación analiza la situación actual de la Universidad Autónoma de los Andes, extensión Tulcán, respecto a la red de información, seguridad e infraestructura, con el objetivo de diseñar un modelo de seguridad de la información, basado en OSSTMMv3, NIST SP 800-30 e ISO 27001, para la Universidad Regional Autónoma de los Andes. A fin de solventar problemas que se presentan en la gestión de recursos,

acceso a la información y en gestión administrativa de la institución. El estudio es de tipo cuantitativo y descriptivo. La técnica utilizada fue la encuesta aplicadas a los estudiantes, docentes / personal administrativo y de TI. La conclusión de esta investigación menciona que el modelo de seguridad propuesto, pone en evidencia serios factores de riesgo para la seguridad de la información y de la gestión de servicios en la Universidad, haciéndose necesario implementar los correctivos necesarios. (p. 84).

Villalba (2015). España. "*La ciberseguridad en España 2011 – 2015 una propuesta de modelo de organización*". Esta investigación estudia los diferentes niveles de seguridad nacional del gobierno de España relacionados a la ciberseguridad; así como organismos internacionales y los planes y diseños de ciberseguridad de países del primer mundo como EEUU, Rusia y China, analizando sus características y puntos más relevantes que ayudaron a cumplir el objetivo de elaborar la propuesta de un Modelo de Organización de Ciberseguridad en España. Dicho estudio es de tipo cuantitativo y de corte descriptivo. En este trabajo de investigación se ha utilizado el método de comparación analítica por similitud, basando su aportación en la comparación de un número reducido de casos seleccionados por sus características. La conclusión de esta investigación indica que el trabajo de investigación se ha construido como un estudio de caso sobre la ciberseguridad en España, estimando su relevancia y su naturaleza en relación con la propuesta de un modelo de organización de la ciberseguridad en España, el cual pueda ser realizable y tenga un impacto positivo en el incremento de los niveles de la seguridad nacional. (p. 400).

Macancela (2015). Ecuador. "*Modelo de gestión de la seguridad informática para garantizar la continuidad del negocio en la cacpe pastaza*". Esta investigación analiza la situación actual de la institución financiera respecto a sus sistemas de seguridad informática y la forma como afrontan las amenazas presentes. El objetivo de esta investigación permitió proponer un Modelo de Gestión de Seguridad Informática para garantizar la continuidad del negocio en la CACPE Pastaza. La metodología de investigación utilizada para el desarrollo de esta tesis fue la investigación de campo y exploratoria, así también se aplicaron encuestas y entrevistas a los diferentes actores durante el despliegue de la investigación. La conclusión de esta investigación menciona que la Seguridad Informática no puede ser considerada como un producto, sino como un proceso basado en un ciclo iterativo, en el que incluyen actividades como valoración del riesgo, prevención, detección y respuesta ante incidentes de seguridad. Así mismo, Para la CACPE Pastaza es fundamental contar con un Modelo de Gestión de la Seguridad Informática, pues a pesar de que se han definido políticas de seguridad, un plan de contingencia institucional y controles, los mismo no son eficientes y eficaces para proteger y asegurar la información, ya que se los aplica solo cuando aparecen los incidentes de Seguridad, es decir actúan de forma reactiva, sin tener un enfoque claro y bien estructurado de un modelo para gestionar la Seguridad Informática. (p. 105).

Mendoza y Vega (2019). Perú. *"Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa sisc".* Esta investigación hace una revisión del nivel de capacidad en la gestión de la ciberseguridad de la empresa, identifica las brechas que permiten diseñar controles claves para fortalecer la ciberseguridad y la elaboración y propuestas de la hoja de ruta de implementación de los controles clave. El alcance se limitó a los aspectos relacionados a la detección y respuesta de eventos relacionados a la ciberseguridad. El objetivo fue el desarrollo del plan de implementación de las mejoras a efectuar en la empresa. Este plan tuvo como base la versión 1.1 del marco de referencia para la mejora de la Infraestructura Crítica en Ciberseguridad del National Institute of Standards and Technology de Estados Unidos (NIST) (2018). Por la naturaleza de la información que se va a recoger para responder al problema planteado, la presente investigación se encuentra dentro del enfoque cualitativo. Asimismo, debido a la naturaleza de sus objetivos, la presente investigación es del tipo exploratoria, porque examina un tema poco estudiado en el ámbito local y explicativo por qué se busca encontrar las causas del problema. La conclusión menciona que el presente trabajo de investigación servirá para que las empresas centradas en implementar soluciones tecnológicas como protección a ciberataques puedan desarrollar un enfoque de procesos que le permita mejorar sus capacidades para detectar y responder a eventos de ciberataques. Así, en el contexto de la empresa evaluada, este trabajo ha servido para que la gerencia mejore su nivel de entendimiento con respecto a los aspectos de ciberseguridad, que conozca a qué tipos de riesgo está expuesto, y que adopte una gestión en los riesgos de ciberseguridad. (p. 52).

Vilcarromero y Vílchez (2018). Perú. "Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones". Esta investigación hace una revisión de la situación actual del SOC; así como también, realiza un análisis cuantitativo y operativo de sus servicios, y una evaluación del estado de ciberseguridad del mismo. El objetivo fue 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, todo esto basado en el Cyber Security Framework (CSF) del National Institute of Standards and Technology (NIST). La conclusión menciona que 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. Así mismo concluye que 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. (p. 66).

Mercado (2016). Perú. "*Modelo de gestión de seguridad de la información para el E-Gobierno".* Esta investigación describe la revisión de modelos de seguridad de la información, analizando su problemática, aspectos comunes y relevantes en la seguridad, por lo que se identificaron ocho (08) elementos (fases, organización, funciones, documentos, niveles, controles, indicadores y métricas), lo que permitió cumplir con el objetivo de proponer un Modelo de Gestión de Seguridad de la Información para el Gobierno Electrónico, el cual se orienta a los procesos que brindan servicios de gobierno electrónico, lo cual a través de una estructura organizacional y funciones permite implementar y gestionar la seguridad de la información de acuerdo a las fases establecidas y nivel de madurez requerido, mediante la actualización, mejora o desarrollo de documentos y controles; asimismo permite el monitoreo del nivel de seguridad a través de la revisión de los indicadores y métricas establecidas. Dicho estudio es de tipo cuantitativo y de corte descriptivo, la técnica utilizada fue la encuesta, respecto al nivel de valoración que las instituciones objeto de la investigación le atribuyen a la seguridad de la información para los procesos que brindan servicio de gobierno electrónico. La conclusión de esta investigación elaboró un modelo de gestión de seguridad de la información para el gobierno electrónico resultado de la revisión y análisis de 11 modelos de seguridad de la información, en los que se identificaron los elementos más relevantes que forman parte del modelo propuesto. (p. 107).

Guzmán (2015). Perú. "Metodología para la Seguridad de Tecnologías de Información y Comunicaciones en la Clínica Ortega". Existen diferentes estándares que se desarrollaron para gestionar la seguridad de la información, algunos más generales, algunos centrados en la gestión de riesgos (serie ISO/IEC 27.000), y otros incluso tendientes a desarrollar un modelo de madurez de la seguridad de la información (por ejemplo ISM3); sin embargo, en la especificación de las mismos no se afronta su aplicación a un grupo empresarial, lo cual requiere consideraciones adicionales. En este trabajo de investigación, se analizaron diferentes enfoques de estos estándares, y se propuso una metodología de implementación, gestión y mejora de seguridad de tecnologías de información y comunicaciones en la clínica Ortega. La investigación fue de tipo descriptiva porque se logró medir o recoger información de manera independiente o conjunta sobre los conceptos o variables a que se refieren. Fue de tipo explicativa porque se partió de un diagnóstico para proponer una alternativa de solución. La obtención de información se realizó a través de sitios web (internet), libros, manuales de mejores prácticas, revistas y profesionales del área de seguridad informática y se revisaron documentaciones para una mejor obtención de

información. La conclusión menciona que para definir el modelo de metodología de seguridad en tecnologías de información y comunicaciones se realizó el análisis de riesgo que permitió detectar las amenazas a los que son sometidos los activos de la información y los requerimientos de seguridad que se presentaron, han permitido delimitar el ámbito del modelo y su estructura. (p. 134).

El trabajo de Marquera (2015) sobre el Diseño de Seguridad para salvaguardar Activos de Información en el campus de la Universidad Nacional del Centro del Perú – UNCP. El objetivo de esta investigación fue determinar el nivel de influencia del diseño de seguridad de redes mediante la formulación de directivas de TI en la salvaguarda de activos de información en el campus de la Universidad Nacional del Centro del Perú. El método de investigación que se utilizo fue el comparativo, el método específico de inferencia mediante la inducción - deducción. Se utilizó el procesamiento estadístico en la información obtenida en las encuestas. Se utilizó la prueba estadística X2. En la conclusión se menciona La gestión de servicios de tecnologías de información se integra en ingestión por procesos mediante el análisis del modelo de procesos de la Oficina General de Informática que mediante el desarrollo de un modelo de procesos logró establecer una propuesta organizada y estructurada de las actividades asignadas a esta dependencia basada en los reglamentos actualmente vigentes que han servido como punto inicial en la identificación de servicios de 11 con el objetivo de controlar los activos de información. Por lo tanto la identificación de servicios de TI tiene un nivel significativo y alto en la salvaguarda de activos de información probada con una prueba estadística Xi cuadrada con un valor - p<0,0001. Así mismo indica que Las directivas de seguridad de TI formuladas para su ejecución en el control de activos son una importante actividad que regula la implementación de estrategias técnicas. Las estrategias de seguridad son percibidas por el usuario mediante niveles de servicio, niveles seguridad y percepción de incidentes que permite determinar el grado de impacto del diseño de seguridad en la salvaguarda de activos de información. Por lo tanto la evaluación de las estrategias de seguridad basada en la gestión de servicios de tecnologías de información - ITIL, la metodología Magerit y la norma 150 27002 deben tener como relación directa a los servicios proporcionados a los usuarios de la Universidad Nacional del Centro del Perú a través de la red de datos. (p. 96).

II.2. Bases Teóricas

II.2.1. Transformación Digital.

La transformación digital nace de una necesidad tangible: los consumidores están cambiado de manera acelerada por el acceso a más información (Internet), la interacción con las empresas y otros usuarios (redes, foros, aplicaciones), el avance digital en plataformas de pago (e-commerce), las mejoras en logística de entrega de productos, y porque la gran parte del mercado es gente joven o nativos digitales, es decir personas que nacieron

o crecieron desde muy pequeños con la tecnología como parte de sus vidas. En resumen, a lo que llamábamos consumidor hace unos años hoy podemos considerarlo un Consumidor Digital, que pasaría a ser un prospecto digital y luego un Cliente Digital. Sin embargo, las empresas no han crecido en atender estas nuevas necesidades de la misma manera. (Lumbreras, 2019, p. 3)

1. Concepto de Transformación Digital.

La transformación digital es la integración de tecnología digital en todas las áreas de una empresa, cambiando fundamentalmente la forma en que opera y brinda valor a sus clientes. También supone un cambio cultural que requiere que las organizaciones desafíen constantemente el status quo, experimenten y se sientan cómodas con el fracaso. (PowerData, parr. 3)

2. Importancia de la Transformación Digital.

Con clientes cada vez más digitales, la Transformación Digital coloca a tu empresa en el mismo nivel de digitalización que ellos, permitiéndote utilizar los mismos canales de comunicación y facilitándote el entendimiento con ellos. (Lauria, 2020, parr. 19)

Te brinda acceso a nuevas oportunidades de negocio, acercándote a mercados a los que no tenías acceso y te permite estar al día de lo que ocurre afuera de tu entorno, actualizarte con softwares y sistemas que favorecen el negocio. (Lauria, 2020, parr. 20)

3. Covid-19: Adaptación digital o Transformación digital

Hace menos de un año, desde el Harvard Business Review daban cuenta de las dificultades que las empresas habían tenido al llevar a cabo iniciativas de transformación digital. En una investigación con resultados del año 2018, los directores generales de las empresas manifestaban que de los 1,3 billones de dólares gastados en transformación digital se desperdiciaron del orden de unos 900.000 millones, al no alcanzar estos proyectos sus objetivos. Sin embargo, la pandemia del COVID-19 ha acelerado los procesos de virtualización de las relaciones económicas y sociales como respuesta a las cuarentenas forzosas, buscando evitar la desaceleración productiva y la posible interrupción total del sistema. Según asegura la Comisión Económica para América Latina y el Caribe (CEPAL), las empresas más avanzadas en transformación digital tienen mayor capacidad de respuesta a los retos generados por el COVID-19 y, por tanto, juegan con ventaja frente a aquellas que no han iniciado su proceso transformador. (Redaccion Tic Pymes, 2020, parr. 1)

Opciones como el teletrabajo, educación virtual, gobierno en línea, telesalud y cultura digital, entre otras, han surgido como alternativas de respuesta de la sociedad ante la crisis. El hecho de que integren la

tecnología puede llevar a una confusión sobre su naturaleza, pero al analizarlas se demuestra que las acciones no generan una verdadera transformación digital. Desde el Innova Institute de La Salle-URL se ha hecho un estudio para tratar de esclarecer cuáles de estas iniciativas tecnológicas se mantendrán como parte de un proceso de transformación digital, y cuáles, en cambio, son solo procesos de adaptación digital temporal y volverán a sus modelos *offline* en el PostCOVID-19. (Redaccion Tic Pymes, 2020, parr. 2)

- Servicios financieros: Los servicios financieros como se conocen hoy en día van a cambiar, adaptándose a modelos más digitales. Tradicionalmente los bancos han sido los principales protagonistas de este segmento. Sin embargo, esto está cambiando a partir de la irrupción de la tecnología y de las famosas fintech (empresas de tecnología financiera). De la misma manera que sucede en otros ámbitos, el sector financiero migrará paulatinamente hacia modelos de ecosistemas y plataformas, donde los bancos serán un actor más entre otro tipo de organizaciones, como servicios de pago, de gestión de datos e identidades, blockchain y criptomonedas, entre otros. Todos ellos coexistirán en ecosistemas y plataformas tecnológicas. Gracias a la transformación digital, los usuarios podrán, a través de dispositivos móviles, acceder a diferentes formas de financiación, de tipo de pagos y también decidir dónde y cómo invertir su capital, dentro de una amplia diversidad de alternativas de generación y utilización del dinero. (Redaccion Tic Pymes, 2020, parr. 4)

- Teletrabajo para empresas y trabajadores: Existe una clara diferencia entre lo que es un teletrabajo y lo que miles de empresas en todo el mundo han puesto en práctica de emergencia para seguir operando durante el período del COVID-19. Debido a las circunstancias muchos trabajadores tuvieron que convertir, de un día a otro, su residencia en su puesto físico de trabajo, muchas veces teniendo que usar recursos propios y poniendo en riesgo los contenidos confidenciales de las empresas por una falta de estrategia predefinida de ciberseguridad. Además, es de suponer que no toda la gente cuenta con espacios en sus hogares adecuados al teletrabajo y, por otra parte, la conexión a la red de las casas, hasta ahora suficiente, se ha demostrado de poca calidad por el uso de plataformas que consumen mucha banda de datos o por compartir la red con otros usuarios. En suma, el teletrabajo ha sido en muchos casos una adaptación a la nueva realidad para que los que estaban en riesgos de un ERTE pudiesen mantener sus puestos. Pero el teletrabajo profesional no es una adaptación. La empresa que desea que sus empleados trabajen fuera de sus oficinas tienen esta actividad considerada en su plan estratégico, que empieza desde la contratación del profesional, pasa por ofrecer equipos y plataformas adecuados, entrenamientos previos y puntos

de control, muchas veces también tecnológicos. (Redaccion Tic Pymes, 2020, parr. 5)

- Pymes - Comercio: El desarrollo empresarial ve en la transformación digital un camino para mejorar sus resultados optimizando sus procesos y facilitando su gestión, lo que se refleja en utilidades, crecimiento y en ventajas sobre aquellas que no hacen estas inversiones. Sistemas como los ERP, aplicaciones como CAD, CAM, y FMS, la inteligencia artificial, computación en la nube, blockchain, Big Data y los desarrollo de IoT y las plataformas como EDI, innovación abierta y el e-commerce mejoran las capacidades para responder a los desafíos del mercado. Sin embargo, las pymes se enfrentan a diversos retos para lograr esta transformación: las pocas competencias digitales de sus empleados y propietarios, el desconocimiento de los beneficios de la digitalización para las empresas, la resistencia al cambio, la falta de recurso para invertir y el grado de sofisticación del negocio. Así, se generan barreras para la evolución de las empresas y, en consecuencia, menos de la mitad de las pymes han iniciado su proceso de transformación digital, especialmente en países en desarrollo. (Redaccion Tic Pymes, 2020, parr. 9)

II.2.2. Cajas Municipales de Ahorro y Créditos.

Son instituciones micro financieras descentralizadas enfocadas en la atención de aquellos sectores de la población no atendidos por la banca formal, que fueron creadas por la ley 23029 autorizando la creación de las CMAC en las municipalidades provinciales. Las cajas son reguladas por la Superintendencia de Banca y Seguro (SBS) y se encuentran afiliadas al Fondo de Seguros de Depósitos (FSD), además pueden operar en cualquier región y capital de Perú. (Micro Finanzas Global, parr. 4)

En los últimos años, la presencia de las Cajas Municipales de Ahorro y Crédito (CMAC) se ha incrementado y consolidado, constituyéndose en un sistema que contribuye de manera relevante en la provisión de servicios financieros descentralizados en el país. Estas entidades financieras constituyen una oferta única en cerca de 90 distritos del país, logrando posicionarse en lugares donde la banca tradicional no lo hace o tiene una ligera presencia, cumpliendo así un rol importante en la inclusión financiera y, por ende, en el desarrollo económico descentralizado del país. Con la finalidad de preservar el éxito del modelo de la CMAC y poner a su disposición las herramientas necesarias para que compitan en igualdad de condiciones que las instituciones micro financieras privadas, la Superintendencia de Banca, Seguros y AFP (SBS), en uso de su facultad de iniciativa legislativa, remitió al Congreso de la República, hace poco más de un año (el 7 de marzo de 2017), un proyecto de ley que modificaba el marco normativo de las CMAC vigente en ese momento (Decreto Supremo N°157-90-EF del 28 de mayo de 1990), el mismo que fue elaborado con la

participación de la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC). Cuatro meses después (el 13 de julio de 2017) se promulgó la Ley N°30607, que modifica y fortalece el funcionamiento de las Cajas Municipales de Ahorro y Crédito, en la que se le encarga a la SBS que emita las normas que reglamenten diversos aspectos, tales como la elección de los directores de las CMAC, las nuevas operaciones y los servicios autorizados, la reinversión de utilidades, entre otros. (SBS Informa, 2018, pág. 1)

FEPCMAC

La Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC), fue creada mediante el Decreto Supremo N° 191-86-EF publicado el 05 de junio de 1986 y se rige por el D.S. N° 157-90-EF que norma el funcionamiento en el país de las Cajas Municipales de Ahorro y Crédito (CMAC), modificado por la Ley N° 30607, Ley que Modifica y Fortalece el Funcionamiento de las CMAC. (Fepcmac, parr. 1)

La FEPCMAC goza de autonomía económica, financiera y administrativa; y está integrada por 11 Cajas Municipales de Ahorro y Crédito que funcionan a lo largo del territorio nacional en forma descentralizada. Representa al Sistema CMAC como facilitador válido en las diversas coordinaciones ante organismos públicos y privados, nacionales e internacionales, que apoyan el desarrollo económico y financiero del sistema CMAC. (Fepcmac, parr. 2)

Por lo tanto, la FEPCMAC busca representar la unidad de las CMAC y promueve la generación de economías de escala, a través de proyectos conjuntos tanto para el desarrollo de nuevos productos y servicios financieros como en una eficiente administración de recursos. (Fepcmac, parr. 3)

Representa a las siguientes cajas municipales:

- Caja Trujillo
- Caja Arequipa
- Caja Cuzco
- Caja del Santa
- Caja Huancayo
- Caja Municipal Ica
- Caja Maynas
- Caja Paita
- Caja Piura
- Caja Sullana
- Caja Tacna

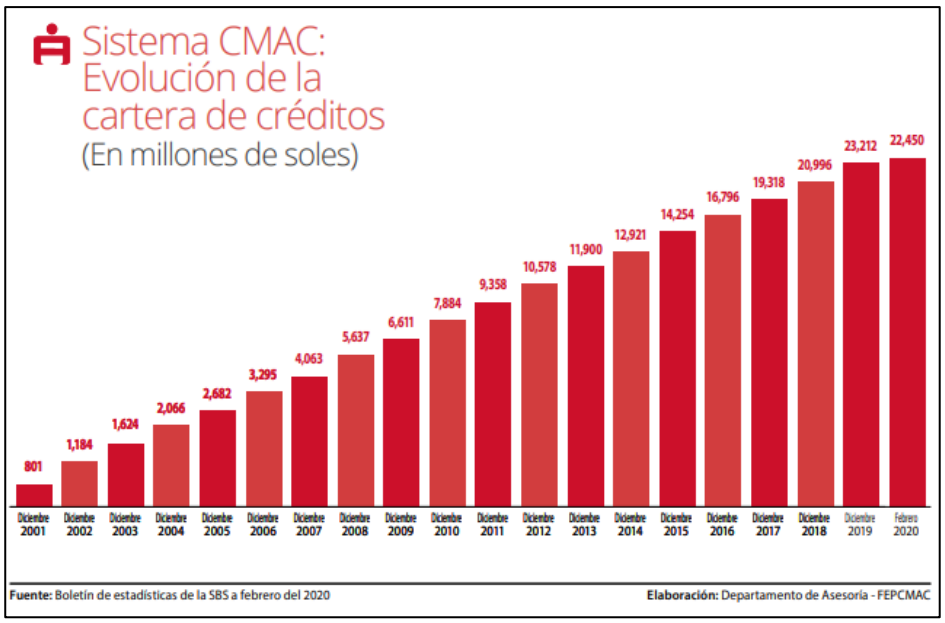


Figura 3. Evolución de la Cartera de créditos

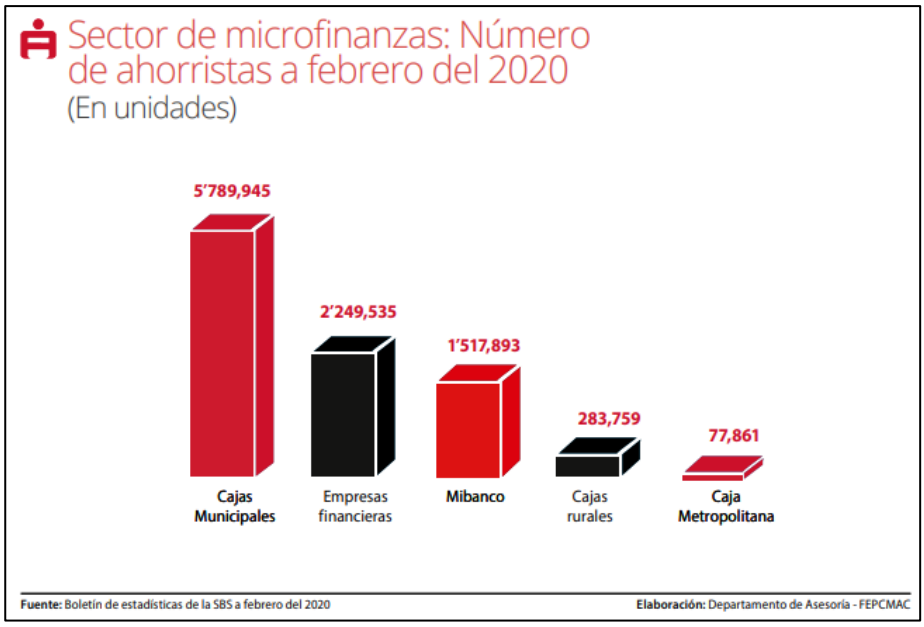


Figura 4. Ahorristas a febrero 2020

Estructura de las CMAC

El directorio de una Caja Municipal está compuesto por siete integrantes, pero cuando incluye terceros accionistas está conformado por un máximo de 9 miembros, como ya lo estipulaba la Ley 30607, publicada en junio del 2017. (Redaccion Gestion, 2018, parr. 2)

Los siete miembros consideran a la mayoría del Concejo Municipal (2), la minoría del Concejo Municipal (1), Cofide (1), la Cámara de Comercio (1),

el Clero (1) y los Pequeños Comerciantes y Productores del ámbito territorial en la cual opera la CMAC (1). (Redaccion Gestion, 2018, parr. 3)

Si el tercer accionista (de existir) tiene por lo menos 7.5% de acciones con derecho a voto, designa a un representante del Directorio; si tiene por lo menos el 15%, designa a 2 representantes. Si el tercer accionista tiene por lo menos el 30% (y designa ahora a 3 representantes), Cofide pierde su derecho a tener un representante. De alcanzar ese porcentaje, y si una CMAC tiene participación accionaria en otra CMAC, quienes pierden su representante son los Pequeños Comerciantes y Productores. A partir del 40%, el tercer accionista designa a 4 representantes, por lo que Cofide y los pequeños comerciantes pierden su derecho a elegir un representante. Si hay otra CMAC involucrada en la participación accionaria, son los pequeños comerciantes y productores, y el clero quienes pierden su derecho a elegir un representante. A partir del 50%, la Caja Municipal se rige por la Ley General y la Ley General de Sociedades. (Redaccion Gestion, 2018, parr. 6)

En cuanto a la estructura orgánica desde el nivel gerencial hacia abajo, las Cajas Municipales también son muy parecidas. Cuentan con una gerencia central mancomunada compuesta por 03 gerencias centrales: Gerencia central de Administración, Gerencia central de Negocios y Gerencia central de Finanzas.

Respecto a los departamentos que tienen que ver directamente con los temas de seguridad de la información, seguridad informática y ciberseguridad; el esquema también es muy similar. El departamento de oficialía de seguridad de la información depende directamente de la Gerencia de Riesgos en la mayoría de casos. La gerencia de Tecnologías de Información cuenta con un departamento de TI pero no cuenta con un departamento encargado específicamente en ver temas de ciberseguridad y Ciberdefensa, lo cual en estos tiempos de transformación digital ya es requerido con urgencia.

A continuación se muestran los organigramas de algunas cajas municipales que pudieron conseguirse desde internet; debido a que, por la coyuntura actual de la pandemia covid-19, no fue posible apersonarse a las instituciones.

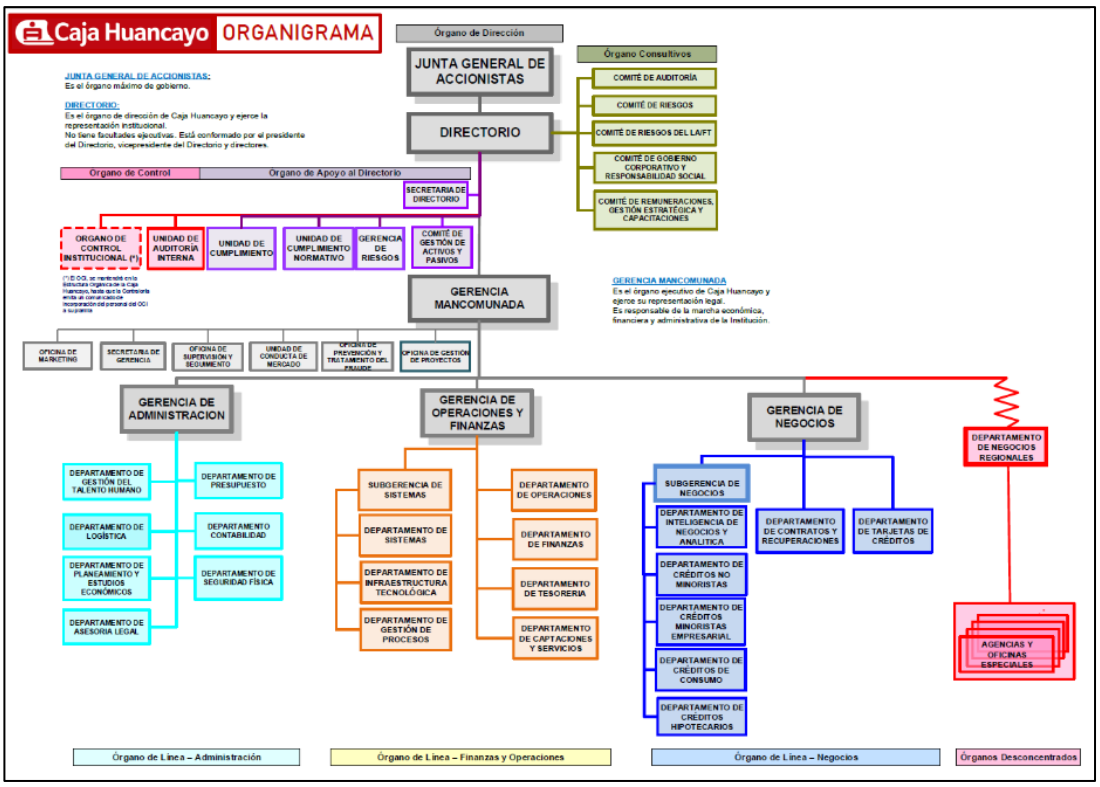


Figura 5. Organigrama Caja Huancayo

Fuente: https://www.cajahuancayo.com.pe/PCM_GobiernoCor/PCM_frmEstructuraOrg.aspx?cCodigo=18

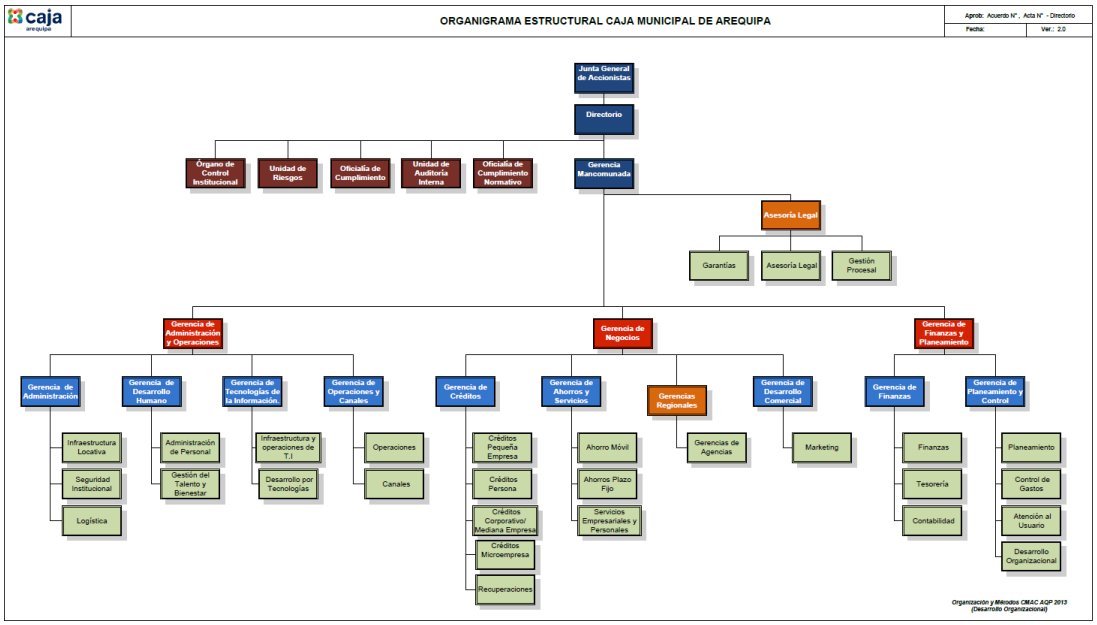


Figura 6. Organigrama Caja Arequipa

Fuente:
https://www.smv.gob.pe/ConsultasP8/temp/Organigrama%20estructural%20Caja%20Arequipa%202013.pdf

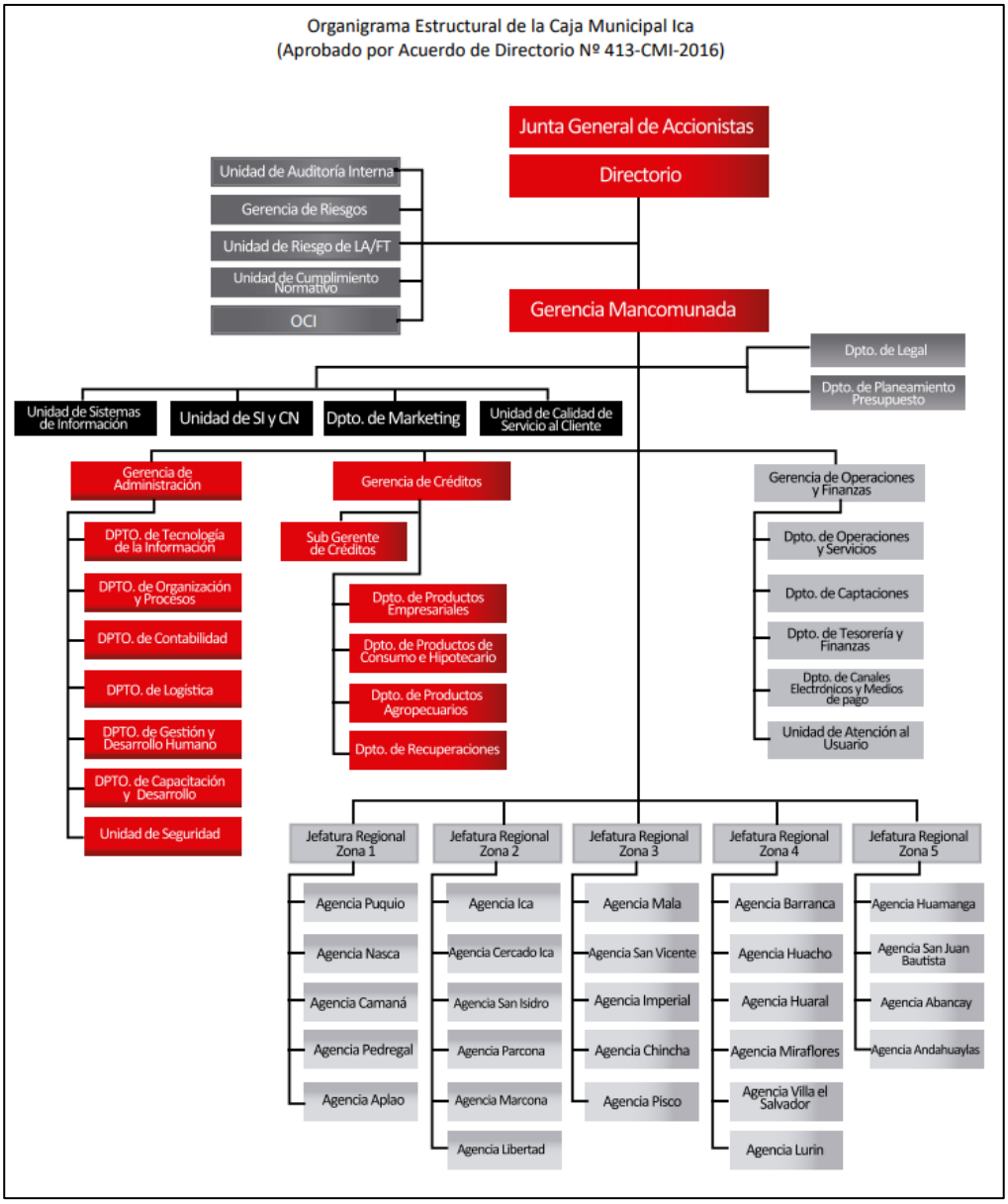


Figura 7. Organigrama Caja Ica

Fuente: https://www.cmacica.com.pe/cmacica/Webcmacica/userfiles/file/nosotros/Memoria_Anual_2016.pdf

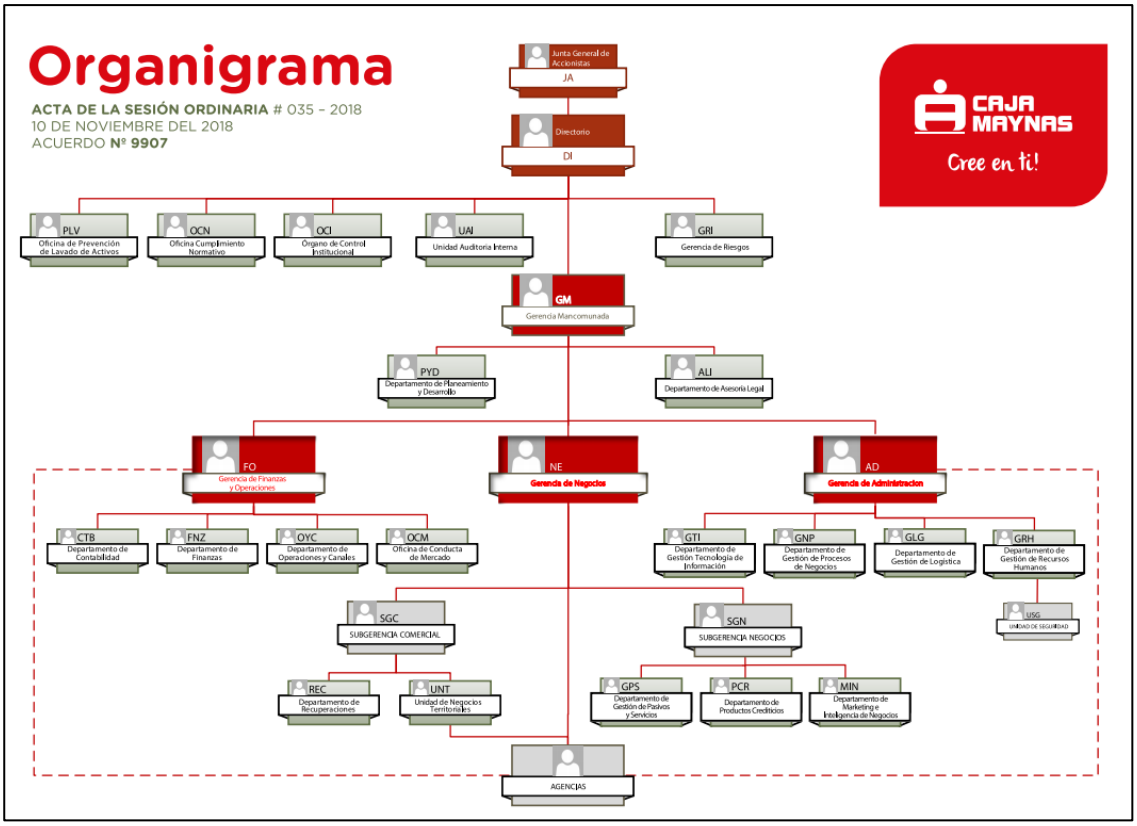


Figura 8. Organigrama Caja Maynas

Fuente: https://www.cajamaynas.pe/wp-content/uploads/2019/01/ORGANIGRAMA-CAJA-MAYNAS.pdf

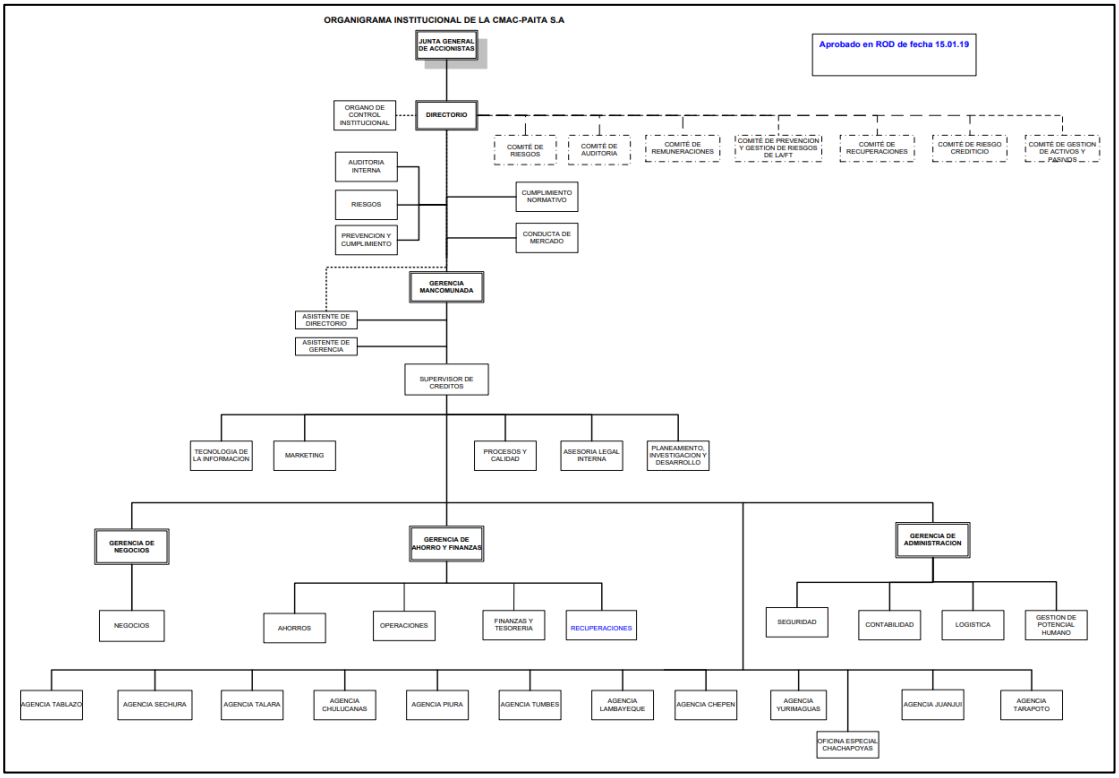


Figura 9. Organigrama Caja Paita

Fuente: https://www.cajapaita.pe/portal/wp-content/files/doc_transparencia/organigramas/Organigrama_25052019.pdf

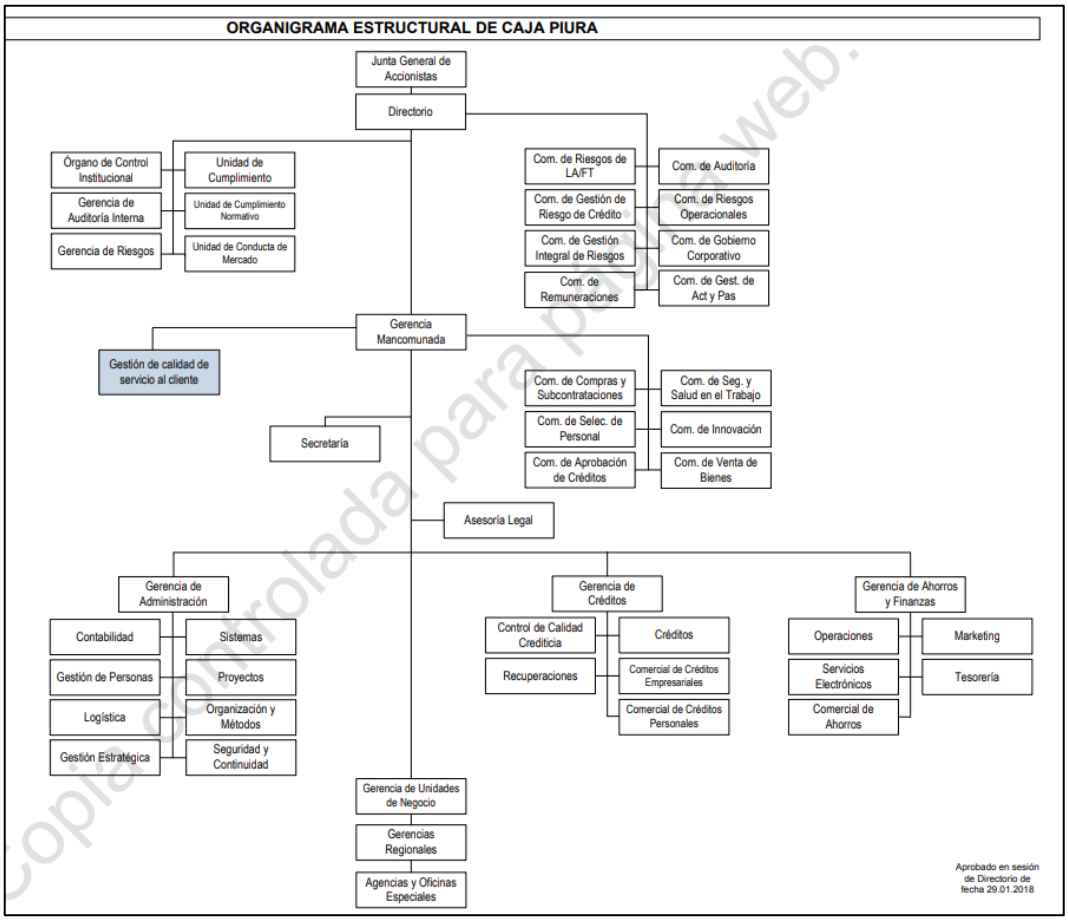


Figura 10. Organigrama Caja Piura

Fuente: https://www.cajapiura.pe/_files/Organigrama_CMAC_PIURA_SAC_29.01.2018.pdf

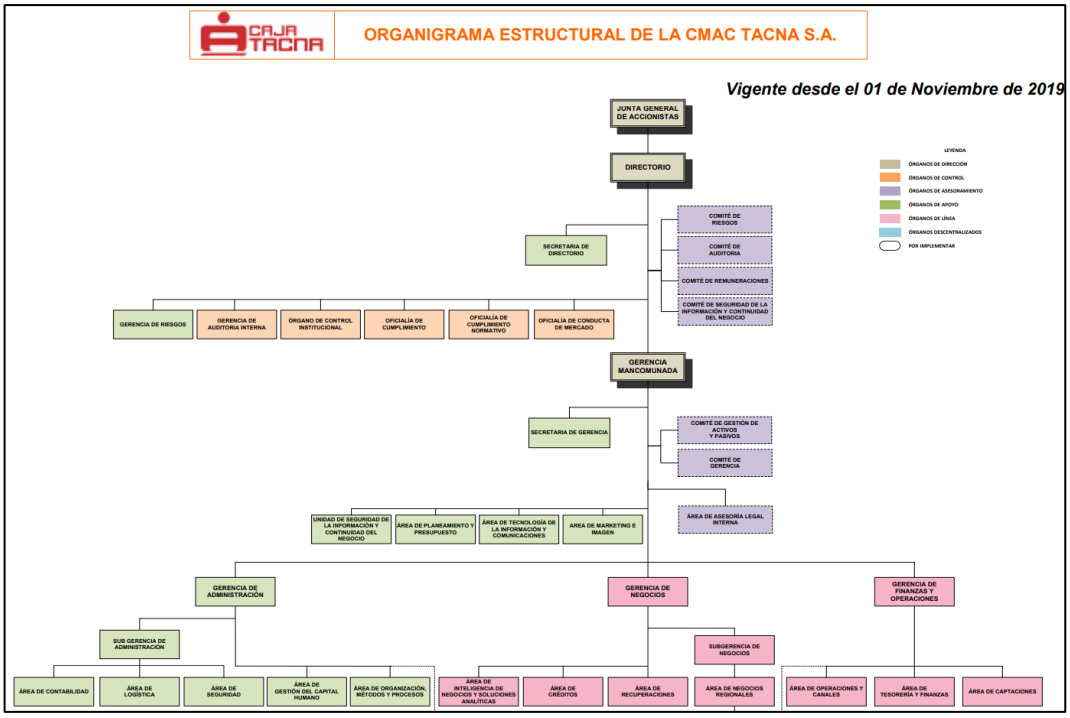


Figura 11. Organigrama Caja Tacna

Fuente: https://cmactacna.com.pe/documentos/transparencia/ORGANIGRAMA_ESTRUCTURAL_CMACTACNA.pdf

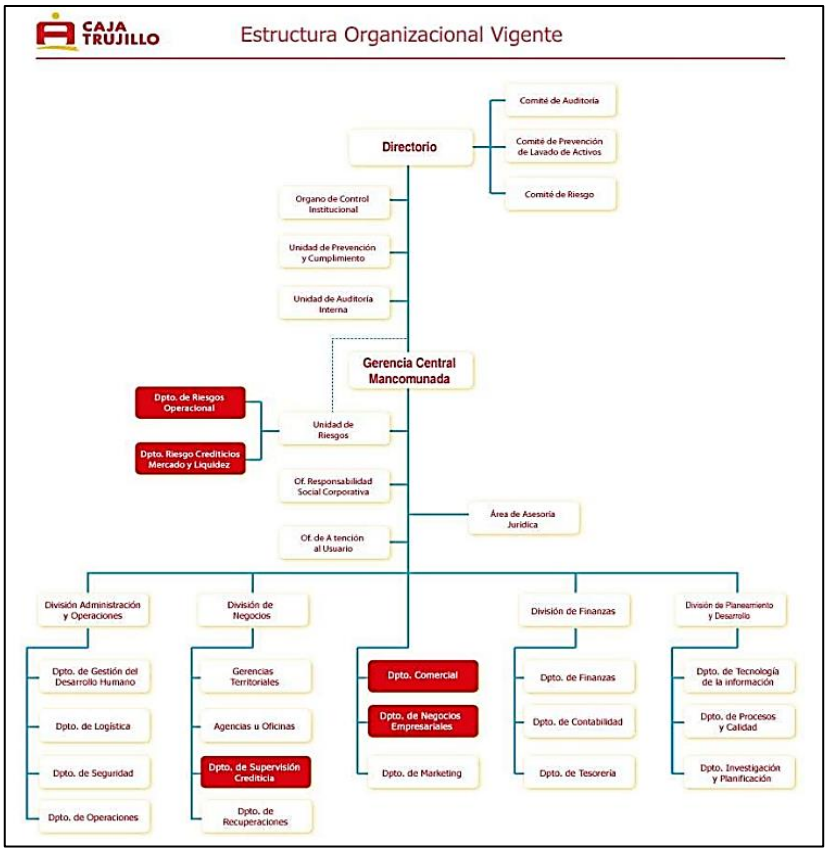


Figura 12. Organigrama Caja Trujillo

Fuente: https://www.cajatrujillo.com.pe/portalnew/doc/transparencia/2012/Organigrama.pdf

II.2.3. Ciberseguridad

Desde hace unos años, la palabra ciberseguridad se ha vuelto un estándar entre las empresas, puesto que la informática es ya una herramienta habitual en los negocios y para mantener los sistemas a salvo hacen faltas medidas de seguridad que nos ayuden a evitar vernos expuestos a grandes riesgos. (Obs business School, parr. 1)

1. Definición de ciberseguridad.

En la pasada edición de bSecure Conference, profesionales de seguridad de ISACA (Information Systems Audit and Control Association) capítulo Monterrey, comenzaron su participación a partir de definir qué es la ciberseguridad. De acuerdo con la asociación, puede entenderse 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". (Mendoza, 2015, parr. 5)

Por lo tanto, la ciberseguridad tiene como foco la protección de la **información digital** que "vive" en los sistemas interconectados. En consecuencia, está comprendida dentro de la seguridad de la información. (Mendoza, 2015, parr. 7)

2. Seguridad de la información vs Seguridad informática vs ciberseguridad.

La seguridad informática y la seguridad de la información pueden parecer lo mismo. Sobre todo si se tiene en cuenta que el desarrollo y la evolución de la tecnología tiende hacia el modelo de digitalizar y manejar cualquier tipo de información mediante un sistema informático. No obstante, aunque se encuentran destinados a vivir en armonía y trabajar de forma conjunta, cada una de las áreas de seguridad tiene objetivos y actividades diferentes. (pmg-ssi, 2017, parr. 1)

La seguridad informática se describe como la distinción táctica y operacional de la seguridad, mientras que la seguridad de la información es la línea estratégica de la seguridad. (Pmg-ssi, 2017, parr. 2)

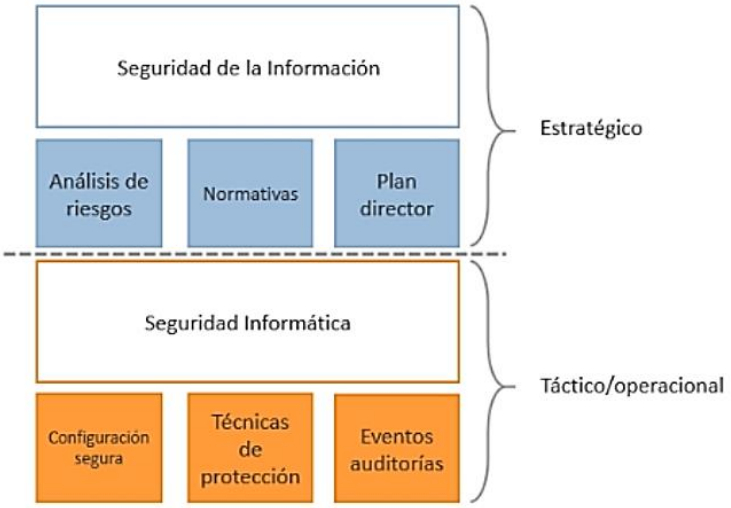


Figura 13: Esquema de seguridad

La seguridad de la información es la disciplina que se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información. Para conseguir el objetivo se apoya a la seguridad informática, es decir, a pesar de ser disciplinas diferentes, la una no puede ir sin la otra. De forma que la seguridad de la información será la encargada de regular y establecer las pautas a seguir para la protección de la información. (Pmg-ssi, 2017, parr. 7)

Muchas veces escuchamos hablar de seguridad de la información y seguridad informática indistintamente. Por una parte, la seguridad informática protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene. Por lo tanto, podríamos decir, que se trata de implementar medidas técnicas que preservaran las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa. (Pmg-ssi, 2017, parr. 10)

La seguridad de la información va mucho más allá, puesto que intenta proveer de medidas de seguridad a otros medios donde se localiza la información como: Impresos en papel, discos duros, medidas de seguridad respecto de las personas que la conocen, etc. (Pmg-ssi, 2017, parr. 11)

La ciberseguridad se enfoca principalmente en la información en formato digital y los sistemas interconectados que la procesan, almacenan o transmiten, por lo que tiene un mayor acercamiento con la seguridad informática. (Mendoza, 2015, parr. 17)

3. Claves de Ciberseguridad

Sin duda, uno de los hackers más grandes de toda la historia (en lo personal, el más grande), es Kevin Mitnick, el cual habló de las claves de ciberseguridad en el evento “Microsoft Security University, en México; hoy

en día convertido en experto consultor en ciberseguridad, y asesor de las más grandes empresas, gobiernos e inclusive la misma CIA.

¿Cuáles fueron los consejos de seguridad otorgados desde la visión del hacker?

- No dejar la seguridad física de lado. Si bien es bueno contar con buenas estrategias de seguridad digital, invertir en seguridad física es algo que no se debe dejar de lado. El papel de las personas sigue siendo importante. (Rodriguez, 2017, parr. 4)

  > *"En el mundo de hoy donde la ciberseguridad es tan avanzada, los esfuerzos se enfocan en proteger las redes, muchas empresas no piensan sobre la seguridad física, pero es algo que no deben dejar de lado, realmente es muy fácil hackear credenciales de acceso, ¿cómo combatimos esto? Con seguridad física",* aseguró Mitnick.

- Actualizaciones: sistemas y programas. Tal vez unos de los consejos más escuchados y si bien diferentes empresas están conscientes de la importancia de mantener sistemas, software y parches de seguridad siempre al día, siguen siendo los principales problemas de seguridad de las empresas. (Rodriguez, 2017, parr. 6)

  > *"Se olvidan de las actualizaciones, y estas son muy importantes para protegerse de los ataques de día cero. Siempre que nos llegue una notificación debemos actualizar", aseguró Mitnick.*

- Phishing sigue siendo el método más sencillo de infección. A pesar del aumento de ataques y consciencia de seguridad, los phishing siguen siendo el método número uno para obtener víctimas fáciles, incluso para aquellos expertos de seguridad. "El phishing es cada vez más sofisticado y difícil de identificar, terminando en grandes robos o ataques avanzados. Hay que notar las señales". (Rodriguez, 2017, parr. 8)

- Amenazas internas. Las compañías están conscientes de la importancia de actualizar los sistemas externos, pero no suelen poner los mismos esfuerzos a los internos, donde muchas veces se originan los ataques. Mitnick recomienda prestar más atención en ello. (Rodriguez, 2017, parr. 9)

- Backups constantes. WannaCry, Petya y más recientemente BadBunny han hecho que las empresas se tomen el respaldo más en serio, pero aún no es suficiente. Mitnick recomienda hacer respaldos diarios para que, en caso de ser atacado, poder recuperar el sistema hasta el modo seguro. (Rodríguez, 2017, parr. 10)

- Apuesten por el Cloud. Por último, Mitnick recomendó no tenerle miedo a la nube ya que ofrece una serie de beneficios de agilidad, además de que tienen un equipo completo de seguridad por muy poco precio.

> "Siempre será más fácil hackear un sistema interno que empresas de nube que tienen equipos completos de seguridad". (Rodríguez, 2017, parr. 11)

4. Situación Actual de la Ciberseguridad.

A medida que la pandemia de coronavirus continúa perturbando los sistemas mundiales de salud, económicos , políticos y sociales, hay otra amenaza invisible en aumento en el espacio digital: el riesgo de ataques cibernéticos que se aprovechan de nuestra mayor dependencia de las herramientas digitales y la incertidumbre de la crisis. (Worl Economic Forum, 2020, parr. 1)

Los expertos en ciberseguridad están cada vez más preocupados por la grave situación de riesgo que se está produciendo a causa de la pandemia, algo que los cibercriminales están aprovechando al máximo. Porque el clima de tensión lleva a las personas a cometer errores en sus interacciones digitales, y los delincuentes están encontrando más vías de acceso para difundir malware y llevar a cabo con éxito estrategias de phishing basadas en el coronavirus. (Ittrends, 2020, parr. 1)

Algunos de los ataques que mas se han realizado durante la pandemia son los siguientes:

- **Multitud de campañas de phishing**: los cibercriminales están agudizando su ingenio alrededor del COVID-19 para lanzar campañas de phishing. Si damos un paseo por internet, veremos campañas de phishing en las que te alertan de que has tenido contacto con una persona infectada y que podrías haberlo contraído obligándote a abrir un documento Excel para ejecutar malware en tu equipo. También se han visto las ya recurrentes campañas de cheques regalos de algunas grandes superficies, así como envíos de SMS con información falsa, instando a los usuarios que reciben este mensaje a que faciliten sus datos personales para comprobar su afectación.

- **Difusión de malware bancario:** usando como gancho el **COVID-19**, una campaña de phishing que suplanta la identidad de un supuesto "casero" indicando en el correo, que dada la situación extraordinaria que vivimos se perdona el mes de alquiler. Pero en realidad, lo que trata es de conseguir que el usuario realice una serie de acciones para instalar el malware bancario Zeus Sphinix que se reutiliza después de 3 años tal y como indica un informe de X-Force de IBM.

- **Fake News (noticias falsas):** en estos días, es bastante común ver como nuestras redes sociales se inundan de mensajes, audios o incluso correos electrónicos con noticias falsas, consejos "caseros" para mitigar los efectos del coronavirus, etc.

Esos ataques pueden representar un duro golpe para cualquier negocio, sobre todo en términos económicos y de credibilidad. Una filtración de datos puede hacer que la empresa pierda la confianza de sus clientes. También puede generar pérdidas económicas ya que la mayoría de los ciberataques se lanzan para paralizar las actividades de la empresa y pedir un rescate. Por tanto, ahora más que nunca, las empresas necesitan reforzar su ciberseguridad. (Eserp Business & Law School, parr. 4)

La World Economic Forum colocó los ciberataques como una de las principales amenazas mundiales en términos de impacto en su Mapa de Riesgos Globales de 2020, donde también se incluyen otros como los desastres naturales o las enfermedades infecciosas.

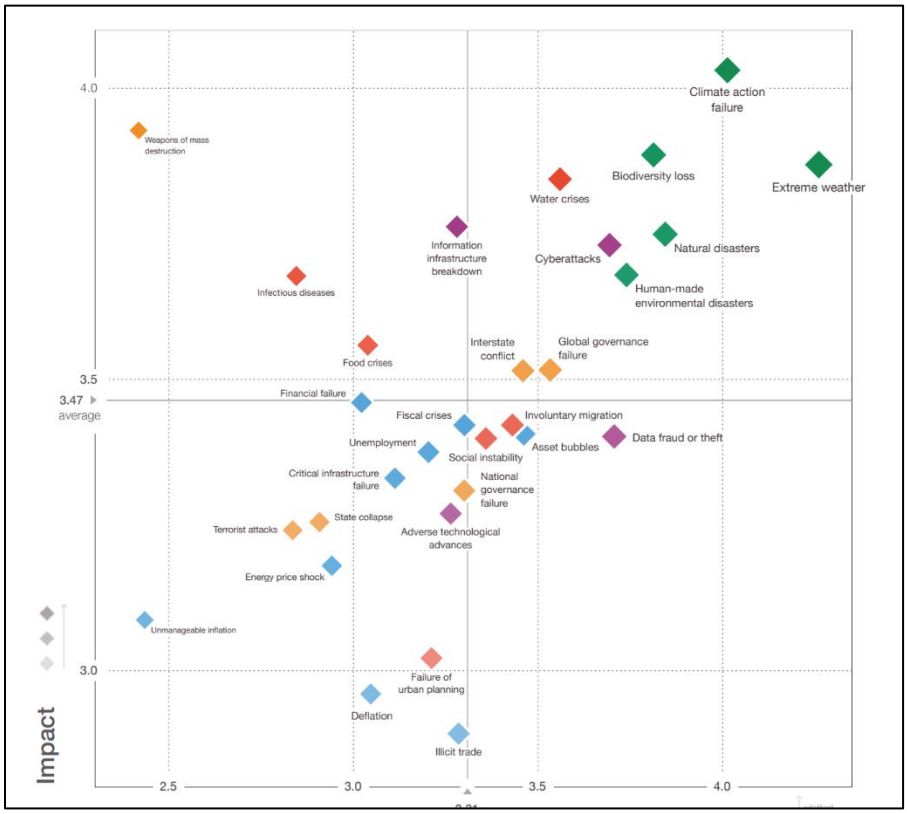


Figura 14. Mapa de Riesgos Globales

Entonces, ¿qué podemos hacer?

Así como abordar la pandemia de COVID-19 requiere cambiar nuestros hábitos y rutinas sociales para impedir las tasas de infección, un cambio en nuestro comportamiento en línea puede ayudar a mantener altos niveles de ciberseguridad.

1. Intensifique sus estándares de higiene cibernética

Además de lavarse las manos después de cada contacto físico para evitar la propagación de COVID-19 y usar una solución de limpieza a base de

alcohol adecuada en su teléfono, teclado, controles de juegos y controles remotos, tómese el tiempo para revisar sus hábitos de higiene digital. Compruebe que tiene una contraseña de enrutador larga y compleja para el wifi de su hogar y que los cortafuegos del sistema están activos en su enrutador. Asegúrese de no reutilizar las contraseñas en la web (un administrador de contraseñas es una gran inversión) y utilice una VPN confiable para acceder a Internet siempre que sea posible. (Worl Economic Forum, 2020, parr. 10)

2. Sea más vigilante en la verificación

Tenga mucho más cuidado de lo habitual al instalar el software y al proporcionar cualquier información personal. No haga clic en los enlaces del correo electrónico. Al suscribirse a nuevos servicios, verifique la fuente de cada URL y asegúrese de que los programas o aplicaciones que instale sean las versiones originales de una fuente confiable. Los virus digitales se propagan de manera similar a los físicos; Sus posibles errores en línea podrían contaminar a otros en su organización, una libreta de direcciones o la comunidad en general. (Worl Economic Forum, 2020, parr. 11)

3. Siga las actualizaciones oficiales

Del mismo modo que presta atención a las fuentes confiables de datos sobre la propagación y el impacto de COVID-19, asegúrese de actualizar regularmente el software y las aplicaciones de su sistema para corregir cualquier debilidad que pueda explotarse. Si en algún momento siente que el consejo que le da suena extraño, ya sea que la amenaza del virus sea fuera de línea o digital, busque en Internet para ver si otros tienen preocupaciones similares y busque un sitio conocido que pueda ayudar a verificar la legitimidad de la información. El comportamiento personal de todos es fundamental para prevenir la propagación de infecciones peligrosas tanto en línea como en el mundo físico. (Worl Economic Forum, 2020, parr. 12)

Estadísticas Actuales de Malware y ataques

En los últimos 10 años, el incremento de malware ha sido increíble. Todos los días, el Instituto AV-TEST registra más de 350,000 nuevos programas maliciosos (malware) y aplicaciones potencialmente no deseadas (PUA).

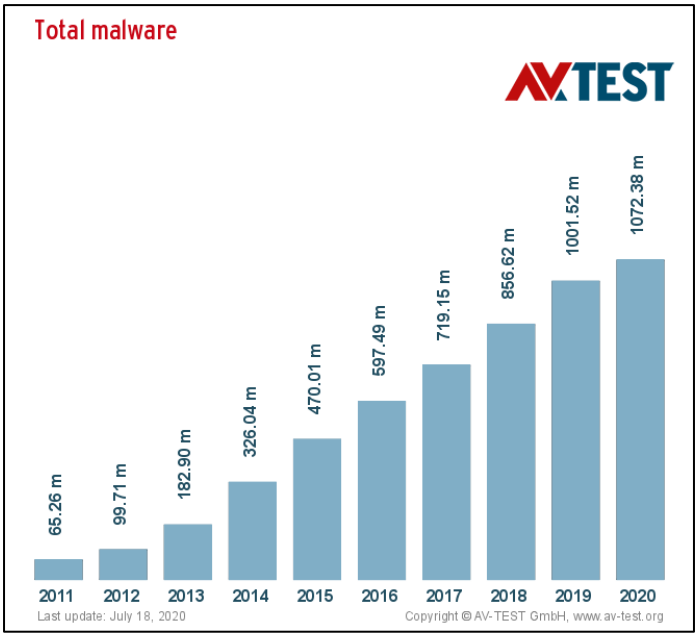


Figura 15. Total malware por año

De acuerdo a un reporte de Palo Alto Netkworks en marzo del 2020 relacionado a amenazas, se identificó que el 41% corresponde a Exploits; el 33% a malware y el 26% a malas prácticas de usuario.

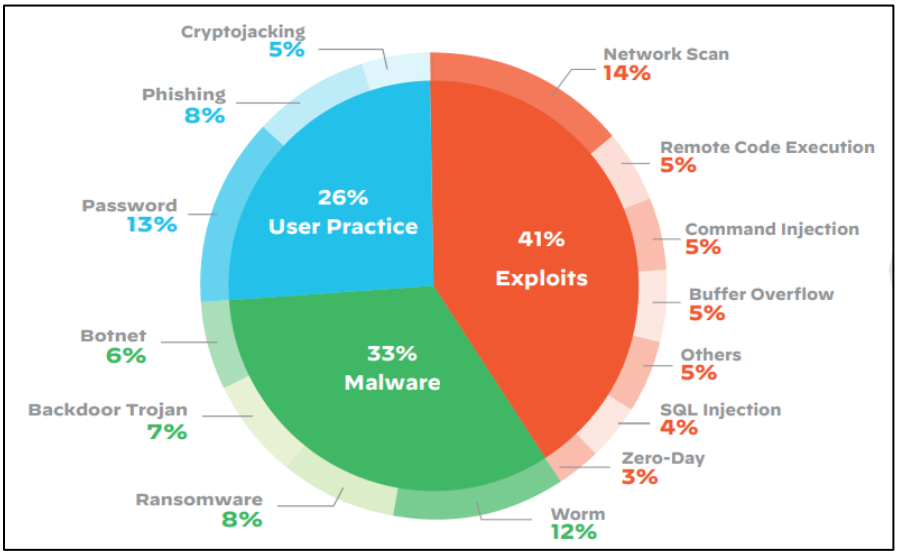


Figura 16. Porcentaje por amenazas.

De acuerdo al reporte de kaspersky, a nivel global, estos son los países con más incidentes de ciberseguridad.

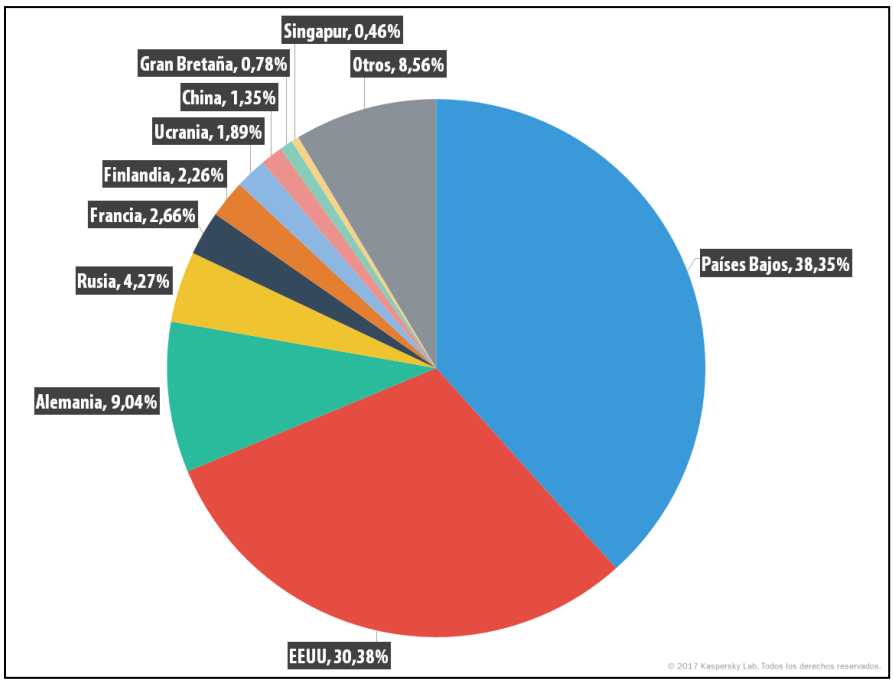


Figura 17. Incidentes de ciberseguridad por países a nivel global

A nivel de Latinoamérica tenemos que Perú se encuentra en el puesto número 4 respecto a ataques informáticos, el cual está liderado por Brasil y México.

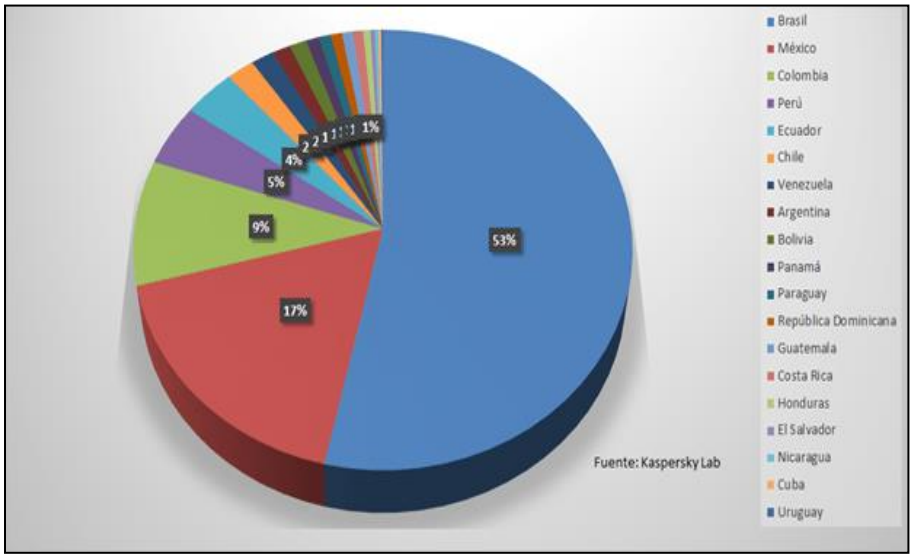


Figura 18. Incidentes de ciberseguridad en Latinoamérica

Los ciberataques se incrementan potencialmente y encuentran una oportunidad debido a que cada vez más usuarios se conectan a internet; así como también, el internet de las cosas va ganando terreno, permitiéndonos interconectar tecnologías, artefactos, automóviles, robots, etc. Con la pandemia del covid 19, esto se ha multiplicado enormemente.

Figura 19. Conexiones a redes sociales por mes

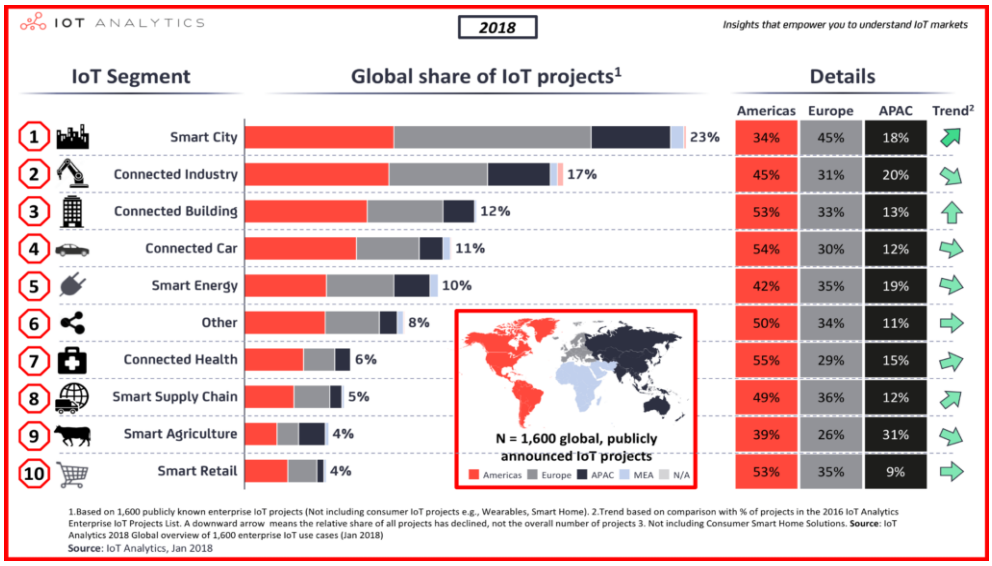


Figura 20. Porcentaje de conexión IoT

Los atacantes también han evolucionado y con ellos las técnicas y estrategias de ciberataques. La tecnología como inteligencia artificial y machine learning nos protegen pero también son usados contra nosotros.

Figura 21. Evolución de los atacantes

II.2.4. Modelos de Ciberseguridad.

(Real Academia Española - RAE) define al modelo como “un esquema teórico de un sistema o de una realidad compleja”.

Por lo tanto, un modelo de ciberseguridad nos permite tener un esquema que engloba técnicas, estrategias y herramientas que nos ayude a proteger los activos de información o servicios conectados a internet.

Modelos Tradicionales

(Real Academia Española - RAE), menciona que: “Lo tradicional sigue las normas y costumbres del pasado”.

En ese sentido, podemos decir que los modelos de ciberseguridad tradicionales, aun mantienen la idea de proteger unicamente todo lo que se encuentra detrás del perimetro de nuestra red; asi como tambien, mantienen la idea de solo contar con soluciones de seguridad tipo firewall, antivirus, ips, etc, que aun son necesarios e importantes pero no suficientes.

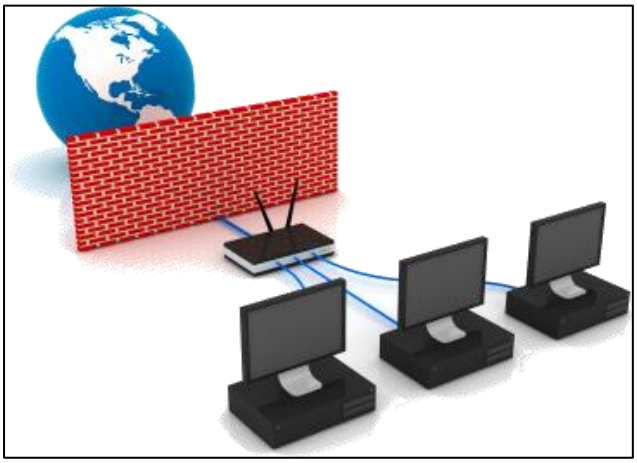


Figura 22. Modelo de seguridad Tradicional

La forma en que las empresas abordan la ciberseguridad es literalmente una locura, al menos según la cita popular atribuida a Albert Einstein: “La definición de locura es hacer lo mismo una y otra vez y esperar resultados diferentes”.

Muchas organizaciones intentan arrojar dinero al problema. Asumen que si solo asignan más presupuesto y compran los productos y servicios correctos, estarán seguros. Sin embargo, algunas de las violaciones de datos más grandes y costosas de la historia ocurrieron en compañías con inversiones significativas en herramientas y plataformas de seguridad cibernética, y que tienen grandes equipos de expertos en seguridad cibernética y vastos recursos a su disposición. En otras palabras, la ciberseguridad es un negocio muy lucrativo, pero comprar más no

garantiza que esté seguro. De hecho, a menudo no cumple su promesa. (Bradley, 2019, parr. 4)

Esto no quiere decir que se deba invertir menos en ciberseguridad; de hecho, los porcentajes de inversion que se destinan a la ciberseguridad en las organizaciones no son las adecuadas y se deben mejorar, y mucho mas si se habla del endpoint, que en un entorno de transformacion digital, y mas aun en tiempos de pandemia, se ha convertido en el punto de atraccion mas importante para los ciberdelincuentes. Lo que se debe lograr es que la inversion debe ir acorde con los objetivos de la organización, y sobre todo, se debe integrar a la arquitectura de seguridad que se tiene, con el objetivo de lograr mayor visibilidad de lo que pasa por nuestra red. Existen organizaciónes que compran tecnologia sin tener en cuenta lo antes mencionado y al final se termina coleccionando diversas marcas sin que estas puedan integrarse entre si.

Prácticamente por cualquier medida objetiva, el modelo tradicional de ciberseguridad ha fallado. No tiene ningún sentido simplemente seguir invirtiendo dinero en la siguiente solución puntual y esperar que las cosas salgan de otra manera. Es hora de que las organizaciones reconozcan que el ecosistema tecnológico y el panorama de amenazas han evolucionado, y que es necesario un nuevo enfoque para una ciberseguridad más efectiva. (Bradley, 2019, parr. 11)

Otro factor que nos indica que los modelos tradicionales son pocos flexibles, es por ejemplo, que cada vez se generan mayor cantidad de alertas a investigar, y lo grave de todo eso es que solo un pequeño porcentaje de esas alertas son investigadas. Esto puede deberse a que no se tiene los recursos necesarios para poder procesar y analizar esa cantidad de incidentes, o no se tiene el tiempo suficiente, o no se cuenta con la capacidad de explotacion de las medidas de seguridad que establecemos. (Franco, 2019)

Figura 23. Alertas investigadas

Algunos indicadores que pueden dar indicio que el modelo tradicional es obsoleto son los siguientes:

Figura 24. Indicadores de obsolescencia

Otros factores de obsolescencia:

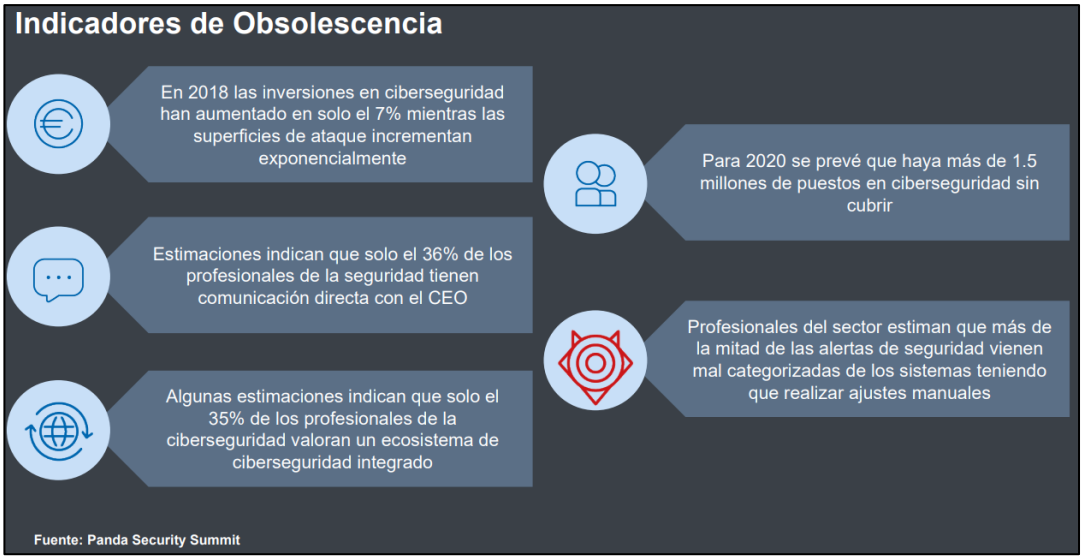


Figura 25. Factores de obsolescencia

Modelos con nuevo enfoque

El nuevo modelo de ciberseguridad gira en torno a tecnologías como la autenticación multifactorial, el análisis de comportamiento y la tecnología de engaño. La autenticación multifactorial o de dos factores eleva el listón para obtener acceso autorizado a sistemas y datos en primer lugar y evita que los atacantes entren solo con credenciales comprometidas o robadas. El análisis del comportamiento y la tecnología de engaño brindan un

monitoreo y protección más completos basados en la suposición de que los atacantes pasarán, que “ellos” son “nosotros” y ya están dentro. (Bradley, 2019, parr. 8)

Con esa suposición, la seguridad se vuelve menos importante para evitar el acceso no autorizado y más para garantizar que las actividades de quienes tienen acceso tengan sentido y no violen ninguna política. La realidad es que la mayoría de los ataques, en el punto en que se detectan, son ataques “internos”, ya que si los realiza un empleado descontento o un atacante externo con credenciales robadas o comprometidas, parecen ser de un usuario “autorizado”. desde la perspectiva del departamento de TI. (Bradley, 2019, parr. 9)

Monitorear el comportamiento es un medio más proactivo y más efectivo para detectar comportamientos sospechosos o maliciosos. Bob puede ser un empleado autorizado para acceder a los datos de los empleados y a los registros financieros de la compañía, pero Bob también tendrá un patrón normal de comportamiento que puede usarse para señalar actividades inusuales. Si Bob trabaja en un horario comercial normal en una oficina en Tulsa, es fácil detectar actividad sospechosa si de repente se conecta desde Tel Aviv a las 3 am del sábado. Si Bob generalmente accede, pero no descarga, datos financieros, el análisis de comportamiento puede alertar a TI si Bob repentinamente decide descargar gigabytes de información confidencial. (Bradley, 2019, parr. 10)

Para ser capaces de adaptarse y reinventar la estructura de servicios, las organizaciones comienzan a apostar por modelos de gobiernos y operación de ciberseguridad, orientados a proporcionar una seguridad operativa, eficaz y eficiente en términos de costes justificables. (El pais economia, 2020, parr. 4)

Como adaptar el modelo de ciberseguridad en la era de la transformacion digital:

Un modelo de ciberseguridad con nuevo enfoque debe tener como minimo las siguientes caracteristicas:

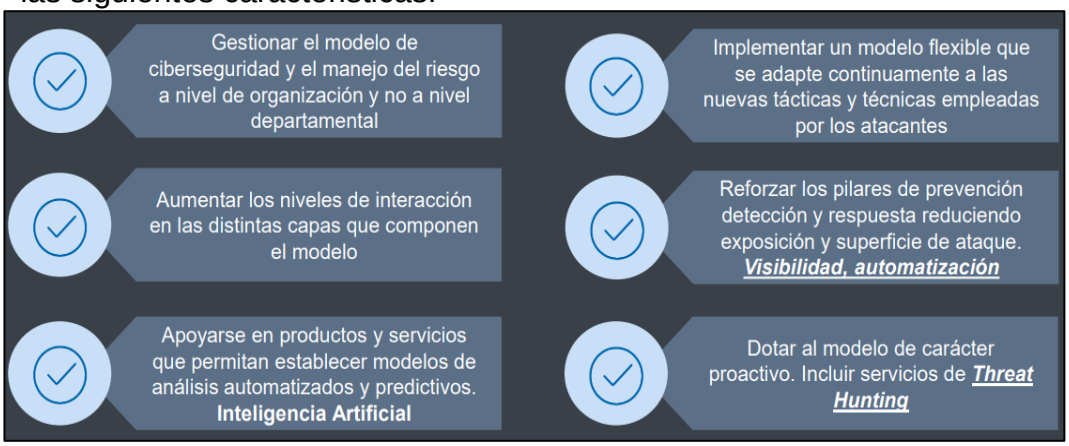


Figura 26. Adaptación del modelo en la era de la transformación digital

Uno de los temas sumamente importantes que conviene tener en cuenta en un nuevo modelo de ciberseguridad es la “Ciber-Resiliencia”.

Gianncarlo Gómez, docente del curso Gestión de la Ciberseguridad del PEE de ESAN, define ciberresiliencia como "la forma con la que una compañía o entidad del gobierno va a poder mantener sus operaciones ante algún tipo de ataque informativo o ataque de ciberseguridad". Es decir, la ciberresiliencia trata sobre la capacidad de una organización para prevenir, identificar y contener las amenazas contra datos o información de mucho valor. Todas estas acciones se ejecutan de forma rápida para reducir el tiempo de exposición. (Esan, 2018, parr. 2)

II.2.4.1. Modelo ISM3.

ISM3 es un modelo de madurez para seguridad con cinco niveles que facilita la mejora y alineación con las necesidades del negocio de los sistemas de gestión de la seguridad de organizaciones de cualquier tipo y tamaño. (Snape, 2020)

Esta basado en el modelo de mejora continua a traves de la aplicación del circulo de deming.

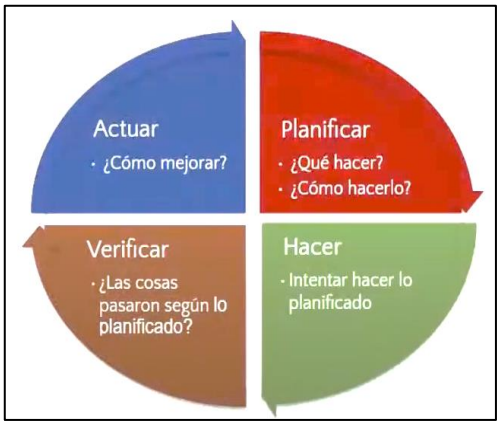


Figura 27. Circulo de deming

Objetivos de ISMP3:

- Incluir metricas, adopcion evolutiva. Mejora continua.
- Enlazar la seguridad al negocio.
- Flexibilidad, adaptarse a distintas capacidades de inversion.
- Crear un ecosistema alrededor de ism3 (cobit, ISO 27000, etc.)

II.2.4.2. Modelo de Seguridad Perimetral.

Un perímetro de red es el límite seguro entre el lado privado y administrado localmente de una red, a menudo la intranet de una empresa, y el lado público de una red, a menudo Internet. (Ciberseguridad, parr. 7)

Un perímetro de red incluye:

- Enrutadores fronterizos: los enrutadores sirven como señales de tráfico de las redes. Dirigen el tráfico hacia, desde y a través de las redes. El enrutador de borde es el enrutador final bajo el control de una organización antes de que el tráfico aparezca en una red no confiable, como Internet.

- Cortafuegos: un cortafuegos es un dispositivo que tiene un conjunto de reglas que especifican qué tráfico permitirá o denegará pasar a través de él. Un cortafuegos generalmente se retiene donde el enrutador de borde deja y hace un paso mucho más completo al filtrar el tráfico.

- Sistema de detección de intrusos (IDS): se trata de un sistema de alarma para la red usado para localizar y avisar de actividades sospechosas. Este sistema se puede construir desde un solo dispositivo o una colección de sensores ubicados en puntos estratégicos de una red.

- Sistema de prevención de intrusiones (IPS): en comparación con un IDS tradicional que simplemente notifica a los administradores de posibles amenazas, un IPS puede intentar defender automáticamente el objetivo sin la intervención directa del administrador.

- Zonas desmilitarizadas / subredes protegidas: DMZ y subred filtrada se refieren a pequeñas redes que contienen servicios públicos conectados directamente y que ofrecen protección por el firewall u otro dispositivo de filtrado.

La seguridad perimetral consiste, por tanto, en la protección de ese perímetro de red para evitar cualquier ataque o intrusión que pueda afectar a la red de una empresa. (Ciberseguridad, parr. 13)

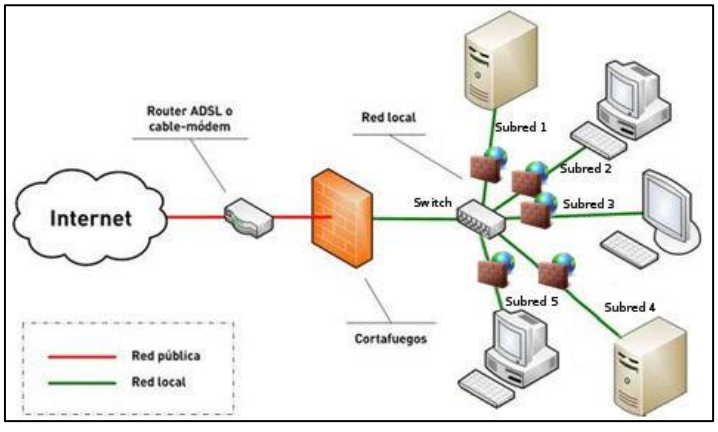


Figura 28. Red Perimetral

II.2.4.3. Modelo Clark-Wilson.

En seguridad informática, el modelo Clark-Wilson es un modelo que se basa en la jerarquización de aplicaciones para el manejo de información de parte de los usuarios. Este modelo se encuentra orientado a proteger la integridad de la información. (Wikipedia, 2020, parr. 1)

Expresa formalmente los requisitos de integridad de una política de seguridad. Es un modelo de integridad basado en transacciones, donde una transacción gramaticalmente correcta es una serie de operaciones que recorren el sistema de un estado a otro estado, todos ellos consistentes. En este modelo la política de integridad dirige la integridad de las transacciones. Como norma el certificador de una transacción y el desarrollador deben ser diferentes entidades. Se considera más adecuado para su uso general por atender a la integridad más que a la confidencialidad. (Tugurium, 2020, parr. 1)

(Aranda, 2007) menciona sobre este modelo que:

- Está basado en políticas de integridad:
  - Elementos de datos restringidos: Sobre estos debe hacerse un chequeo de consistencia.
- Elementos de datos no restringidos.
- Procedimientos de transformación.
- Procedimiento de verificación de integridad.

II.2.4.4. Modelo Thin Security.

El impacto de la crisis relacionada con la covid-19 ha afectado prácticamente a todos los aspectos de negocio. Ahora, en estos momentos de incertidumbre, es previsible que el entorno económico en contracción afecte de manera relevante a las inversiones en ciberseguridad. Se trata de una situación paradójica. Las organizaciones se encuentran ante la dicotomía de tener que hacer frente a una previsible explosión de nuevas ciberamenazas durante un periodo de recesión de los presupuestos dedicados a defenderse. (Retina, 2020, parr. 1)

Vivimos tiempos extraordinarios que transformarán nuestro mundo tal y como lo conocíamos. La sociedad, los entornos corporativos y por supuesto la ciberseguridad, van a cambiar y evolucionar hacia modelos de eficiencia y efectividad, y como CISOS y como industria, debemos estar preparados para ello. Es el momento de abordar la efectividad en su más pura esencia, en lo que a mitigación del riesgo tecnológico se refiere, aportando soluciones que permitan (con un presupuesto que va a ser limitado) seguir enfrentándonos a los mismos problemas, con menos recursos pero mejor dirigidos, es lo que hemos denominado “Thin Security” (seguridad ligera). (Hurtado & Ruiz, 2020, pág. 78)

Al calor de una economía en crecimiento, con la transformación digital omnipresente en la agenda de todas las organizaciones del mundo, la Ciberseguridad ha vivido una época de abundancia en el mundo Pre-COVID19. Durante muchos años, las organizaciones han tenido presupuestos "Cyber" en expansión y la lucha por el talento ha sido feroz entre los proveedores de servicios y los clientes, todos tratando de adquirir la mejor tecnología y personas disponibles. (Hurtado & Ruiz, 2020, pág. 78)

En el mundo "posterior a COVID19", las organizaciones se enfrentarán a la dicotomía de tener que afrontar la probable explosión de nuevas amenazas durante una recesión, en un escenario de economía en contracción. (Hurtado & Ruiz, 2020, pág. 78)

Es más que probable que los presupuestos de IT se reduzcan y que cada inversión (ya pregunta es: ¿es esto posible? ¿Podemos reinventar nuestra estructura de servicios alrededor de la ciberseguridad para conseguir que la seguridad sea más efectiva (y no sólo eficiente)? Para conseguirlo, se deben apostar por modelos de gobierno y operación en Ciberseguridad, delegados en gestión muy orientados a una seguridad operativa, eficaz y eficiente en términos de costes justificables. Es lo que hemos denominado Thin Security (seguridad ligera). (Hurtado & Ruiz, 2020, pág. 78)

Thin Security bajo NIST CSF

Para poder articular nuestras recomendaciones para este escenario post COVID-19 y articular nuestra propuesta Thin Security, vamos a usar el esquema NIST CSF. En cada uno de sus bloques se indicarán los detalles y drivers de nuestro modelo de gobierno, operación y eficiencia. (Hurtado & Ruiz, 2020, pág. 78)

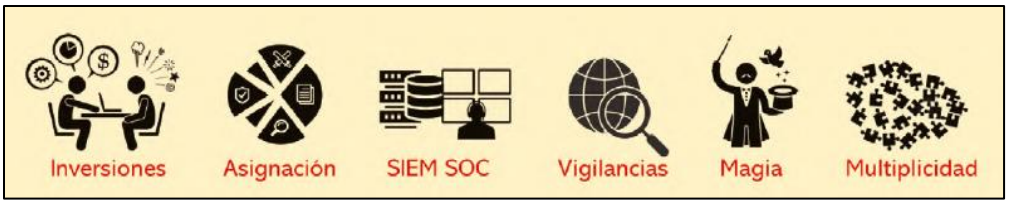


Figura 29. Dilemas a los que se enfrenta diariamente el CISO

Pilares del Thin Security basados en NIST CSF

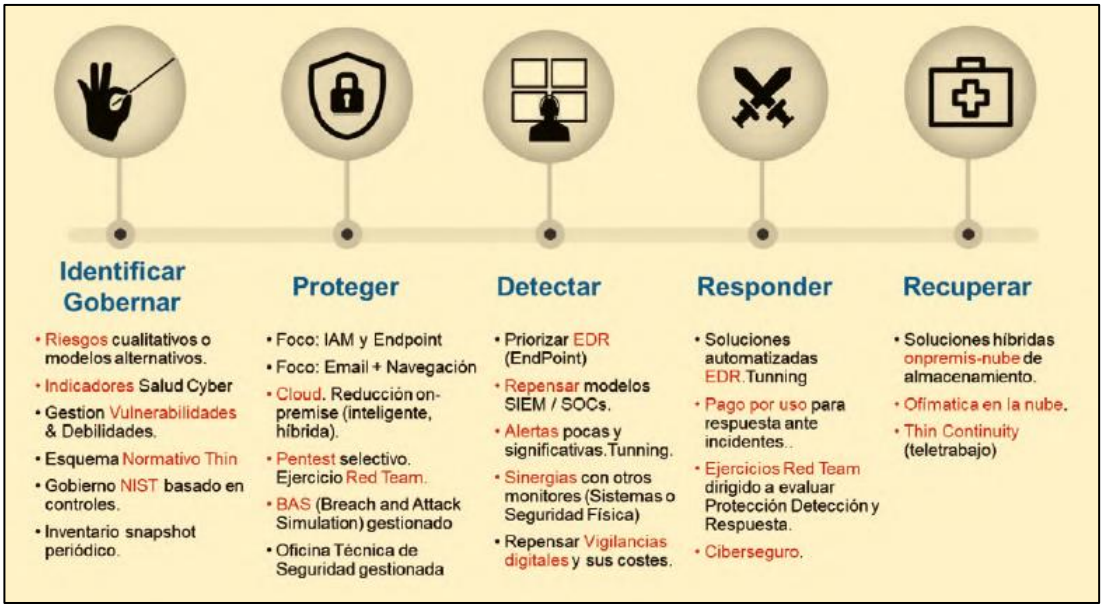


Figura 30. Pilares del Thin Security basados en NIST

II.2.4.5. Modelo Bell-LaPadula.

En seguridad informática, el modelo de seguridad Bell-Lapadula, llamado así por sus creadores Billy Elliott Bell y Len LaPadula, consiste en dividir el permiso de acceso de los usuarios a la información en función de etiquetas de seguridad. Por ejemplo, en sistemas militares norteamericanos, categorizándola en 4 niveles: no clasificado, confidencial, secreto y ultrasecreto. (Wikipedia, 2021, parr. 1)

Este modelo se centra en la confidencialidad y no en la integridad. Se distinguen 2 tipos de entidades, sujetos y objetos. Se define estados seguros y se prueba que cualquier transición se hace de un estado seguro a otro. Un estado se define como estado seguro si el único modo de acceso permitido de un sujeto a un objeto está en concordancia con la política de seguridad. Para determinar si un modo de acceso específico está permitido, se compara la acreditación de un sujeto con la clasificación del objeto (más precisamente, la combinación de la clasificación y el conjunto de compartimientos) para determinar si el sujeto está autorizado para el modo de acceso especificado. El esquema de clasificación/acreditación se expresa en términos de un retículo. El modelo define 2 reglas de control de acceso mandatorio (MAC) y una regla de control de acceso discrecional (DAC) con 3 propiedades: (Wikipedia, 2021, parr. 2)

1. Propiedad de seguridad simple: Un sujeto de un determinado nivel de seguridad no puede leer un objeto perteneciente a un nivel de seguridad más alto.

2. Propiedad (Propiedad estrella): Un sujeto de un determinado nivel de seguridad no puede escribir un objeto perteneciente a un nivel de seguridad más bajo. (También llamada propiedad de confinamiento).
3. Propiedad de seguridad discrecional: Se utiliza una matriz de acceso para especificar el control de acceso discrecional.

Con Bell-LaPadula, los usuarios pueden crear contenido sólo en su nivel de seguridad o por encima (investigadores en el nivel secreto pueden crear archivos secretos o super secretos pero no archivos públicos). Inversamente, los usuarios pueden ver solamente contenido de su propio nivel o inferior.

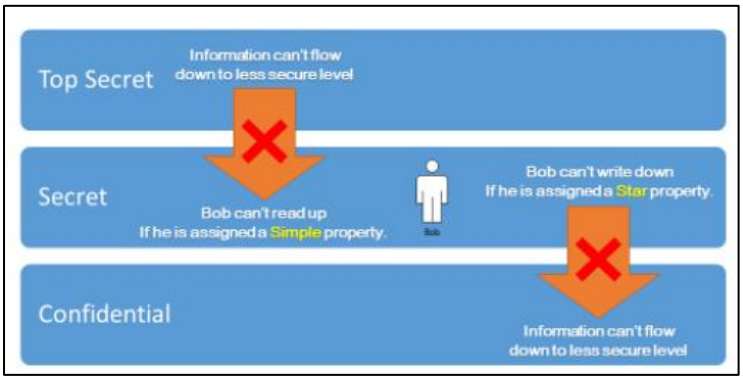


Figura 31. Modelo Bell LaPadula

II.2.4.6. Modelo Zero Trust.

Zero Trust aparece como un modelo que busca combatir de manera conjunta las amenazas externas e internas, aunque no es nuevo (fue mencionado por primera vez en 2010 por un investigador de Forrester llamado John Kindervag.) (Gonzalez, 2019, parr. 4)

El incremento en las amenazas internas ha hecho que este modelo tome gran importancia. Zero Trust propone a diferencia de los modelos mencionados, “nunca confiar, siempre verificar”, poniendo un alto a la “confianza” en el usuario y dispositivo interno. Utiliza el aseguramiento del dato como centro de la estrategia, proponiendo granularidad en los controles basados en pequeñas zonas de seguridad llamadas microperímetros, ofuscación de datos, disminución de privilegios excesivos a los usuarios, uso de analítica avanzada y automatización para optimizar la investigación, detección y respuesta. (Gonzalez, 2019, parr. 5)

(Gonzalez, 2019, parr. 6) menciona que: para abordar de manera adecuada el modelo, lograr los niveles de seguridad esperados y mantener la operación normal de las actividades de sus usuarios, usted debe tener en cuenta los siguientes pasos:

- Identifique sus datos sensibles: al ser un modelo centrado en los datos, lo primero es conocer dónde están y realizar su correcta clasificación.

- Identifique el uso de los datos sensibles: comprenda cómo fluyen los datos a través de la red, entre recursos, personas y aplicaciones.

- Diseñe los micro-perímetros: aplique políticas de seguridad granulares sobre los datos confidenciales para permitir únicamente los flujos válidos.

- Realice monitoreo continuo: implemente tecnologías de analítica de seguridad avanzada para detectar amenazas desconocidas y ataques complejos.

- Integre y automatice los controles de seguridad: reduzca el tiempo de mitigación por medio de acciones automatizadas, y coordinadas a través de múltiples tecnologías.

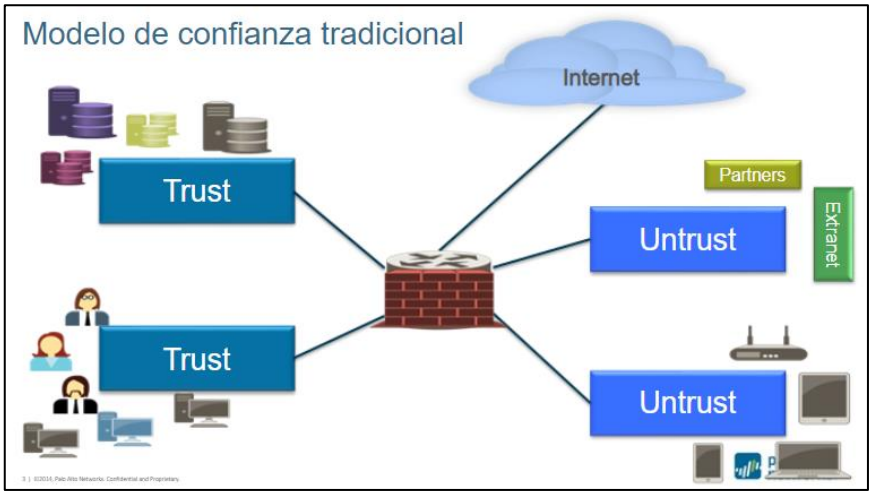


Figura 32: Modelo de confianza tradicional

En el modelo de confianza tradicional, se validaba la seguridad a traves de equipos perimetrales como firewall y se les brindaba acceso a traves de politicas establecidas que conectaban con zonas de confianza; sin embargo, las zonas que no eran de confianza (Untrust - Internet) muy poco se validaba aspectos como: tipo de sistema operativo desde donde conectan, antivirus actualizados, sistemas actualizados, multifactor de autenticacion, analisis de comportamientos, entre otros; es decir, se aceptaban accesos desde zonas que no tenias confianza y se confiaban unicamente en los equipos de seguridad tradicionales.

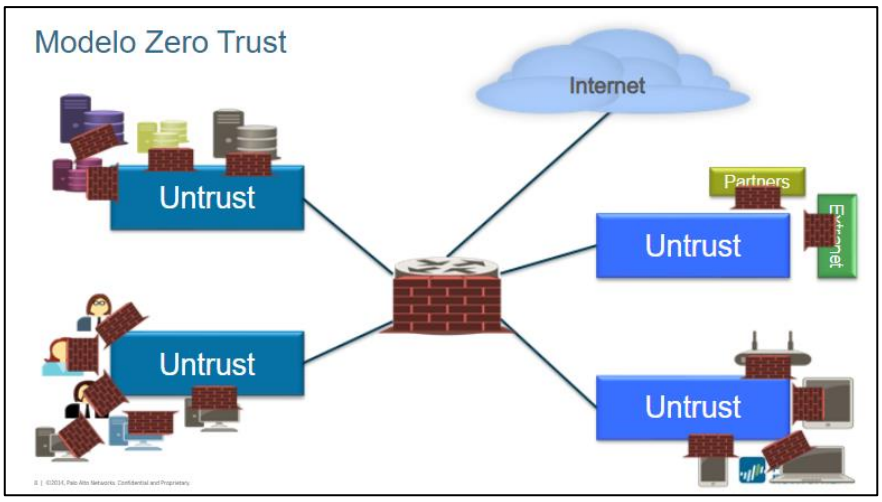


Figura 33. Modelo Zero Trust

Este nuevo modelo tiene como lema bien definido: **"Nunca confíes, siempre verifica";** es decir, asume que todo es malo y verifica cada punto de acceso, cada conexión, cada patron, cada comportamiento.

Implementar una arquitectura Zero Trust (ZT) no necesariamente significa la trasformación total de la arquitectura existente en la organización. Por eso, se vuelve imprescindible conocer el contexto organizacional y responder a las siguientes preguntas: ¿Qué debo proteger?, ¿Cuáles son los controles actuales?, ¿Quién accede a la información? y ¿de qué forma acceden?, como sabemos que es más fácil plantearlas que darles una respuesta le guiaremos. (Grajales, 2019, parr. 2)

¿Por dónde empezar?

El desarrollo del modelo Zero Trust en una organización depende de su postura de ciberseguridad y sus procesos actuales, sin embargo, se han definido unas actividades iniciales que deben ser abordadas para que el modelo se lleve a cabo con éxito. (Grajales, 2019, parr. 3)

- **Contexto organizacional:** empezaré abordando la primera pregunta ¿Qué debo proteger?, la implementación del modelo requiere del conocimiento de los activos (físicos y digitales), usuarios y procesos de negocio. Una carencia frente a este conocimiento podría provocar que la estrategia no impacte lo que se necesita proteger, complicar los procesos o que no se cumpla con las expectativas de las partes interesadas. (Grajales, 2019, parr. 4)

- **Identificación y clasificación de activos:** a partir de la identificación del contexto organizacional se hace más fácil identificar los recursos que son fuente de información y se encuentran involucrados en los procesos de tratamiento, para posteriormente clasificarlos y categorizar los sensibles y/o

confidenciales, los cuales serán objeto de aseguramiento y controles más fuertes. Recordemos que Zero Trust comienza con los datos, este paso es crucial para identificar qué se necesita proteger y el nivel de protección requerido. (Grajales, 2019, parr. 5)

- **Identificación y valoración de controles:** el siguiente paso es identificar los controles asociados a los activos clasificados como confidenciales y valorar la eficacia de los mismos. (Grajales, 2019, parr. 6)

- **Identificación del uso de los datos sensibles:** detallar los flujos de información clasificada como confidencial identificando ¿quién?, ¿qué?, ¿cuándo?, ¿dónde? y ¿por qué? acceden a la información. (Grajales, 2019, parr. 7)

- **Gestión de riesgos:** la implementación del modelo implica el desarrollo de lineamientos de microsegmentación y control de accesos a partir del conocimiento del entorno de riesgo, dentro del cual se identifican, analizan y tratan a través de un plan que se convierte en la estrategia de despliegue de los controles del modelo. (Grajales, 2019, parr. 8)

Como ya se ha mencionado la implementación del modelo Zero Trust no es un reemplazo de la infraestructura o procesos actuales, es muy importante construir sobre lo existente, identificando las necesidades de protección y el contexto de la organización. La implementación debe desarrollarse progresivamente y con metas realistas, partiendo de la premisa que los cambios no solo se ejecutarán a nivel tecnológico sino también involucrando el recurso humano. (Grajales, 2019, parr. 9)

Por último, las actividades mencionadas deben obedecer a un ciclo continuo de gestión que permita mantener actualizado el modelo Zero Trust. En un momento inicial proporcionan el principal insumo para direccionar la estrategia, y luego se convierten en actividades críticas de gestión que aseguran que el modelo se mantenga acorde con los cambios organizacionales y respondan a los nuevos escenarios de riesgo. (Grajales, 2019, parr. 10)

II.2.4.7. Modelo Defensa en Profundidad.

Desde hace siglos, los ejércitos del mundo la utilizan en su estrategia militar para la fortificación y defensa de enclaves estratégicos. El objetivo no es otro que ir mermando la capacidad y fuerza inicial de los atacantes. (Olleros, 2019, parr. 1)

Consistía en colocar varias líneas defensivas consecutivas en lugar de colocar una línea única muy fuerte. Se construían fortalezas de altos muros, en zonas rocosas o rodeadas de agua a modo de obstáculos y se

repartían fuerzas en distintos francos escalonados, siempre con el mismo objetivo de mermar la capacidad del atacante. (Olleros, 2019, parr. 2)

El sector informático lleva décadas trabajando la defensa en profundidad, concatenando protocolos, firewalls, antivirus, niveles de acceso por contraseñas complejas, software, servidor, control de acceso al espacio físico, etcétera. (Olleros, 2019, parr. 3)

(Bortnik, 2010) menciona que "la defensa en profundidad (también conocido como Defense in Depth), se trata de un modelo que pretende aplicar controles en seguridad para proteger los datos en diferentes capas

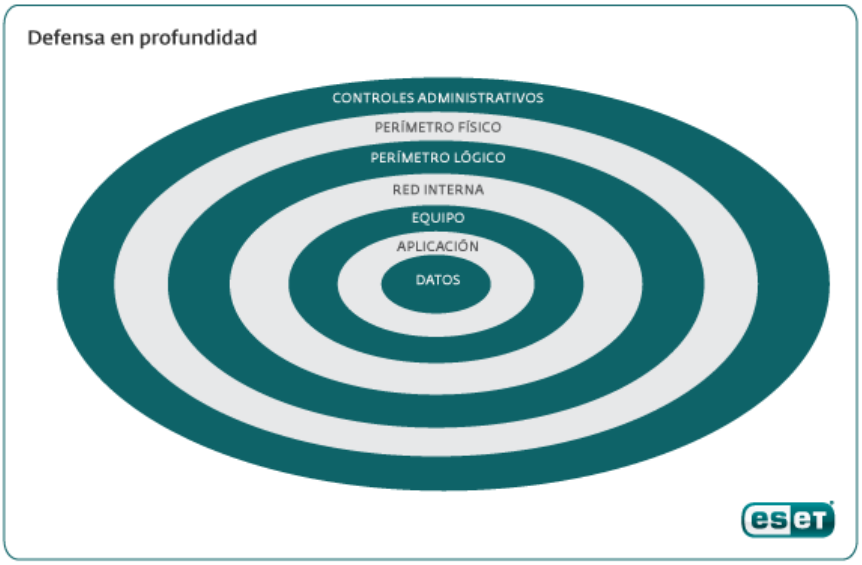


Figura 34. Seguridad por capas

La idea de este modelo es muy sencilla: si es posible proteger a un activo de la organización con más de una medida de seguridad, hágalo. El objetivo del modelo también es claro: para que un atacante llegue a un dato o información, debe poder vulnerar más de una medida de seguridad. (Bortnik, 2010, parr. 2)

Así, se presentan varias capas donde es posible aplicar diversos controles. Por ejemplo, aunque un servidor esté protegido por usuario y contraseña (capa equipo), eso no quita que no se implementen medidas de acceso por contraseña a las aplicaciones que estén instaladas en el equipo (capa aplicación), o que no se apliquen controles como protección por llaves para que no sea sencillo acceder al equipo (capa perímetro físico). Citando otro ejemplo, el tener instalado un software antivirus en los puestos de trabajo no es motivo para dejar de controlar la presencia de malware en los servidores de transporte como puede ser un servidor de correo. Dos capas de protección siempre ofrecerán mayor seguridad que una sola, y

continuando con el ejemplo, un incidente en un equipo servidor no comprometería a los usuarios finales, o viceversa. (Bortnik, 2010, parr. 3)

Obviamente que aplicar un control de seguridad tiene un costo asociado, y por lo tanto será necesario evaluar si el valor de la información a proteger justifica una, dos, tres, o las capas de seguridad que sean necesarias. Pero mientras los costos lo justifiquen, el modelo pretende proteger la información sensible de forma tal que un atacante si llegara a sortear algún mecanismo de seguridad, esto no sea suficiente para llegar a la información corporativa. (Bortnik, 2010, parr. 4)

Una estrategia de defensa en profundidad incluye el uso de cortafuegos, creación de DMZ, el uso de soluciones para la detección de intrusiones, políticas de seguridad efectivas, programas de formación, respuesta ante incidentes, mecanismos para garantizar la seguridad física y mecanismos para la monitorización y alerta de incidentes. De esta manera, si una salvaguarda en particular falla, existirán otras en las capas inferiores que mantendrán el riesgo en niveles aceptables. (Ciberseguridadlogitek, 2019, parr. 11)

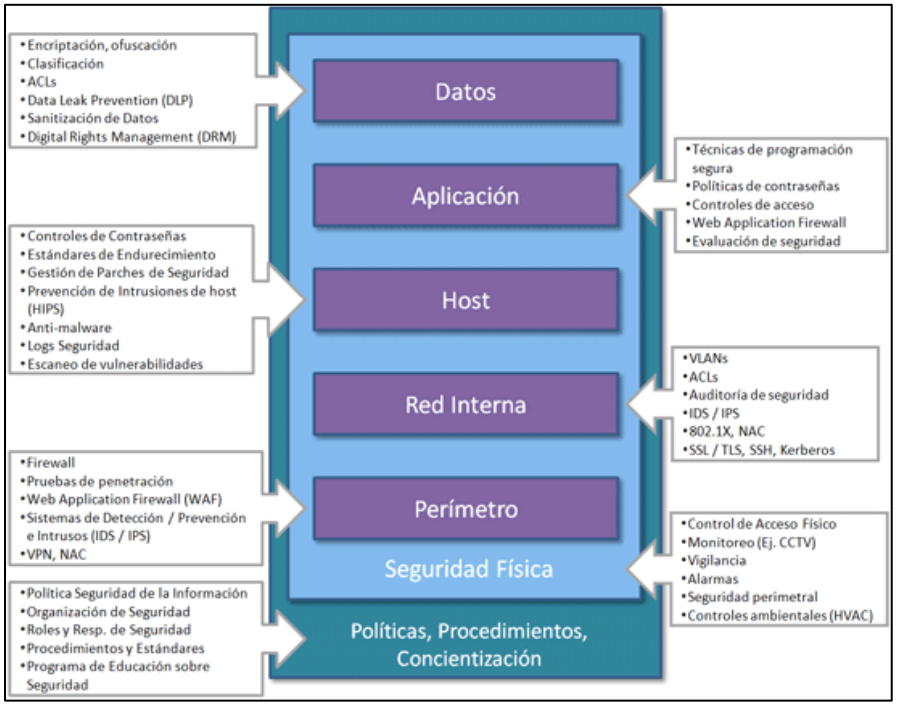


Figura 35. Capas de la Defensa en Profundidad

II.2.5. Marcos de Gestión de Ciberseguridad.

II.2.5.1. Marco de ciberseguridad NIST.

Este marco ayuda a las empresas de todos los tamaños a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos.

Les proporciona un lenguaje común y un resumen de las mejores prácticas en ciberseguridad. (Morales, 2019, parr. 1)

El marco de ciberseguridad de NIST

El Instituto Nacional de Normas y Tecnología (NIST), una agencia perteneciente al Departamento de Comercio de los Estados Unidos, desarrolló este marco voluntario de manera coherente con su misión de promover la innovación y la competitividad en el país. El Cybersecurity Framework de NIST utiliza un lenguaje común para guiar a las compañías de todos los tamaños a gestionar y reducir los riesgos de ciberseguridad y proteger su información. (Morales, 2019, parr. 4)

Este marco no provee nuevas funciones o categorías de ciberseguridad, sino recopila las mejores prácticas (ISO, ITU, CIS, NIST, entre otros) y las agrupa según afinidad. Se centra en el uso de impulsores de negocio para guiar las actividades de ciberseguridad y considerar los riesgos cibernéticos como parte de los procesos de gestión de riesgos de la organización. El framework consta de tres partes: el marco básico, el perfil del marco y los niveles de implementación. (Morales, 2019, parr. 5)

Marco básico (Framework Core)	Niveles de implementación del marco (Framework Implementation Tiers)	Perfiles del marco (Framework Profiles)
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 de implementación/operación. El Framework Core consta de cinco funciones simultáneas y continuas: identificar, proteger, detectar, responder y recuperar.	Los niveles de implementación le permiten a la organización catalogarse en un umbral predefinido en función de las prácticas 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.	Los perfiles se emplean para describir el estado actual (Current Profile) y el estado objetivo (Target 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.

Figura 36. Partes del framework NIST

El Framework Core comprende un conjunto de actividades de ciberseguridad, resultados y referencias informativas que son comunes a través de los sectores de infraestructura crítica. Así, proporciona la orientación detallada para el desarrollo de perfiles individuales de la compañía. Mediante el uso de los perfiles, el marco ayudará a la organización a alinear sus actividades de ciberseguridad con sus requisitos de negocio, tolerancias de riesgo y recursos. Por su parte, los niveles de implementación del marco (*tiers*) proporcionan un mecanismo para que las empresas puedan ver y comprender las características de su enfoque para la gestión del riesgo de ciberseguridad. (Morales, 2019, parr. 6)

Nucleo del Marco

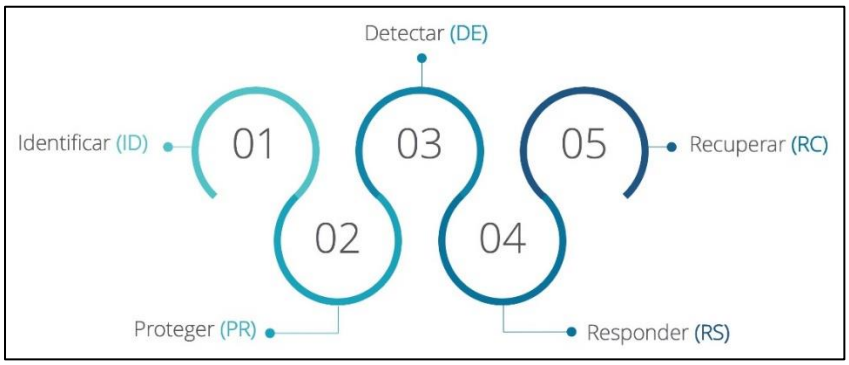


Figura 37. Núcleo del Marco NIST

El núcleo proporciona cinco funciones continuas, vistas más arriba. Asimismo, también brinda un conjunto de actividades para lograr resultados específicos de ciberseguridad y hace referencia a ejemplos de orientación para lograr esos resultados. El núcleo no es una lista de comprobación de las acciones a realizar. Presenta los resultados clave de ciberseguridad identificados por la industria como útiles para gestionar el riesgo cibernético. Comprende cuatro elementos: funciones, categorías, subcategorías y referencias informativas. (Morales, 2019, parr. 7)

Figura 38. Elementos del núcleo NIST

Categoria de funcion y de identificadores unicos

FUNCIÓN IDENTIFICADOR ÚNICO	FUNCIONES	CATEGORÍA IDENTIFICADOR ÚNICO	CATEGORIAS
ID	IDENTIFICAR	ID.AM	Gestión de activos
		ID.BE	Ambiente de negocios
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	PROTEGER	PR.AC	Gestión de identidad, autenticación y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología de protección
DE	DETECTAR	DE.AE	Anomalías y Eventos
		DE.CM	Monitoreo continuo de seguridad
		DE.DP	Procesos de Detección
RS	RESPONDER	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
		RS.RP	Planificación de respuesta
RC	RECUPERAR	RC.RP	Planificación de la recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Figura 39. Categorías NIST

Niveles de Implementacion

Los tiers proporcionan un contexto sobre cómo una organización ve el riesgo de la ciberseguridad y los procesos implementados para manejarlo. Las escalas describen el grado en que las prácticas de gestión de riesgos cibernéticos de una empresa exhiben las características definidas en el marco. Por ejemplo: riesgo y amenaza, repetible y adaptable. (Morales, 2019, parr. 8)

Los niveles de implementación caracterizan las prácticas de una compañía en un rango, desde parcial hasta adaptativo. Estos niveles reflejan una progresión desde respuestas informales y reactivas hasta enfoques que son ágiles y están informados sobre el riesgo. Durante el proceso de selección de un tier, la empresa debe considerar sus actuales prácticas de gestión de riesgos, entorno de amenazas, requisitos legales y regulatorios, objetivos de negocio/misión y restricciones de organización. (Morales, 2019, parr. 9)

TIER 1: Parcial

***Proceso de gestión de riesgos*:** Las prácticas de gestión de riesgos de ciberseguridad de la organización no están formalizadas, y el riesgo se gestiona de forma ad hoc y, en ocasiones, de forma reactiva. La priorización de las actividades de ciberseguridad puede no estar directamente informada por los objetivos de riesgo de la organización, el

entorno de amenaza o los requisitos de negocios / misión. (Ramiro, 2018, parr. 22)

Programa integrado de gestión de riesgos: Existe una conciencia limitada sobre el riesgo de seguridad cibernética a nivel organizacional y no se ha establecido un enfoque de toda la organización para gestionar el riesgo de ciberseguridad. La organización implementa la gestión del riesgo de ciberseguridad en forma irregular caso por caso debido a la experiencia variada o la información obtenida de fuentes externas. La organización puede no tener procesos que permitan compartir información de ciberseguridad dentro de la organización. (Ramiro, 2018, parr. 23)

***Participación externa*:** La organización puede no tener los procesos establecidos para participar en la coordinación o colaboración con otras entidades. (Ramiro, 2018, parr. 24)

TIER 2: Riesgos de información

***Proceso de gestión de riesgos*:** Las prácticas de gestión de riesgos son aprobadas por la administración pero no pueden establecerse como políticas de toda la organización. La priorización de las actividades de ciberseguridad está directamente relacionada con los objetivos de riesgo de la organización, el entorno de amenazas o los requisitos de negocios / misiones. (Ramiro, 2018, parr. 25)

***Programa integrado de gestión de riesgos*:** Existe una conciencia del riesgo de ciberseguridad a nivel organizacional, pero no se ha establecido un enfoque de toda la organización para gestionar el riesgo de ciberseguridad. Los procesos y procedimientos informados por el riesgo, aprobados por la gerencia, se definen e implementan, y el personal cuenta con los recursos adecuados para realizar sus tareas de ciberseguridad. La información de ciberseguridad se comparte dentro de la organización de manera informal. (Ramiro, 2018, parr. 26)

***Participación externa*:** La organización conoce su rol en el ecosistema más grande, pero no ha formalizado sus capacidades para interactuar y compartir información externamente. (Ramiro, 2018, parr. 27)

TIER 3: Repetible

***Proceso de gestión de riesgos*:** Las prácticas de gestión de riesgos de la organización se aprueban formalmente y se expresan como políticas. Las prácticas de ciberseguridad organizacional se actualizan periódicamente en función de la aplicación de los procesos de gestión de riesgos a los cambios en los requisitos empresariales / de la misión y un panorama cambiante de amenazas y tecnología. (Ramiro, 2018, parr. 28)

***Programa integrado de gestión de riesgos*:** Existe un enfoque de toda la organización para gestionar el riesgo de ciberseguridad. Las políticas, procesos y procedimientos informados sobre riesgos se definen, implementan según lo previsto y se revisan. Se han implementado métodos consistentes para responder de manera efectiva a los cambios en el riesgo. El personal posee el conocimiento y las habilidades para realizar sus roles y responsabilidades asignados. (Ramiro, 2018, parr. 29)

***Participación externa*:** La organización entiende sus dependencias y socios y recibe información de estos socios que permite la colaboración y las decisiones de gestión basadas en riesgos dentro de la organización en respuesta a los eventos. (Ramiro, 2018, parr. 30)

TIER 3: Adaptable

***Proceso de gestión de riesgos*:** La organización adapta sus prácticas de ciberseguridad en función de las lecciones aprendidas y los indicadores predictivos derivados de las actividades de ciberseguridad anteriores y actuales. A través de un proceso de mejora continua que incorpora prácticas y tecnologías avanzadas de ciberseguridad, la organización se adapta activamente a un entorno cambiante de ciberseguridad y responde a las amenazas cambiantes y sofisticadas de manera oportuna.

***Programa integrado de gestión de riesgos*:** Existe un enfoque de toda la organización para gestionar el riesgo de ciberseguridad que utiliza políticas, procesos y procedimientos informados sobre riesgos para abordar posibles eventos de ciberseguridad. La gestión del riesgo de ciberseguridad forma parte de la cultura organizacional y evoluciona a partir de la conciencia de las actividades previas, la información compartida por otras fuentes y el conocimiento continuo de las actividades en sus sistemas y redes.

***Participación externa*:** La organización gestiona los riesgos y comparte activamente la información con los socios para garantizar que la información precisa y actualizada se distribuya y consuma para mejorar la ciberseguridad antes de que se produzca un evento de seguridad.

II.2.5.2. ISO/IEC 27032.

La norma ISO/IEC 27032:2012 "Tecnología de la información - Técnicas de seguridad - Directrices para la Ciberseguridad" (publicada en julio del 2012) 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: (Morales, 2017, parr. 3)

- Seguridad de la información (considerando que la información es el activo mas relevante de cualquier organización),
- Seguridad en redes,

- Seguridad en el Internet, y
- La protección de infraestructuras críticas de información.

Estructura de la norma

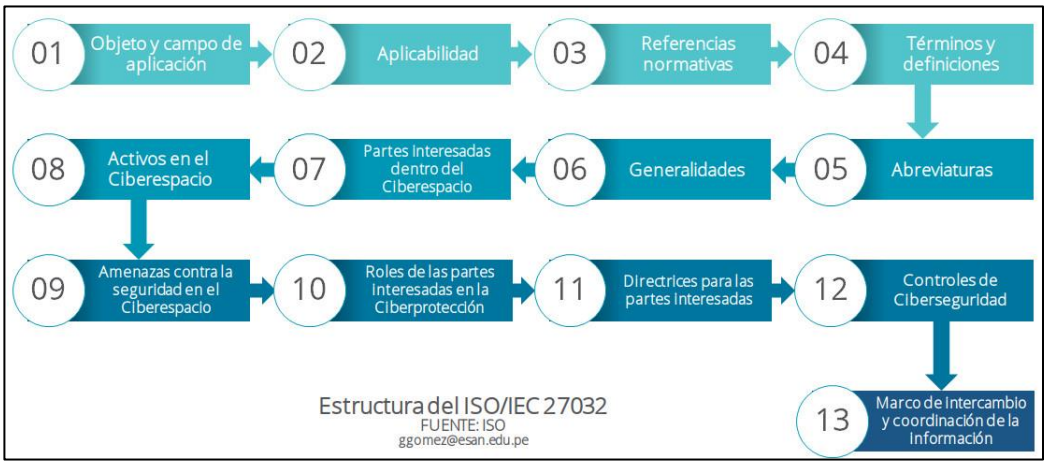


Figura 40. Estructura Norma ISO 27032

Atendiendo al reto de los escenarios actuales de la Ciberseguridad y gracias a la amplia experiencia del equipo de Internet Security Auditors, diseñamos una metodología que permite implementar CSF basado en el estándar ISO/IEC 27032:2012 que incluye cuatro focos de trabajo o dominios. (Isec Auditors, parr. 2)

Figura 41. Focos de trabajo ISO 27032

(Isec Auditors, parr. 3) indica que "el Marco de Ciberseguridad que se desarrollará tendrá un acercamiento en la gestión de riesgos en 4 áreas:"

- **Prevención:** La prevención se basa en la implantación de medidas y controles que limiten y contengan los impactos de posibles eventos de ciberseguridad.

- **Protección y Detección:** Donde se implementan controles destinados a la gestión de la seguridad y la monitorización de eventos de seguridad con el fin de detectar y protegerse ante este tipo de eventos.

- **Respuesta y Comunicación:** Debemos estar preparados ante posibles incidentes relacionados con la ciberseguridad y constará de acciones para mitigar elementos adversos una vez se hayan materializado.

- **Recuperación y Aprendizaje:** Acciones para restaurar los sistemas y servicios relacionados con el ciberespacio y se definirán procedimientos para reducir la probabilidad de ocurrencia de estos incidentes

El proceso seguido en nuestra metodología se desarrolla en cinco fases.

Figura 42. Fases de la metodología de implementación ISO 27032

Fase I: Entendimiento de la Organización

En esta primera fase se realiza un trabajo importante de inmersión en los procesos de la empresa para conocer el funcionamiento de éstos y que uso realizan del Ciberespacio sus servicios. Para llevar a cabo esta tarea será necesario: (Isec Auditors, parr. 5)

- Revisar productos y servicios
- Revisar el marco normativo de seguridad en uso
- Recopilar y revisar documentación de seguridad
- Conocer los flujos de información en los procesos
- Conocer las medidas técnicas de seguridad implementadas, etc

Esta fase permitirá también disponer de un inventario de activos de los servicios en el alcance. (Isec Auditors, parr. 6)

Fase II: Análisis de Riesgos

La toma de decisiones en cuanto a los controles y medidas de seguridad que se van a implementar debe estar basada en la gestión de los riesgos y el alineamiento con las necesidades de la empresa. Es por ello que, en esta fase, se llevará a cabo esta evaluación considerando, entre otros, aspectos como: (Isec Auditors, parr. 7)

- Activos críticos
- Amenazas
- Vulnerabilidades
- Impacto y riesgo
- Responsabilidades

Esta tarea se lleva a cabo con alineamientos a normas reconocidas a nivel internacional, que permiten su mantenimiento y gestión en el tiempo. (Isec Auditors, parr. 8)

Fase III: Plan de Acción

En esta fase, y gracias al trabajo realizado en las fases anteriores, se redactará el plan que permita conocer la priorización y medidas que deberán desarrollarse para la consecución de los alineamientos de la ISO/IEC 27032:2012 en base a las exigencias del negocio. (Isec Auditors, parr. 9)

Este Plan afrontará diferentes estrategias que incluirán y deberán aplicarse a diferentes niveles de la organización, incluyendo:

- Políticas
- Identificación de roles
- Métodos de implementación
- Procesos afectados
- Controles tecnológicos

Fase IV: Implementación

Como tal, esta es la etapa que más esfuerzos va a requerir habitualmente dado que es en la que todas las acciones definidas en la fase anterior se plasmarán en el Plan de Acción. Es importante tener presente que la ISO/IEC 27032:2012 pretende obligar a quien la implemente, a ser proactivo en las medidas de seguridad, con énfasis importante en los mecanismos de prevención en los procesos que hacen uso del Ciberespacio. (Isec Auditors, parr. 10)

Esta fase del proyecto se focalizará entonces en la implementación de controles que deberán tener en cuenta el nivel de madurez en la gestión de la seguridad existente y que considerará, entre otros, aspectos como:

- Existencia de Política de Seguridad
- Procedimientos de Seguridad en SDLC
- Marcos existentes para el intercambio de información
- Planes de concienciación del personal
- Metodología de AARR
- Monitorización TIC

- Gestión de incidentes

Además de esto, en esta fase del proyecto se establecerán controles adicionales que incluirán:

- Controles a nivel de aplicación: gestión de sesiones, validación de datos, protección ante ataques, procesos de autenticación, etc.
- Controles a nivel de servidores: configuraciones seguras, gestión de parches, monitorización., revisiones periódicas, etc.
- Controles para los usuarios finales: Actualizaciones de SO, uso de aplicaciones, antivirus, herramientas y configuraciones de seguridad, etc.
- Controles contra ataques de Ingeniería social: Programas de concienciación, pruebas regulares, controles de seguridad, etc.

II.2.6. Tecnologías y técnicas avanzadas en ciberseguridad

II.2.6.1. Técnica de ciberseguridad avanzada: Threat Hunting

¿Qué es Threat Hunting? Se puede definir como "…el proceso de búsqueda iterativa y *proactiva* a través de las redes para detectar y aislar amenazas avanzadas capaces de evadir las soluciones de seguridad existentes." (Pandasecurity, 2018, parr. 5)

¿Qué lo hace diferente? La proactividad es lo que realmente diferencia el Threat Hunting de medidas tradicionales de gestión de amenazas como firewalls, intrusion detection systems (IDS), sandboxing, y sistemas SIEM. Todas estas medidas implican una investigación después de que se haya producido una alerta de un ataque potencial o un incidente de seguridad, es decir son medidas reactivas, no proactivas.
Es más, la proactividad es muy importante en las soluciones de ciberseguridad avanzadas. El cambio de enfoque de EPP (Endpoint Protection) a EDR (endpoint detection and response) significa que existe una telemetría en tiempo real, lo que es fundamental para poder realizar el Threat Hunting. (Pandasecurity, 2018, parr. 6)

Características de Threat Hunting

La característica más importante de Threat Hunting es, tal como hemos comentado, su enfoque: aquí hablamos de un enfoque proactivo frente a las amenazas. Esto quiere decir que no es una respuesta ante incidentes, aunque sí están conectados, ya que a partir de los resultados de la investigación y las conclusiones es posible establecer nuevos indicadores

de ataque o de compromiso. **Las medidas de Threat Hunting tratan de suplir lo que las herramientas más tradicionales no pueden ver**. (Pandasecurity, 2018, parr. 7)

II.2.6.3. Análisis de vulnerabilidades, Test de intrusión, Red Team, Blue Team

Análisis de Vulnerabilidades, Test de Intrusión y Red Team son unos tipos de evaluaciones con características diferentes pero que en muchas ocasiones, de forma errónea, se usan de forma intercambiada. No es extraño ver que cuando se habla de ellos a alto nivel, los tres se acaben englobando en proyectos de Ethical Hacking. Esto hace que no se entiendan correctamente los objetivos, beneficios y resultados de cada una de estas actividades haciendo un grato favor a la industria de la seguridad informática. (Alvarez, 2020, parr. 1)

Así tenemos que un **Análisis de Vulnerabilidades** (en inglés Vulnerability Assessment) está centrado en analizar sistemas con el objetivo de detectar vulnerabilidades y priorizarlas según su riesgo. En este tipo de evaluaciones la explotación de las vulnerabilidades no es parte del alcance y la verificación de estas se da en juicio al resultado de las herramientas utilizadas. Este tipo de análisis nos da una visión muy amplia del número y tipo de vulnerabilidades pero con muy poca profundidad. Tras aplicar las mitigaciones después de los resultados de un Análisis de Vulnerabilidades se reducirá la superficie de ataque. (Alvarez, 2020, parr. 6)

Por otro lado, los **Test de Intrusión** son ataques simulados sobre sistemas con el objetivo de ver el riesgo real tras la explotación de vulnerabilidades. En estos test se intentan descubrir todas las vulnerabilidades posibles, explotarlas y ver los riesgos asociados a ellas. Por lo tanto, tienen un alcance amplio pero con una profundidad superior al de los Vulnerability Assessment. El resultado final tras aplicar mitigaciones también será la reducción de la superficie de ataque. (Alvarez, 2020, parr. 7)

Por último, los ejercicios de **Red Team**, pese a que en la teoría puedan parecer similares a los Test de Intrusión debido a la explotación de vulnerabilidades y al uso de herramientas similares, se diferencian principalmente por el objetivo y la intención del ejercicio. El objetivo del Red Team es entrenar al equipo de seguridad y respuesta a incidentes además de medir los tiempos de respuesta así como la efectividad de la tecnología, las personas y los procesos. Es importante indicar que en los ejercicios de Red Team se simulan escenarios reales basados en información de las tácticas, técnicas y procedimientos utilizados a día de hoy por grupos implicados en intrusiones. El alcance del Red Team es mucho menos amplio que en un Test de Intrusión, ya que solo se explotarán las vulnerabilidades necesarias para cumplir los objetivos, pero por otro lado tienen mucha más profundidad. (Alvarez, 2020, parr. 8)

Por lo tanto, podemos ver de forma clara que los tres ejercicios son diferentes entre ellos y tienen unos objetivos diferentes. Mientras que los Análisis de Vulnerabilidades y los Test de Intrusión se basan en reducir la superficie de ataque de formas diferentes, los ejercicios de Red Team se centran en entrenar y probar la efectividad y la capacidad de respuesta del equipo de Ciberseguridad. (Alvarez, 2020, parr. 9)

Cuando hablamos de seguridad informática y protección de datos entran en juego dos equipos fundamentales: los Red Team y los Blue Team. Ambos realizan un trabajo complementario para detectar vulnerabilidades, prevenir ataques informáticos y emular escenarios de amenaza. (Unir Revista, 2020, parr. 2)

Figura 43. Defensa vs Ataque

II.2.6.4. Soluciones tecnológicas en los esquemas de ciberseguridad

Solución IPS/IDS

Las siglas IDS se corresponde con Sistema de Detección de Intrusiones, las siglas IPS se corresponde con Sistema de Prevención de Intrusiones. Es un conjunto de sistemas que se complementan para proveer de mayor seguridad a las redes de distintos tamaños. En especial, aquellas redes que requieren de un alto nivel de respuesta y servicio. Estos sistemas pueden aplicarse tanto a nivel de software o bien, a nivel hardware mediante equipos especializados. Se habla normalmente de IDS/IPS porque trabajan conjuntamente. (Fernandez, 2020, parr. 2)

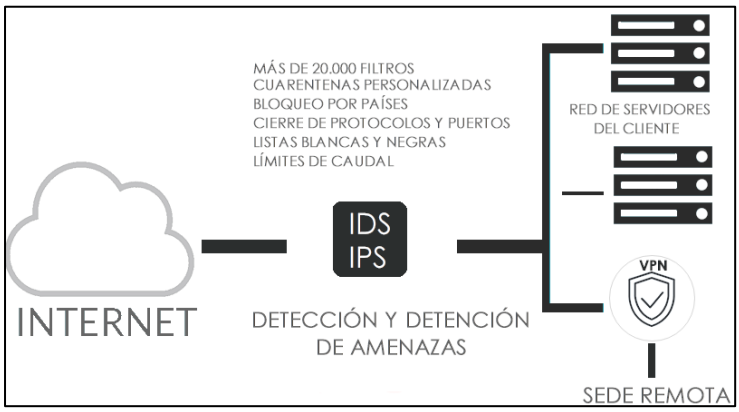


Figura 44. IPS/IDS

Solución WAF

Un WAF (Web Application Firewall) es un dispositivo hardware o software que permite proteger los servidores de aplicaciones web de determinados ataques específicos en Internet. Se controlan las transacciones al servidor web de nuestro negocio. (Director-it, parr. 1)

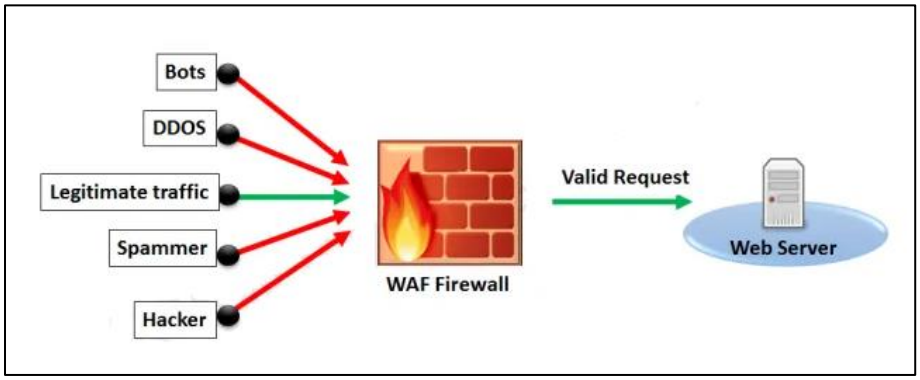


Figura 45. WAF

Solucion CASB

Un *Cloud Access Security Manager (CASB)* o en castellano “Gestores de Seguridad para el Acceso a la Nube" es una solución que cada vez necesitarán más las organizaciones, a causa de la gran demanda de aplicaciones en la nube. Según distintas fuentes, pronto será tan importante como contar con un Firewall. (Ingens Networks, 2020, parr. 6)

La principal característica que poseen es que operan como intermediarios entre las aplicaciones de la nube y los usuarios, con el objetivo de proveer visibilidad (que puede incluir entre otras cosas registros de auditoría, alertas de seguridad o reportes) y seguridad de los datos (a través de

control de acceso, prevención de fuga de información, cifrado, entre otras opciones). (Welivesecurity, 2014, parr. 9)

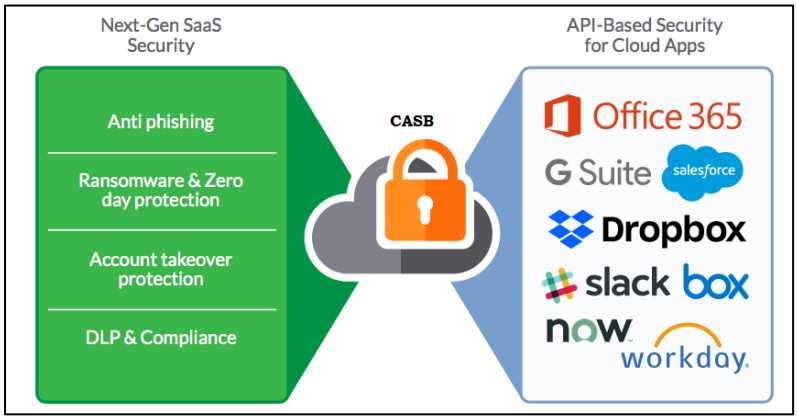


Figura 46. Cloud Access Security Manager

Solución UEBA

UEBA (User and Entity Behavior Analytics) se utiliza para la detección de amenazas, tanto para la detección de fallos externos como para la identificación de intrusos. Desde una perspectiva del comportamiento, aprende lo que las personas y las entidades hacen sobre una base "normal", a dónde se conectan normalmente, a qué servidores de archivos y aplicaciones están accediendo, desde qué dispositivos se conectan, qué privilegios tienen, cómo de fuertes son sus contraseñas, etc. buscando establecer una línea base de lo que es el comportamiento habitual del que no lo es. Al entender lo que es este comportamiento normal de los usuarios y las entidades, cuando algo inusual ocurre, UEBA lo detectará y bloqueará.

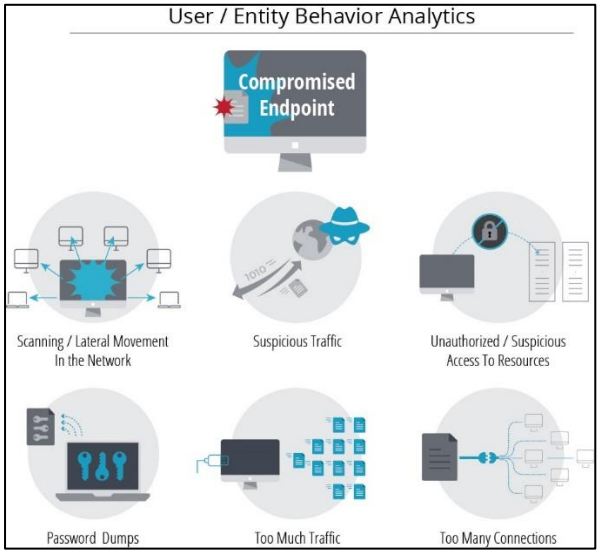


Figura 47. UEBA

Solución NAC

Network Access Control (NAC), es una tecnología que permite controlar de forma muy granular que dispositivos pueden acceder a la red, permitiendo establecer políticas de gestión de los dispositivos, tanto fijos como móviles, e integrar estas políticas con BYOD. De este modo, se evitaría la propagación de malware y otras amenazas que pueden dañar la infraestructura y dejar su empresa vulnerable a los ataques y pérdida de datos. (Secure IT, parr. 1)

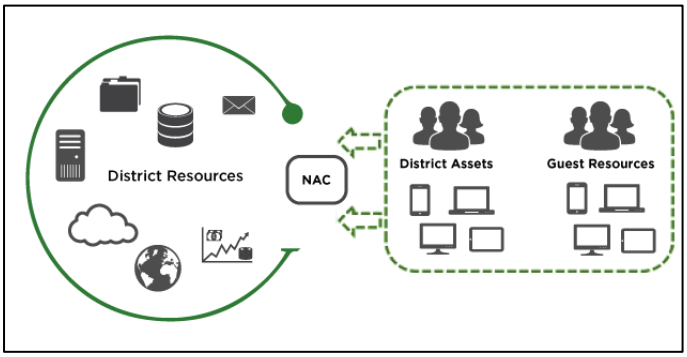


Figura 48. Network Access Control

Solución DLP

Las soluciones DLP (Data Lost Prevention) pueden ayudar a proteger tanto los datos en reposo como en movimiento y en uso; además tienen en cuenta muchos canales por los que se puede producir la pérdida de la información, como el email, el endpoint, la red, etc.; también ayudan a centralizar políticas y las refuerzan para prevenir la pérdida de datos. (Itdigitalsecurity, 2019, parr. 7)

Figura 49. Detección de fuga de información

Solución SIEM

SIEM significa Security Information and Event Management, las soluciones SIEM se basan en detectar actividades sospechosas que amenazan los sistemas de una empresa y resolverlas de forma inmediata. Estas soluciones SIEM pueden procesar una gran cantidad de registros de

eventos, enviando alertas sobre los fallos de seguridad encontrados en el sistema y las actividades sospechosas que están ocurriendo. Con SIEM podremos garantizar la seguridad de la red de la empresa y también el cumplimiento de la normativa de seguridad. (Luz, 2015, parr. 1)

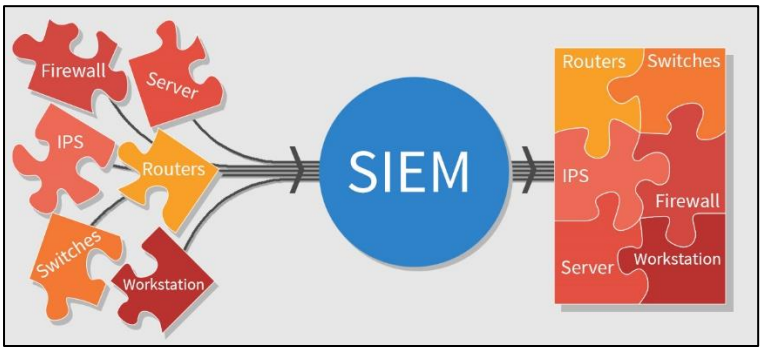


Figura 50. Correlacionador de eventos SIEM

Solución Anti DDOS

Protección Anti DDoS, es un servicio que permite mitigar un ataque distribuido de denegación del servicio a un sistema de computadoras o red que están expuestos a la red pública de Internet. (Claro, parr. 1)

Beneficios

- Especialistas en protección Anti DDoS monitorizan el flujo de tráfico de la red de su empresa.
- Supervisa, detecta e inicia el proceso de mitigación de ataques inmediatamente.
- Acuerdos de nivel de servicio (SLA) que garantizan la mitigación de DDoS en minutos.
- Despliegue en línea para brindar protección contra ataques en tiempo real.
- Protección de IPS en línea, no solo para la protección de los servicios del cliente sino también de los equipos de red o seguridad perimetral (Firewalls, Balanceadores de Enlaces, entre otros).
- Atención 24 horas

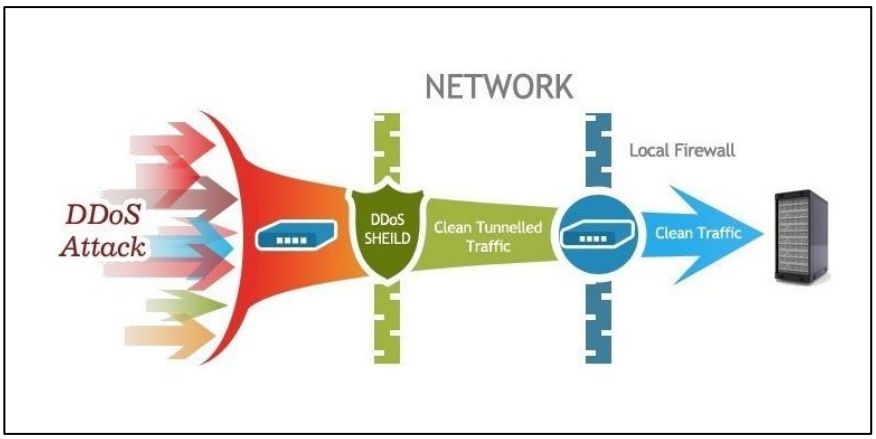


Figura 51. Ataque DDos

Accesos VPN

Una VPN (*Virtual Private Network*) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar estas redes para que sus empleados, desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían. Sin embargo, conectar la computadora de un empleado a los recursos corporativos es tan solo una de las funciones de una VPN. Una implementación correcta de esta tecnología permite asegurar la confidencialidad e integridad de la información. (Goujon, 2012, parr. 2)

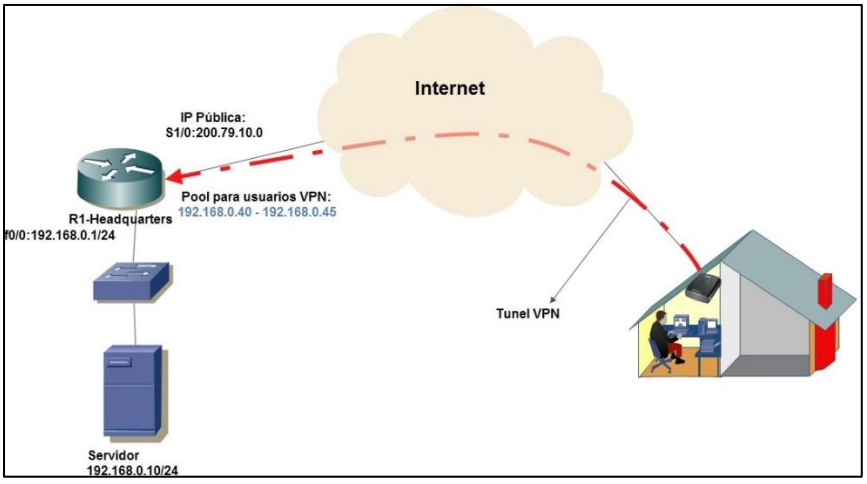


Figura 52. Accesos VPN

Control de dispositivos MDM

MDM (Mobile Device Management) es un conjunto de software que permite monitorizar, controlar y asegurar dispositivos móviles.
El software MDM surgió como un método para controlar la información de la empresa. Con el tiempo fueron evolucionando y hoy colaboran administrando y dando soporte a los dispositivos. (Atlas - Proyectos Informaticos, 2017, parr. 2)

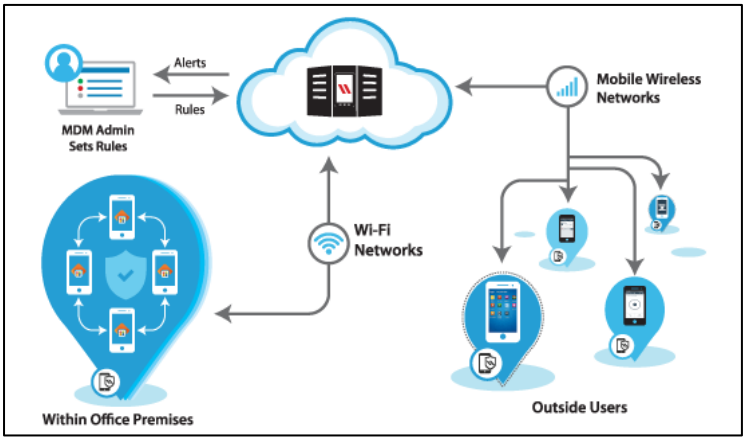


Figura 53. Mobile Device Control

SandBox

El término Sandbox o Sandboxing, tal y como indica su nombre, se refiere a un “cajón de arena” o un entorno controlado. Todos conocemos esos cajones de arena donde los padres dejan que sus hijos jueguen con sus juguetes. Son lugares seguros donde la arena les protege de golpes y donde pueden divertirse aislados de los peligros del exterior. (Romero, 2019, pág. 3)

Basándose en este concepto, los expertos en ciberseguridad pensaron que una buena forma de proteger las máquinas de los virus era aislarlos en una "caja de arena", es decir, aislar el programa infectado con un virus informático del resto del sistema para que el virus no se extienda. Esto es lo que se conoce como tecnología Sandbox. (Romero, 2019, pág. 4)

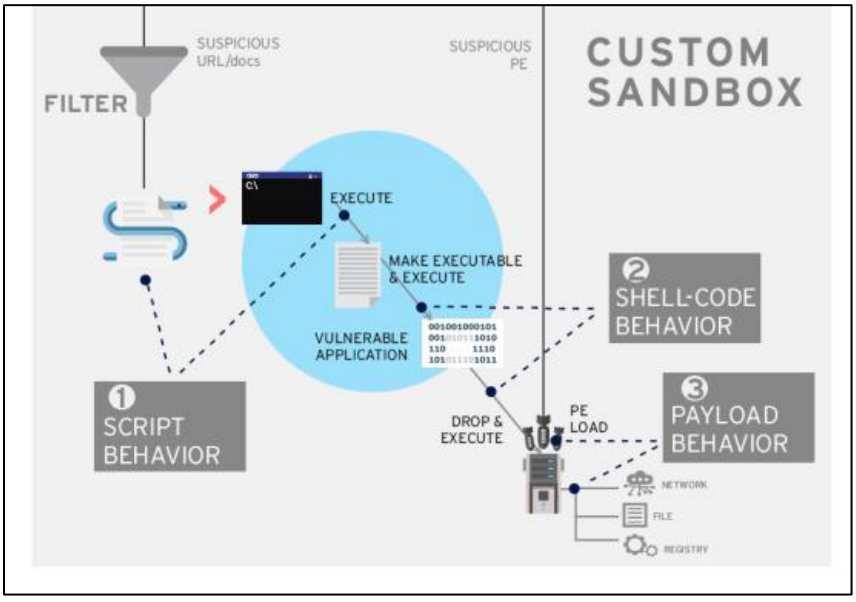


Figura 54. Validación de archivo en SandBox

HoneyPot

El honeypot es una estrategia de ciberseguridad dirigida, entre otras cosas, a engañar a los posibles cibercriminales. Ya sea mediante software o a través de la acción humana, el honeypot hace que una empresa simule tener algunas 'puertas de entrada' a sus sistemas que no han sido suficientemente protegidas. (Pandasecurity, 2018, parr. 4)

La táctica es la siguiente. De manera previa, una empresa decide habilitar una serie de servidores o sistemas cuyo aspecto parezca sensible. Aparentemente, esa empresa se ha dejado varios cabos sin atar y parece vulnerable. Una vez dejada la trampa, la intención es atraer al atacante, que acudirá a la llamada para intentar entrar. Sin embargo, lo que el cibercriminal no sabe es que, lejos de estar encontrando una puerta vulnerable, en realidad está siendo perfectamente controlado y monitorizado por la empresa en cuestión. (Pandasecurity, 2018, parr. 5)

De este modo, las empresas obtienen un beneficio triple: en primer lugar, contener posibles ataques verdaderamente peligrosos; en segundo, entretener y desgastar al atacante haciéndole perder el tiempo; y en tercero, analizar sus movimientos para detectar posibles nuevas formas de ataque que se estén llevando a cabo en el sector. (Pandasecurity, 2018, parr. 6)

Next Generation Firewall

Los firewalls de próxima generación filtran el tráfico de red para proteger a una organización de amenazas externas. Al mantener las funciones de los firewalls tradicionales, como el filtrado de paquetes, el soporte de VPN, la supervisión de la red y las funciones de mapeo de IP, los NGFW también poseen capacidades de inspección más profundas que les brindan una capacidad superior para identificar ataques, malware y otras amenazas. Los firewalls de próxima generación brindan a las organizaciones control de aplicaciones, prevención de intrusiones y visibilidad avanzada en toda la red. A medida que el panorama de amenazas continúa desarrollándose rápidamente, los firewalls tradicionales se quedan atrás y ponen en riesgo a su organización. Los NGFW no solo bloquean el malware, sino que también incluyen rutas para futuras actualizaciones, dándoles la flexibilidad de evolucionar con el paisaje y mantener la red segura a medida que surgen nuevas amenazas. (Fortinet, parr. 1)

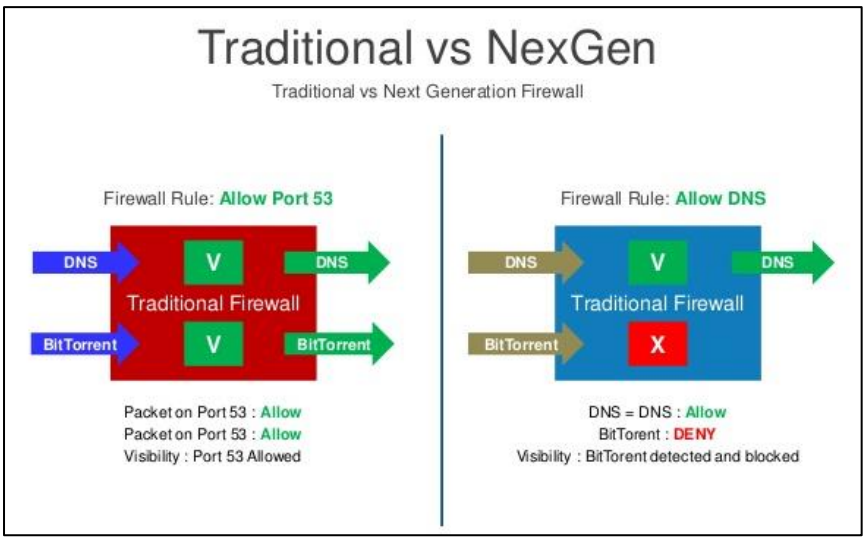


Figura 55. Tradicional y nuevo Firewall

Solución Antivirus

(Mcafee, parr. 1) menciona que: "Un antivirus es un software diseñado para detectar y destruir amenazas tales como virus, malware, ransomware y spyware, entre otras".

El análisis de malware usado por los antivirus o plataformas de protección de punto final (EPP) se basa en firmas. Hoy en día esto ya no es suficiente. Para afrontar amenazas avanzadas se necesitan herramientas avanzadas como la detección y respuesta endpoint.

Solución EDR

EDR (Endpoint Detection and Response) es una tecnología de ciberseguridad que aborda la necesidad de una supervisión en tiempo real, de centrarse en los análisis de seguridad y en la respuesta al incidente de los endpoints corporativos. Ofrece una visibilidad completa de extremo a extremo sobre la actividad de cada equipo de la infraestructura corporativa, administrada desde una única consola, junto con una valiosa inteligencia de seguridad que podría usar un experto de seguridad informático para una investigación y respuesta mayores. (Shevchenko, 2018, parr. 21)

El objetivo principal de EDR es la detección proactiva de amenazas nuevas o desconocidas, infecciones previamente no identificadas que penetran en la organización directamente a través de endpoints y servidores. (Shevchenko, 2018, parr. 23)

Actualización de parches de seguridad

Las actualizaciones son añadidos o modificaciones realizadas sobre los sistemas operativos o aplicaciones que tenemos instalados en nuestros dispositivos y cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad. Si no mantenemos nuestros equipos al día nos exponemos a todo tipo de riesgos: robo de información, pérdida de privacidad, perjuicio económico, suplantación de identidad, etc. (Osi, parr. 1)

Es importante contar con una solucion que realice las actualizaciones de seguridad tanto a nivel de sistema operativo como de aplicación; como por ejemplo, la solucion System Center Configuration Manager SCCM de Microsoft, que se encarga de actualizar los equipos de todo tu dominio local o de agencias remotas, a traves de reglas previamente configuradas.

Solución Antispam

Antispam es una solución de seguridad que permite a los usuarios prevenir o restringir la entrega de spam (correos no deseados). Analiza automáticamente todos los correos electrónicos entrantes enviados a un buzón de correo. (Ionos, parr. 1)

Los análisis identifican las direcciones de correo electrónico y las direcciones IP que se sabe que son los remitentes de spam o malware, así como las características que son típicas del spam, como la estructura y el contenido del correo. (Ionos, parr. 2)

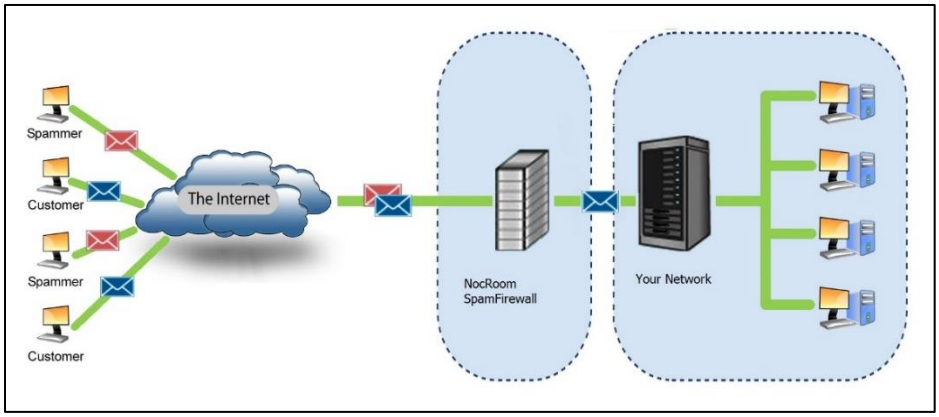


Figura 56. Solución Antispam

Solución Proxy

Los servidores proxy generalmente se usan como un puente entre el origen y el destino de una solicitud. En nuestra imagen, puedes ver que la computadora necesita pasar por el servidor proxy para acceder a Internet, y este es uno de los usos comunes de los servidores proxy. (Barbosa, 2020, parr. 2)

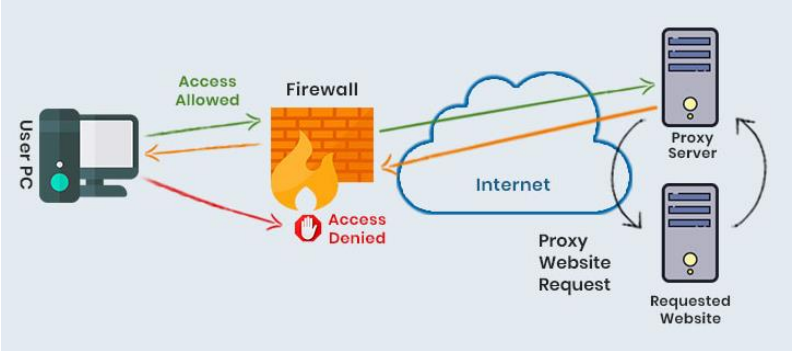


Figura 57. Como trabaja un proxy

El proxy puede cumplir algunas de las siguientes funciones:

- Control de acceso: es posible que los administradores del servidor proxy permitan que ciertos usuarios tengan o no acceso a Internet a través de restricciones en su propio inicio de sesión o direcciones IP, proporcionando al entorno una capa adicional de protección. (Barbosa, 2020, parr. 3)

- Filtrado de contenido: al estar en el medio del camino, el servidor también permite, o no, el acceso a ciertos sitios. Entre las reglas que se pueden aplicar están aquellas para bloquear sitios web específicos, pudiendo llegar a bloquear categorías completas. (Barbosa, 2020, parr. 4)

II.2.7. Cultura en ciberseguridad

A la hora de hablar de seguridad de la información, siempre suele hablarse de tecnologías y procesos. Son una pieza importante pero, en realidad, los auténticos protagonistas de la seguridad en las empresas son los empleados, que son los que gestionan y utilizan los dispositivos tecnológicos de nuestra organización para gestionar nuestro principal activo: la información. (Incibe - Instituto Nacional de Ciberseguridad, parr. 1)

Igual que realizamos controles médicos de empresa y concienciamos en materia de prevención de riesgos laborales a nuestros empleados, también es importante concienciarles y formarles en materia de ciberseguridad. (Incibe - Instituto Nacional de Ciberseguridad, parr. 2)

Esta formación en ciberseguridad creará una cultura de seguridad en la empresa que servirá para establecer las bases de la protección, tanto de nuestra información confidencial, como la de nuestros clientes y proveedores. (Incibe - Instituto Nacional de Ciberseguridad, parr. 3)

«El usuario es el eslabón más IMPORTANTE de la cadena de la seguridad»

Desde el presidente hasta el portero, todos los que ingresan la red corporativa deben tener conciencia sobre la importancia de una navegación segura por el internet, manipulación de datos y apertura de e-mails. (Blogmexico Comstor, 2019, parr. 2)

El hecho es que todos los ataques de ransomware prosperan a partir de un error humano, los colaboradores necesitan ser abordados y pasar por un entrenamiento sobre lo que la empresa espera de su comportamiento digital. (Blogmexico Comstor, 2019, parr. 3)

La falta de cultura en ciberseguridad es la principal amenaza para las empresas

Mediante técnicas de ingeniería social es relativamente fácil engañar a los empleados que confían en que lo que se les remite al correo o los archivos que hay en USB son legítimos. Es necesario que las empresas inviertan en formación que permita a los empleados conocer cómo es un uso ciberseguro de las herramientas TIC. (ITreseller Tech&Consulting, 2020, parr. 1)

Este tipo de acciones son las que facilitan la propagación de ciberdelitos como el phishing o el llamado “fraude al CEO”, por ejemplo. Es por tanto necesario que las empresas inviertan en formación que permita a los empleados conocer cómo es un uso ciberseguro de las herramientas TIC. “En este sentido, hay que concienciar de forma continua a todo el personal y darle los elementos oportunos para la gestión efectiva del riesgo para que sepa cómo actuar cuando este se materialice. Además, no se puede reducir a dar cursos sin más, hay que asegurarse que son efectivos y que la cultura de la compañía en ciberseguridad mejora, es decir, madura”. (ITreseller Tech&Consulting, 2020, parr. 3)

II.3. Marco Legal

II.3.1. Ley General del sistema financiero y del sistema de seguros y orgánica de la Superintendencia de Banca y Seguros N° 26702

Actualmente, las CMAC se rigen por lo establecido en la Ley 26702, Ley General del Sistema Financiero y de Seguros, y Orgánica de la SBS, norma que en el año 1996 derogó el Decreto Legislativo 770. (Vilela, pág. 2)

En la actualidad la ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Ley Orgánica de la Superintendencia de Banca y Seguro promulgada en diciembre de 1996, dispone en su quinta disposición complementaria que las cajas municipales como empresas del

sistema financiero sean regidas además por las normas contenidas en sus leyes respectivas. (Caja Arequipa, parr. 2)

Las cajas municipales como empresas financieras están supervisadas por la Superintendencia de Banca y Seguros y el Banco Central de Reserva, sujetándose a las disposiciones sobre encaje y otras normas obligatorias, así mismo de acuerdo a ley son miembros del Fondo de Seguro de Depósitos. La Ley General permite el crecimiento modular de operaciones de las instituciones financieras, así la Caja Arequipa, es la única institución no bancaria que cumple con los requisitos exigidos para poder operar nuevos productos y servicios, según lo dispone el art. 290 de la Ley General. (Caja Arequipa, parr. 3)

II.3.2. Ley N° 30607 que fortalece el funcionamiento de las CMAC

El 13 de julio de 2017 se promulgó la Ley N°30607, que modifica y fortalece el funcionamiento de las Cajas Municipales de Ahorro y Crédito, en la que se le encarga a la SBS que emita las normas que reglamenten diversos aspectos, tales como la elección de los directores de las CMAC, las nuevas operaciones y los servicios autorizados, la reinversión de utilidades, entre otros. (SBS Informa, 2018, pág. 1)

II.3.3. Circular G-139-2009

En abril del 2009, la Superintendencia de Banca, Seguros y AFP (SBS), publicó los circulares G-139-2009 y G-140-2009, referidos a la Gestión de Continuidad del Negocio y Gestión de Seguridad de la Información, respectivamente.(Businesscontinuity,2012,parr.1)

El circular G-139-2009 es de cumplimiento obligatorio para las empresas del sector financiero peruano, incluidos los bancos, cajas municipales de ahorro y crédito, financieras, compañías de seguros y administradoras de fondos de pensiones (AFP); y tiene como propósito definir los criterios mínimos para elevar el nivel de preparación de las organizaciones para poder hacer frente a eventos externos que puedan interrumpir sus actividades críticas, así como contar con la capacidad para recuperar dichas actividades en el menor tiempo posible. (Businesscontinuity, 2012, parr.2)

Basado en la norma BS 25999, el circular establece cinco fases, como parte del sistema de gestión de continuidad del negocio:

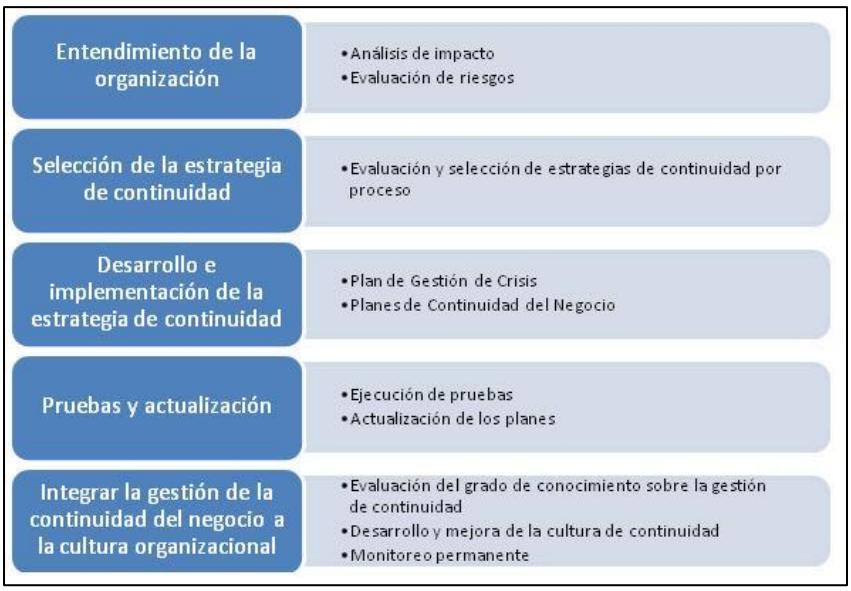


Figura 58. Fases del SGCN

II.3.4. Circular G-140-2009

La circular G-140-2009-SBS, elaborada en abril del 2009 por la Superintendencia de Banca y Seguros, obliga a las entidades financieras que son reguladas por este organismo a establecer, mantener y documentar un Sistema de Gestión de Seguridad de la Información (SGSI) tomando como referencia la ISO 17799 e ISO 27001. El objetivo de implementar el SGSI es de brindar seguridad a los activos de información más importantes como resultado del análisis de riesgo y sobre todo cumpliendo con las expectativas de todos los interesados del sistema, clientes, comunidad, estado, proveedores, y la misma entidad financiera entre otros. (Chang, 2011, pág. 18)

Los controles con los que cuenta la circular, especificados en el artículo 5º, son los siguientes:

- Seguridad lógica.
- Seguridad de personal.
- Seguridad física y ambiental.
- Inventario de activos y clasificación de la información.
- Administración de las operaciones y comunicaciones.
- Adquisición, desarrollo y mantenimiento de sistemas informáticos.
- Procedimientos de respaldo.
- Gestión de incidentes de seguridad de información.
- Cumplimiento normativo.

II.3.5. Ley de protección de datos personales

La vigente Ley de Protección de Datos Personales – Ley 29733 tiene por objeto garantizar el derecho fundamental de las personas a la protección de su privacidad, para lo cual prescribe que el tratamiento de sus datos personales sea proporcional y seguro, de acuerdo con finalidades consentidas por tales personas o habilitadas por ley, previniendo así que tales datos sean objeto de tráfico y/o uso ilícito. (Stucchi, 2017, parr. 2)

Esta legislación establece obligaciones sobre las empresas para que aseguren un adecuado tratamiento de los datos personales de sus clientes, proveedores, trabajadores y otras personas vinculadas a su actividad. Asimismo, esta legislación y su reglamentación reconocen los derechos de las personas a quienes pertenecen dichos datos. (Stucchi, 2017, parr. 3)

Figura 59. Requerimientos Ley Protección de Datos

II.4. Marco Conceptual

Acceso remoto: Conectarse a una red privada desde una ubicación externa a través de internet.
Activo: Es todo lo que le da valor a la organización.
Actualizaciones: Puesta al día de algo que se ha quedado atrasado. Renovación, modernización.
Adaptación: Conjunto de cambios que se realizan para convivir en un nuevo entorno.
Amenaza: Posibilidad de ocurrencia de cualquier tipo o acción que puede causar daño a la organización.
Amenazas Internas: Ataques informáticos que se realizan dentro de la organización.
Análisis de datos: Proceso que consiste en inspeccionar, limpiar y transformar datos con el objetivo de resaltar información útil, para sugerir conclusiones y apoyo en la toma de decisiones.
Análisis de riesgo: Uso sistemático de información para identificar amenazas y estimar el riesgo.

Aplicaciones: Programa de computadora que se utiliza como herramienta para una operación o tarea específica.
Arquitectura de seguridad: Parte de la arquitectura de la empresa que se centra en la seguridad de la información.
Ataque Cibernético: Explotación deliberada de sistemas informáticos, empresas y redes dependientes de la tecnología a través de internet.
Automatización de procesos: Proceso de racionalización, optimización y automatización de los procesos clave que impulsan una organización con el objetivo principal de reducir los costos mediante la integración de aplicaciones, reduciendo la mano de obra, acelerando el tiempo de ejecución de las actividades y sustituyendo los procesos manuales con aplicaciones de software.
Back Office: Conjunto de actividades de apoyo al negocio, es la parte de las empresas o unidad de ella que lleva a cabo las tareas destinadas a gestionar la propia empresa y que no tienen contacto directo con el cliente, como las labores informáticas y de comunicaciones, de gestión de recursos humanos, contabilidad o finanzas.
BackUp: Es una copia de seguridad o el proceso de copia de seguridad.
Big Data: Está formado por conjuntos de datos de mayor tamaño y más complejos, especialmente procedentes de nuevas fuentes de datos. Estos conjuntos de datos son tan voluminosos que el software de procesamiento de datos convencional sencillamente no puede gestionarlos. Sin embargo, estos volúmenes masivos de datos pueden utilizarse para abordar problemas empresariales que antes no hubiera sido posible solucionar.
Blue Team: Seguridad Defensiva.
BYOD: Bring your own device, es una política empresarial consistente en que los empleados lleven sus propios dispositivos personales a su lugar de trabajo para tener acceso a recursos de la organización.
Caja Municipal: Una caja de ahorro y crédito es una entidad que resulta muy similar en su funcionamiento a un banco. De hecho, las cajas de ahorro y crédito están sujetas a las mismas regulaciones de las entidades bancarias. La diferencia es que los socios de las cajas de ahorro en lugar de un fin de lucro, tienen uno social.
Cibercriminales: Personas que realizan alguna actividad delictiva que afecta o abusa de una computadora, una red informática o un dispositivo en red.
Ciberesiliencia: capacidad de las organizaciones de recuperarse de forma rápida de los ciberataques.
Ciberseguridad: La ciberseguridad busca proteger la información digital en los sistemas interconectados. Está comprendida dentro de la seguridad de la información.

Computación en la Nube: Modelo de computación que permite ofrecer servicios informáticos a través de internet.
Confidencialidad: Es la información que se encuentra disponible exclusivamente para personas que cuentan con autorización.
Continuidad del Negocio: Se refiere a prevenir, mitigar y recuperarse de una interrupción de los servicios o procesos de la empresa.
Covid 19: Enfermedad infecciosa causada por el coronavirus que se ha

descubierto más recientemente.
Cultura en ciberseguridad: Nivel de educación de los usuarios en temas de ciberseguridad.
Dato: Representación simbólica de un atributo o variable cuantitativa o cualitativa.
Defensa en profundidad: Estrategia que consiste en la protección de los activos colocando múltiples capas de seguridad.
Digitalización: Proceso por el que la tecnología digital se implanta en la economía en su conjunto afectando a la producción, el consumo y a la propia organización, estructura y gestión de las empresas.
Disponibilidad: Utilización de la información por personas autorizadas en el horario que lo requieran.
Dispositivo móvil: Pequeño dispositivo de computación portátil que generalmente incluye una pantalla y un método de entrada (ya sea táctil o teclado en miniatura).
DMZ: Zona desmilitarizada (conocida también como DMZ, sigla en inglés de demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.
Educación Virtual: Nuevos métodos de enseñanza en la actualidad que utiliza la tecnología para educar de forma remota, eliminando las barreras de la distancia.
Endpoint: Dispositivo informático remoto que se comunica con una red a la que está conectado.
Estrategia de ciberseguridad: Serie de acciones muy meditadas, encaminadas a la protección de los activos de información contra la amenazas en internet.
Fake News: Noticias falsas.
FEPCMAC: Federación Peruana de Cajas Municipales de Ahorro y Crédito, que representa a todas las cajas municipales en el Perú.
Filtración de datos: Acceso no autorizado a información restringida.
Front Office: Abarca aquellas estructuras empresariales encargadas de interactuar directamente con el cliente.
Gestión de ciberseguridad: Administrar de una manera eficiente los riesgos de ciberseguridad asociados a los activos de información.

Indicadores de riesgo: Miden el potencial de un riesgo eventual para luego tomar acciones oportunas basadas en ellos.
Información: Es el activo más importante que posee la organización, como también es un conjunto organizados de datos procesados, que constituyen un mensaje para el conocimiento del usuario.
Ingeniería Social: Es el método de obtener información confidencial, es una técnica mediante engaños a los usuarios o administradores de la organización, empleada por investigadores o delincuentes informáticos.
Innovación: Cambio que introduce novedades, y que se refiere a modificar elementos ya existentes con el fin de mejorarlos, aunque también es posible en la implementación de elementos totalmente nuevos.
Integridad: Mantenimiento de la información en cuanto a su contenido, protegiéndola de modificaciones o alteraciones no autorizadas

manteniendo su validez.

Inteligencia Artificial: Serie de tecnologías que sirven para emular características o capacidades exclusivas del intelecto humano.

Internet de las cosas: Internet de las cosas es una red de objetos físicos –vehículos, máquinas, electrodomésticos y más– que utiliza sensores y Apis para conectarse e intercambiar datos por internet.

ISO: International Organization for Standardization, es una federación mundial de organismos nacionales de normalización, alrededor de 160 países, trabajan a nivel de comités técnicos.

ISO 27032: Pretende garantizar la seguridad en los intercambios de información en la Red para lograr hacer frente de una manera más efectiva al Cibercrimen con más cooperación entre todos.

Logs: grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso particular.

Malware: Programa malicioso que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Modelo con nuevo enfoque: Brindan protección tanto al perímetro como a los endpoint ubicados fuera de él. Utiliza nuevas técnicas y estrategias a través de machine learning e inteligencia artificial.

Modelo de ciberseguridad: Esquema que engloba técnicas, estrategias y herramientas que nos ayude a proteger los activos de información o servicios conectados a internet.

Modelo de Negocio: Representación abstracta de una organización, ya sea de manera textual o gráfica, de todos los conceptos relacionados, acuerdos financieros, y el portafolio central de productos o servicios que la organización ofrece y ofrecerá con base en las acciones necesarias para alcanzar las metas y objetivos estratégicos.

Modelo Tradicional: Mantienen la idea de proteger únicamente todo lo que se encuentra detrás del perímetro de nuestra red utilizando los mismos equipos y estrategias.

Pandemia: Propagación mundial de una nueva enfermedad.

Perímetro de red: Límite seguro entre el lado privado y administrado localmente de una red, a menudo la intranet de una empresa, y el lado público de una red, a menudo Internet.

Phishing: Conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

Procesos: Unidad de actividad que se caracteriza por la ejecución de una secuencia de instrucciones, un estado actual, y un conjunto de recursos del sistema asociados.

Ransomware: Programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.

Red Team: Seguridad Ofensiva.

Riesgo: Probabilidad de que ocurra un desastre ante una amenaza interna o externa.

Seguridad de la información: Conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten

resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.
Seguridad Física: Conjunto de mecanismos y acciones que buscan la detección y prevención de riesgos, con el fin de proteger algún recurso o bien material.
Seguridad informática: Disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático.
Servicios financieros: Actividades realizadas con el propósito de movilizar los recursos de un grupo de personas determinado.
Servidores: Equipamiento que almacena procesos en ejecución capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
Tecnología: Aplicación de la ciencia a la resolución de problemas concretos.

Teletrabajo: Se caracteriza por el desempeño subordinado de labores sin la presencia física del trabajador, denominado “teletrabajador”, en la empresa con la que mantiene vínculo laboral, a través de medios informáticos, de telecomunicaciones y análogos, mediante los cuales se ejercen a su vez el control y la supervisión de las labores.
Threat Hunting: Proceso de búsqueda proactiva e iterativa a través de redes para detectar y aislar amenazas avanzadas que evaden las soluciones de seguridad existentes.
Trabajo remoto: se caracteriza por la prestación de servicios subordinada con la presencia física del trabajador en su domicilio o lugar de aislamiento domiciliario, utilizando cualquier medio o mecanismo que posibilite realizar las labores fuera del centro de trabajo, siempre que la naturaleza de las labores lo permita.
Este no se limita al trabajo que puede ser realizado mediante medios informáticos, de telecomunicaciones u análogos, sino que se extiende a cualquier tipo de trabajo que no requiera la presencia física del trabajador en el centro de labores.
Tráfico Asegurado: Todas las comunicaciones deben ir propiamente cifradas, usando SSH o TLS. Se asume que todo mundo está escuchando.
Tráfico Autorizado: Significa que cada usuario debe presentar sus credenciales validas actuales, además de un módulo de autenticación múltiple.
Transformación Digital: Cambio asociado con la aplicación de tecnologías digitales en todos los aspectos de la sociedad humana.
Virtualización: Creación a través de software de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento o cualquier otro recurso de red.
Vulnerabilidad: Es una debilidad que se presenta en un sistema, aplicación, equipo de la infraestructura de la organización, proceso, en la cual puede ser explotada para violar o adulterar la integridad del activo.
Zero Trust: Modelo de ciberseguridad que busca proteger los activos bajo el enfoque "nunca confiar, siempre verificar".

III. HIPÓTESIS

III.1. Declaración de hipótesis

No aplica.

III.2. Operacionalización de variables

Tabla 1. Operacionalización de la variable características para un modelo de ciberseguridad con nuevo enfoque.

Variable	*Definición conceptual*	*Definición operacional*	*Categorías o Dimensiones*	*Definición Conceptual (Dimensión)*	*Indicador*	*Nivel de Medición*
Características para un modelo de ciberseguridad con nuevo enfoque	El nuevo modelo de ciberseguridad gira en torno a tecnologías como la autenticación multifactorial, el análisis de comportamiento y la tecnología de engaño. La autenticación multifactorial o de dos factores eleva el listón para obtener acceso autorizado a sistemas y datos en primer lugar y evita que los atacantes entren solo con credenciales comprometidas o robadas. El análisis del comportamiento y la tecnología de engaño brindan un monitoreo y protección más completos basados en la suposición de que los atacantes pasarán. (Bradley, 2019, parr. 13)	Revisión documental de bibliografías, casos de éxitos, eventos de ciberseguridad, tesis, papers, etc.	Marco Legal	Que comprende la identificación de las leyes y normas vigentes que reglamentan las características de ciberseguridad que deben tener las cajas municipales.	• Uso de la normativa legal • Cumplimiento de políticas internas • Acuerdos / convenios	Nominal
			Marco Tecnológico	Recursos y tecnología necesaria para el correcto funcionamiento del modelo propuesto	• Uso de las TICs • Integración de las TICs	
			Marco Organizacional	Es el modelo organizacional en la cual se desenvuelve el modelo de ciberseguridad y es el componente que hace posible se cumplan los objetivos propuestos.	• Cumplimiento de objetivos / Metas • Nivel de integración organizacional • Nivel de cultura en ciberseguridad • Frecuencia de capacitación	

IV. DESCRIPCIÓN DE MÉTODOS Y ANÁLISIS

IV.1. Tipo de Investigación

La presente investigación es aplicada, porque busca la resolución de un problema coyuntural (Sampieri, 2014, pág. 25), así mismo, es un estudio de alcance descriptivo porque tiene como prioridad describir cualidades, características de un fenómeno o grupo de personas. Su función principal es profundizar, describir o medir conceptos o situaciones (Investigacion Cientifica, parr. 5), en este caso, los modelos de ciberseguridad. Es de corte transversal dado que la investigación se realizó en un momento determinado, en un tiempo único. (Sampieri, 214, pág. 154)

IV.2. Diseño de Investigación

El presente trabajo de investigación corresponde a un diseño de investigación no experimental porque se realizó sin la manipulación deliberada de variables y en los que solo se observaron fenómenos en su ambiente natural para analizarlos. (Sampieri, 2014, pág. 152) El esquema es:

Donde:

Muestra: Cajas Municipales de Ahorro y Créditos.

Ox: Observación de la variable características del modelo de ciberseguridad con nuevo enfoque.

IV.2.1. Población, muestra y muestreo.

Población.

La población está conformada por las 11 Cajas Municipales de Ahorro y Créditos del Perú.

Muestreo.

No probabilístico - por conveniencia

La muestra de la población se selecciona porque esta convenientemente disponible para el investigador y en un entorno

próximo a él; además, es fácil de reclutar en la coyuntura actual de la pandemia que nos toca vivir. No se consideró seleccionar una muestra que represente a toda la población.

Muestra.

CMACT Trujillo, CMACT Sullana, CMACT Santa, CMACT Piura.

IV.2.2. Método.

El método empleado en la investigación fue cuantitativo.

IV.2.3. Técnicas e instrumentos.

Las técnicas e instrumentos utilizados se detallan a continuación:

Tabla 2. Técnicas e instrumentos

Técnicas	Instrumentos
Análisis documental	Ficha bibliográfica
Observación	Lista de cotejo
Juicio de experto	Matriz de juicio de experto

IV.2.4. Procedimiento para recolección de datos.

Para poder recolectar la información se hizo revisión de bibliografía, trabajos de investigación, conferencias, videos, relacionados a modelos de ciberseguridad y todo lo que guarde conexión con ello como por ejemplo: Marcos de gestión de ciberseguridad, estrategias de Ciberdefensa, situación actual de la ciberseguridad; todo ello, desde la perspectiva de un entorno actual de transformación digital.

IV.2.5. Análisis estadístico e interpretación de datos

Para la investigación, después de haber revisado la bibliografía descrita líneas arriba, se elaboró los resultados utilizando mapas mentales, figuras, organigrama, diseño de arquitectura de seguridad, esquema de gestión, los cuales permitieron describir y cumplir con los objetivos de la investigación.

V. RESULTADOS

V.1. Identificación de modelos de ciberseguridad

Los modelos de ciberseguridad fueron identificados a través de búsquedas sistemáticas en bibliografías e internet.

Se identificaron los siguientes:

- Modelo ISM3
- Modelo de seguridad perimetral
- Modelo Clark-Wilson
- Modelo Thin Security
- Modelo Bell-LaPadula
- Modelo Zero Trust
- Modelo defensa en profundidad

V.2. Comparación de modelos de ciberseguridad

Identificados los modelos, se procedió a acotarlos a un número más adecuado con la opinión de expertos en ciberseguridad (ver anexo 1); para lo cual se desarrolló una matriz de priorización.

Tabla 3. Matriz de priorización

Criterio / Modelo	Relación con el tema de investigación	Integridad	Disponibilidad	Confidencialidad	Total
ISM3	1	2	2	1	6
Seguridad Perimetral	4	3	3	2	12
Clark-Wilson	2	4	2	1	9
Thin Security	5	4	4	3	16
Bell-LaPadula	2	2	3	4	11
Zero Trust	5	4	4	5	18
Defensa en Profundidad	4	4	3	4	15

Del desarrollo de la matriz de priorización, se seleccionaron 4 modelos que obtuvieron el mayor puntaje de acuerdo a la recomendación de los expertos:

- Defensa en profundidad
- Modelo perimetral
- Modelo Zero Trust
- Modelo Thin Security

Después se definieron las características obtenidas del análisis e investigación de diferentes bibliografías, tesis, papers, congresos, revistas; así como también de la experiencia del autor; las cuales se verifican en su respectivo marco teórico. Luego se evaluó qué modelos de ciberseguridad identificados en el paso anterior guardaba mayor relación con las características de ciberseguridad listadas; para lo cual se elaboró una matriz de comparación que fue resuelta por expertos en ciberseguridad (Ver anexo 2).

Tabla 4: Matriz de comparación de características versus modelos de ciberseguridad

N°	CARACTERISTICAS / MODELOS DE CIBERSEGURIDAD	DEFENSA EN PROFUNDIDAD	PERIMETRAL	ZERO TRUST	THIN SECURITY
1	Múltiples niveles de seguridad	✓	X	✓	✓
2	Protección del endpoint detrás del perímetro	✓	✓	✓	✓
3	Integración de la arquitectura de seguridad	X	X	✓	✓
4	Gestión de ciberseguridad y manejo del riesgo a nivel organizacional (pirámide)	X	X	✓	✓
5	Visibilidad en toda la red	X	X	✓	✓
6	Gestión de ciberseguridad y manejo del riesgo a nivel departamental	✓	✓	X	X
7	Interacción con las distintas capas del modelo	X	X	✓	✓
8	Protección del endpoint fuera del perímetro	X	X	✓	✓
9	Adaptarse continuamente a nuevas tácticas y técnicas de ataque	X	X	✓	✓
10	Acciones proactivas para la caza de amenazas.	X	X	✓	✓
11	Protección reactiva	✓	✓	X	X
12	Autenticación Multifactorial	X	X	✓	✓
13	Prevención, detección y respuesta para reducir superficie de ataque	X	X	✓	✓
14	Análisis de comportamientos de usuario	X	X	✓	✓

15	Protección proactiva	X	X	✓	✓
16	Análisis de amenazas automatizados y predictivos	X	X	✓	✓
17	Protección de amenazas internas y externas	✓	✓	✓	✓
18	Adaptación al modelo o arquitectura de seguridad existente	X	X	✓	X
19	Se adapta a un ciclo continuo de gestión de ciberseguridad	X	X	✓	✓
20	Permite reducir las alertas reportando las más significativas	X	X	✓	✓
21	Análisis de amenazas basado solo en firmas	✓	✓	X	X
22	Análisis de amenazadas basado en IA tipo EDR	X	X	✓	✓
23	Utiliza ejercicios de red Team	X	X	✓	✓
24	Se adapta a soluciones en la nube	X	X	✓	✓
25	Gestión de accesos fuera del perímetro	X	X	✓	✓
26	Detección de bots	X	X	✓	✓

Del desarrollo de la matriz de comparación se determinó que el modelo de ciberseguridad que cuenta con la mayor cantidad de características propuestas fue el modelo Zero trust; por esa razón, se utilizó este modelo, así como también las características seleccionadas para elaborar la propuesta.

V.3. Características de un modelo de seguridad con nuevo enfoque

El siguiente mapa mental muestra las características propuestas para un modelo de ciberseguridad con nuevo enfoque, que fueron obtenidos de la evaluación anterior, y validadas a través de una lista de cotejo realizada a expertos y usuarios potenciales (ver anexo 3).

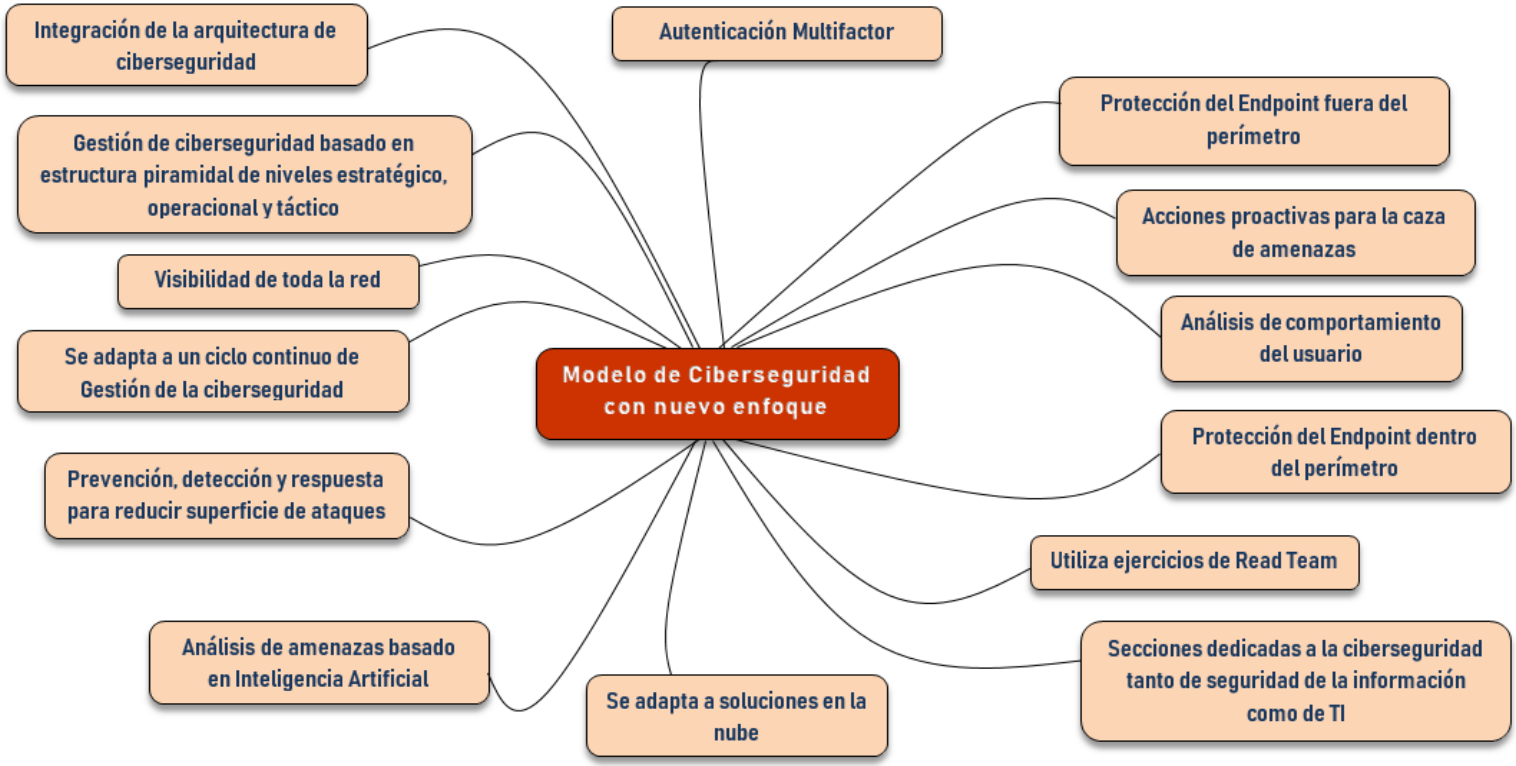


Figura 60: Características de ciberseguridad para el modelo propuesto

V.4. Propuesta del modelo de ciberseguridad

Con las características seleccionadas y validadas con el juicio de los expertos; se elaboró la siguiente propuesta que tiene como base el modelo de ciberseguridad Zero Trust y el marco de Gestión de ciberseguridad NIST; así como también, características adicionales que se adaptaron como consecuencia de la investigación realizada y la experiencia del autor.

La selección del modelo Zero Trust obedece a la evaluación realizada en pasos anteriores y a que se adapta perfectamente a un entorno de transformación digital donde el endpoint no se encuentra únicamente detrás del perímetro; así como el uso de tecnología avanzada para caza de amenazas. Así mismo, este modelo no reemplaza la estructura ni los procesos de ciberseguridad existente en las cajas municipales; si no que se adapta a ellos y lo mejora. Existen esfuerzos en ciberseguridad que las cajas municipales vienes realizando, y este modelo pretende reforzarlas, mejorarlas e incluirlas de ser necesario.

"Zero Trust es una forma de trabajar, pensar y actuar"

La propuesta comprende las siguientes partes:

1. Contexto organizacional – Decisión estratégica
2. Marco de ciberseguridad
3. Diseño de arquitectura de ciberseguridad
4. Creación de cultura en ciberseguridad

V.4.1. Contexto Organizacional

En este punto es importante tener en claro los activos que vamos a proteger, y conocer los usuarios y agentes del negocio completamente; sin embargo, también es importante conocer cómo estos actores van a interactuar a nivel organizacional en todos los niveles del modelo de ciberseguridad. Este punto es clave para el buen funcionamiento del modelo.

Sobre la base de una estructura piramidal, nuestra propuesta es que se jerarquice la gestión de la ciberseguridad a través de la creación de 3

niveles: nivel estratégico, nivel operacional y/o gerencial, y nivel táctico y/o técnico, tal como se muestra en la siguiente figura:

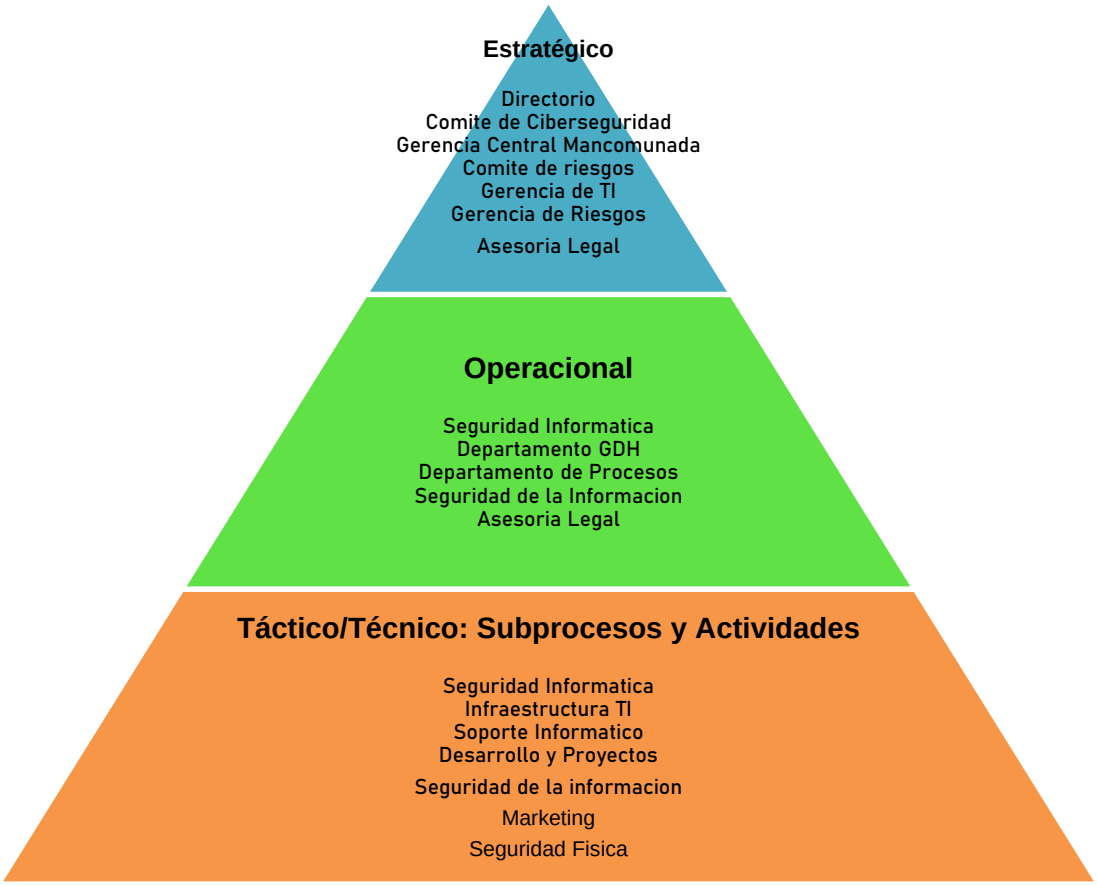


Figura 61. Pirámide Nivel Estratégico

Nivel Estratégico

En este nivel se tiene que definir los objetivos de ciberseguridad, y que estos estén alineados a los objetivos de la organización. Se analizan y definen también las estrategias, políticas, riesgos y planes de ciberseguridad y se evalúa la situación actual para proponer oportunidades de mejora para fortalecer la Ciberdefensa de la organización.

Deben participar activamente, el directorio, la Gerencia Central Mancomunada (Gerencias centrales de Administración, Finanzas y Negocio), el comité de riesgos, la Gerencia de Tecnologías de Información,

la Gerencia de Riesgos, el oficial de Seguridad de la información y asesoría legal.

En este nivel, proponemos también, la creación del **"comité de ciberseguridad",** liderada, por la Gerencia de TI y la Oficialía de Seguridad de la información; la cual se encargará de la planificación estratégica y de la aplicación de una política de investigación, prevención y reacción de defensa contra amenazas cibernéticas. La estructura quedaría de la siguiente manera:

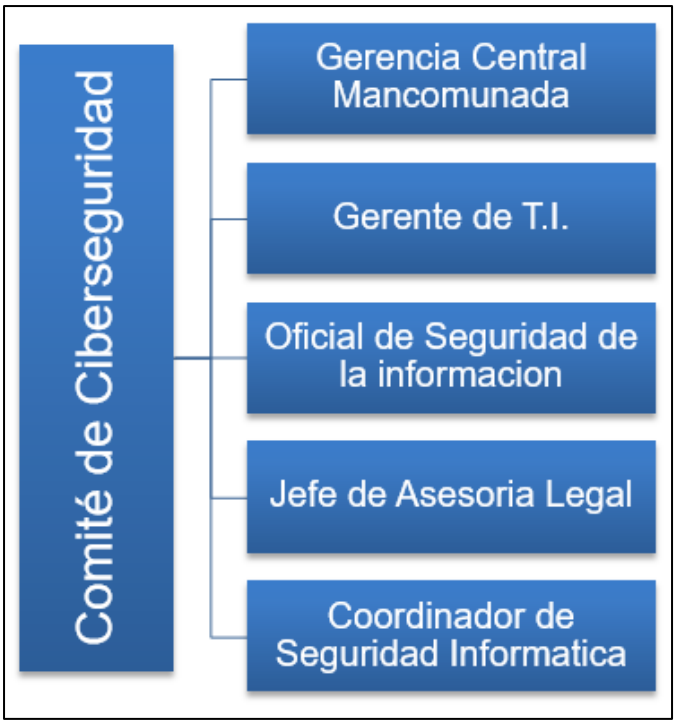


Figura 62: Comité de ciberseguridad

Este comité, tendrá las siguientes funciones:

- Asesorar a la Gerencia Central Mancomunada, en el análisis y definición de la **Política General de Ciberseguridad**, la que contendrá las medidas, planes y programas de acción específicos que se aplicarán para su ejecución y cumplimiento.

- Identificar las amenazas actuales y potenciales en el ámbito del ciberespacio, proponiendo las acciones tendientes a superar las brechas que se identifiquen y monitorear su cumplimiento.
- Analizar y proponer las alternativas de estructura orgánica para la ciberseguridad en la Organización.
- Analizar y estudiar la legislación vigente aplicable en materia de ciberseguridad, proponiendo las modificaciones, legales y reglamentarias que sean necesarias.
- Evaluar la correcta implementación y funcionamiento de un marco de gestión de ciberseguridad.
- Proponer la organización y funcionamiento de la Ciberdefensa, en las siguientes áreas: protección de las infraestructuras críticas (Data Centers), manejo de crisis, ciberesiliencia, inteligencia y ciberdelitos.
- Coordinar las actividades de Ciberseguridad entre la Súper intendencia de Banca y Seguros (SBS) y la Federación Peruana de Cajas Municipales de Ahorro y Crédito (Fepcmac), las cajas municipales, entidades financieras y la población en general, articulando un sistema de intercambio de información y comunicación de incidentes.

El Comité sesionará mensualmente o por citación extraordinaria en cualquier momento en caso de incidentes críticos.

Nivel Operacional

En este nivel se encuentran las secciones encargadas de traducir la estrategia decidida por el nivel estratégico en acciones concretas a cumplir por el nivel táctico y técnico.

Es importante que la traducción de estas estrategias cuente con el asesoramiento de los equipos especializados en ciberseguridad tanto de lado de Oficialía de Seguridad de la Información, como un equipo dedicado exclusivamente a ver temas de ciberseguridad de lado de Tecnologías de Información. Estos equipos se deben complementar para lograr una

sinergia que nos permita identificar, prevenir, responder y lograr la resiliencia esperada anta algún incidente en ciberseguridad; así como también, un nivel adecuado en Ciberdefensa.

En ese sentido, se propone la creación de una nueva sección llamada **"Seguridad Informática"** dentro del departamento de TI; así como también, la modificación de la sección de oficialía de seguridad de la información.

A continuación se muestra la estructura orgánica y las macro funciones que proponemos:

Estructura Orgánica:

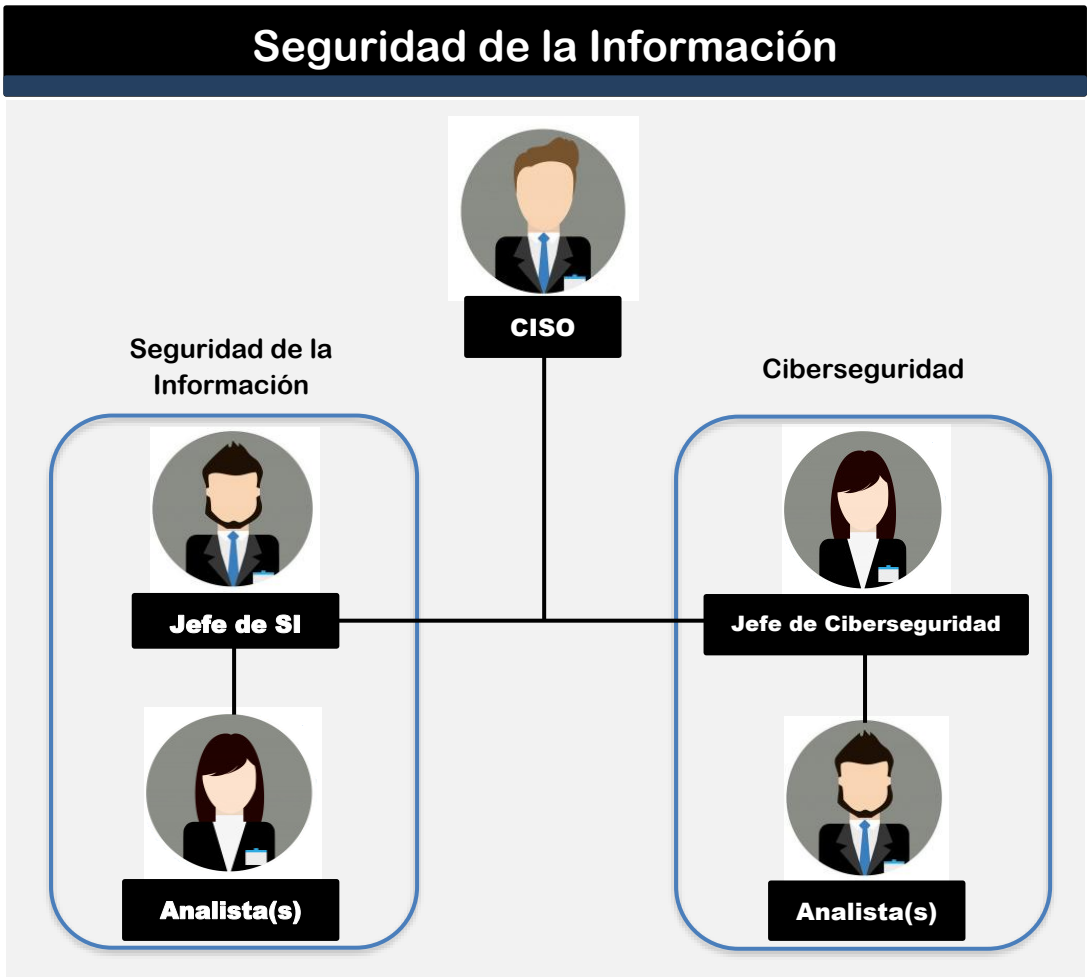


Figura 63. Organigrama Seguridad de la Información

Lo que se intenta lograr es segmentar funcionalmente todo lo referente al cumplimiento y lo relacionado a la ciberseguridad en esta sección; de esa manera, logramos que las actividades se realicen de manera ordenada y eficaz sin perder de vista los objetivos compartidos de las dos secciones creadas.

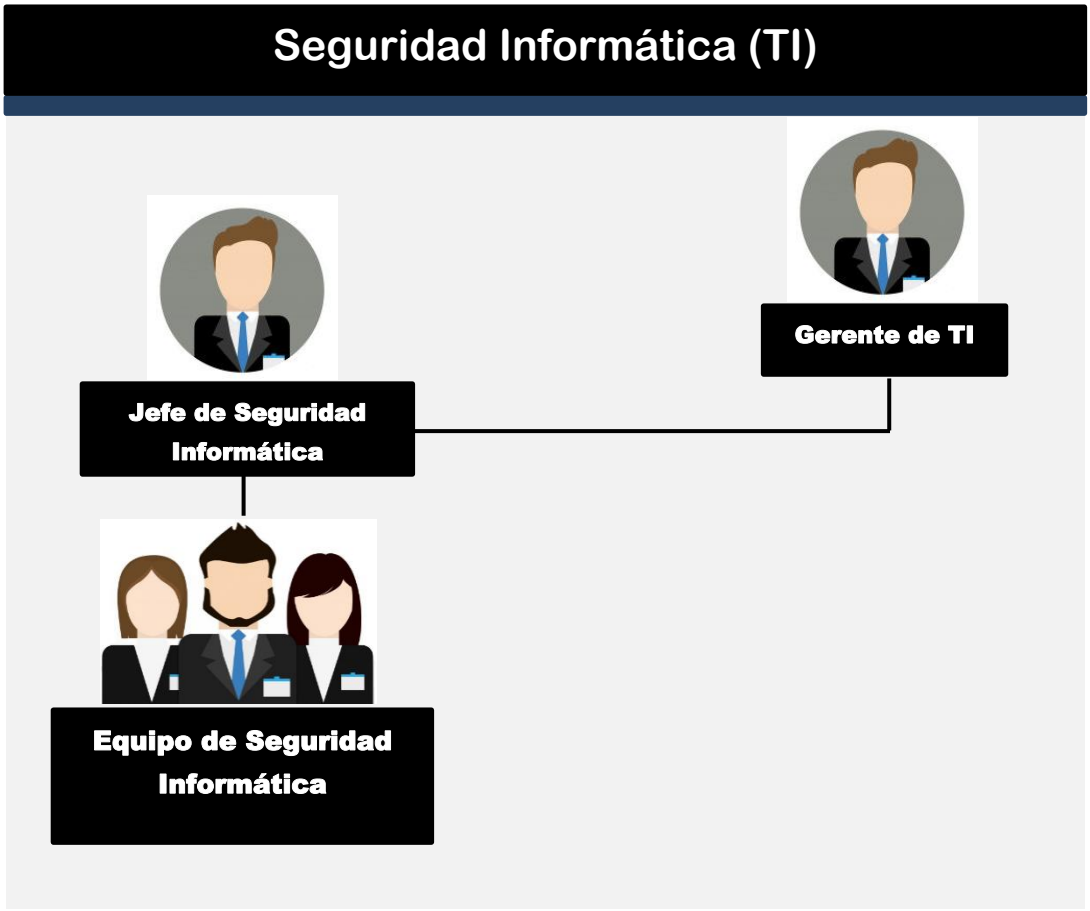


Figura 64. Organigrama Seguridad Informática

Es importante que las actividades relacionadas con seguridad informática o ciberseguridad se administren de manera independiente; debido a la importancia que significan en el entorno actual y lo critico de sus procesos. En el mundo digital de hoy en día y en un nuevo modelo de ciberseguridad, se debe garantizar que estas actividades las lleve a cabo una sección separada de las demás actividades que tiene tecnologías de información y que no guardan relación con la ciberseguridad.

Estructura y Macro funciones

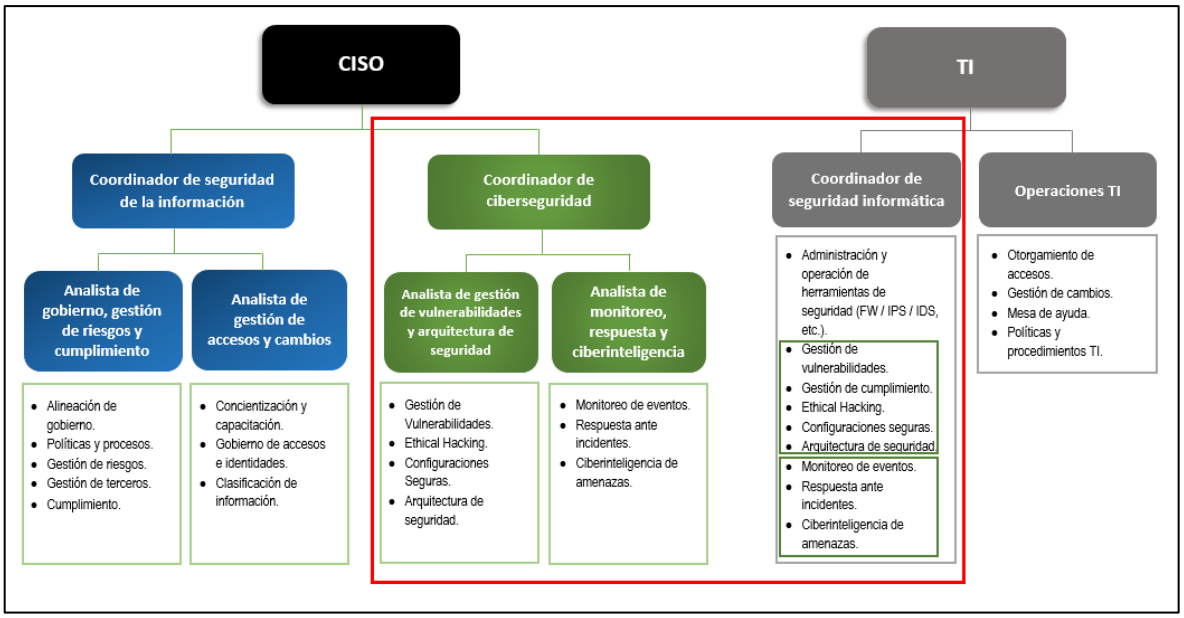


Figura 65. Macro funciones SI y Seguridad Informática

En la imagen anterior, se muestran las funciones macro propuestas para cada sección.

Es importante explicar que lo resaltado en cuadro rojo se refiere a la importancia de la comunicación que debe existir entre las secciones de ciberseguridad (Oficialía de Seguridad de la información) y seguridad Informática (TI) para obtener los resultados esperados y propuestos en este modelo. Existen actividades en las dos secciones mencionadas que se parecen; pero que sin embargo, no tienen la misma funcionalidad; por ejemplo: Gestión de vulnerabilidades, desde el punto de vista de seguridad de la información, se aboca al análisis y monitoreo de las diversas vulnerabilidades que pueden encontrarse en los activos de información de la organización para luego reportarlo a TI para su remediación. En el caso de seguridad informática, el análisis de vulnerabilidades es el mismo, con la diferencia que ellos pueden tomar acción inmediata para mitigar esas vulnerabilidades realizando las actualizaciones de seguridad correspondientes.

Nivel Táctico/Técnico

En el nivel táctico se integran los objetivos diseñados en proceso de planeamiento del nivel operacional.

Son parte de este nivel, las secciones de seguridad informática, seguridad de la información, infraestructura tecnológica, soporte informático, proyectos y desarrollo, seguridad física y marketing.

Además, se introduce un nivel técnico, relacionado con las capacidades en las fases de prevención, detección y respuesta a incidentes de ciberseguridad; en ese sentido, se propone la creación del Equipo de Respuesta ante Incidentes Informáticos, CERT, el cual incluye a los siguientes representantes:

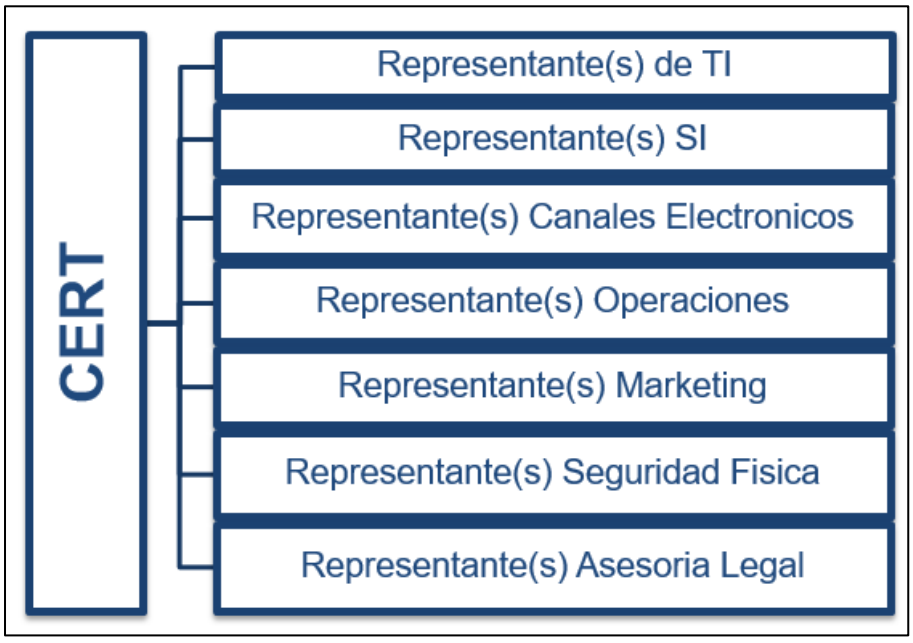


Figura 66: Equipo CERT

Ante alguna incidencia, es importante que se puedan reunir para la coordinación respectiva, todas las áreas involucradas con el flujo de información que pudo haber sido vulnerada; por ejemplo, ante un incidente de phishing, estas áreas deben poder rastrear y detectar en qué punto se dio la vulnerabilidad, el grado e impacto de la misma, que accesos se

deben cerrar, que usuarios o clientes fueron afectados y como se debe comunicar el incidente. Este equipo, debe ser activado en coordinación con el comité de ciberseguridad.

V.4.2. Marco de ciberseguridad

Se propone la utilización del Marco NIST porque nos proporciona una estructura de organización común para múltiples enfoques de ciberseguridad mediante la conformación de estándares, directrices y prácticas que funcionan de manera efectiva en la actualidad.

Se propone utilizar los siguientes pasos como guía para crear un nuevo programa de ciberseguridad o mejorar el programa existente:

Paso 1: Priorización y alcance

En este paso, las cajas municipales deberán identificar sus objetivos empresariales, visión – misión, y sus prioridades organizacionales de alto nivel. Con ello, se tomaran las decisiones estratégicas con respecto a las implementaciones de ciberseguridad, y se determinara el alcance de los sistemas y activos que respaldan la línea o proceso comercial seleccionado. Todo esto se refuerza y complementa con lo propuesto en la parte organizacional, respecto al diseño piramidal de niveles Estratégico, operacional y táctico; y el funcionamiento del comité de ciberseguridad.

Cada Caja Municipal, probablemente tendrá una tolerancia al riesgo diferente; la cual podrá reflejarse en un Nivel de Implementación objetivo.

Proponemos que los niveles de implementación del marco sean analizados por la Gerencia de Riesgo de cada Caja Municipal, en coordinación con el Oficial de Seguridad y con el apoyo de la Gerencia de Tecnologías de Información; sin embargo, consideramos que el nivel inicial de implementación podría encontrarse entre el nivel 2 y el nivel 3, por las siguientes razones:

- Las prácticas de gestión de riesgo son aprobadas formalmente y se expresan como políticas en toda la organización.

- Existe una conciencia del riesgo de ciberseguridad a nivel organizacional, pero no se ha establecido un enfoque de toda la organización para gestionar el riesgo de ciberseguridad.
- La organización conoce su rol en el ecosistema más grande, pero no ha formalizado sus capacidades para interactuar y compartir información externamente.

Figura 67. Niveles de Implementación

Paso 2: Orientación

Con el alcance determinado en el paso anterior, se deberá identificar los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general. Luego, se consultaran las fuentes para identificar las amenazas y vulnerabilidades que afectan estos activos.

Proponemos que el programa utilice los activos, amenazas y vulnerabilidades que ya se encuentran mapeadas en la matriz que maneja departamento de riesgos de cada Caja Municipal.

Paso 3: Crear un perfil actual

En este paso, validaremos que resultados de las categorías y subcategorías del marco NIST (detallado más adelante), se están logrando actualmente; y con ello, crearemos un perfil actual. Si se logra parcialmente un resultado, se debe tomar nota de ello para que nos ayude a respaldar los pasos posteriores.

Proponemos que la validación de este paso sea desarrollada por la Gerencia de Riesgos y oficialía de Seguridad de la Información; en coordinación con la Gerencia de Tecnologías de Información; y sea informado a la alta dirección con participación del comité de ciberseguridad.

Paso 4: Realizar una evaluación de riesgos

Proponemos que esta evaluación tenga como punto de partida la matriz de riesgos actual y los diferentes análisis de impacto y probabilidad desarrollados por la Gerencia de Riesgos y la Oficialía de Seguridad de la Información de cada Caja Municipal. Esta evaluación no busca reemplazar lo ya existente; si no por el contrario, fortalecer los procesos y procedimientos actuales referentes a la gestión del riesgo.

Las plantillas y documentos utilizados para llevar a cabo esta evaluación, serán los mismos que se utilizan actualmente en cada Empresa.

Los resultados deberán ser informados, evaluados y aprobados en conjunto con la alta dirección, el comité de riesgos y el comité de ciberseguridad.

Paso 5: Crear un perfil objetivo

En este paso, crearemos un perfil objetivo basado en la evaluación de las categorías y subcategorías del marco que se realizó en el paso anterior. Este perfil debe describir los objetivos de ciberseguridad deseados de cada Caja Municipal.

El Perfil Objetivo debe reflejar adecuadamente los criterios dentro del Nivel de Implementación objetivo.

Paso 6: Determinar, analizar y priorizar brechas

Una vez que se tiene creados los dos perfiles (actual y objetivo); deberán ser comparados para poder determinar las brechas.

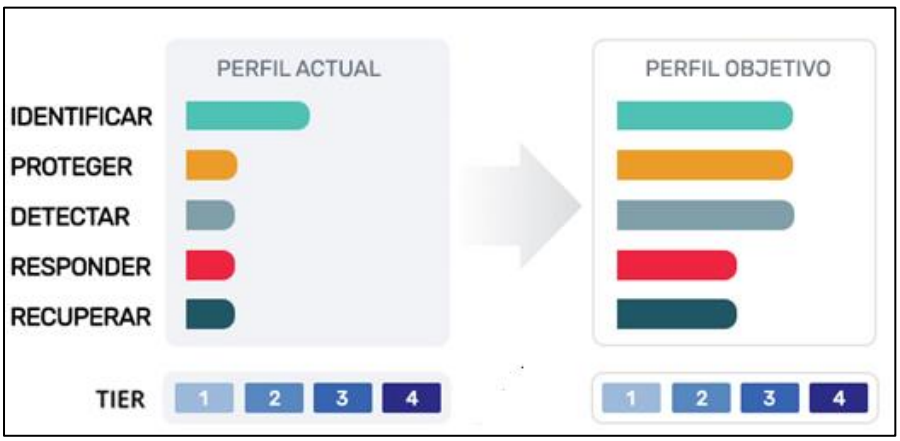


Figura 68. Perfil del Riesgo

Luego, se deberá crear un plan de acción priorizado para abordar las brechas y lograr los resultados en el perfil objetivo. El plan deberá reflejar los impulsores, los costos y beneficios, y los riesgos de ejecución.

Así mismo, cada Caja Municipal, determinará los recursos necesarios para abordar las brechas, que incluyen los recursos económicos y los recursos humanos.

Se recomienda utilizar de esta manera el uso de perfiles para fortalecer a cada Caja Municipal en la toma de decisiones informadas sobre las actividades de ciberseguridad, respaldar la gestión de riesgos y permitirles realizar mejoras específicas y rentables.

Paso 7: Implementar plan de acción

En este paso determinamos qué acciones se tomarán para abordar las brechas identificadas en el paso anterior; y luego, ajustar sus prácticas de ciberseguridad para lograr el perfil objetivo.

Para proveer más dirección, el marco puede identificar ejemplos de referencias informativas sobre las categorías y sub categorías; pero serán las Cajas Municipales las que deben determinar que normas, directrices y prácticas funcionan mejor para sus necesidades.

Se recomienda repetir los pasos según sea necesario para evaluar y mejorar continuamente su ciberseguridad. Por ejemplo, cada Caja Municipal puede encontrar que una repetición más frecuente del paso orientación mejora la calidad de las evaluaciones de riesgos. Además, pueden supervisar el progreso a través de actualizaciones iterativas al Perfil Actual, y luego compararlo con el Perfil Objetivo. Así mismo, pueden utilizar este proceso para alinear su programa de ciberseguridad con su Nivel de Implementación del Marco deseado.

Núcleo del Marco.

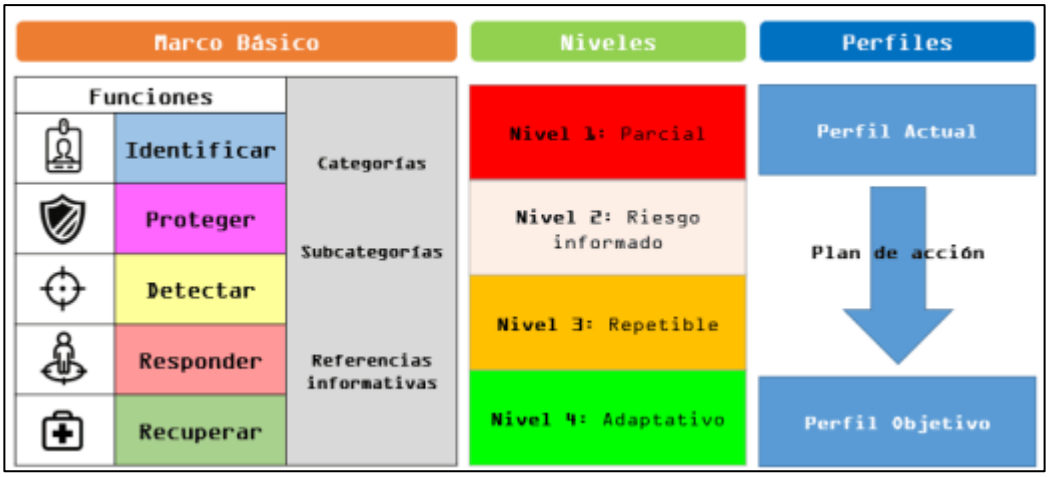


Figura 69. Marco de trabajo ciberseguridad NIST

Adicional a los pasos descritos anteriormente, proponemos fortalecer los siguientes puntos de acuerdo a cada función del núcleo del marco NIST:

- **Identificar**
  - Establecer indicadores de salud de ciberseguridad básicos para lograr una gestión efectiva y operativa, como por ejemplo: N° de incidentes gestionados, estado de parchado, nivel de obsolescencia, estado de actualización solución EDR, etc.
  - Gestión de vulnerabilidades desde el lado de seguridad de la información (Preventivo) y seguridad informática (Proactivo).
  - Evaluar la posibilidad de establecer un modelo de riesgo cualitativo en vez de cuantitativo para guiar las estrategias de ciberseguridad.

- **Proteger**
  - Control de acceso a través del mínimo privilegio y confianza cero utilizando perfiles de acceso sin importar el punto de origen de la conexión.
  - Centrarse en **IAM (**Identity and Access Management**) y el endpoint**, como las dos fronteras que definen el nuevo perímetro que protege los datos corporativos.

- No tenerle miedo al **"Cloud";** por el contrario, se debe aprovechar su elasticidad, visibilidad, protección y resistencia implícita para los activos digitales.
- Mejorar los procesos de Ethical Hacking o evaluaciones de seguridad (pentesting) que se realizan cada año; ya que pierden todo su valor y razón de ser si se les brinda a los pentesters todos los accesos sin ninguna restricción, ya que eso se traduce en un simple escaneo de vulnerabilidades con un reporte final que puede llevarse a cabo tranquilamente por la misma organización. Se debe realizar la prueba sin retirar ningún control de seguridad para conocer realmente el estado de seguridad de la organización.
- Apostar por al menos un **ejercicio de red Team** que ponga en contexto la situación real frente a un ataque dirigido y una evaluación 360 (Protección, Detección, Respuesta).
- Fortalecer el área de seguridad informática, empoderándolo en la toma de decisiones y propuestas para la mejora de la arquitectura de seguridad de la organización que cambia y se actualiza constantemente. Crear un plan de capacitación continua en ciberseguridad para su equipo.
- Mejorar el proceso de habilitación de accesos a usuario, eliminando las "excepciones". Todo acceso a los recursos de la organización deberá adjuntar previamente los permisos correspondientes.
- Fortalecer la capacitación en temas de ciberseguridad al mismo nivel que las capacitaciones sobre lavado de activos. Estas capacitaciones deberán incluirse como parte de la inducción para los nuevos ingresantes a la organización; así como también, para todos los clientes que realizan alguna operación o tramite.

- **Detectar**

- Hay que huir de las tecnologías antivirus tradicionales, basadas en firmas y aprovechar el enfoque EDR basado en el comportamiento con la capacidad de responder.
- Si es posible, hay que alejarse de las soluciones SoC + SieM tradicionales y personalizadas**.** Este tipo de servicios rara vez proporciona un valor instantáneo y requiere mucho tiempo y esfuerzo, con una capacidad de detección marginal. Se debe pensar (si es viable) en una solución tipo **SOAR** (Security Orchestration, Automation and Response).
- Realizar un "tunning" de las herramientas de seguridad, con la finalidad de reducir las alertas generadas, priorizando de acuerdo al riesgo sobre los activos. Menos alertas equivale a menos recursos para gestionarlas, por lo que se podrán establecer reducciones significativas en el coste de la operación de seguridad, mediante esta medida.
- Aprovechar la creación del equipo CERT dentro de la sección de seguridad informática para el monitoreo de las alertas de ciberseguridad, en coordinación continua con las secciones de redes y comunicaciones, infraestructura y seguridad física.

- **Responder**
  - Confiar tanto como sea posible en soluciones basadas en el comportamiento, como EDR y detección de registro y seguimiento basada en la nube y respuesta automatizada.
  - Es necesario un alineamiento entre las secciones de seguridad de la información y seguridad informática para unir esfuerzos en asegurar la información.
  - Algunas actividades de monitoreo y respuesta ante incidentes como por ejemplo, fraude electrónico, pueden ser subcontratadas; sin embargo, la sección de seguridad informática debe coordinar todas las actividades que esto implique.

- Utilizar alguna solución que utilice servicios de Threat Hunting.

- **Recuperar**
  - Hay que confiar en soluciones híbridas on premise - nube para el almacenamiento que con cierta habilidad de diseño y configuración proporcionan la misma (o mejor) respuesta a esquemas clásicos, tediosos y costosos de Backups.
  - Se debe pensar en modelos SaaS que ofrecen soluciones ofimáticas, que aportan protección y simplifican los esquemas de respuesta y recuperación.
  - Los esquemas clásicos de continuidad de Negocio después de COVID-19 deben revisarse. Las organizaciones se han dado cuenta de que necesitan una continuidad comercial pragmática. Se necesita fortalecer ante este escenario el acceso a los sistemas, almacenamiento, correo, acceso remoto, etc. Y todo con la seguridad que esto conlleva.

	Función	Categoría	ID
¿Qué activos y procesos necesitan protección?	Identificar	Gestión de Activos	ID.AM
		El Negocio y el Medioambiente	ID.BE
		Gobierno	ID.GV
		Evaluación de Riesgo	ID.RA
		Estrategia de Gestión de Riesgo	ID.RM
¿Qué medidas de resguardo y de seguridad he aplicado?	Proteger	Control de Acceso	PR.AC
		Conciencia y Entrenamiento	PR.AT
		Seguridad de Datos	PR.DS
		Procedimientos y Procesos de Seguridad de la Información	PR.IP
		Mantenimiento	PR.MA
		Seguridad Tecnológica	PR.PT
¿Cuál es la estrategia que permite detectar los incidentes?	Detectar	Anomalías y Eventos	DE.AE
		Monitoreo Continuo de Seguridad	DE.CM
		Detección de Procesos	DE.DP
¿Qué estrategia puede ayudar a mitigar el impacto generado por los incidentes?	Responder	Plan de Respuesta a Incidente	RS.RP
		Plan de Comunicación	RS.CO
		Análisis	RS.AN
		Plan de Mitigación	RS.MI
		Plan de Mejoras	RS.IM
¿Qué estrategia puede ayudar a restaurar las capacidades de recuperación?	Recuperar	Plan de Recuperación	RC.RP
		Plan de Mejoras	RC.IM
		Plan de Comunicación	RC.CO

Figura 70. Núcleo del Marco NIST

Todas estas funciones juntas nos darán una visión estratégica de alto nivel del ciclo de vida del proceso de gestión de riesgos de la ciberseguridad en la organización.

Es importante tener presente que el marco de trabajo no es un documento estático, sino que cada organización puede determinar con base en sus necesidades las actividades que considera prioritarias, permitiendo de esa forma un despliegue personalizado y paulatino.

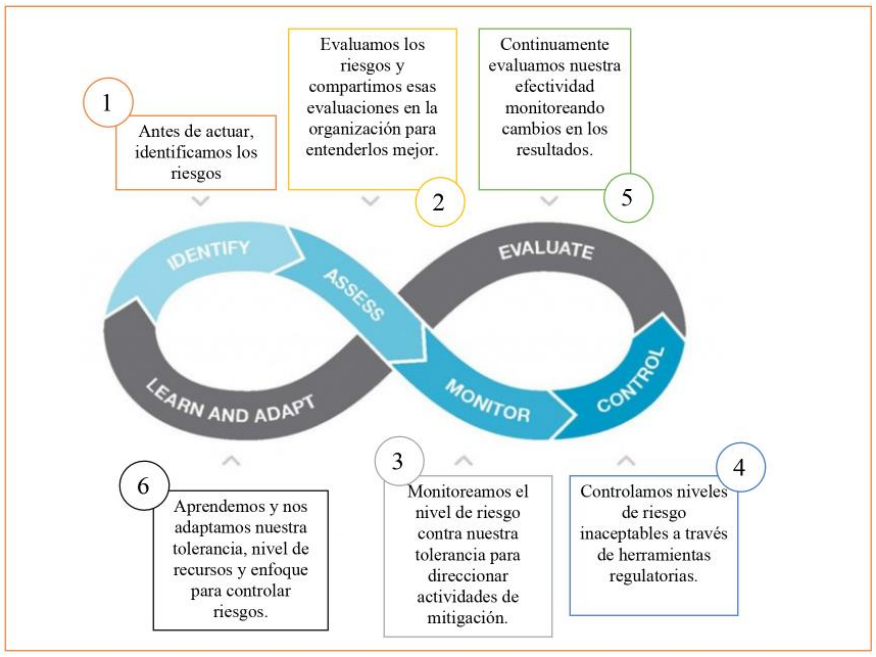


Figura 71. Ciberseguridad Holística

La siguiente tabla se debe utilizar para la creación del perfil actual mencionada en el paso 3 del marco de ciberseguridad:

Tabla 5. Funciones, Categorías y subcategorías del Marco NIST

Función	Categoría	Sub Categoría	Referencias Informativas
IDENTIFICAR (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma	**ID.AM-1:** Los dispositivos y sistemas físicos dentro de la organización están inventariados.	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Las plataformas	CIS CSC 2

	coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	de software y las aplicaciones dentro de la organización están inventariadas.	COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 NIST SP 800-53 Rev. 4 CM-8, PM-5
		I**D.AM-3:** La comunicación organizacional y los flujos de datos están mapeados.	CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Los sistemas de información externos están catalogados.	CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.	CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.	CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
	Entorno empresarial (ID.BE): Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	**ID.BE-1:** Se identifica y se comunica la función de la organización en la cadena de suministro.	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: Se identifica y se comunica el lugar de la organización en la infraestructura crítica y su sector industrial.	COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Cláusula 4.1 NIST SP 800-53 Rev. 4 PM-8

		ID.BE-3: Se establecen y se comunican las prioridades para la misión, los objetivos y las actividades de la organización.	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.BE-4: Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.	COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).	COBIT 5 BAI03.02, DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-14
	Gobernanza (ID.GV): Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de seguridad cibernética.	**ID.GV-1:** Se establece y se comunica la política de seguridad cibernética organizacional.	CIS CSC 19 COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02 ISA 62443-2-1:2009 4.3.2.6 ISO/IEC 27001:2013 A.5.1.1 NIST SP 800-53 Rev. 4-1 controles de todas las familias de control de seguridad
		ID.GV-2: Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.	CIS CSC 19 COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1 NIST SP 800-53 Rev. 4 PS-7, PM-1, PM-2
		ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y	CIS CSC 19 COBIT 5 BAI02.01, MEA03.01, MEA03.04 ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5

		libertades civiles.	NIST SP 800-53 Rev. 4-1 controles de todas las familias de control de seguridad
		ID.GV-4: Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.	COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Evaluación de riesgos (ID.RA): La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	**ID.RA-1:** Se identifican y se documentan las vulnerabilidades de los activos.	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.	CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16
		ID.RA-3: Se identifican y se documentan las amenazas, tanto internas como externas.	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Cláusula 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Se identifican los impactos y las probabilidades del negocio.	CIS CSC 4 COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.16.1.6, Cláusula 6.1.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	CIS CSC 4 COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16

		ID.RA-6: Se identifican y priorizan las respuestas al riesgo.	CIS CSC 4 COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Cláusula 6.1.3 NIST SP 800-53 Rev. 4 PM-4, PM-9
	Estrategia de gestión de riesgos (ID.RM): Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.	**ID.RM-1:** Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	CIS CSC 4 COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3 NIST SP 800-53 Rev. 4 PM-9
		ID.RM-2: La tolerancia al riesgo organizacional se determina y se expresa claramente.	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.2.6.5 ISO/IEC 27001:2013 Cláusula 6.1.3, Cláusula 8.3 NIST SP 800-53 Rev. 4 PM-9
		ID.RM-3: La determinación de la tolerancia del riesgo de la organización se basa en parte en su rol en la infraestructura crítica y el análisis del riesgo específico del sector.	COBIT 5 APO12.02 ISO/IEC 27001:2013 Cláusula 6.1.3, Cláusula 8.3 NIST SP 800-53 Rev. 4 SA-14, PM-8, PM-9, PM-11
	Gestión del riesgo de la cadena de suministro (ID.SC): Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.	**ID.SC-1:** Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.	CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9
		ID.SC-2: Los proveedores y socios externos de los sistemas de información, componentes y servicios se identifican, se priorizan y se evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético.	COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del	COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05

		programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.	ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3 NIST SP 800-53 Rev. 4 SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.	COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 ISA 62443-2-1:2009 4.3.2.6.7 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Las pruebas y la planificación de respuesta y recuperación se llevan a cabo con proveedores.	CIS CSC 19, 20 COBIT 5 DSS04.04 ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
PROTEGER (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-1:** Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.	CIS CSC 1, 5, 15, 16 COBIT 5 DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.3.5.1 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Se gestiona y se protege el acceso físico a los activos.	COBIT 5 DSS01.04, DSS05.05 ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Se gestiona el	CIS CSC 12

		acceso remoto.	COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 ISA 62443-3-3:2013 SR 1.13, SR 2.6 ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1
		PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.	CIS CSC 3, 5, 12, 14, 15, 16, 18 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.7.3 ISA 62443-3-3:2013 SR 2.1 ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).	CIS CSC 9, 14, 15, 18 COBIT 5 DSS01.05, DSS05.02 ISA 62443-2-1:2009 4.3.3.4 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7
		PR.AC-6: Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.	CIS CSC, 16 COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 ISO/IEC 27001:2013, A.7.1.1, A.9.2.1 NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).	CIS CSC 1, 12, 15, 16 COBIT 5 DSS05.04, DSS05.10, DSS06.10 ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8,

			4.3.3.6.9
	Concienciación y capacitación (PR.AT): El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	**PR.AT-1:** Todos los usuarios están informados y capacitados.	CIS CSC 17, 18 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 NIST SP 800-53 Rev. 4 AT-2, PM-13
		PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.	CIS CSC 5, 17, 18 COBIT 5 APO07.02, DSS05.04, DSS06.03 ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.	CIS CSC 17 COBIT 5 APO07.03, APO07.06, APO10.04 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 NIST SP 800-53 Rev. 4 PS-7, SA-9, SA-16
		PR.AT-4: Los ejecutivos superiores comprenden sus roles y responsabilidades.	CIS CSC 17, 19 COBIT 5 EDM01.01, APO01.02, APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13
		PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.	CIS CSC 17 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
	Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de 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.	CIS CSC 13, 14 COBIT 5 APO01.06, BAI02.01, BAI06.01 ISA 62443-3-3:2013 SR 3.4, SR 4.1 ISO/IEC 27001:2013 A.8.2.3 NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28
		PR.DS-2: Los datos en tránsito están protegidos.	CIS CSC 13, 14 COBIT 5 APO01.06, DSS05.02, DSS06.06 ISA 62443-3-3:2013 SR 3.1, SR 3.8 ISO/IEC 27001:2013 A.8.2.3, A.13.1.1 A.13.2.3, A.14.1.2, A.14.1.3 NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12
		PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.	CIS CSC 1 COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1 A.8.3.3, A.11.2.5, A.11.2.7

			NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad.	CIS CSC 1, 2, 13 COBIT 5 APO13.01, BAI04.04 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.12.1.3, A.17.2.1 NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
		PR.DS-5: Se implementan protecciones contra las filtraciones de datos.	CIS CSC 13 COBIT 5 APO01.06, DSS05.04, DSS05.07 ISA 62443-3-3:2013 SR 5.2 ISO/IEC 27001:2013 A.6.1.2, A.7.1.1
		PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.	CIS CSC 2, 3 COBIT 5 APO01.06, BAI06.01, DSS06.02 ISA 62443-3-3:2013 SR 3.1, SR 3.3 ISO/IEC 27001:2013 A.12.2.1, A.12.5.1 NIST SP 800-53 Rev. 4 SC-16, SI-7
		PR.DS-7: Los entornos de desarrollo y prueba(s) están separados del entorno de producción.	CIS CSC 18, 20 COBIT 5 BAI03.08, BAI07.04 ISO/IEC 27001:2013 A.12.1.4 NIST SP 800-53 Rev. 4 CM-2
		PR.DS-8: Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware.	COBIT 5 BAI03.05 ISA 62443-2-1:2009 4.3.4.4.4 ISO/IEC 27001:2013 A.11.2.4 NIST SP 800-53 Rev. 4 SA-10, SI-7
	Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-1:** Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).	CIS CSC 3, 9, 11 COBIT 5 BAI10.01, BAI10.02, BAI10.03 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6
		PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.	CIS CSC 18 COBIT 5 APO13.01, BAI03.01, BAI03.02 ISA 62443-2-1:2009 4.3.4.3.3
		PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.	CIS CSC 3, 11 COBIT 5 BAI01.06, BAI06.01 ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 ISA 62443-3-3:2013 SR 7.6 ISO/IEC 27001:2013 A.12.1.2
		PR.IP-4: Se realizan, se	CIS CSC 10

		mantienen y se prueban CIS CSC 10 copias de seguridad de la información.	COBIT 5 APO13.01, DSS01.01, DSS04.07 ISA 62443-2-1:2009 4.3.4.3.9 ISA 62443-3-3:2013 SR 7.3, SR 7.4 ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
		PR.IP-5: Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.	ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2 ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 NIST SP 800-53 Rev. 4 PE-10, PE-12
		PR.IP-6: Los datos son eliminados de acuerdo con las políticas.	ISA 62443-2-1:2009 4.3.4.4.4 ISA 62443-3-3:2013 SR 4.2 ISO/IEC 27001:2013 A.8.2.3, A.8.3.1 NIST SP 800-53 Rev. 4 MP-6
		PR.IP-7: Se mejoran los procesos de protección.	COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2 ISO/IEC 27001:2013 A.16.1.6, Cláusula 9 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2
		PR.IP-8: Se comparte la efectividad de las tecnologías de protección.	COBIT 5 BAI08.04, DSS03.04 ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
		PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).	CIS CSC 19 COBIT 5 APO12.06, DSS04.03 ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.1, A.17.1.1
		PR.IP-10: Se prueban los planes de respuesta y recuperación.	CIS CSC 19, 20 COBIT 5 DSS04.04 ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.17.1.3 NIST SP 800-53 Rev. 4 CP-4, IR-3, PM-14
		PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal).	CIS CSC 5, 16 COBIT 5 APO07.01, APO07.02, APO07.03 ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2 ISO/IEC 27001:2013 A.7.1.1, A.7.1.2 NIST SP 800-53 Rev. 4 PS-1, PS-2, PS-3

		PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.	CIS CSC 4, 18, 20 COBIT 5 BAI03.10, DSS05.01, DSS05.02 ISO/IEC 27001:2013 A.12.6.1, A.14.2.3 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
	Mantenimiento (PR.MA): El mantenimiento y la reparación de los componentes del sistema de información y del control industrial se realizan de acuerdo con las políticas y los procedimientos.	**PR.MA-1:** El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas.	COBIT 5 BAI03.10, BAI09.02, BAI09.03 ISA 62443-2-1:2009 4.3.3.3.7 ISO/IEC 27001:2013 A.11.1.2, A.11.2.4 NIST SP 800-53 Rev. 4 MA-2, MA-3
		PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.	CIS CSC 3, 5 COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.6.5 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1 NIST SP 800-53 Rev. 4 MA-4
	Tecnología de protección (PR.PT): Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-1:** Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.	CIS CSC 1, 3, 5, 6, 14, 15, 16 COBIT 5 APO11.04, BAI03.05, DSS05.04 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8 ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10
		PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.	CIS CSC 8, 13 COBIT 5 APO13.01, DSS05.02, DSS05.06 ISA 62443-3-3:2013 SR 2.3 ISO/IEC 27001:2013 A.8.2.1, A.8.2.2
		PR.PT-3: Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.	CIS CSC 3, 11, 14 COBIT 5 DSS05.02, DSS05.05, DSS06.06 ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2
		PR.PT-4: Las redes de comunicaciones y control están protegidas.	CIS CSC 8, 12, 15 COBIT 5 DSS05.02, APO13.01 ISA 62443-3-3:2013 SR 3.1, SR 3.5 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1
		PR.PT-5: Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o "hot swap") para lograr los requisitos de resiliencia en situaciones normales y adversas.	COBIT 5 BAI04.01, BAI04.02, BAI04.03 ISA 62443-2-1:2009 4.3.2.5.2 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.17.1.2, A.17.2.1

			NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11
DETECTAR (DE)	**Anomalías y Eventos (DE.AE):** se detecta actividad anómala y se comprende el impacto potencial de los eventos.	**DE.AE-1:** Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.	CIS CSC 1, 4, 6, 12, 13, 15, 16 COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 ISO/IEC 27001:2013 A.12.1.1, A.12.1.2 NIST SP 800-53 Rev. 4 AC-4, CA-3
		DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.	CIS CSC 3, 6, 13, 15 COBIT 5 DSS05.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7 ISA 62443-3-3:2013 SR 2.8, SR 2.9 ISO/IEC 27001:2013 A.12.4.1, A.16.1.1 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4
		DE.AE-3: Cos datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.	CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14 COBIT 5 BAI08.02 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1, A.16.1.7 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4
		DE.AE-4: Se determina el impacto de los eventos.	CIS CSC 4, 6 COBIT 5 APO12.06, DSS03.01 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3
		DE.AE-5: Se establecen umbrales de alerta de incidentes.	CIS CSC 6, 19 COBIT 5 APO12.06, DSS03.01 ISA 62443-2-1:2009 4.2.3.10 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
	Monitoreo Continuo de la Seguridad (DE.CM): El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia	**DE.CM-1:** Se monitorea la red para detectar posibles eventos de seguridad cibernética.	CIS CSC 1, 7, 8, 12, 13, 15, 16 COBIT 5 DSS01.03, DSS03.05, DSS05.07 ISA 62443-3-3:2013 SR 6.2 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7
		DE.CM-2: Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.	COBIT 5 DSS01.04, DSS01.05 ISA 62443-2-1:2009 4.3.3.3.8 ISO/IEC 27001:2013 A.11.1.1, A.11.1.2 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6
		DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.	CIS CSC 5, 7, 14, 16 COBIT 5 DSS05.07 ISA 62443-3-3:2013 SR 6.2 ISO/IEC 27001:2013 A.12.4.1, A.12.4.3 NIST SP 800-53 Rev. 4 AC-2, AU-12
		DE.CM-4: Se detecta el código malicioso.	CIS CSC 4, 7, 8, 12 COBIT 5 DSS05.01 ISA 62443-2-1:2009 4.3.4.3.8 ISA 62443-3-3:2013 SR 3.2

			ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3, SI-8
		DE.CM-5: Se detecta el código móvil no autorizado.	CIS CSC 7, 8 COBIT 5 DSS05.01 ISA 62443-3-3:2013 SR 2.4 ISO/IEC 27001:2013 A.12.5.1, A.12.6.2 NIST SP 800-53 Rev. 4 SC-18, SI-4, SC-44
		DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.	COBIT 5 APO07.06, APO10.05 ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4
		DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.	CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16 COBIT 5 DSS05.02, DSS05.05 ISO/IEC 27001:2013 A.12.4.1, A.14.2.7 NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3
		DE.CM-8: Se realizan escaneos de vulnerabilidades.	COBIT 5 BAI03.10, DSS05.01 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-5
	Procesos de Detección (DE.DP): Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.	**DE.DP-1:** Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.	CIS CSC 19 COBIT 5 APO01.02, DSS05.01, DSS06.03 ISA 62443-2-1:2009 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
		DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.	COBIT 5 DSS06.01, MEA03.03, MEA03.04 ISA 62443-2-1:2009 4.4.3.2 ISO/IEC 27001:2013 A.18.1.4, A.18.2.2 NIST SP 800-53 Rev. 4 AC-25, CA-2, CA-7
		DE.DP-3: Se prueban los procesos de detección.	COBIT 5 APO13.02, DSS05.02 ISA 62443-2-1:2009 4.4.3.2 ISA 62443-3-3:2013 SR 3.3 ISO/IEC 27001:2013 A.14.2.8 NIST SP 800-53 Rev. 4 CA-2, CA-7
		DE.DP-4: Se comunica la información de la detección de eventos.	CIS CSC 19 COBIT 5 APO08.04, APO12.06, DSS02.05 ISA 62443-2-1:2009 4.3.4.5.9 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.16.1.2, A.16.1.3 NIST SP 800-53 Rev. 4 AU-6, CA-2
		DE.DP-5: los procesos de detección se mejoran continuamente.	COBIT 5 APO11.06, APO12.06, DSS04.05 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6

			NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2
RESPONDER (RS)	**Planificación de la Respuesta (RS.RP):** Los procesos y procedimientos de respuesta se ejecutan y se mantienen a fin de garantizar la respuesta a los incidentes de seguridad cibernética detectados.	**RS.RP-1:** El plan de respuesta se ejecuta durante o después de un incidente.	CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10
	Comunicaciones (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley).	**RS.CO-1:** El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.	CIS CSC 19 COBIT 5 EDM03.02, APO01.02, APO12.03 ISA 62443-2-1:2009 4.3.4.5.2 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, CP-3
		RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.	CIS CSC 19 COBIT 5 DSS01.03 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8
		RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.	CIS CSC 19 COBIT 5 DSS03.04 ISA 62443-2-1:2009 4.3.4.5.2 ISO/IEC 27001:2013 A.16.1.2 16.1.2 NIST SP 800-53 Rev. 4 CA-2, CA-7
		RS.CO-4: La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.	CIS CSC 19 COBIT 5 DSS03.04 ISA 62443-2-1:2009 4.3.4.5.5 ISO/IEC 27001:2013 Cláusula 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.CO-5: El intercambio voluntario de información se produce con las partes interesadas externas para lograr una mayor conciencia situacional de seguridad cibernética.	CIS CSC 19 COBIT 5 BAI08.04 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15
	Análisis (RS.AN): Se lleva a cabo el análisis para garantizar una respuesta eficaz y apoyar las actividades de recuperación.	**RS.AN-1**: Se investigan las notificaciones de los sistemas de detección.	CIS CSC 4, 6, 8, 19 COBIT 5 DSS02.04, DSS02.07 ISA 62443-2-1:2009 4.3.4.5.6 ISA 62443-3-3:2013 SR 6.1 ISO/IEC 27001:2013 A.12.4.1 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4
		RS.AN-2: Se comprende el	COBIT 5 DSS02.02

		impacto del incidente.	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7 ISO/IEC 27001:2013 A.16.1.4, A.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4
		RS.AN-3: Se realizan análisis forenses.	COBIT 5 APO12.06, DSS03.02, DSS05.07 ISA 62443-3-3:2013 SR 2.8, SR 2.9 2.11, SR 2.12, SR 3.9, SR 6.1 ISO/IEC 27001:2013 A.16.1.7 NIST SP 800-53 Rev. 4 AU-7, IR-4
		RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta.	CIS CSC 19 COBIT 5 DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6 ISO/IEC 27001:2013 A.16.1.4 NIST SP 800-53 Rev. 4 CP-2, IR-4
		RS.AN-5: Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad).	CIS CSC 4, 19 COBIT 5 EDM03.02, DSS05.07 NIST SP 800-53 Rev. 4 SI-5, PM-15
	Mitigación (RS.MI): Se realizan actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.	**RS.MI-1:** Los incidentes son contenidos.	CIS CSC 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6 ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5
		RS.MI-2: Los incidentes son mitigados.	CIS CSC 4, 19 COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4
		RS.MI-3: Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.	CIS CSC 4 COBIT 5 APO12.06 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
	Mejoras (RS.IM): Las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección y	**RS.IM-1:** Los planes de respuesta incorporan las lecciones aprendidas.	COBIT 5 BAI01.13 ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Cláusula 10

	respuesta actuales y previas.		NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.IM-2: Se actualizan las estrategias de respuesta.	COBIT 5 BAI01.13, DSS04.08 ISO/IEC 27001:2013 A.16.1.6, Cláusula 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
RECUPERAR (RC)	**Planificación de la recuperación (RC.RP):** Los procesos y procedimientos de recuperación se ejecutan y se mantienen para asegurar la restauración de los sistemas o activos afectados por incidentes de seguridad cibernética.	**RC.RP-1:** El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	CIS CSC 10 COBIT 5 APO12.06, DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
	Mejoras (RC.IM): La planificación y los procesos de recuperación se mejoran al incorporar en las actividades futuras las lecciones aprendidas.	**RC.IM-1:** Los planes de recuperación incorporan las lecciones aprendidas.	COBIT 5 APO12.06, BAI05.07, DSS04.08 ISA 62443-2-1:2009 4.4.3.4 ISO/IEC 27001:2013 A.16.1.6, Cláusula 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.IM-2: Se actualizan las estrategias de recuperación.	COBIT 5 APO12.06, BAI07.08 ISO/IEC 27001:2013 A.16.1.6, Cláusula 10 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
	Comunicaciones (RC.CO): Las actividades de restauración se coordinan con partes internas y externas (por ejemplo, centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores).	**RC.CO-1:** Se gestionan las relaciones públicas.	COBIT 5 EDM03.02 ISO/IEC 27001:2013 A.6.1.4, Cláusula 7.4
		RC.CO-2: La reputación se repara después de un incidente.	COBIT 5 MEA03.02 ISO/IEC 27001:2013 Cláusula 7.4
		RC.CO-3: Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.	COBIT 5 APO12.06 ISO/IEC 27001:2013 Cláusula 7.4 NIST SP 800-53 Rev. 4 CP-2, IR-4

En base a las funciones, categorías y subcategorías anteriores, se propone utilizar 20 Controles críticos de seguridad (CCS) NIST.

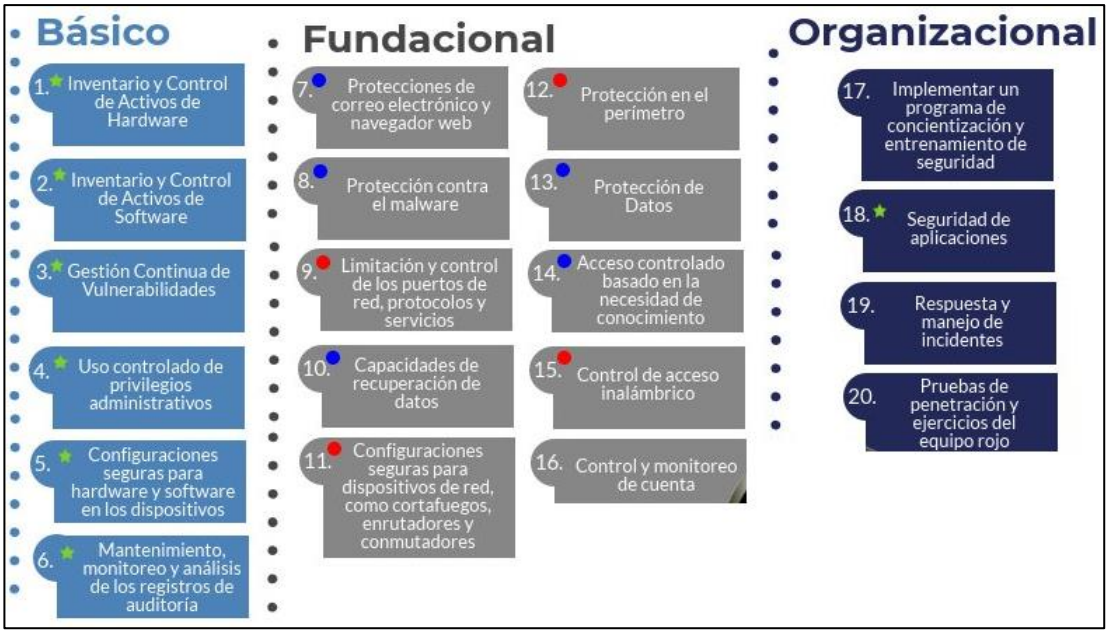


Figura 72: 20 controles críticos de seguridad

Para ello, se propone utilizar la siguiente matriz como guía:

Tabla 6. Controles Críticos de seguridad propuestos - CIS

Control CIS	Subcontrol CIS	Tipo de activo	Función de seguridad	Título	Descripción
1				**Inventario y control de activos de hardware** ***Administre activamente (inventario, seguimiento y corrección) todos los dispositivos de hardware en la red para que solo los dispositivos autorizados tengan acceso, y se encuentren dispositivos no autorizados y no administrados y se les impida acceder.***	
1	1.1	Dispositivos	Identificar	Utilice una herramienta de descubrimiento activo	Utilice una herramienta de descubrimiento activa para identificar dispositivos conectados a la red de la organización y actualizar el inventario de activos de hardware.
1	1.2	Dispositivos	Identificar	Utilice una herramienta pasiva de descubrimiento de activos	Utilice una herramienta de descubrimiento pasivo para identificar dispositivos conectados a la red de la organización y actualice automáticamente el inventario de activos de hardware de la organización.
1	1.3	Dispositivos	Identificar	Utilice el registro de DHCP para actualizar el inventario de activos	Utilice el registro del Protocolo de configuración dinámica de host (DHCP) en todos los servidores DHCP o herramientas de administración de direcciones IP para actualizar el inventario de activos de hardware de la organización.
1	1.4	Dispositivos	Identificar	Mantener inventario de activos detallado	Mantenga un inventario preciso y actualizado de todos los activos tecnológicos con el potencial de almacenar o procesar información. Este inventario debe incluir todos los activos de hardware, estén o no conectados a la red de la organización.
1	1.5	Dispositivos	Identificar	Mantener información de inventario de activos	Asegúrese de que el inventario de activos de hardware registre la dirección de red, la dirección de hardware, el nombre de la máquina, el propietario del activo de datos y el departamento para cada activo y si el activo de hardware ha sido aprobado para conectarse a la red.
1	1.6	Dispositivos	Responder	Abordar los activos no autorizados	Asegúrese de que los activos no autorizados se eliminen de la red, se pongan en cuarentena o que el inventario se actualice de manera oportuna.

1	1.7	Dispositivos	Proteger	Implementar control de acceso a nivel de puerto	Utilice el control de acceso a nivel de puerto, siguiendo los estándares 802.1x, para controlar qué dispositivos pueden autenticarse en la red. El sistema de autenticación se vinculará a los datos del inventario de activos de hardware para garantizar que solo los dispositivos autorizados puedan conectarse a la red.
1	1.8	Dispositivos	Proteger	Utilice certificados de cliente para autenticar activos de hardware	Use certificados de cliente para autenticar activos de hardware que se conectan a la red confiable de la organización.
2				**Inventario y control de activos de software** **Administre activamente (inventario, seguimiento y corrección) todo el software en la red para que solo el software autorizado esté instalado y pueda ejecutarse, y que el software no autorizado y no administrado se encuentre y se evite su instalación o ejecución.**	
2	2.1	Aplicaciones	Identificar	Mantener inventario de software autorizado	Mantenga una lista actualizada de todo el software autorizado que se requiere en la empresa para cualquier propósito comercial en cualquier sistema comercial.
2	2.2	Aplicaciones	Identificar	Asegúrese de que el software sea compatible con el proveedor	Asegúrese de que solo se agreguen al inventario de software autorizado de la organización las aplicaciones de software o los sistemas operativos actualmente admitidos y que reciben actualizaciones de proveedores. El software no compatible debe etiquetarse como no compatible en el sistema de inventario.
2	2.3	Aplicaciones	Identificar	Utilizar herramientas de inventario de software	Utilice herramientas de inventario de software en toda la organización para automatizar la documentación de todo el software en los sistemas empresariales.
2	2.4	Aplicaciones	Identificar	Seguimiento de la información del inventario de software	El sistema de inventario de software debe rastrear el nombre, la versión, el editor y la fecha de instalación de todo el software, incluidos los sistemas operativos autorizados por la organización.
2	2.5	Aplicaciones	Identificar	Integrar inventarios de activos de software y hardware	El sistema de inventario de software debe estar vinculado al inventario de activos de hardware para que todos los dispositivos y el software asociado se rastreen desde una única ubicación.
2	2.6	Aplicaciones	Responder	Abordar el software no aprobado	Asegúrese de que el software no autorizado se elimine o que el inventario se actualice de manera oportuna
2	2.7	Aplicaciones	Proteger	Utilizar la lista blanca de aplicaciones	Utilice la tecnología de listas blancas de aplicaciones en todos los activos para garantizar que solo se ejecute el software autorizado y que se bloquee la ejecución de todo el software no autorizado en los activos.

2	2.8	Aplicaciones	Proteger	Implemente la lista blanca de aplicaciones de las bibliotecas	El software de la lista blanca de aplicaciones de la organización debe garantizar que solo las bibliotecas de software autorizadas (como * .dll, * .ocx, * .so, etc.) puedan cargarse en un proceso del sistema.
2	2.9	Aplicaciones	Proteger	Implemente la lista blanca de scripts de la aplicación	El software de la lista blanca de aplicaciones de la organización debe garantizar que solo los scripts autorizados y firmados digitalmente (como * .ps1, * .py, macros, etc.) puedan ejecutarse en un sistema.
2	2.10	Aplicaciones	Proteger	Segregar física o lógicamente aplicaciones de alto riesgo	Los sistemas segregados física o lógicamente deben usarse para aislar y ejecutar el software que se requiere para las operaciones comerciales pero que conlleva un mayor riesgo para la organización.
3				**Gestión continua de vulnerabilidades** ***Adquiera, evalúe y tome medidas continuamente sobre nueva información para identificar vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes.***	
3	3.1	Aplicaciones	Detectar	Ejecutar herramientas de escaneo de vulnerabilidades automatizadas	Utilice una herramienta actualizada de escaneo de vulnerabilidades que cumpla con el Protocolo de Automatización de Contenido de Seguridad (SCAP) para escanear automáticamente todos los sistemas en la red semanalmente o con mayor frecuencia para identificar todas las vulnerabilidades potenciales en los sistemas de la organización.
3	3.2	Aplicaciones	Detectar	Realizar escaneo de vulnerabilidad autenticada	Realice un análisis de vulnerabilidad autenticado con agentes que se ejecutan localmente en cada sistema o con escáneres remotos que estén configurados con derechos elevados en el sistema que se está probando.
3	3.3	Los usuarios	Proteger	Proteger cuentas de evaluación dedicadas	Use una cuenta dedicada para escaneos de vulnerabilidad autenticados, que no deben usarse para ninguna otra actividad administrativa y deben estar vinculados a máquinas específicas en direcciones IP específicas.
3	3.4	Aplicaciones	Proteger	Implementar herramientas de administración de parches del sistema operativo automatizado	Implemente herramientas de actualización de software automatizadas para garantizar que los sistemas operativos ejecuten las actualizaciones de seguridad más recientes proporcionadas por el proveedor de software.

3	3.5	Aplicaciones	Proteger	Implementar herramientas automatizadas de administración de parches de software	Implemente herramientas de actualización de software automatizadas para garantizar que el software de terceros en todos los sistemas ejecute las actualizaciones de seguridad más recientes proporcionadas por el proveedor de software.
3	3.6	Aplicaciones	Responder	Comparar análisis de vulnerabilidades consecutivos	Compare regularmente los resultados de los análisis de vulnerabilidades consecutivos para verificar que las vulnerabilidades se hayan corregido de manera oportuna.
3	3.7	Aplicaciones	Responder	Utilizar un proceso de calificación de riesgo	Utilice un proceso de calificación de riesgo para priorizar la reparación de vulnerabilidades descubiertas.
4				**Uso controlado de privilegios administrativos** ***Los procesos y herramientas utilizados para rastrear / controlar / prevenir / corregir el uso, asignación y configuración de privilegios administrativos en computadoras, redes y aplicaciones.***	
4	4.1	Los usuarios	Detectar	Mantener inventario de cuentas administrativas	Use herramientas automatizadas para hacer un inventario de todas las cuentas administrativas, incluidas las cuentas de dominio y locales, para garantizar que solo las personas autorizadas tengan privilegios elevados.
4	4.2	Los usuarios	Proteger	Cambiar contraseñas predeterminadas	Antes de implementar cualquier nuevo activo, cambie todas las contraseñas predeterminadas para que tengan valores consistentes con las cuentas de nivel administrativo.
4	4.3	Los usuarios	Proteger	Garantizar el uso de cuentas administrativas dedicadas	Asegúrese de que todos los usuarios con acceso de cuenta administrativa utilicen una cuenta dedicada o secundaria para actividades elevadas. Esta cuenta solo debe usarse para actividades administrativas y no para navegar por Internet, correo electrónico o actividades similares.
4	4.4	Los usuarios	Proteger	Use contraseñas únicas	Cuando no se admite la autenticación Multifactor (como las cuentas de administrador local, raíz o servicio), las cuentas utilizarán contraseñas exclusivas de ese sistema.
4	4.5	Los usuarios	Proteger	Utilice la autenticación Multifactor para todo el acceso administrativo	Use autenticación Multifactor y canales encriptados para todo el acceso a la cuenta administrativa.

4	4.6	Los usuarios	Proteger	Use estaciones de trabajo dedicadas para todas las tareas administrativas	Asegúrese de que los administradores usen una máquina dedicada para todas las tareas administrativas o tareas que requieren acceso administrativo. Esta máquina estará segmentada de la red principal de la organización y no se permitirá el acceso a Internet. Esta máquina no se utilizará para leer correos electrónicos, redactar documentos o navegar por Internet.
4	4.7	Los usuarios	Proteger	Limite el acceso a las herramientas de script	Limite el acceso a las herramientas de secuencias de comandos (como Microsoft® PowerShell y Python) solo a usuarios administrativos o de desarrollo con la necesidad de acceder a esas capacidades.
4	4.8	Los usuarios	Detectar	Registro y alerta sobre cambios en la membresía del grupo administrativo	Configure los sistemas para emitir una entrada de registro y una alerta cuando se agregue o elimine una cuenta de cualquier grupo con privilegios administrativos asignados.
4	4.9	Los usuarios	Detectar	Registro y alerta sobre inicio de sesión de cuenta administrativa fallido	Configure los sistemas para emitir una entrada de registro y alertar sobre inicios de sesión fallidos en una cuenta administrativa.
5				**Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores** ***Establezca, implemente y administre activamente (rastree, informe, corrija) la configuración de seguridad de dispositivos móviles, computadoras portátiles, servidores y estaciones de trabajo utilizando una gestión de configuración rigurosa y un proceso de control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.***	
5	5.1	Aplicaciones	Proteger	Establecer configuraciones seguras	Mantenga estándares de configuración de seguridad documentados para todos los sistemas operativos y software autorizados.
5	5.2	Aplicaciones	Proteger	Mantener imágenes seguras	Mantenga imágenes o plantillas seguras para todos los sistemas de la empresa según los estándares de configuración aprobados por la organización. Cualquier despliegue de sistema nuevo o sistema existente que se vea comprometido debe tomarse una imagen usando una de esas imágenes o plantillas.
5	5.3	Aplicaciones	Proteger	Almacene de forma segura imágenes maestras	Almacene las imágenes maestras y las plantillas en servidores configurados de forma segura, validados con herramientas de monitoreo de integridad, para garantizar que solo sean posibles los cambios autorizados a las imágenes.

5	5.4	Aplicaciones	Proteger	Implementar herramientas de administración de configuración del sistema	Implemente herramientas de administración de configuración del sistema que impondrán y volverán a implementar automáticamente los ajustes de configuración en los sistemas a intervalos regulares programados.
5	5.5	Aplicaciones	Detectar	Implemente sistemas automatizados de monitoreo de configuración	Utilice un sistema de monitoreo de configuración que cumpla con el Protocolo de Automatización de Contenido de Seguridad (SCAP) para verificar todos los elementos de configuración de seguridad, excepciones aprobadas por catálogo y alertar cuando ocurran cambios no autorizados.
6				**Mantenimiento, monitoreo y análisis de registros de auditoría** ***Recopile, administre y analice registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.***	
6	6.1	Red	Detectar	Utilice tres fuentes de tiempo sincronizadas	Utilice al menos tres fuentes de tiempo sincronizadas de las que todos los servidores y dispositivos de red recuperen información de tiempo de manera regular para que las marcas de tiempo en los registros sean consistentes.
6	6.2	Red	Detectar	Activar registro de auditoría	Asegúrese de que el registro local se haya habilitado en todos los sistemas y dispositivos de red.
6	6.3	Red	Detectar	Habilitar registro detallado	Habilite el registro del sistema para incluir información detallada, como un origen de eventos, fecha, usuario, marca de tiempo, direcciones de origen, direcciones de destino y otros elementos útiles.
6	6.4	Red	Detectar	Garantizar un almacenamiento adecuado para los registros	Asegúrese de que todos los sistemas que almacenan registros tengan espacio de almacenamiento adecuado para los registros generados.
6	6.5	Red	Detectar	Administración central de registros	Asegúrese de que los registros apropiados se agreguen a un sistema central de administración de registros para su análisis y revisión.
6	6.6	Red	Detectar	Implementar SIEM o herramientas analíticas de registro	Implemente información de seguridad y gestión de eventos (SIEM) o herramienta analítica de registros para la correlación y análisis de registros.
6	6.7	Red	Detectar	Revise regularmente los registros	Regularmente, revise los registros para identificar anomalías o eventos anormales.

6	6.8	Red	Detectar	Sintonice regularmente SIEM	Regularmente, ajuste su sistema SIEM para identificar mejor los eventos procesables y disminuir el ruido de los eventos.
7				**Protecciones de correo electrónico y navegador web** ***Minimice la superficie de ataque y las oportunidades para que los atacantes manipulen el comportamiento humano a través de su interacción con los navegadores web y los sistemas de correo electrónico.***	
7	7.1	Aplicaciones	Proteger	Asegure el uso de solo navegadores y clientes de correo electrónico totalmente compatibles	Asegúrese de que solo los navegadores web y los clientes de correo electrónico totalmente compatibles puedan ejecutarse en la organización, idealmente solo con la última versión de los navegadores y clientes de correo electrónico proporcionados por el proveedor.
7	7.2	Aplicaciones	Proteger	Deshabilite los navegadores innecesarios o no autorizados o los complementos del cliente de correo electrónico	Desinstale o deshabilite cualquier navegador no autorizado o complementos de clientes de correo electrónico o aplicaciones complementarias.
7	7.3	Aplicaciones	Proteger	Limite el uso de lenguajes de secuencias de comandos en navegadores web y clientes de correo electrónico	Asegúrese de que solo los lenguajes de secuencias de comandos autorizados puedan ejecutarse en todos los navegadores web y clientes de correo electrónico.
7	7.4	Red	Proteger	Mantener y aplicar filtros de URL basados en red	Aplicar filtros de URL basados en la red que limitan la capacidad de un sistema para conectarse a sitios web no aprobados por la organización. Este filtrado se aplicará para cada uno de los sistemas de la organización, ya sea que estén físicamente en las instalaciones de una organización o no.
7	7.5	Red	Proteger	Suscríbase al servicio de categorización de URL	Suscríbase a los servicios de categorización de URL para asegurarse de que estén actualizados con las definiciones de categoría de sitio web más recientes disponibles. Los sitios no categorizados se bloquearán por defecto.
7	7.6	Red	Detectar	Registrar todo solicitante de URL	Registre todas las solicitudes de URL de cada uno de los sistemas de la organización, ya sea en el sitio o en un dispositivo móvil, para identificar actividades potencialmente maliciosas y ayudar a los manejadores de incidentes a identificar sistemas potencialmente comprometidos.

7	7.7	Red	Proteger	Uso de servicios de filtrado de DNS	Utilice los servicios de filtrado del Sistema de nombres de dominio (DNS) para ayudar a bloquear el acceso a dominios maliciosos conocidos.
7	7.8	Red	Proteger	Implemente DMARC y habilite la verificación del lado del receptor	Para reducir la posibilidad de correos electrónicos falsificados o modificados de dominios válidos, implemente la política y verificación de autenticación, informes y conformidad de mensajes (DMARC) basada en el dominio, comenzando por la implementación del Marco de Políticas del Remitente (SPF) y los estándares de Correo Identificado de DomainKeys (DKIM).
7	7.9	Red	Proteger	Bloquear tipos de archivos innecesarios	Bloquee todos los archivos adjuntos de correo electrónico que ingresen a la puerta de enlace de correo electrónico de la organización si los tipos de archivos no son necesarios para el negocio de la organización.
7	7.10	Red	Proteger	Sandbox Todos los archivos adjuntos de correo electrónico	Use Sandboxing para analizar y bloquear archivos adjuntos de correo electrónico entrante con comportamiento malicioso.
8				**Defensas de malware** ***Controle la instalación, difusión y ejecución de código malicioso en múltiples puntos de la empresa, mientras optimiza el uso de la automatización para permitir la actualización rápida de defensa, recopilación de datos y acciones correctivas.***	
8	8.1	Dispositivos	Proteger	Utilice software antimalware administrado centralmente	Utilice un software antimalware administrado centralmente para monitorear y defender continuamente cada una de las estaciones de trabajo y servidores de la organización.
8	8.2	Dispositivos	Proteger	Asegúrese de que el software y las firmas antimalware se actualicen	Asegúrese de que el software antimalware de la organización actualice su motor de escaneo y su base de datos de firmas de manera regular.
8	8.3	Dispositivos	Proteger	Habilite las características de lucha contra la explotación del sistema operativo / Implemente tecnologías de lucha contra la explotación	Habilite las funciones contra la explotación, como la Prevención de ejecución de datos (DEP) o la Aleatorización del diseño del espacio de direcciones (ASLR) que están disponibles en un sistema operativo o implemente los juegos de herramientas adecuados que se pueden configurar para aplicar protección a un conjunto más amplio de aplicaciones y ejecutables.
8	8.4	Dispositivos	Detectar	Configurar el escaneo antimalware de dispositivos extraíbles	Configure los dispositivos para que realicen automáticamente un análisis antimalware de los medios extraíbles cuando se insertan o conectan.

8	8.5	Dispositivos	Proteger	Configurar dispositivos para no ejecutar automáticamente el contenido	Configure dispositivos para que no se ejecuten automáticamente contenidos desde medios extraíbles.
8	8.6	Dispositivos	Detectar	Centralice el registro antimalware	Envíe todos los eventos de detección de malware a las herramientas de administración antimalware de la empresa y a los servidores de registro de eventos para su análisis y alertas.
8	8.7	Red	Detectar	Habilitar el registro de consultas DNS	Habilite el registro de consultas del Sistema de nombres de dominio (DNS) para detectar búsquedas de nombres de host para dominios maliciosos conocidos.
8	8.8	Dispositivos	Detectar	Habilitar el registro de auditoría de línea de comandos	Habilite el registro de auditoría de línea de comandos para shells de comandos, como Microsoft PowerShell y Bash.
9				**Limitación y control de puertos de red, protocolos y servicios** ***Administre (rastree / controle / corrija) el uso operativo continuo de puertos, protocolos y servicios en dispositivos en red para minimizar las ventanas de vulnerabilidad disponibles para los atacantes.***	
9	9.1	Dispositivos	Identificar	Asociar puertos activos, servicios y protocolos al inventario de activos	Asociar puertos activos, servicios y protocolos a los activos de hardware en el inventario de activos.
9	9.2	Dispositivos	Proteger	Asegúrese de que solo se ejecuten los puertos, protocolos y servicios aprobados	Asegúrese de que solo los puertos de red, protocolos y servicios que escuchan en un sistema con necesidades comerciales validadas se ejecuten en cada sistema.
9	9.3	Dispositivos	Detectar	Realizar escaneos automáticos regulares de puertos	Realice escaneos automáticos de puertos de forma regular en todos los sistemas y avise si se detectan puertos no autorizados en un sistema.
9	9.4	Dispositivos	Proteger	Aplicar firewalls basados en host o filtrado de puertos	Aplique firewalls basados en host o herramientas de filtrado de puertos en los sistemas finales, con una regla de denegación predeterminada que elimina todo el tráfico, excepto aquellos servicios y puertos que están explícitamente permitidos.
9	9.5	Dispositivos	Proteger	Implementar firewalls de aplicaciones	Coloque firewalls de aplicaciones frente a cualquier servidor crítico para verificar y validar el tráfico que va al servidor. Cualquier tráfico no autorizado debe ser bloqueado y registrado.

10				**Capacidades de recuperación de datos** ***Los procesos y herramientas utilizados para realizar una copia de seguridad adecuada de la información crítica con una metodología probada para la recuperación oportuna de la misma.***	
10	10.1	Datos	Proteger	Garantizar copias de seguridad automatizadas regulares	Asegúrese de que todos los datos del sistema se respalden automáticamente de forma regular.
10	10.2	Datos	Proteger	Realizar copias de seguridad completas del sistema	Asegúrese de que todos los sistemas clave de la organización estén respaldados como un sistema completo, a través de procesos como la creación de imágenes, para permitir la recuperación rápida de un sistema completo.
10	10.3	Datos	Proteger	Probar datos en medios de respaldo	
10	10.4	Datos	Proteger	Proteger copias de seguridad	Asegúrese de que las copias de seguridad estén protegidas adecuadamente mediante seguridad física o cifrado cuando se almacenan, así como cuando se mueven a través de la red. Esto incluye copias de seguridad remotas y servicios en la nube.
10	10.5	Datos	Proteger	Asegúrese de que todas las copias de seguridad tengan al menos un destino de copia de seguridad sin conexión	Asegúrese de que todas las copias de seguridad tengan al menos un destino de copia de seguridad fuera de línea (es decir, no accesible a través de una conexión de red).
11				**Configuración segura para dispositivos de red, como firewalls, enrutadores y conmutadores** ***Establezca, implemente y administre activamente (rastree, informe, corrija) la configuración de seguridad de los dispositivos de infraestructura de red utilizando una gestión de configuración rigurosa y un proceso de control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.***	
11	11.1	Red	Identificar	Mantener configuraciones de seguridad estándar para dispositivos de red	Mantenga estándares de configuración de seguridad documentados para todos los dispositivos de red autorizados.

11	11.2	Red	Identificar	Reglas de configuración del tráfico de documentos	Todas las reglas de configuración que permiten que el tráfico fluya a través de los dispositivos de red deben documentarse en un sistema de administración de configuración con un motivo comercial específico para cada regla, el nombre de un individuo específico responsable de esa necesidad comercial y una duración esperada de la necesidad.
11	11.3	Red	Detectar	Use herramientas automatizadas para verificar configuraciones de dispositivos estándar y detectar cambios	Compare todas las configuraciones de dispositivos de red con las configuraciones de seguridad aprobadas definidas para cada dispositivo de red en uso, y avise cuando se descubran desviaciones.
11	11.4	Red	Proteger	Instale la última versión estable de cualquier actualización relacionada con la seguridad en todos los dispositivos de red	Instale la última versión estable de cualquier actualización relacionada con la seguridad en todos los dispositivos de red.
11	11.5	Red	Proteger	Administre dispositivos de red utilizando autenticación multifactor y sesiones cifradas	Administre todos los dispositivos de red utilizando autenticación multifactor y sesiones cifradas.
11	11.6	Red	Proteger	Use máquinas dedicadas para todas las tareas administrativas de red	Asegúrese de que los ingenieros de red usen una máquina dedicada para todas las tareas administrativas o tareas que requieren acceso elevado. Esta máquina debe estar segmentada de la red principal de la organización y no se debe permitir el acceso a Internet. Esta máquina no debe usarse para leer correos electrónicos, redactar documentos o navegar por Internet.
11	11.7	Red	Proteger	Administre la infraestructura de red a través de una red dedicada	Administre la infraestructura de red a través de conexiones de red que están separadas del uso comercial de esa red, confiando en VLAN separadas o, preferiblemente, en conectividad física completamente diferente para sesiones de administración para dispositivos de red.
12				**Defensa de límites** ***Detectar / prevenir / corregir el flujo de información que transfiere redes de diferentes niveles de confianza con un enfoque en datos que dañan la seguridad.***	
12	12.1	Red	Identificar	Mantener un inventario de los límites de la red	Mantenga un inventario actualizado de todos los límites de la red de la organización.

12	12.2	Red	Detectar	Busque conexiones no autorizadas a través de límites de red confiables	Realice exploraciones periódicas desde fuera de cada límite de red confiable para detectar cualquier conexión no autorizada a la que se pueda acceder a través del límite.
12	12.3	Red	Proteger	Denegar comunicaciones con direcciones IP maliciosas conocidas	Denegar las comunicaciones con direcciones IP de Internet maliciosas o no utilizadas conocidas y limitar el acceso solo a los rangos de direcciones IP confiables y necesarios en cada uno de los límites de la red de la organización.
12	12.4	Red	Proteger	Denegar la comunicación a través de puertos no autorizados	Denegar la comunicación a través de puertos TCP o UDP no autorizados o tráfico de aplicaciones para garantizar que solo los protocolos autorizados puedan cruzar el límite de la red dentro o fuera de la red en cada uno de los límites de la red de la organización.
12	12.5	Red	Detectar	Configurar sistemas de monitoreo para grabar paquetes de red	Configure sistemas de monitoreo para registrar los paquetes de red que pasan por el límite en cada uno de los límites de la red de la organización.
12	12.6	Red	Detectar	Implemente sensores IDS basados en red	Implemente sensores de sistemas de detección de intrusiones (IDS) basados en la red para buscar mecanismos de ataque inusuales y detectar el compromiso de estos sistemas en cada uno de los límites de la red de la organización.
12	12.7	Red	Proteger	Implementar sistemas de prevención de intrusiones basados en la red	Implemente sistemas de prevención de intrusiones (IPS) basados en la red para bloquear el tráfico de red malicioso en cada uno de los límites de la red de la organización.
12	12.8	Red	Detectar	Implemente la colección NetFlow en dispositivos de límite de red	Habilite la recopilación de NetFlow y los datos de registro en todos los dispositivos de límite de red.
12	12.9	Red	Detectar	Implemente el servidor proxy de filtrado de la capa de aplicación	Asegúrese de que todo el tráfico de red hacia o desde Internet pase a través de un proxy de capa de aplicación autenticado que esté configurado para filtrar conexiones no autorizadas.
12	12.10	Red	Detectar	Descifrar el tráfico de red en proxy	Descifre todo el tráfico de red cifrado en el proxy de límite antes de analizar el contenido. Sin embargo, la organización puede usar listas blancas de sitios permitidos a los que se puede acceder a través del proxy sin descifrar el tráfico.

12	12.11	Los usuarios	Proteger	Requerir que todos los inicios de sesión remotos utilicen la autenticación multifactor	Requerir todo el acceso de inicio de sesión remoto a la red de la organización para cifrar los datos en tránsito y utilizar la autenticación multifactor.
12	12.12	Dispositivos	Proteger	Administre todos los dispositivos de forma remota iniciando sesión en la red interna	Escanee todos los dispositivos empresariales iniciando sesión de forma remota en la red de la organización antes de acceder a la red para asegurarse de que cada una de las políticas de seguridad de la organización se haya aplicado de la misma manera que los dispositivos de red locales.
13				**Protección de Datos** ***Los procesos y herramientas utilizados para evitar la filtración de datos, mitigar los efectos de los datos filtrados y garantizar la privacidad e integridad de la información confidencial.***	
13	13.1	Datos	Identificar	Mantener un inventario de información confidencial	Mantenga un inventario de toda la información confidencial almacenada, procesada o transmitida por los sistemas tecnológicos de la organización, incluidos los ubicados en el sitio o en un proveedor de servicios remotos.
13	13.2	Datos	Proteger	Eliminar datos confidenciales o sistemas a los que la organización no accede regularmente	Elimine de la red los datos o sistemas confidenciales a los que la organización no accede regularmente. Estos sistemas solo se utilizarán como sistemas independientes (desconectados de la red) por la unidad de negocios que necesita usar ocasionalmente el sistema o completamente virtualizado y apagado hasta que sea necesario.
13	13.3	Datos	Detectar	Monitoree y bloquee el tráfico de red no autorizado	Implemente una herramienta automatizada en los perímetros de la red que supervisa la transferencia no autorizada de información confidencial y bloquea dichas transferencias mientras alerta a los profesionales de seguridad de la información.
13	13.4	Datos	Proteger	Solo permitir el acceso a proveedores autorizados de almacenamiento en la nube o correo electrónico	Solo permita el acceso a proveedores autorizados de almacenamiento en la nube o correo electrónico.
13	13.5	Datos	Detectar	Monitoree y detecte cualquier uso no autorizado de cifrado	Monitoree todo el tráfico que sale de la organización y detecte cualquier uso no autorizado de cifrado.
13	13.6	Datos	Proteger	Cifrar datos del dispositivo móvil	Utilice mecanismos criptográficos aprobados para proteger los datos empresariales almacenados en todos los dispositivos móviles.

13	13.7	Datos	Proteger	Administrar dispositivos USB	Si se requieren dispositivos de almacenamiento USB, se debe utilizar un software empresarial que pueda configurar sistemas para permitir el uso de dispositivos específicos. Se debe mantener un inventario de dichos dispositivos.
13	13.8	Datos	Proteger	Administre las configuraciones de lectura / escritura de los medios extraíbles externos del sistema	Configure los sistemas para que no escriban datos en medios extraíbles externos, si no hay necesidad comercial de admitir dichos dispositivos.
13	13.9	Datos	Proteger	Cifrar datos en dispositivos de almacenamiento USB	Si se requieren dispositivos de almacenamiento USB, todos los datos almacenados en dichos dispositivos deben cifrarse mientras están en reposo.
14				**Acceso controlado basado en la necesidad de saber** ***Los procesos y herramientas utilizados para rastrear / controlar / prevenir / corregir el acceso seguro a activos críticos (por ejemplo, información, recursos, sistemas) de acuerdo con la determinación formal de qué personas, computadoras y aplicaciones tienen la necesidad y el derecho de acceder a estos activos críticos basado en una clasificación aprobada.***	
14	14.1	Red	Proteger	Segmente la red según la sensibilidad	Segmente la red según la etiqueta o el nivel de clasificación de la información almacenada en los servidores, ubique toda la información confidencial en redes de área local virtuales (VLAN) separadas
14	14.2	Red	Proteger	Habilitar el filtrado de firewall entre VLAN	Habilite el filtrado de firewall entre las VLAN para garantizar que solo los sistemas autorizados puedan comunicarse con otros sistemas necesarios para cumplir con sus responsabilidades específicas.
14	14.3	Red	Proteger	Deshabilitar comunicación de estación de trabajo a estación de trabajo	Desactive todas las comunicaciones de estación de trabajo a estación de trabajo para limitar la capacidad de un atacante de moverse lateralmente y comprometer los sistemas vecinos, a través de tecnologías como VLAN privadas o micro segmentación.
14	14.4	Datos	Proteger	Cifre toda la información confidencial en tránsito	Cifre toda la información confidencial en tránsito.
14	14.5	Datos	Detectar	Utilice una herramienta de descubrimiento activo para identificar datos confidenciales	Utilice una herramienta de descubrimiento activa para identificar toda la información confidencial almacenada, procesada o transmitida por los sistemas de tecnología de la organización, incluidos los ubicados en el sitio o en un proveedor de servicios remotos, y actualice el inventario de información confidencial de la organización.

14	14.6	Datos	Proteger	Proteja la información a través de listas de control de acceso	Proteja toda la información almacenada en los sistemas con listas de control de acceso específicas del sistema de archivos, redes compartidas, reclamos, aplicaciones o bases de datos. Estos controles harán cumplir el principio de que solo las personas autorizadas deben tener acceso a la información en función de su necesidad de acceder a la información como parte de sus responsabilidades.
14	14.7	Datos	Proteger	Hacer cumplir el control de acceso a los datos a través de herramientas automatizadas	Utilice una herramienta automatizada, como la prevención de pérdida de datos basada en el host, para imponer controles de acceso a los datos, incluso cuando los datos se copian de un sistema.
14	14.8	Datos	Proteger	Cifrar información confidencial en reposo	Cifre toda la información confidencial en reposo utilizando una herramienta que requiere un mecanismo de autenticación secundario no integrado en el sistema operativo, para acceder a la información.
14	14.9	Datos	Detectar	Hacer cumplir el registro detallado para acceso o cambios a datos confidenciales	Aplicar registros de auditoría detallados para acceder a datos confidenciales o cambios a datos confidenciales (utilizando herramientas como Monitoreo de integridad de archivos o Monitoreo de eventos e información de seguridad).
15				**Control de acceso inalámbrico** ***Los procesos y herramientas utilizados para rastrear / controlar / prevenir / corregir el uso de seguridad de las redes de área local inalámbricas (WLAN), puntos de acceso y sistemas de clientes inalámbricos.***	
15	15.1	Red	Identificar	Mantener un inventario de puntos de acceso inalámbrico autorizados	Mantenga un inventario de puntos de acceso inalámbrico autorizados conectados a la red cableada.
15	15.2	Red	Detectar	Detectar puntos de acceso inalámbrico conectados a la red cableada	Configure las herramientas de escaneo de vulnerabilidades de red para detectar y alertar sobre puntos de acceso inalámbrico no autorizados conectados a la red cableada.
15	15.3	Red	Detectar	Use un sistema inalámbrico de detección de intrusiones	Use un sistema inalámbrico de detección de intrusos (WIDS) para detectar y alertar sobre puntos de acceso inalámbrico no autorizados conectados a la red.
15	15.4	Dispositivos	Proteger	Deshabilite el acceso inalámbrico en dispositivos si no es necesario	Inhabilite el acceso inalámbrico en dispositivos que no tienen un propósito comercial para el acceso inalámbrico.

15	15.5	Dispositivos	Proteger	Limite el acceso inalámbrico en dispositivos cliente	Configure el acceso inalámbrico en máquinas cliente que tienen un propósito comercial inalámbrico esencial, para permitir el acceso solo a redes inalámbricas autorizadas y restringir el acceso a otras redes inalámbricas.
15	15.6	Dispositivos	Proteger	Deshabilite las capacidades de red inalámbrica punto a punto en clientes inalámbricos	Deshabilite las capacidades de red inalámbrica punto a punto (ad hoc) en clientes inalámbricos.
15	15.7	Red	Proteger	Aproveche el Estándar de cifrado avanzado (AES) para cifrar datos inalámbricos	Aproveche el Estándar de cifrado avanzado (AES) para cifrar datos inalámbricos en tránsito.
15	15.8	Red	Proteger	Use protocolos de autenticación inalámbricos que requieren autenticación mutua y de múltiples factores	Asegúrese de que las redes inalámbricas utilicen protocolos de autenticación como el Protocolo de autenticación extensible-Seguridad de la capa de transporte (EAP / TLS), que requiere autenticación mutua y de múltiples factores.
15	15.9	Dispositivos	Proteger	Deshabilitar acceso periférico inalámbrico de dispositivos	Deshabilite el acceso periférico inalámbrico de dispositivos [como Bluetooth y Near Field Communication (NFC)], a menos que dicho acceso sea necesario para fines comerciales.
15	15.10	Red	Proteger	Cree una red inalámbrica separada para dispositivos personales y no confiables	Cree una red inalámbrica separada para dispositivos personales o no confiables. El acceso empresarial desde esta red debe tratarse como no confiable y filtrado y auditado en consecuencia.
16				**Monitoreo y control de cuentas** ***Administre activamente el ciclo de vida de las cuentas de sistemas y aplicaciones (su creación, uso, latencia, eliminación) para minimizar las oportunidades para que los atacantes las aprovechen.***	
16	16.1	Los usuarios	Identificar	Mantener un inventario de sistemas de autenticación	Mantenga un inventario de cada uno de los sistemas de autenticación de la organización, incluidos los ubicados en el sitio o en un proveedor de servicios remotos.
16	16.2	Los usuarios	Proteger	Configurar punto centralizado de autenticación	Configure el acceso para todas las cuentas a través de la menor cantidad posible de puntos centralizados de autenticación, incluida la red, la seguridad y los sistemas en la nube.
16	16.3	Los usuarios	Proteger	Requerir autenticación multifactor	Requerir autenticación de múltiples factores para todas las cuentas de usuario, en todos los sistemas, ya sea administrado en el sitio o por un proveedor externo.

16	16.4	Los usuarios	Proteger	Cifrar o Hash todas las credenciales de autenticación	Cifre o mezcle con sal todas las credenciales de autenticación cuando esté almacenado.
16	16.5	Los usuarios	Proteger	Cifrar la transmisión del nombre de usuario y las credenciales de autenticación	Asegúrese de que todos los nombres de usuario y las credenciales de autenticación de la cuenta se transmitan a través de redes que utilizan canales cifrados.
16	16.6	Los usuarios	Identificar	Mantener un inventario de cuentas	Mantener un inventario de todas las cuentas organizadas por sistema de autenticación.
16	16.7	Los usuarios	Proteger	Establecer un proceso para revocar el acceso	Establezca y siga un proceso automatizado para revocar el acceso al sistema deshabilitando las cuentas inmediatamente después de la terminación o cambio de responsabilidades de un empleado o contratista. Deshabilitar estas cuentas, en lugar de eliminar cuentas, permite preservar las pistas de auditoría.
16	16.8	Los usuarios	Responder	Deshabilitar cualquier cuenta no asociada	Deshabilite cualquier cuenta que no pueda asociarse con un proceso comercial o propietario de la empresa.
16	16.9	Los usuarios	Responder	Deshabilitar cuentas inactivas	Deshabilita automáticamente las cuentas inactivas después de un período establecido de inactividad.
16	16.10	Los usuarios	Proteger	Asegúrese de que todas las cuentas tengan una fecha de vencimiento	Asegúrese de que todas las cuentas tengan una fecha de vencimiento que se controle y aplique.
16	16.11	Los usuarios	Proteger	Bloquear sesiones de estación de trabajo después de inactividad	Bloquee automáticamente las sesiones de la estación de trabajo después de un período estándar de inactividad.
16	16.12	Los usuarios	Detectar	Supervisar los intentos de acceder a cuentas desactivadas	Supervise los intentos de acceder a cuentas desactivadas a través del registro de auditoría.
16	16.13	Los usuarios	Detectar	Alerta en la cuenta Desviación del comportamiento de inicio de sesión	Alerta cuando los usuarios se desvían del comportamiento normal de inicio de sesión, como la hora del día, la ubicación de la estación de trabajo y la duración.
17				**Implementar un programa de concientización y capacitación sobre seguridad**	

				Para todos los roles funcionales en la organización (priorizando a aquellos críticos para la empresa y su seguridad), identifique los conocimientos, habilidades y capacidades específicas necesarias para apoyar la defensa de la empresa; desarrollar y ejecutar un plan integrado para evaluar, identificar brechas y remediar a través de políticas, planificación organizacional, capacitación y programas de concientización.	
17	17,1	N / A	N / A	Realizar un análisis de brecha de habilidades	Realice un análisis de brecha de habilidades para comprender las habilidades y comportamientos a los que los miembros de la fuerza laboral no se adhieren, utilizando esta información para construir una hoja de ruta educativa de referencia.
17	17,2	N / A	N / A	Entregar entrenamiento para llenar la brecha de habilidades	Brinde capacitación para abordar la brecha de habilidades identificada para impactar positivamente el comportamiento de seguridad de los miembros de la fuerza laboral.
17	17.3	N / A	N / A	Implementar un programa de concientización de seguridad	Cree un programa de concientización de seguridad para que todos los miembros de la fuerza laboral lo completen regularmente para asegurarse de que comprenden y exhiben los comportamientos y habilidades necesarios para ayudar a garantizar la seguridad de la organización. El programa de concientización sobre seguridad de la organización debe comunicarse de manera continua y atractiva.
17	17.4	N / A	N / A	Actualice el contenido de conciencia con frecuencia	Asegúrese de que el programa de conciencia de seguridad de la organización se actualice con frecuencia (al menos una vez al año) para abordar las nuevas tecnologías, amenazas, estándares y requisitos comerciales.
17	17,5	N / A	N / A	Capacitar a la fuerza laboral en la autenticación segura	Capacite a los miembros de la fuerza laboral sobre la importancia de habilitar y utilizar la autenticación segura.
17	17,6	N / A	N / A	Capacitar a la fuerza laboral en la identificación de ataques de ingeniería social	Capacite a la fuerza laboral sobre cómo identificar diferentes formas de ataques de ingeniería social, como phishing, estafas telefónicas y llamadas de suplantación.
17	17,7	N / A	N / A	Capacitar a la fuerza laboral en el manejo de datos confidenciales	Capacite a los miembros de la fuerza laboral sobre cómo identificar y almacenar, transferir, archivar y destruir adecuadamente la información confidencial.
17	17,8	N / A	N / A	Capacitar a la fuerza laboral sobre las causas de la exposición involuntaria de datos	Capacite a los miembros de la fuerza laboral para que sean conscientes de las causas de la exposición involuntaria de datos, como la pérdida de sus dispositivos móviles o el envío de correos electrónicos a la persona incorrecta debido al autocompletado en el correo electrónico.

17	17,9	N / A	N / A	Capacitar a los miembros de la fuerza laboral en la identificación y notificación de incidentes	Capacite a los miembros de la fuerza laboral para que puedan identificar los indicadores más comunes de un incidente y puedan informar dicho incidente.
18				**Seguridad del software de aplicación** ***Administre el ciclo de vida de seguridad de todo el software desarrollado y adquirido internamente para prevenir, detectar y corregir las debilidades de seguridad.***	
18	18,1	N / A	N / A	Establecer prácticas de codificación seguras	Establezca prácticas de codificación seguras apropiadas para el lenguaje de programación y el entorno de desarrollo que se utiliza.
18	18,2	N / A	N / A	Asegúrese de que se realice una comprobación explícita de errores para todo el software desarrollado internamente	Para el software desarrollado internamente, asegúrese de que la verificación explícita de errores se realice y documente para todas las entradas, incluido el tamaño, el tipo de datos y los rangos o formatos aceptables.
18	18,3	N / A	N / A	Verifique que el software adquirido aún sea compatible	Verifique que la versión de todo el software adquirido fuera de su organización aún sea compatible con el desarrollador o se haya reforzado adecuadamente según las recomendaciones de seguridad del desarrollador.
18	18,4	N / A	N / A	Utilice solo componentes de terceros actualizados y confiables	Utilice únicamente componentes de terceros actualizados y confiables para el software desarrollado por la organización.
18	18,5	N / A	N / A	Utilice solo algoritmos de cifrado estandarizados y ampliamente revisados	Utilice solo algoritmos de cifrado estandarizados, actualmente aceptados y ampliamente revisados.
18	18,6	N / A	N / A	Asegúrese de que el personal de desarrollo de software esté capacitado en codificación segura	Asegúrese de que todo el personal de desarrollo de software reciba capacitación para escribir código seguro para su entorno de desarrollo específico y sus responsabilidades.
18	18,7	N / A	N / A	Aplicar herramientas de análisis de código estático y dinámico	Aplique herramientas de análisis estático y dinámico para verificar que se cumplan las prácticas de codificación segura para el software desarrollado internamente.
18	18,8	N / A	N / A	Establecer un proceso para aceptar y abordar informes de vulnerabilidades de software	Establezca un proceso para aceptar y abordar informes de vulnerabilidades de software, incluido el suministro de un medio para que entidades externas se comuniquen con su grupo de seguridad.

18	18,9	N / A	N / A	Sistemas separados de producción y no producción	Mantener entornos separados para sistemas de producción y no producción. Los desarrolladores no deberían tener acceso sin supervisión a los entornos de producción.
18	18.10	N / A	N / A	Implementar firewalls de aplicaciones web	Proteja las aplicaciones web mediante la implementación de firewalls de aplicaciones web (WAF) que inspeccionan todo el tráfico que fluye a la aplicación web para detectar ataques comunes de aplicaciones web. Para las aplicaciones que no están basadas en la web, se deben implementar firewalls de aplicaciones específicos si tales herramientas están disponibles para el tipo de aplicación dado. Si el tráfico está encriptado, el dispositivo debe estar detrás del encriptado o ser capaz de desencriptar el tráfico antes del análisis. Si ninguna de las opciones es apropiada, se debe implementar un firewall de aplicación web basado en host.
18	18.11	N / A	N / A	Use plantillas de configuración de endurecimiento estándar para bases de datos	Para aplicaciones que dependen de una base de datos, use plantillas de configuración de refuerzo estándar. Todos los sistemas que forman parte de los procesos críticos del negocio también deben ser probados.
19				**Respuesta a incidentes y gestión** ***Proteja la información de la organización, así como su reputación, desarrollando e implementando una infraestructura de respuesta a incidentes (p. Ej., Planes, roles definidos, capacitación, comunicaciones, supervisión administrativa) para descubrir rápidamente un ataque y luego contener el daño de manera efectiva, erradicando la presencia del atacante. y restaurar la integridad de la red y los sistemas.***	
19	19,1	N / A	N / A	Documentar los procedimientos de respuesta a incidentes	Asegúrese de que haya planes escritos de respuesta a incidentes que definan los roles del personal, así como las fases de manejo / gestión de incidentes.
19	19,2	N / A	N / A	Asignar títulos de trabajo y deberes para la respuesta a incidentes	Asigne títulos de trabajo y deberes para manejar incidentes informáticos y de red a individuos específicos, y garantice el seguimiento y la documentación durante todo el incidente a través de la resolución.
19	19,3	N / A	N / A	Designar personal de administración para apoyar el manejo de incidentes	Designe personal de gestión, así como copias de seguridad, que apoyarán el proceso de manejo de incidentes actuando en roles clave de toma de decisiones.
19	19,4	N / A	N / A	Diseñar estándares para toda la organización para informar incidentes	Diseñe estándares para toda la organización durante el tiempo requerido para que los administradores de sistemas y otros miembros de la fuerza laboral informen los eventos anómalos al equipo de manejo de incidentes, los mecanismos para dichos informes y el tipo de información que debe incluirse en la notificación del incidente.

19	19,5	N / A	N / A	Mantener información de contacto para informar incidentes de seguridad	Reúna y mantenga información sobre información de contacto de terceros que se utilizará para informar un incidente de seguridad, como la aplicación de la ley, los departamentos gubernamentales pertinentes, los proveedores y los socios del Centro de Análisis e Intercambio de Información (ISAC).
19	19,6	N / A	N / A	Publicar información sobre informes de anomalías e incidentes informáticos	Publique información para todos los miembros de la fuerza laboral, con respecto a la notificación de anomalías e incidentes informáticos, al equipo de manejo de incidentes. Dicha información debe incluirse en actividades rutinarias de concientización de los empleados.
19	19,7	N / A	N / A	Realizar sesiones periódicas de escenarios de incidentes para el personal	Planifique y realice incidentes de rutina, ejercicios de respuesta y escenarios para la fuerza laboral involucrada en la respuesta al incidente para mantener la conciencia y la comodidad en la respuesta a amenazas del mundo real. Los ejercicios deben probar los canales de comunicación, la toma de decisiones y las capacidades técnicas de los respondedores de incidentes utilizando herramientas y datos disponibles para ellos.
19	19.8	N / A	N / A	Crear un esquema de puntuación de incidentes y priorización	Cree un esquema de clasificación de incidentes y priorización basado en el impacto conocido o potencial para su organización. Utilice la puntuación para definir la frecuencia de las actualizaciones de estado y los procedimientos de escalación.
20				**Pruebas de penetración y ejercicios del equipo rojo (Read Team)** ***Pruebe la fuerza general de la defensa de una organización (la tecnología, los procesos y las personas) simulando los objetivos y acciones de un atacante.***	
20	20,1	N / A	N / A	Establecer un programa de pruebas de penetración	Establezca un programa para pruebas de penetración que incluya un alcance completo de ataques combinados, como ataques inalámbricos, basados en el cliente y aplicaciones web.
20	20,2	N / A	N / A	Realizar pruebas regulares de penetración externa e interna	Realice pruebas de penetración internas y externas periódicas para identificar vulnerabilidades y vectores de ataque que puedan utilizarse para explotar con éxito los sistemas empresariales.
20	20,3	N / A	N / A	Realizar ejercicios periódicos del equipo rojo	Realice ejercicios periódicos del Equipo Rojo para evaluar la preparación de la organización para identificar y detener ataques o para responder de manera rápida y efectiva.

20	20,4	N / A	N / A	Incluir pruebas de presencia de información y artefactos del sistema desprotegido	Incluya pruebas para detectar la presencia de información del sistema desprotegido y artefactos que serían útiles para los atacantes, incluidos diagramas de red, archivos de configuración, informes de pruebas de penetración anteriores, correos electrónicos o documentos que contienen contraseñas u otra información crítica para el funcionamiento del sistema.
20	20,5	N / A	N / A	Crear banco de pruebas para elementos que normalmente no se prueban en producción	Cree un banco de pruebas que imite un entorno de producción para pruebas de penetración específicas y ataques del Equipo Rojo contra elementos que normalmente no se prueban en la producción, como los ataques contra el control de supervisión y la adquisición de datos y otros sistemas de control.
20	20,6	N / A	N / A	Utilice las herramientas de escaneo de vulnerabilidades y pruebas de penetración en concierto	Utilice las herramientas de escaneo de vulnerabilidades y pruebas de penetración en concierto. Los resultados de las evaluaciones de escaneo de vulnerabilidades deben usarse como punto de partida para guiar y enfocar los esfuerzos de prueba de penetración.
20	20,7	N / A	N / A	Asegúrese de que los resultados de la prueba de penetración estén documentados utilizando estándares abiertos y legibles por máquina	Siempre que sea posible, asegúrese de que los resultados del Equipo Rojo se documenten utilizando estándares abiertos y legibles por máquina (por ejemplo, SCAP). Diseñe un método de puntuación para determinar los resultados de los ejercicios del Equipo Rojo para que los resultados puedan compararse con el tiempo.
20	20,8	N / A	N / A	Controle y monitoree las cuentas asociadas con las pruebas de penetración	Cualquier cuenta de usuario o sistema utilizada para realizar pruebas de penetración debe controlarse y monitorearse para asegurarse de que solo se usen con fines legítimos, y se eliminen o restablezcan a su funcionamiento normal una vez finalizadas las pruebas.

V.4.4. Diseño de arquitectura de ciberseguridad

Basados en el modelo Zero Trust (confianza cero), proponemos que la arquitectura de ciberseguridad se base en lo siguiente:

- Garantizar el acceso seguro a todos los recursos independientemente de donde estén localizados (internet o intranet).
- Seguir una estrategia de mínimo privilegio y seguir una política estricta de control de acceso.
- Inspeccionar y registrar todo el tráfico (entrante y saliente) para validar la actividad en la red.
- Segmentar cada tráfico de red diferente en una VLAN diferente.
- Analizar el comportamiento de los usuarios una vez que accedieron a la red.

Figura 73: Base para el Diseño de arquitectura

Se propone definir perfiles de conexión, para identificar quién, cómo, dónde y a qué información se accede, independientemente de que un usuario se conecte por cable, wifi, vpn, intranet o internet.

Los perfiles que proponemos son los siguientes:

- **Perfil basado en dispositivo**
  - Smartphone
  - PC
  - Teléfono IP
  - Impresora
  - Cámaras IP
  - Etc.
- **Perfil basado en identidad**
  - Grupos de Active Directory
  - Certificado Digital
  - Usuario y Contraseña (Portal Cautivo)
  - Etc.

Podemos también unir estos dos tipos de perfiles para que los accesos sean lo más limitados posibles como por ejemplo: Podríamos crear una política para que cuando un usuario de Contabilidad se conecte internamente a la red a través de un switch o un Acces Point, tenga acceso únicamente a servicios específicos, siempre y cuando, se conecte de una PC marca HP y tenga como sistema operativo Windows 10 (entre otras características); y que además de eso, el usuario en mención, pertenezca también al grupo “contabilidad” de directorio activo. Una vez validada esta información, recién se le otorgara acceso al usuario.

Otro ejemplo de política que podríamos crear seria cuando un usuario ingrese desde internet a nuestra red corporativa a través de alguna VPN. En este caso, se podría validar previamente, que el equipo origen cuente con una solución antivirus, y esta se encuentre debidamente actualizada, que el equipo no tenga algún tipo de vulnerabilidad de nivel alto, o que el usuario pertenezca algún grupo específico. El acceso se otorgara una vez validado lo antes mencionado.

Todo esto lo fortalecemos con un correcto análisis del comportamiento del usuario conectado a la red.

Proponemos, que el enfoque Zero trust y la arquitectura de ciberseguridad, se base en soluciones tecnológicas que puedan integrarse entre sí, para garantizar acciones preventivas y proactivas; así como también, conseguir mayor visibilidad en toda la red

. De acuerdo a los perfiles propuestos líneas arriba, limitaremos los accesos al mínimo, basándonos en una solución de control de acceso a la red (NAC), una solución de autenticación segura y granular a través de VPN, una solución EDR y Firewalls de última generación. Todo ello lo integraremos a soluciones tipo CASB para protección de servicios en la nube y una solución tipo UEBA para análisis de comportamiento. Esto, sumado a las demás soluciones tecnológicas de seguridad, permitirán tener una arquitectura no solo robusta en cuanto a ciberseguridad; si no también, adaptables a los cambios actuales que implica la transformación digital y las nuevas amenazas que evolucionan constantemente.

Las soluciones tecnológicas que proponemos para nuestra arquitectura de seguridad son las siguientes:

1. CASB – Agente de seguridad de acceso a la nube
2. UEBA – Análisis de comportamiento del usuario
3. IPS /IDS – Sistemas de prevención y detección de intrusos
4. Firewalls perimetrales e internos
5. Seguridad a nivel de Endpoint – Antivirus, antimalware
6. EDR - Detección y respuesta de punto final
7. Escáner de Vulnerabilidad
8. WAF – Firewall de aplicaciones web
9. Proxy – Acceso seguro a internet
10. NAC – Control de Acceso a la red
11. Equipo para administración de identidad y acceso – VPN
12. Acces Point – Acceso inalámbrico
13. Servidor de actualización de parches de seguridad
14. Solución Antispam – Bloqueo de correo spam y maliciosos
15. Solución SandBox – Equipo virtual para detección de malware
16. HoneyPot – Sistema señuelo para ataques informáticos

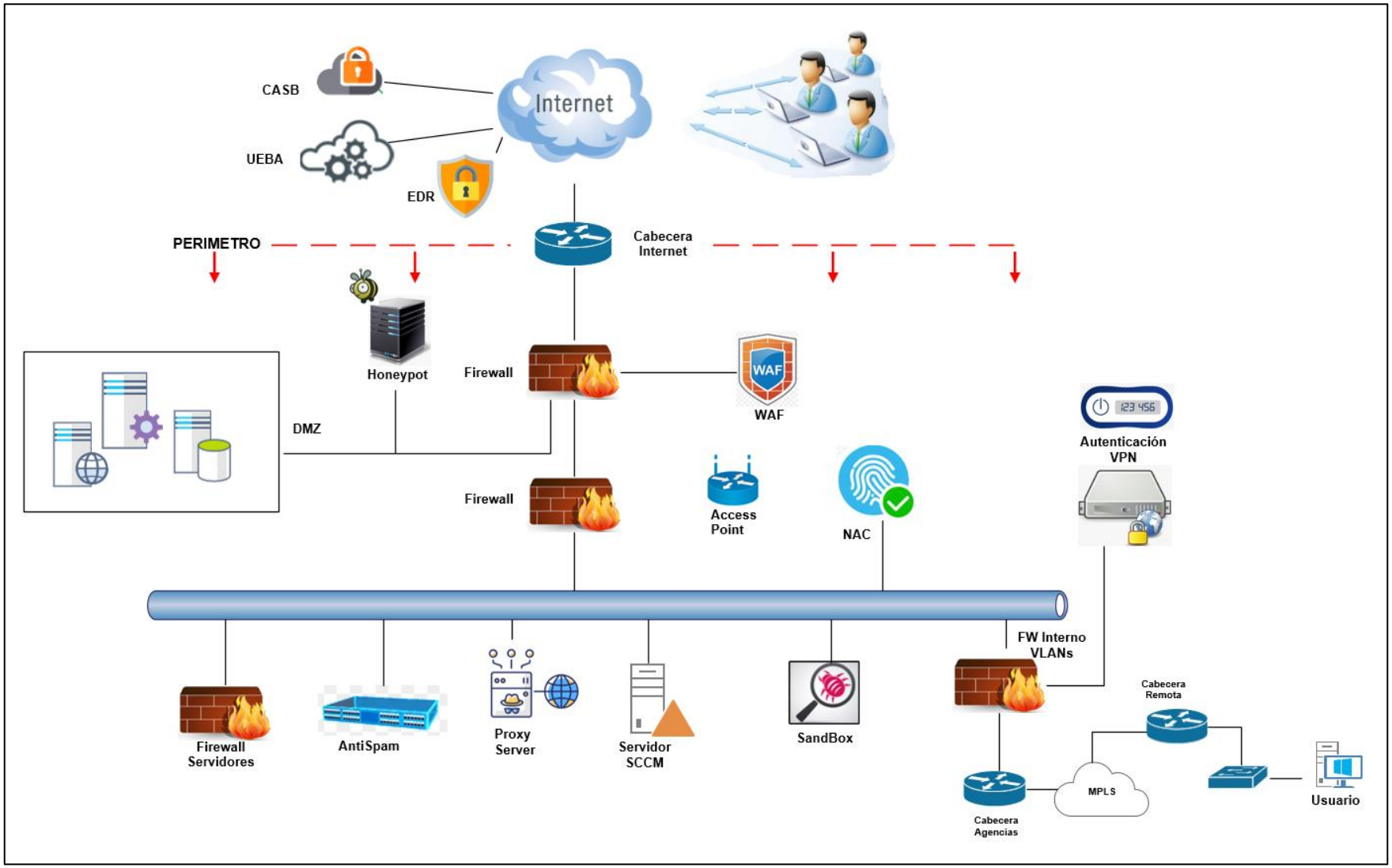


Figura 74. Diseño de Arquitectura de ciberseguridad propuesto

V.4.5. Cultura en ciberseguridad

Estoy convencido que nada de lo arriba mencionado tendrá éxito si no se aborda de manera responsable y activa, el tema de capacitación continua para lograr una cultura robusta y continúa en ciberseguridad.

Podemos implantar los mejores antivirus, cortafuegos y otras herramientas de seguridad a nuestro alcance para mejorar la ciberseguridad de nuestra empresa. Podemos establecer políticas internas para tener copias de seguridad y para configurar y administrar nuestros sistemas de forma segura. Pero, estas herramientas y políticas no serán muy útiles si los empleados no siguen una serie de buenas prácticas. Si no están atentos y no conocen qué puede pasar, podrán cometer errores que deriven en incidentes o los delincuentes encontrarán la forma de engañarlos para atacar a nuestra empresa.

Para esto proponemos (adicional a lo descrito en el control CIS N° 17) lo siguiente:

- **Advertir a los trabajadores.**
  La mayoría no estudia las metodologías que se emplean en los ciberataques. Necesitan conocer que la amenaza existe y que ellos suelen ser un objetivo predilecto para los Ciberdelincuentes.

- **Comunicar las expectativas.**
  Desde el primer día de trabajo, los empleados han de comprender que la empresa necesita que ejerzan cierto nivel de vigilancia frente a posibles ciberamenazas. En ese sentido es importante que los empleados comprendan que pueden estar en situación de riesgo tanto en su casa como en la oficina, y que sus acciones pueden marcar la diferencia en materia de seguridad al margen de dónde estén trabajando. Se propone que dentro de los temas de capacitación durante la inducción de un nuevo colaborador, se incluyan de manera primordial temas de ciberseguridad.

- **Entrenamiento y evaluación**

Implementando programas de formación para concienciar a la plantilla en materia de ciberseguridad y mantener a los empleados informados y al tanto. Las empresas pueden realizar incluso un ejercicio de "simulacro" haciendo que un empleado o todo un equipo sean víctimas de un ataque orquestado por el departamento de TI o por un servicio contratado externamente.

Este podría adoptar la forma de un ataque de suplantación de identidad mediante el envío de un correo electrónico. A posteriori, el equipo debería revisar conjuntamente lo sucedido y aprender la lección correspondiente. Esta clase de entrenamiento en materia de seguridad podría continuar a lo largo del año, extendiéndose en la organización a todos los niveles e incluyendo partes específicas adecuadas al trabajo de cada departamento.

- **Crear un plan formal**

  Se debe desarrollar un programa formal de entrenamiento en materia de ciberseguridad debidamente documentado, y actualizarlo con frecuencia para incluir en él información sobre nuevos vectores de ataque y otros riesgos.

- **Señalar la importancia que tiene la seguridad tanto en el trabajo como en casa**

  Los expertos en TI más experimentados deben ayudar a los trabajadores a comprender la importancia de la "ciber-higiene" tanto en el trabajo como en casa. Una cuestión que tiene cada vez mayor relevancia debido al aumento de la interconectividad entre herramientas empresariales y su manejo por medio de dispositivos móviles manuales.

- **Nombrar a personas encargadas de mantener la ciberseguridad.**

  Se debe designar a un encargado de ciberseguridad en cada departamento. Podría recibir más formación y ayudar a los CTO y

CIO a mantener a los empleados bien preparados y motivados. ¿Por qué emplear los recursos TI sólo al servicio del equipo de TI?

- **Conseguir el compromiso de la dirección.**
  Se debe informar a la alta dirección y al comité de ciberseguridad sobre las ramificaciones que puede tener una posible brecha de seguridad y solicitar su opinión sobre el plan de ciberseguridad.

- **Recompensar a los empleados.**
  Reconozca y recompense a los usuarios que identifiquen correos electrónicos maliciosos y comparta sus historias sobre cómo los descubrieron y lo que hicieron. Igualmente, empatice con los usuarios que cometen errores, pero asegúrese de que sepan qué hacer en el futuro.

V.4.6. Plan de Acción

- **Responsables del proyecto:** Se definieron los responsables de las diferentes actividades a realizar dentro de las 4 etapas de la propuesta.

Tabla 7: Responsables del proyecto

Fuente: Elaboración propia

N°	ETAPA / FASE	RESPONSABLE
	ETAPA 1: CONTEXTO ORGANIZACIONAL	
	CONTEXTO ORGANIZACIONAL	
1	Definir el flujo de información y de toma de decisiones sobre la base de una estructura piramidal a través de la creación de tres niveles: Estratégico, Operacional y táctico que soporte el modelo y la gestión de ciberseguridad.	Departamento de procesos y calidad, Gerencia central, consultor
2	Creación del "Comité de ciberseguridad", el cual se encargará de asesorar a la alta dirección en el análisis y la definición de la Política General de Ciberseguridad; proponer acciones para superar las brechas encontradas; evaluar la correcta implementación y funcionamiento del marco de ciberseguridad; entre otras.	Departamento de procesos y calidad, RRHH

3	Reestructurar el departamento de seguridad de la información, creando las siguientes secciones que dependerán directamente del oficial de seguridad: sección de Seguridad de la información, sección de continuidad del negocio y sección de ciberseguridad.	Departamento de procesos y calidad, RRHH, Dpto. Seguridad de la información, Gerencia de Riesgos
4	Creación del área "Seguridad Informática", dentro del departamento de T.I. que se encargue directamente de todas las actividades relacionadas a la ciberseguridad.	Departamento de procesos y calidad, RRHH, Gerencia de TI
5	Creación del Equipo de Respuesta ante Incidentes Informáticos, CERT que involucrara a todas las áreas relacionadas con la ciberseguridad y el riesgo cibernético. Se activara en coordinación con el comité de ciberseguridad para atender incidentes presentados y tomar acción inmediata sobre ellos.	Departamento de procesos y calidad, Gerencia TI, Gerencia Riesgos
ETAPA 2: MARCO DE CIBERSEGURIDAD		
	PASO 1: PRIORIZACION Y ALCANCE	
6	Identificar objetivos empresariales de alto nivel para la toma de decisiones estratégicas con respecto a las implementaciones de ciberseguridad.	Gerencia Central, Gerencia Riesgos, Gerencia TI
7	Determinar el alcance de los sistemas y activos que respaldan el proceso de negocio; y que se reforzaran con el diseño piramidal de niveles estratégico, operacional y táctico.	Procesos y calidad, Dpto. Seguridad de la información. Dpto. TI, consultor
8	Definir el nivel de implementación del marco, de acuerdo a las prácticas de ciberseguridad y riesgo actuales.	Gerencia Riesgos, Gerencia TI, consultor
	PASO 2: ORIENTACION	
9	Identificar los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general.	Dpto. Seguridad de la información, Seguridad informática
10	Identificar las amenazas y vulnerabilidades que afectan los activos.	Dpto. Seguridad de la información, Seguridad informática
	PASO 3: PERFIL ACTUAL	
11	Identificar los resultados de las categorías y sub categorías del marco NIST logrados actualmente.	Dpto. Seguridad de la información
12	Crear un perfil actual en base al análisis anterior.	Dpto. Seguridad de la información, consultor
	PASO 4: EVALUACION DE RIESGOS	
13	Realizar un análisis de riesgos tomando como base la matriz de riesgos y el análisis de impacto y probabilidad actuales; con el objetivo de fortalecer y no reemplazar lo ya trabajado.	Gerencia de riesgos
	PASO 5 : PERFIL OBJETIVO	
14	Crear un perfil objetivo basado en el análisis de resultados de categorías y subcategorías del marco, y en los objetivos de ciberseguridad deseados por la organización.	Dpto. Seguridad de la información, seguridad informática, consultor
	PASO 6 : BRECHAS EXISTENTES	
15	Identificar las brechas existentes a través de la comparación del perfil actual y el perfil objetivo.	Dpto. Seguridad de la información, seguridad informática, consultor
	PASO 7 : PLAN DE ACCION	

16	Crear un plan de acción priorizado para abordar las brechas y lograr los resultados en el perfil objetivo.	Dpto. Seguridad de la información, seguridad informática, consultor
17	Determinar los recursos necesarios para abordar las brechas, que incluyen los recursos económicos y los recursos humanos.	Dpto. Seguridad de la información, seguridad informática, consultor
ETAPA 3: DISEÑO DE ARQUITECTURA DE CIBERSEGURIDAD		
18	Garantizar el acceso seguro a los recursos sin importar donde se encuentren localizados (intranet o internet). Utilizar Multifactor.	Gerencia TI, seguridad informática
19	Seguir una estrategia de mínimo privilegio y una política estricta de control de acceso.	Gerencia TI, seguridad informática
20	Inspeccionar y registrar todo el tráfico (entrante y saliente) para validar la actividad en la red.	Gerencia TI, seguridad informática
21	Segmentar cada tráfico de red diferente en una VLAN diferente.	Gerencia TI, seguridad informática
22	Analizar el comportamiento de los usuarios una vez que accedieron a la red.	Gerencia TI, seguridad informática
23	Definir perfiles de conexión basado en dispositivos e identidad.	Gerencia TI, seguridad informática
24	Validar que las soluciones tecnológicas puedan integrarse entre sí, para garantizar acciones preventivas y proactivas; así como también, conseguir mayor visibilidad en toda la red.	Gerencia TI, seguridad informática
ETAPA 4: CULTURA EN CIBERSEGURIDAD		
25	Comunicar constantemente a los trabajadores sobre las nuevas metodologías y técnicas empleadas en un ciberataque.	Dpto. Seguridad de la información, seguridad informática, marketing
26	Incluir dentro del proceso de inducción para nuevos colaboradores una correcta capacitación sobre las políticas de ciberseguridad de la organización.	RRHH, Dpto. seguridad de la información
27	Implementar programas de capacitaciones y evaluaciones continuas para los colaboradores en materia de ciberseguridad.	RRHH, Dpto. seguridad de la información
28	Desarrollar un programa formal de entrenamiento en materia de ciberseguridad debidamente documentado, y actualizarlo con frecuencia para incluir en él información sobre nuevos vectores de ataque y otros riesgos.	RRHH, Dpto. seguridad de la información
29	Conseguir el compromiso de la alta dirección para que respaldas las acciones tomadas.	Gerencia de Riesgos, Gerencia TI

- **Plan del proyecto:** Su objetivo es contar con toda la información oportuna para la toma de decisiones relacionada a la implementación de la propuesta a través de la ejecución de un proyecto.

Tabla 8: Plan del proyecto

Fuente: Elaboración propia

Tipo de Proyecto	Proyecto Estratégico
Descripción	Implementación de la propuesta del modelo de ciberseguridad
Patrocinador	Gerencia de Riesgos – Gerencia de TI
Área Responsable	Dpto. Seguridad de la información – Dpto. TI

- **Plan de participantes:** Establecemos la organización del equipo del proyecto para garantizar una gestión efectiva y lograr el éxito del plan de acción.

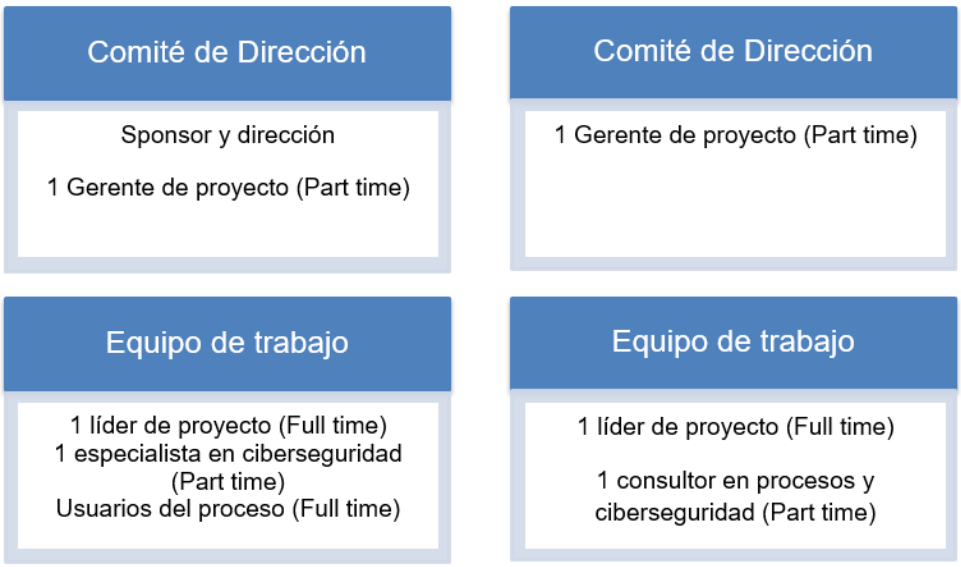


Figura 75. Equipo de trabajo

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

Tabla 9: 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
Gerente de Proyecto	Liderazgo del proyecto. Responsable de la gestión y monitoreo del proyecto	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.
Consultor 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.
Usuarios del proceso	Responsable de brindar. Facilidades para generar información.	Que sus necesidades puedan ser atendidas de forma ágil y sencilla.
Especialista en ciberseguridad	Resolver principales problemas y riesgos que se presenten en el proyecto.	Asegurar la correcta implementación desde el punto de vista técnico.

- **Plan de costos:**

Costo del equipo de trabajo

En la siguiente tabla se muestra un resumen del presupuesto aproximado del equipo de trabajo encargado de ejecutar la implementación de la propuesta con el apoyo de consultores y provisión de personal parte del equipo de Tecnologías de Información de la CMAC.

Tabla 10. Presupuesto equipo de trabajo

Fuente: Elaboración propia.

Recursos	Valor estimado
Líder de proyecto (12 meses)	S/ 78,000.00
Equipo TI (1 recurso por 12 meses)	S/ 36,000.00
Consultor en procesos	S/ 32,000.00

Especialista en ciberseguridad	S/ 32,000.00
Gastos administrativos	S/ 10,000.00
Contingencia	S/ 5,000.00
Total	S/ 193,000.00

Costo creación de nuevo cargo

Sustento técnico de la propuesta

1. **Diagnóstico de la situación inicial**

   En esta parte se tiene que elaborar un informe con tablas, indicadores, estadísticas que justifiquen la creación de estos nuevos cargos que contribuirá en el logro de los objetivos de ciberseguridad alineados a los objetivos estratégicos. Este diagnóstico varía de acuerdo a la realidad interna de cada CMAC.

2. **Propuesta de la mejora**

   Teniendo en cuenta el diagnóstico señalado en el paso anterior se propone incluir el cargo de Jefe de seguridad informática, modificando para ello el MOF y Manual de Gestión de Perfiles de la siguiente manera:

   2.1. A nivel de MOF

   Incluir el cargo de Jefe de seguridad informática que dependerá directamente de la Gerencia de Tecnologías de Información, el cual tendrá a su cargo a los asistentes y/o analistas de seguridad informática.

   NOTA: Las jefaturas propuestas también en este proyecto como son la jefatura de seguridad de la información y la jefatura de ciberseguridad, en algunas CMAC pueden existir con nombres diferentes; sin embargo, el presupuesto será similar al descrito para el cargo de jefe de seguridad informática por estar en el mismo nivel.

   Su función principal será: Brindar el soporte técnico a la Gerencia de Tecnologías de la información sobre las decisiones respecto a los temas de seguridad informática; realizando el seguimiento y propuestas de planes de acción sobre el Plan de Trabajo, indicadores de desempeño y estrategias gerenciales. Asimismo,

realizar el seguimiento y la gestión directa de los proyectos especiales que se le encargue relacionados a la seguridad informática.

Las funciones específicas del cargo propuestas son las siguientes:

De Planificación:
(01) Planificar y coordinar la eficiente comunicación con los usuarios involucrados en la implementación de actividades y proyectos de seguridad informática, durante la duración de los mismos.
(02) Planificar, organizar y dirigir la implementación de proyectos tecnológicos relacionados con seguridad informática y ciberseguridad en todos los niveles (perímetro, nube, red interna, etc.), así como gestión de cambios planificados y de emergencia de seguridad informática.
(03) Planificar, organizar, y dirigir el adecuado cumplimiento de la política y procedimientos de seguridad informática.

De Ejecución:

(04) Definir y formular las políticas y procedimientos internos relacionados con la seguridad informática.
(05) Administrar la seguridad informática en la CMAC, buscando las mejores tecnologías acorde a las necesidades y exigencias actuales.
(06) Planificar, organizar, dirigir y controlar el cumplimiento de las políticas y procedimientos de seguridad de la información.
(07) Gestionar los inventarios de la infraestructura tecnológica relacionada a seguridad informática.
(08) Gestionar el licenciamiento de software de los equipos y soluciones tecnológicas relacionadas a seguridad informática.
(09) Apoyar en el desarrollo de procedimientos para la protección de los activos de información.
(10) Proponer y coordinar la realización de análisis de vulnerabilidades formal en la red de la CMAC.
(11) Cumplir con las metas asignadas por su Jefe Inmediato con la finalidad de alcanzar los objetivos de desempeño de su unidad orgánica.

De Control:

(12) Supervisar la administración de la seguridad informática en la CMAC.
(13) Supervisar la seguridad informática a nivel de infraestructura y equipamiento que alberga servicios informáticos para la CMAC.
(14) Supervisar la seguridad de la arquitectura de redes y comunicaciones.
(15) Supervisar la seguridad en los nuevos proyectos y servicios tecnológicos de la CMAC.

(16) Supervisar el adecuado cumplimiento de la política y procedimientos de Backups y recuperación de información.
(17) Dirigir y controlar el adecuado cumplimiento de las políticas y procedimientos de capacitación a usuarios en temas de seguridad informática de la CMAC.

De Retroalimentación y/o mejora:
(18) Proponer indicadores relacionados con la disponibilidad del servicio de infraestructura tecnológica basados en controles de seguridad informática.

En el ámbito administrativo:
(19) Administrar eficientemente los recursos asignados a su cargo salvaguardando los intereses de la CMAC.
(20) Mantener un adecuado clima laboral del personal bajo su mando con la finalidad de aumentar la productividad y la retención del talento humano.
(21) Atender con oportunidad, celeridad y objetividad, las observaciones y recomendaciones que efectúen las auditorías tanto internas como externas.
(22) Revisar sus propios procesos administrativos bajo la supervisión del área de procesos y en coordinación con su jefatura inmediata.
(23) Cumplir y hacer cumplir dentro del marco de su competencia y función, las políticas, procedimientos y demás disposiciones señaladas en las normas internas o externas aplicables a CMAC.
(24) Otras funciones asignadas por su jefe inmediato o por documentos normativos.

3. Impacto de la propuesta

- **Impacto a nivel de procesos y normativa**
  a) Modificación del MOF y Manual de Gestión de Perfiles de Cargos por Competencia, PPE.

b) Fortalecimiento de las funciones de la Gerencia de tecnologías de la información con el apoyo de un cargo táctico y técnico.

- **Impacto presupuestal**
  Teniendo en cuenta que el cargo tiene un nivel de Jefatura y considerando el presupuesto por 12 meses; se resumen los costos de su implementación, los cuales, incluido el sobrecosto laboral, asciende a **S/. 137, 280.**

Tabla 11. Presupuesto anual nuevo cargo

Fuente: Elaboración propia

UNIDAD ORGÁNICA	PLAZAS	Acciones a la implementación de la Estructura	N° Plazas	Variación en Sueldo	Mes	Total
GERENCIA DE TECNOLOGIAS DE INFORMACION	Jefe de seguridad Informática	Convocatoria	1	S/.8,000	12	S/ 96, 0000
					CTS JUNIO Y NOVIEMBRE: ((sueldo+(sueldo/6))/360)*180	**S/. 9,333.34**
					GRATIFICACION	**S/. 13,493.00**
					VACACIONES	**S/. 8,666.67**
					TOTAL	**S/. 127, 493.01**
					TOTAL (Incluyendo Sobrecosto laboral: 40%)	**S/ 178, 490.214**

(*) Cabe señalar que este sueldo puede variar de acuerdo a la política de compensaciones de cada CMACT, al igual que el porcentaje de sobrecosto laboral.

- **Impacto logístico**
  Para el nuevo cargo, hay un mínimo impacto logístico, referido a:

- Nuevos sellos de V°B° y tarjetas personales
- Asignación de equipos celulares y de cómputo al nuevo cargo.
- Difusión de nuevas unidades y funciones hacia toda la red de agencias.

Costo de capacitación en ciberseguridad

Consideramos que se tiene que hacer una buena inversión en entrenamiento del personal para poder crear una cultura en ciberseguridad. Existe una variedad de plataformas digitales de entrenamiento para poder capacitar al personal; sin embargo, recomendamos utilizar la plataforma líder en entrenamiento digital llamada “KnowBe4”; quien tiene como fundador al experto en seguridad informática Stu Sjouwerman y como Chief Hacking

Officer a Kevin Mitnick, uno de los hackers más famosos del mundo. Esta herramienta permitirá a los empleados tomar decisiones de seguridad más inteligentes y gestionar eficazmente el problema de la ingeniería social; además le permitirá a las CMAC poder medir el nivel de cultura en ciberseguridad de su organización.

Se trabajara en base al siguiente principio:

- **Entrenar a los usuarios:** A través de videos tipo netflix, módulos interactivos, videojuegos, carteles, etc.)
- **Probar a los usuarios con campañas de phishing simulado:** Para medir los conocimientos aprendidos.
- **Analizar los resultados:** Estadísticas e informes.

La siguiente matriz muestra los perfiles sobre los cuales se asignaran los diferentes temas y estrategias de entrenamiento; ya que cada tema varía según el tipo de colaborador:

Tabla 12: Perfil para capacitaciones

Fuente: Elaboración propia

Perfil	Descripción
Estratégico	Personal gerencial, jefaturas
Operacional	Personal administrativos, coordinadores
Técnico	Personal técnico

Se medirán los siguientes indicadores:

- Asistencia a las capacitaciones
- Tasa de retención
- Satisfacción con el aprendizaje
- Tasa de clics de las simulaciones de phishing
- Tasa de denuncias de las simulaciones de phishing

El costo anual de la plataforma varía en función al tipo de licencia que se desea adquirir y a la cantidad de colaboradores a capacitar, como se puede visualizar en la siguiente imagen:

				Most Popular		
MSRP Pricing By Seat - 1 Year	Silver	Gold	Platinum	Diamond	Compliance Plus	PhishER
25-50	$18.00	$21.75	$25.50	$30.50	-	-
51-100	$16.00	$19.25	$22.50	$27.50	-	-
101-500	$13.00	$15.50	$18.00	$23.00	$7.50	$10.00
501-1000	$12.00	$14.25	$16.50	$21.50	$6.50	$7.00
1001-2000	$11.00	$13.00	$15.00	$20.00	$5.75	$6.00
2001-3000	$10.00	$11.75	$13.50	$18.50	$5.00	$5.00
3001-5000	$9.00	$10.50	$12.00	$17.00	$4.25	$4.50

Figura 76. Costo de licencia anual

Fuente: www.knowbe4.com

Se propone adquirir la licencia Platinium por 1 año para 1500 colaboradores. Posterior a ello y validando su efectividad, se propone adquirir la licencia por 3 años solicitando los descuentos respectivos por el tiempo de contratación. De acuerdo a lo antes mencionado, el costo de capacitación para comenzar a crear cultura en ciberseguridad sería el siguiente:

Tabla 13: Costo de capacitación

Fuente: Elaboración propia

Servicio de capacitación	Costo	Periodo
Acceso a la plataforma KnowBe4 Security Awareness Training	S/ 99,000.00	01 año

PRESUPUESTO GENERAL

En base a lo presupuestado referente al costo del equipo de trabajo, costo de creación de nuevo cargo y el costo de capacitación en ciberseguridad; se tiene la siguiente tabla que resume el presupuesto total de la implementación de la propuesta:

Tabla 14: Presupuesto general

Fuente: Elaboración propia

Concepto	Costo anual
Equipo de trabajo	**S/ 193,000.00**
Creación de nuevo cargo	**S/ 178, 490.214**
Capacitación en ciberseguridad	**S/ 99,000.00**
TOTAL	**S/ 470,490.214**

V.4.7. Validación de la propuesta

Para la validación de la propuesta, se utilizó el método de juicio de expertos (ver Anexo 2); y fue realizado a profesionales con experiencia en temas de ciberseguridad y seguridad de la información. Los criterios evaluados fueron la pertinencia, relevancia y claridad de la propuesta.

Los criterios de inclusión utilizados para la selección de los expertos fueron los siguientes:

- Que trabajen o hayan trabajado en alguna caja municipal.
- Que trabajen o hayan trabajado en áreas como seguridad de la información, seguridad e infraestructura, ciberseguridad, seguridad informática.

Los criterios de exclusión utilizados para la selección de los expertos fueron los siguientes:

- No encontrarse laborando en la actualidad en algunas de las áreas descritas anteriormente.
- Experiencia menor a 02 años laborando en las áreas descritas anteriormente.

De la validación realizada, se evidencio que de los 05 expertos, la mayoría coincide en los puntos de pertinencia, relevancia y claridad de la propuesta,

tales como: Restructuración del departamento de seguridad de la información, creación del área seguridad informática, Manejo de los niveles Estratégico, Operacional y táctico que soporte el modelo y la gestión de ciberseguridad, uso del marco de ciberseguridad NIST, diseño de la arquitectura de ciberseguridad basado en Zero Trust, programa de capacitación constante para mejorar la cultura en ciberseguridad, entre otros; sin embargo, proporcionaron las siguientes sugerencias y oportunidades de mejora:

Experto 1: Arnaldo Alvarado Lachira, Ex colaborador de Caja Piura y actual Analista de sistemas de seguridad de la información y continuidad del negocio en caja Trujillo.

- Respecto al punto 14 de la etapa 2 - Marco de ciberseguridad: *"Realizar un análisis de riesgos tomando como base la matriz de riesgos y el análisis de impacto y probabilidad actual; con el objetivo de fortalecer y no reemplazar lo ya trabajado",* sugiere que se debe considerar a futuro un catálogo de riesgos versus controles.

Experto 2: Juan Carlos Plasencia Cabanillas, ex analista de seguridad e infraestructura y actual coordinador de canales tecnológicos del departamento de tecnologías de información en caja Trujillo.

- Respecto al punto 3 de la etapa 1 – Contexto organizacional: *"Reestructurar el departamento de seguridad de la información creando las siguientes secciones que dependerán directamente del oficial de seguridad: sección de seguridad de la información, sección de continuidad del negocio y sección de ciberseguridad";* sugiere que la entidad evalué su estructura y determine si unifica el departamento o lo mantiene independiente del departamento de TI.
- Respecto al punto 4 de la etapa 1, *"Creación del área seguridad informática, dentro del departamento de TI, que se encargue directamente de todas las actividades relacionadas a la ciberseguridad"*; sugiere que es necesario independizar funciones para una correcta gestión, con sus perfiles definidos.

- Respecto al punto 10 de la etapa 2 – Marco de ciberseguridad, *"Identificar los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general"*; sugiere que es necesario contar con una política de actualización de inventarios periódica.
- Respecto al punto 22 de la etapa 3 – Diseño de arquitectura de ciberseguridad, *"Seguir una estrategia de mínimo privilegio y una política estricta de control de acceso"*; sugiere que la política debe estar asociada a una matriz de accesos.
- Respecto al punto 23 de la etapa 3 – Diseño de arquitectura de ciberseguridad, *"Inspeccionar y registrar todo el tráfico (entrante y saliente) para validar la actividad en la red"*; sugiere que esta actividad se acompañe con reportes de monitoreo.
- Respecto al punto 25 de la etapa 3 – Diseño de arquitectura de ciberseguridad, *"Analizar el comportamiento de los usuarios una vez que accedieron a la red"*; sugiere que se debe integrar la trazabilidad de los accesos.
- Respecto al punto 26 de la etapa 3 – Diseño de arquitectura de ciberseguridad, *"Definir perfiles de conexión basados en dispositivos e identidad"*; sugiere que se debe integrar listas blancas de accesos.
- Respecto al punto 27 de la etapa 3 – Diseño de arquitectura de ciberseguridad, *"Validar que las soluciones tecnológicas puedan integrarse entre sí, para garantizar acciones preventivas y proactivas; así como también, conseguir mayor visibilidad en toda la red"*; comenta que este punto es necesario para garantizar un correcto control integral inmediato.
- Respecto al punto 28 de la etapa 4 – Cultura en ciberseguridad, *"Comunicar constantemente a los trabajadores sobre las nuevas metodologías y técnicas empleadas en un ciberataque"*; sugiere que se debe sensibilizar y concientizar continuamente.
- Respecto al punto 32 de la etapa 4 – Cultura en ciberseguridad, *"Conseguir el compromiso de la alta dirección para que respalden*

las acciones tomadas"; comenta que es muy necesario para mantener en el tiempo el compromiso.

Experto 3: Omar Carbajal Llosa, ex jefe de tecnologías de información en caja Santa y actual Jefe de tecnologías de información en Cooperativa de ahorro y créditos ILO.

- Respecto al punto 1 de la etapa 1 – Contexto organizacional: *"Creación del comité de ciberseguridad, el cual se encargara de asesorar a la alta dirección en el análisis y la definición de la política general de ciberseguridad; proponer acciones para superar las brechas encontradas; evaluar la correcta implementación y funcionamiento del marco de ciberseguridad; entre otras";* sugiere enfocarse más a una política de gestión y control de seguridad.
- Respecto al punto 2 de la etapa 1 – Contexto organizacional: *"Reestructurar el departamento de seguridad de la información, creando las siguientes secciones que dependerán directamente del oficial de seguridad: sección de Seguridad de la información, sección de continuidad del negocio y sección de ciberseguridad.";* comenta que la ciberseguridad impacta transversalmente tanto a la SI y CN, también a TI, por lo que deberían reforzar en ambas.
- Respecto al punto 6 de la etapa 1 – Contexto organizacional: *"Asignar los recursos necesarios para la adecuada implementación de los procesos.";* sugiere especificar los procesos a fin.
- Respecto al punto 7 de la etapa 2 – Marco de ciberseguridad, *"Identificar objetivos empresariales de alto nivel para la toma de decisiones estratégicas con respecto a las implementaciones de ciberseguridad."*; sugiere alinear los objetivos estratégico empresariales con los objetivos estratégicos de la Ciberseguridad.
- Respecto al punto 11 de la etapa 2 – Marco de ciberseguridad, *"Identificar las amenazas y vulnerabilidades que afectan los activos."*; sugiere que se deben considerar en una matriz de riesgos.

Experto 4: Omar Gil Cuba, ex analista de riesgos y seguridad de la información en Caja Trujillo y actual analista de riesgos y seguridad de la información en banco Ripley.

- Respecto al punto 3 de la etapa 1 – Contexto organizacional: "*Reestructurar el departamento de seguridad de la información, creando las siguientes secciones que dependerán directamente del oficial de seguridad: sección de Seguridad de la información, sección de continuidad del negocio y sección de ciberseguridad.";* sugiere que debe utilizarse la misma política pero de manera independiente.

Experto 5: Ricardo Ramírez Quevedo, ex analista de seguridad de la información en Caja Sullana y actual analista de seguridad de la información y continuidad del negocio en Caja Trujillo.

- Respecto al punto 2 de la etapa 1 – Contexto organizacional: "*Creación del "Comité de ciberseguridad", el cual se encargará de asesorar a la alta dirección en el análisis y la definición de la Política General de Ciberseguridad; proponer acciones para superar las brechas encontradas; evaluar la correcta implementación y funcionamiento del marco de ciberseguridad; entre otras.";* sugiere que se debe tener en cuenta que según la ISO/IEC 27032 La Ciberseguridad se encuentra embebido dentro de la Seguridad de la Información, motivo por el Cual inclusive según la Resolución SBS 504 - 2021 se considera la creación del "Comité de Seguridad de la Información y Ciberseguridad". En ese sentido, se debería crear un comité considerando ambos frentes.
- Respecto al punto 11 de la etapa 2 – Marco de ciberseguridad: "*Identificar las amenazas y vulnerabilidades que afectan los activos.";* sugiere que se deben especificar activos de información que están interconectados al ciberespacio.
- Respecto al punto 20 de la etapa 3 – Diseño de arquitectura de ciberseguridad: "*Garantizar el acceso seguro a los recursos sin importar donde se encuentren localizados (intranet o internet).*

Utilizar Multifactor."; sugiere que la definición del diseño de la Arquitectura de Ciberseguridad debería considerar modelos de Arquitectura de Seguridad Empresarial como por ejemplo SABSA o TOGAF, después de definir las capas de seguridad se pueden considerar los controles a aplicar.

VI. DISCUSIÓN, CONCLUSIONES Y RECOMENDACIONES

VI.1. Discusión

La presente investigación tuvo como objetivo general determinar las características que debe adoptar un modelo de ciberseguridad con nuevo enfoque en tiempos de transformación digital. Los resultados obtenidos fueron la identificación de las estrategias de ciberseguridad, la elaboración de la propuesta del uso del modelo de ciberseguridad Zero Trust y del marco de gestión de ciberseguridad NIST; el diseño de un modelo de gestión organizacional dividido en 3 niveles: Estratégico, Operacional y táctico; la restructuración del departamento de seguridad de la información y la creación del área de seguridad informática dentro del departamento de tecnologías de información; el diseño de una matriz para el uso de los 20 controles de ciberseguridad CIS; el diseño de una nueva arquitectura de ciberseguridad y los pasos para la creación de cultura en ciberseguridad

Podemos afirmar que los resultados obtenidos guardan relación con el trabajo de investigación de Villalba (2015), quien a través del análisis de características y puntos relevantes de planes y diseños de ciberseguridad de países de primer mundo como EEUU, Rusia y China, le permitieron elaborar la propuesta de un Modelo de Organización de Ciberseguridad en España. Este trabajo también se basó en el análisis comparativo de características para poder elaborar la propuesta. Así mismo, su estudio es de tipo cuantitativo y de corte descriptivo.

Por otra parte, Lara (2019), en su tesis de maestría Diseño de un modelo de seguridad de la información, basado en osstmmv3, nist sp 800-30 e iso

27001, para centros de educación: caso de estudio universidad regional autónoma de los andes, extensión Tulcán, analiza el panorama actual de la Universidad Autónoma de los Andes, respecto a la red de información y la seguridad e infraestructura, con el objetivo de diseñar un modelo de seguridad de la información. Esta investigación coincide en la utilización del marco NIST para la gestión de ciberseguridad. El estudio también es de tipo cuantitativo y descriptivo; y aunque la técnica de recolección de datos fue diferente al utilizar una encuesta aplicada a los estudiantes, los resultados obtenidos permitieron la elaboración del diseño propuesto.

Así mismo, Macancela (2015) en su tesis de maestría Modelo de gestión de la seguridad informática para garantizar la continuidad del negocio en la cacpe pastaza, analiza la situación actual de la institución financiera respecto a sus sistemas de seguridad informática y la forma como afrontan las amenazas presentes; y al igual que nuestra investigación, los resultados le permitieron proponer un modelo de Gestión de seguridad informática para garantizar la continuidad del negocio. Aunque su investigación de campo y exploratoria, y su técnica de encuestas y entrevistas no coindicen con nuestro trabajo de investigación; en lo que si coincidimos es en que la seguridad no puede debe basarse en procesos iterativos como en el que propusimos en el marco NIST y que las actividades deben agregar valor en el riesgo, prevención, detección y respuesta ante incidentes de seguridad.

De igual manera, Vilcarromero y Vílchez (2018), realiza la revisión de la situación actual de un Centro de operaciones de seguridad – SOC en una empresa de telecomunicaciones en Perú, con el objetivo de proveer al área del SOC, un marco de gestión de ciberseguridad para implantar, operar, monitorear, revisar y mejorar los controles de ciberseguridad; lo cual, guarda relación con nuestro trabajo de investigación, ya que se pretende del mismo modo, que la propuesta del modelo, pueda servir como marco de gestión para las cajas municipales. También coincide con nuestra

investigación, en el uso del marco de ciberseguridad NIST para elaborar la propuesta.

Además, (Bradley, 2019, parr. 8), coincide en que un nuevo modelo de ciberseguridad debe girar en torno a tecnologías como la autenticación multifactorial, el análisis de comportamiento y la tecnología de engaño; así como también, menciona que el monitorear el comportamiento de los usuarios, es un medio más proactivo y efectivo para detectar comportamientos sospechosos o maliciosos.

VI.2. Conclusiones

Se logró elaborar la propuesta para un modelo de ciberseguridad con nuevo enfoque para cajas municipales, en tiempo de transformación digital, que incluya características de integridad, confidencialidad y disponibilidad.
Las principales a relevar son: Autenticación multifactorial, protección del endpoint fuera del perímetro, integración de las soluciones de seguridad en la arquitectura de ciberseguridad, analizar el comportamiento de los usuarios, adaptación a un ciclo continuo de gestión de la ciberseguridad y el riesgo, considerar una estructura piramidal que comprenda los niveles estratégicos, operaciones y tácticos para la gestión de la ciberseguridad, desconfiar de todo el tráfico y verificarlo todo. Esto se evidencia en:

1. Se logró identificar los modelos de ciberseguridad: Modelo defensa en profundidad, modelo perimetral, modelo Zero Trust, Modelo Thin Security, a través del desarrollo de una matriz de priorización validada por expertos en ciberseguridad; los cuales tienen características de protección del endpoint dentro o fuera del perímetro, desconfianza y verificación de todo el tráfico que pasa por la red, integración de soluciones de seguridad, entre otras.
2. Se logró comparar los modelos de ciberseguridad identificados, a través de una matriz de comparación validada por expertos en

ciberseguridad, logrando identificar al modelo que guardaba la mayor relación con las características de ciberseguridad listadas.

3. Se propusieron características que debe adoptar un modelo de ciberseguridad con nuevo enfoque en tiempos de transformación digital, validadas a través de una lista de cotejo de usuarios potenciales.

4. Se logró elaborar la propuesta validada a través de una matriz de juicio de expertos; obteniendo como resultados: la selección del modelo de ciberseguridad Zero Trust basado en el marco NIST, el diseño de una nueva estructura del departamento de seguridad de la información, el diseño y la propuesta de creación del área de seguridad informática, la creación de la matriz de soporte para la aplicación de 20 controles de seguridad CIS, el diseño de una nueva arquitectura de ciberseguridad y los pasos para la creación de cultura en ciberseguridad en toda la organización.

VI.3. Recomendaciones

Se recomienda la adopción del modelo Zero Trust para poder proteger las aplicaciones, los datos, los usuarios y los dispositivos que hoy en día se están trasladando cada vez más fuera del perímetro de la organización y de la zona de control; lo cual ha sido evidenciado con la pandemia del covid-19 que nos toca vivir; y como consecuencia, se ha acelerado el proceso de transformación digital en las empresas.

Se recomienda el uso del marco de gestión de ciberseguridad NIST, que ayudara a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos a través del uso de las mejores prácticas en ciberseguridad.

Se recomienda el uso del modelo de organización de 3 niveles: Estratégico, operacional y táctico; para que sirva como soporte del modelo Zero Trust; debido a que sin una sinergia y comunicación efectiva entre todos los

departamentos de la organización y principalmente la alta dirección, el modelo no será efectivo.

Se recomienda la creación de una nueva área llamada “Seguridad Informática” dentro del departamento de TI; así como también, la reestructuración propuesta del departamento de seguridad de la información. Sin una sección que enfocada directamente en los temas de ciberseguridad; y sin la sinergia con el departamento de seguridad de la información, este modelo no lograra los objetivos planteados.

Se recomienda, como oportunidad de mejora y una vez que estas dos secciones alcancen la madurez correspondiente; puedan ubicarse en posiciones diferentes en el organigrama institucional para poder tener más autonomía en las decisiones respecto a la ciberseguridad. Los dos departamentos deberían en algún momento dejar de depender de la Gerencia de Riesgos y la Gerencia de TI respectivamente, y pasar a reportar directamente a la Gerencia Central Mancomunada.

Se recomienda incluir las capacitaciones en ciberseguridad, dentro de los procesos de inducción y dentro de los programas de capacitación que se realizan a lo largo del año, de igual importancia que los referidos al lavado de activos. Nada de lo propuesto en la presente investigación tendrá éxito si no se asume con responsabilidad y compromiso, el objetivo de lograr crear “cultura en ciberseguridad” en la organización.

REFERENCIAS

Alvarez, A. (2020, abril 7). *Análisis de Vulnerabilidades, Test de Intrusión y Red Team*. https://www.a2secure.com/blog/analisis-de-vulnerabilidades-test-de-intrusion-y-red-team/

Aranda, J. (2007). *Seguridad Informática.* https://slideplayer.es/slide/2261929/

Atlas - Proyectos Informáticos. (2017, enero 6). *¿QUÉ ES EL MDM (MOBILE DEVICE MANAGEMENT)*. atlas-pi.com. https://www.atlas-pi.com/2017/01/06/que-es-el-mdm-mobile-device-management/

Barbosa, D. C. (2020, enero 21). *Qué es un proxy y para qué sirve*. welivesecurity. https://www.welivesecurity.com/la-es/2020/01/02/que-es-proxy-para-que-sirve/

Blogmexico Comstor. (2019, enero 14). *¿Qué es cultura en ciberseguridad y como desarrollarla?*. blogmexico.comstor.com. https://blogmexico.comstor.com/que-es-cultura-de-ciberseguridad-y-como-desarrollarla

Bortnik, S. (2010, mayo 24). *Defensa en Profundidad.* welivesecurity. https://www.welivesecurity.com/la-es/2010/05/24/defensa-en-profundidad/

Bradley, T. (2019, octubre 17). *El modelo estandar de ciberseguridad esta fundamentalmente roto.* IA Latam. https://ia-latam.com/2019/10/17/el-modelo-estandar-de-ciberseguridad-esta-fundamentalmente-roto/

Businesscontinuity. (2012, setiembre 21). Businesscontinuity. http://businesscontinuity-pe.blogspot.com/2012/09/circular-g-139-2009-de-la-sbs-peru.html

Businesscontinuity. (2012, setiembre 21). *Circular G-139-2009 de la SBS (Perú).* businesscontinuity-pe.blogspot.com. http://businesscontinuity-pe.blogspot.com/2012/09/circular-g-139-2009-de-la-sbs-peru.html

Caja Arequipa. (s.f.). *Caja Arequipa*. Marco Legal. https://www.cajaarequipa.pe/marco-legal/

Chang, C. E. (2011, abril). *Diseño de un sistema de gestion de seguridad de la informacion para una compañia de seguros.*

Ciberseguridad. (s.f.). *Seguridad Perimetral*. Ciberseguridad.com. https://ciberseguridad.com/servicios/seguridad-perimetral/

Ciberseguridadlogitek. (2019, noviembre 8). *Estrategia de Defensa en Profundidad. Ciberseguridadlogitek.* https://www.ciberseguridadlogitek.com/estrategia-de-defensa-en-profundidad-en-ciberseguridad-industrial/

Claro. (s.f.). claro.com.pe. https://www.claro.com.pe/empresas/servicios-gestionados/anti-ddos/#:~:text=Protecci%C3%B3n%20Anti%20DDoS%2C%20es%20un,la%20red%20p%C3%BAblica%20de%20Internet.&text=Especialistas%20en%20protecci%C3%B3n%20Anti%20DDoS,la%20red%20de%20su%20empresa.

Director-it. (s.f.). Director-it. *¿Qué es un WAF? - Web Application Firewall*. http://director-it.com/index.php/es/ssoluciones/seguridad/firewall-y-dmz/118-que-es-un-waf-web-application-firewall.html

El pais economia. (2020, julio 2). *Ciberseguridad: modelos eficientes y efectivos ante el impacto de la covid-19.* Retina . https://retina.elpais.com/retina/2020/06/29/tendencias/1593456689_101916.html

Esan. (2018, setiembre 13). *En qué consiste la ciberresiliencia y cuál es su importancia. Conexion Esan.* https://www.esan.edu.pe/apuntes-empresariales/2018/09/en-que-consiste-la-ciberresiliencia-y-cual-es-su-importancia/

Eserp Business & Law School. (s.f.). Eserp. https://es.eserp.com/articulos/ciberseguridad-empresas/

Fepcmac. (s.f.). Fepcmac. https://www.fpcmac.org.pe/nosotros

Fernandez, L. (2020, abril 10). *Protege tu red con sistemas IDS/IPS y descubre cuáles son los mejores. Redes Zone.* Protege tu red con sistemas IDS/IPS y descubre cuáles son los mejores. https://www.redeszone.net/tutoriales/seguridad/sistemas-deteccion-prevencion-intrusiones-ids-ips/

Fortinet. (s.f.). Fortinet. https://www.fortinet.com/products/next-generation-firewall

Franco, . R. (2019, enero 10). *Evolución del modelo de ciberseguridad en tiempos de transformación digital*. https://www.youtube.com/watch?v=MvFwhHj3ko0

Gonzalez, F. (2019, octubre 28). *Zero Trust: redefiniendo la estrategia de ciberseguridad*. B-secure. https://www.b-secure.co/blog/zero-trust-redefiniendo-la-estrategia-de-ciberseguridad

Goujon, A. (2012, setiembre 10). *¿Qué es una VPN y cómo funciona para la privacidad de la información?.* Welivesecurity. https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/

Grajales, L. (2019, noviembre 25). *¿Cómo abordar la implementación del modelo Zero Trust?.* Blog B-Secure. https://www.b-secure.co/blog/como-abordar-la-implementacion-del-modelo-zero-trust

Grajales, L. (2019, abril 24). *Estrategia de ciberseguridad*. Blog B-Secure. https://www.b-secure.co/blog/claves-desarrollar-estrategia-ciberseguridad-gobierno-gesti%C3%B3n

Hurtado, J., & Ruiz, D. (2020, abril). *Thin security, o cómo maximizar la efectividad de la ciberseguridad para sobrevivir en el mundo post-covid19*. Revista S21sec. https://revistasic.es/sic139/revistasic139.pdf

Incibe - Instituto Nacional de Ciberseguridad. (s.f.). *Desarrollar cultura en seguridad*. Incibe - Instituto Nacional de Ciberseguridad. https://www.incibe.es/protege-tu-empresa/que-te-interesa/desarrollar-cultura-en-seguridad

Ingens Networks. (2020, enero 7). *¿Qué es CASB? y ¿por qué es la palabra de moda de la seguridad perimetral?*. Info.ingens-networks. https://info.ingens-networks.com/blog/qu%C3%A9-es-casb-y-por-qu%C3%A9-es-la-palabra-de-moda-de-la-seguridad-perimetral

Investigacion Cientifica. (s.f.). InvestigacionCientifica.org. https://investigacioncientifica.org/alcance-la-investigacion-cientifica/#:~:text=Alcance%20descriptiva,o%20medir%20conceptos%20o%20situaciones.

Ionos. (s.f.). *Que es Antispam*. Ionos. https://www.ionos.es/ayuda/correo/glosario-explicaciones-sobre-conceptos-y-temas-importantes/antispam/

Isec Auditors. (s.f.). Isec Auditors. https://www.isecauditors.com/consultoria-csf-iso-27032

Itdigitalsecurity. (2019, enero 14). *DLP, o cómo prevenir la fuga de datos*. Itdigitalsecurity. https://www.itdigitalsecurity.es/reportajes/2019/01/dlp-o-como-prevenir-la-fuga-de-datos

ITreseller Tech&Consulting. (2020, febrero 17). *La falta de cultura en ciberseguridad es la principal amenaza para las empresas.* Iitreseller. https://www.itreseller.es/seguridad/2020/02/la-falta-de-cultura-en-ciberseguridad-es-la-principal-amenaza-para-las-empresas

Ittrends. (2020, m arzo 23). Ittrends. https://www.ittrends.es/seguridad/2020/03/aumentan-los-riesgos-de-ciberseguridad-y-los-consiguientes-ataques-por-el-coronavirus

Lauria, G. (2020, enero 2). debmedia. https://debmedia.com/blog/transformacion-digital/

Lumbreras, J. (2019). *Claves para la Transformación Digital en las empresas peruanas. Lima*. Top Publications S.A.C.

Luz, S. d. (2015, marzo 19). *¿Qué son las soluciones SIEM para la seguridad interna de una empresa?.* Redeszone. https://www.redeszone.net/2015/03/19/que-son-las-soluciones-siem-para-la-seguridad-interna-de-una-empresa/

Mcafee. (s.f.). Mcafee. https://www.mcafee.com/es-pe/antivirus.html

Mendoza, M. A. (2015, junio 16). Welivesecurity. https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Micro Finanzas Global. (s.f.). MicroFinanzas. https://microfinanzasglobal.com/caja-municipal/

Morales, G. G. (2017, marzo 10). *Gestión de la Ciberseguridad según el ISO/IEC 27032:2012*. Linkedin. https://es.linkedin.com/pulse/gesti%C3%B3n-de-la-ciberseguridad-seg%C3%BAn-el-isoiec-gianncarlo-g%C3%B3mez-morales

Morales, G. G. (2019, abril 30). *¿Qué es el Cybersecurity Framework de NIST de los Estados Unidos?.* ESAN. https://www.esan.edu.pe/conexion/actualidad/2019/04/30/que-es-el-cybersecurity-framework-de-nist-de-los-estados-unidos/

Obs business School. (s.f.). Tendencias & Innovacion. https://obsbusiness.school/int/blog-investigacion/sistemas/que-es-ciberseguridad-y-de-que-fases-consta

Olleros, J. M. (2019, noviembre 29). *Defensa en profundidad contra la intrusion*. Angelolleros. https://www.angelolleros.com/defensa-profundidad-contra-intrusion/

Osi. (s.f.). Osi. https://www.osi.es/es/actualizaciones-de-seguridad

Pandasecurity. (2018, noviembre 15). *¿Qué es Threat Hunting y por qué es necesario?. Pandasecurity.* https://www.pandasecurity.com/spain/mediacenter/adaptive-defense/threat-hunting-por-que-necesario/

Pandasecurity. (2018, setiembre 12). *¿En qué se diferencian el sandboxing y los honeypots?*. pandasecurity.com. https://www.pandasecurity.com/spain/mediacenter/seguridad/diferencias-sandboxing-honeypot/

Pmg-ssi. (2017, enero 26). Blog especializado en SGSI. https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

PowerDara. (s.f.). PowerData. https://www.powerdata.es/transformacion-digital

Ramiro, R. (2018, julio 7). *Cómo implantar el Framework NIST*. ciberseguridad.blog. https://ciberseguridad.blog/como-implantar-el-framework-nist/#:~:text=Los%20Niveles%20de%20Implementaci%C3%B3n%20del%20Framework%20NIST%20(%22TIERs%22),establecidos%20para%20gestionar%20ese%20riesgo.

Real Academia Española - RAE. (s.f.). Real Academia Española - RAE. https://dle.rae.es/modelo

Real Academia Española - RAE. (s.f.). Real Academia Española - RAE. https://dle.rae.es/tradicional?m=form

Redaccion Gestion. (2018, abril 6). Gestion.pe. https://gestion.pe/economia/sbs-directorio-cajas-municipales-tendra-nueve-miembros-son-absorbidas-terceros-230929-noticia/

Redaccion Tic Pymes. (2020, abril 22). TicPymes. https://www.ticpymes.es/autonomos/noticias/1118120025204/covid-19-adaptacion-digital-transformacion-digital.1.html

Retina. (2020, julio 2). *Ciberseguridad: modelos eficientes y efectivos ante el impacto de la covid-19.* Retina. https://retina.elpais.com/retina/2020/06/29/tendencias/1593456689_101916.html

Rodriguez, K. (2017, noviembre 3). CIO Mexico. http://cio.com.mx/claves-ciberseguridad-kevin-mitnick-hacker-buscado/

Romero, M. S. (2019, noviembre 16). *¿Qué es Sandbox y en qué consiste?.* Computerhoy. https://computerhoy.com/reportajes/tecnologia/que-es-sandbox-529177

Sampieri, R. H. (2014). *Metodologia de la Investigacion*. Mexico: Interamericana editores S.A.

SBS Informa. (2018, abril). *Boletin Semanal Nro 13*. sbs.gob.pe. https://www.sbs.gob.pe/Portals/0/Boletin_Semanal_13_2018.pdf

SBS Informa. (2018, abril 13). SBS - Boletin Semanal. https://www.sbs.gob.pe/Portals/0/Boletin_Semanal_13_2018.pdf

Secure IT. (s.f.). *Network Access Control*. Secure IT. https://www.secureit.es/sistemas-de-seguridad-it/network-access-control-nac/

Shevchenko, Y. (2018, mayo 16). *EPP y EDR: El futuro de la ciberseguridad endpoint.* kaspersky. https://www.kaspersky.es/blog/epp-edr-importance/16154/

Snape, E. (2020, mayo 14). *Gestión de seguridad con ISMP3: La alternativa luego de un pentest*. https://www.youtube.com/watch?v=T_0PHFV03H0

Stucchi, P. (2017, junio 5). *El ABC de la protección de datos personales (data privacy).* gestion.pe. https://gestion.pe/blog/reglasdejuego/2017/06/el-abc-de-la-proteccion-de-datos-personales-data-privacy.html/?ref=gesr

Tugurium. (2005, Diciembre 3). *Clark Wilson Model.* Tugurium. http://www.tugurium.com/gti/termino.php?Tr=Clark-Wilson%20model

Unir Revista. (2020, enero 7). *Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias?.* Unir Revista. https://www.unir.net/ingenieria/revista/noticias/red-blue-purple-team-ciberseguridad/549204773062/

Vilela, M. d. (s.f.). *Negocios Tecnologia Banca y Desarrollo*. NetBankDes. http://netbankdes.com/aplication/webroot/archivos/130320034959las%20cajas%20municipales%20de%20ahorro%20y%20cr%C3%A9dito%20%C2%BFempresas%20municipales%20o%20empresas%20ajenas%20al%20ambito%20normativo%20del%20sector%20p%C3%BAblico.pdf

Welivesecurity. (2014, setiembre 24). *Seguridad en la nube para empresas: ¿qué son los CASB?.* Welivesecurity. https://www.welivesecurity.com/la-es/2014/09/24/seguridad-nube-empresas-que-son-casb/

Wikipedia. (2020, diciembre 25). *Modelo Clark Wilson.* Wikipedia. https://es.wikipedia.org/wiki/Modelo_Clark-Wilson

Wikipedia. (2021, octubre 19). *Modelo Bell-Lapadula.* Wikipedia. https://es.wikipedia.org/wiki/Modelo_Bell-LaPadula

Worl Economic Forum. (2020, marzo 17). weforum.org. https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/

Anexos

Anexo 1 – Matriz de priorización

UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

MATRIZ DE PRIORIZACION

Nombre del especialista: Alan Cuadra Pacheco

Especialidades y/o certificaciones: Certified Ethical Hacker, CyberArk Certified Defender, NSE 7 Network Security Architect, Cisco Certified Network Associate Security, PECB Certified ISO/IEC 27001 Lead Implementer, Tenable Io Certificate Proficiency, VMware Certified Professional

Autor del Instrumento: Alan Pierre Salinas Tomapasca

INSTRUCCIONES:

Cada opción puede obtener una puntuación de 1 a 5 por cada criterio, siendo 1 lo más bajo y 5 lo más alto; de acuerdo a la relación encontrada entre el modelo y los criterios respectivos.

Criterio / Modelo	Relación con el tema de investigación	Integridad	Disponibilidad	Confiabilidad	Total
ISM3	1	2	2	1	6
Seguridad Perimetral	4	3	3	2	12
Clark-Wilson	2	4	2	1	9
Thin Security	5	4	4	3	16
Bell-LaPadula	2	2	3	4	11
Zero Trust	5	4	4	5	18
Defensa en Profundidad	4	4	3	4	15

- ¿Cuántos modelos se deben seleccionar para el trabajo de investigación de acuerdo a los resultados de la matriz de priorización?

  Los cuatro modelos con mayor puntaje.

Firma del especialista
Fecha: 11/11/2021

UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

MATRIZ DE PRIORIZACION

Nombre del especialista: ANIBAL STEIFAN CUNIA

Especialidades y/o certificaciones: ITIL FOUNDATION CERTIFICATE, NSE 7 NETWORK SECURITY ARCHITEC, NSE 4 NETWORK SECURITY PROFESSIONAL, ETHICAL HACKER FUNDAMENTAL DE EXIN.

Autor del Instrumento: Alan Pierre Salinas Tomapasca

INSTRUCCIONES:

Cada opción puede obtener una puntuación de 1 a 5 por cada criterio, siendo 1 lo más bajo y 5 lo más alto; de acuerdo a la relación encontrada entre el modelo y los criterios respectivos.

Criterio / Modelo	Relación con el tema de investigación	Integridad	Disponibilidad	Confiabilidad	Total
ISM3	1	2	2	2	7
Seguridad Perimetral	4	3	3	2	12
Clark-Wilson	2	4	2	1	9
Thin Security	4	4	4	3	15
Bell-LaPadula	2	2	3	4	11
Zero Trust	5	4	5	4	18
Defensa en Profundidad	4	4	3	4	15

- ¿Cuántos modelos se deben seleccionar para el trabajo de investigación de acuerdo a los resultados de la matriz de priorización?

  SE DEBEN SELECCIONAR 4 MODELOS QUE OBTENGAN LA MAYOR CALIFICACIÓN.

Firma del especialista
Fecha: 11/11/2021

Anexo 2 – Matriz de comparación

UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

MATRIZ DE COMPARACION

Nombre del especialista: Alan Cuadra Pacheco

Especialidades y/o certificaciones: Certified Ethical Hacker, CyberArk Certified Defender, NSE 7 Network Security Architect, Cisco Certified Network Associate Security, PECB Certified ISO/IEC 27001 Lead Implementer, Tenable Io Certificate Proficiency, VMware Certified Professional.

INSTRUCCIONES:

Coloque un "✓" en la casilla correspondiente si encuentra relación entre los modelos y características de ciberseguridad mostrados en la siguiente tabla. Caso contrario, deberá colocar una **"X"**.

N°	CARACTERISTICAS / MODELOS DE CIBERSEGURIDAD	DEFENSA EN PROFUNDIDAD	PERIMETRAL	ZERO TRUST	THIN SECURITY
1	Múltiples niveles de seguridad	✓	X	✓	✓
2	Protección del endpoint detrás del perímetro	✓	✓	✓	✓
3	Integración de la arquitectura de seguridad	X	X	✓	✓
4	Gestión de ciberseguridad y manejo del riesgo a nivel organizacional	X	X	✓	✓
5	Visibilidad en toda la red	X	X	✓	✓
6	Gestión de ciberseguridad y manejo del riesgo a nivel departamental	✓	✓	X	X
7	Interacción con las distintas capas del modelo	X	X	✓	✓
8	Protección del endpoint fuera del perímetro	X	X	✓	✓
9	Adaptarse continuamente a nuevas tácticas y técnicas de ataque	X	X	✓	✓
10	Acciones proactivas para la caza de amenazas.	X	X	✓	✓
11	Protección reactiva	✓	✓	X	X
12	Autenticación Multifactorial	X	X	✓	✓
13	Prevención, detección y respuesta para reducir superficie de ataque	X	X	✓	✓
14	Análisis de comportamientos de usuario	X	X	✓	✓
15	Protección proactiva	X	X	✓	✓
16	Análisis de amenazas automatizados y predictivos	X	X	✓	✓
17	Protección de amenazas internas y externas	✓	✓	✓	✓
18	Adaptación al modelo o arquitectura de seguridad existente	X	X	✓	X
19	Se adapta a un ciclo continuo de gestión de ciberseguridad	X	X	✓	✓
20	Permite reducir las alertas reportando las más significativas	X	X	✓	✓
21	Análisis de amenazas basado en firmas	✓	✓	X	X
22	Análisis de amenazadas basado en IA tipo EDR	X	X	✓	✓
23	Utiliza ejercicios de red Team	X	X	✓	✓
24	Se adapta a soluciones en la nube	X	X	✓	✓
25	Gestión de accesos fuera del perímetro	X	X	✓	✓
26	Detección de bots	X	X	✓	✓

Firma del especialista
Fecha: 11/11/2021

UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

MATRIZ DE COMPARACION

Nombre del especialista: ANIBAL STEIFAN CUNIA

Especialidades y/o certificaciones: ITIL FOUNDATION CERTIFICATE, NSE7 NETWORK SECURITY ARCHITEC, NSE 4 NETWORK SECURITY PROFESSIONAL, ETHICAL HACKER FUNDAMENTAL EXIN

INSTRUCCIONES:

Coloque un "✓" en la casilla correspondiente si encuentra relación entre los modelos y características de ciberseguridad mostrados en la siguiente tabla. Caso contrario, deberá colocar una "X".

N°	CARACTERISTICAS / MODELOS DE CIBERSEGURIDAD	DEFENSA EN PROFUNDIDAD	PERIMETRAL	ZERO TRUST	THINK BE CURITY
1	Múltiples niveles de seguridad	✓	X	✓	✓
2	Protección del endpoint detrás del perímetro	✓	✓	✓	✓
3	Integración de la arquitectura de seguridad	X	✓	✓	✓
4	Gestión de ciberseguridad y manejo del riesgo a nivel organizacional	X	X	✓	✓
5	Visibilidad en toda la red	X	X	✓	✓
6	Gestión de ciberseguridad y manejo del riesgo a nivel departamental	✓	✓	X	X
7	Interacción con las distintas capas del modelo	✓	X	✓	✓
8	Protección del endpoint fuera del perímetro	X	X	✓	✓
9	Adaptarse continuamente a nuevas tácticas y técnicas de ataque	X	X	✓	✓
10	Acciones proactivas para la caza de amenazas.	X	X	✓	✓
11	Protección reactiva	✓	✓	X	X
12	Autenticación Multifactorial	✓	✓	✓	✓
13	Prevención, detección y respuesta para reducir superficie de ataque	✓	X	✓	✓
14	Análisis de comportamientos de usuario	✓	✓	✓	✓
15	Protección proactiva	X	X	✓	✓
16	Análisis de amenazas automatizados y predictivos	X	X	✓	✓
17	Protección de amenazas internas y externas	✓	✓	✓	✓
18	Adaptación al modelo o arquitectura de seguridad existente	X	X	✓	X
19	Se adapta a un ciclo continuo de gestión de ciberseguridad	X	X	✓	X
20	Permite reducir las alertas reportando las más significativas	X	X	✓	✓
21	Análisis de amenazas basado en firmas	✓	✓	X	X
22	Análisis de amenazadas basado en IA tipo EDR	X	X	✓	✓
23	Utiliza ejercicios de red Team	✓	X	✓	✓
24	Se adapta a soluciones en la nube	X	X	✓	✓
25	Gestión de accesos fuera del perímetro	X	X	✓	✓
26	Detección de bots	✓	X	✓	✓

Firma del especialista
Fecha: 11 / 11 / 2021

Anexo 3 – Listas de Cotejo

UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

LISTA DE COTEJO

Nombres del especialista: Arnaldo Martín Alvarado Jacliva

Institución donde labora: Caja Trujillo

Cargo en la institución: Analista de Seguridad de la Información y Continuidad del Negocio

Trabajó en alguna Caja Municipal? (Nombre de la institución y cargo): Caja Piura - Asistente de Continuidad del Negocio / Asistente de Seguridad de la Información

Autor del instrumento: Alan Pierre Salinas Tomapasca

N°	PREGUNTA	APRECIACIÓN		APORTES Y/O SUGERENCIAS
		SI	NO	
1	¿Considera que la autenticación multifactorial debe ser una característica para un modelo de ciberseguridad en tiempos de transformación digital?	X		
2	¿Considera que la protección del endpoint fuera del perímetro debe ser una característica para un modelo de ciberseguridad en tiempo de transformación digital?	X		
3	¿Un modelo de ciberseguridad en tiempos de transformación digital debe tener la capacidad de integrar sus soluciones de seguridad en el diseño de su arquitectura para una mejor protección y visibilidad de toda la red?	X		
4	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe adoptar estrategias de Threat Hunting para la detección proactiva de amenazas avanzadas?	X		
5	¿El análisis del comportamiento del usuario debe ser una característica para un modelo de ciberseguridad en tiempos de transformación digital?	X		
6	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital solo debe desconfiar del tráfico proveniente desde internet y confiar plenamente en todo el tráfico interno?		X	Se debe validar toda actividad en la red.
7	¿Un modelo de ciberseguridad en tiempos de transformación digital debe adaptarse a un ciclo continuo de gestión de la ciberseguridad y el riesgo?	X		
8	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe hacerle frente a los malware únicamente a través del análisis basado en firmas?		X	Se debe considerar todo tipo de amenazas
9	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe utilizar ejercicios de Red Team para simular ciberataques avanzados?	X		
10	¿A nivel organizacional, considera que una estructura piramidal que comprenda los niveles Estratégicos, operacionales y tácticos para la gestión de la ciberseguridad en toda la organización fortalecería el modelo?	X		
11	¿A nivel organizacional, considera que deben existir secciones dedicadas exclusivamente a ver temas de ciberseguridad, tanto de lado de Seguridad de la información, como de tecnologías de la información?	X		
12	¿Considera que el modelo Zero Trust, basado en desconfiar de todo el tráfico y verificarlo todo, cumpliría con las exigencias de la transformación digital y de la coyuntura actual?	X		

Nombre y Firma
Fecha: 02/09/2021
Arnaldo Alvarado Jacliva

UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

LISTA DE COTEJO

Nombres del especialista: Juan Carlos Plasencia Cabrerillos

Institución donde labora: Caja Trujillo

Cargo en la institución: Coordinador Canales Tecnológicos

Trabajó en alguna Caja Municipal? (Nombre de la institución y cargo):

.....

Autor del Instrumento: Alan Pierre Salinas Tomapasca

N°	PREGUNTA	APRECIACIÓN		APORTES Y/O SUGERENCIAS
		SI	NO	
1	¿Considera que la autenticación multifactorial debe ser una característica para un modelo de ciberseguridad en tiempos de transformación digital?	✓		
2	¿Considera que la protección del endpoint fuera del perímetro debe ser una característica para un modelo de ciberseguridad en tiempo de transformación digital?	✓		
3	¿Un modelo de ciberseguridad en tiempos de transformación digital debe tener la capacidad de integrar sus soluciones de seguridad en el diseño de su arquitectura para una mejor protección y visibilidad de toda la red?	✓		
4	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe adoptar estrategias de Threat Hunting para la detección proactiva de amenazas avanzadas?	✓		
5	¿El análisis del comportamiento del usuario debe ser una característica para un modelo de ciberseguridad en tiempos de transformación digital?	✓		
6	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital solo debe desconfiar del tráfico proveniente desde internet y confiar plenamente en todo el tráfico interno?		✓	Debe cumplir un monitoreo 360. Cubriendo vectores internos y externos.
7	¿Un modelo de ciberseguridad en tiempos de transformación digital debe adaptarse a un ciclo continuo de gestión de la ciberseguridad y el riesgo?	✓		
8	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe hacerle frente a los malware únicamente a través del análisis basado en firmas?		✓	Complementado con Analisis heuristico.
9	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe utilizar ejercicios de Red Team para simular ciberataques avanzados?	✓		Muy necesesorio para medir los niveles de seguridad existentes.
10	¿A nivel organizacional, considera que una estructura piramidal que comprenda los niveles Estratégicos, operacionales y tácticos para la gestión de la ciberseguridad en toda la organización fortalecería el modelo?	✓		
11	¿A nivel organizacional, considera que deben existir secciones dedicadas exclusivamente a ver temas de ciberseguridad, tanto de lado de Seguridad de la información, como de tecnologías de la información?	✓		
12	¿Considera que el modelo Zero Trust, basado en desconfiar de todo el tráfico y verificarlo todo, cumpliría con las exigencias de la transformación digital y de la coyuntura actual?	✓		

Juan C. Plasencia

Nombre y Firma

Fecha: 26.08.2021

UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

LISTA DE COTEJO

Nombres del especialista: .....OMAR FRANCISCO CARBAJAL LLOSA.....

Institución donde labora: .....CAC ILO.....

Cargo en la institución: .....JEFE DE TECNOLOGÍAS DE LA INFORMACIÓN.....

Trabajó en alguna Caja Municipal? (Nombre de la institución y cargo):
.....CMAC SANTA.....JEFE DE TECNOLOGÍAS DE LA INFORMACION .....

Autor del Instrumento: Alan Pierre Salinas Tomapasca

N°	PREGUNTA	APRECIACIÓN		APORTES Y/O SUGERENCIAS
		SI	NO	
1	¿Considera que la autenticación multifactorial debe ser una característica para un modelo de ciberseguridad en tiempos de transformación digital?	X		
2	¿Considera que la protección del endpoint fuera del perímetro debe ser una característica para un modelo de ciberseguridad en tiempo de transformación digital?	X		Para el trabajo remoto con acceso a servicios internos de la red empresarial.
3	¿Un modelo de ciberseguridad en tiempos de transformación digital debe tener la capacidad de integrar sus soluciones de seguridad en el diseño de su arquitectura para una mejor protección y visibilidad de toda la red?	X		
4	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe adoptar estrategias de Threat Hunting para la detección proactiva de amenazas avanzadas?	X		
5	¿El análisis del comportamiento del usuario debe ser una característica para un modelo de ciberseguridad en tiempos de transformación digital?	X		Para todo momento.
6	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital solo debe desconfiar del tráfico proveniente desde internet y confiar plenamente en todo el tráfico interno?		X	Deben protegerse extena e internamente.
7	¿Un modelo de ciberseguridad en tiempos de transformación digital debe adaptarse a un ciclo continuo de gestión de la ciberseguridad y el riesgo?	X		
8	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe hacerle frente a los malware únicamente a través del análisis basado en firmas?		X	Deben considerar soluciones EDR.
9	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe utilizar ejercicios de Red Team para simular ciberataques avanzados?	X		Debe ser una política, tener planificado cada cierto tiempo (mínimo 2 al año) y controlado.
10	¿A nivel organizacional, considera que una estructura piramidal que comprenda los niveles Estratégicos, operacionales y tácticos para la gestión de la ciberseguridad en toda la organización fortaleceria el modelo?		X	No necesariamente, claro que ayuda, pero lo importante es bajo el control y visión por procesos en toda la organización.
11	¿A nivel organizacional, considera que deben existir secciones dedicadas exclusivamente a ver temas de ciberseguridad, tanto de lado de Seguridad de la información, como de tecnologías de la información?	X		Las áreas tanto de Seguridad de Información como Tecnologías de la Información deben contar con especialistas en seguridad, monitoreando.
12	¿Considera que el modelo Zero Trust, basado en desconfiar de todo el tráfico y verificarlo todo, cumpliría con las exigencias de la transformación digital y de la coyuntura actual?	X		Es importante por el elevado tráfico que genera.

Ms. Ing. Omar Francisco Carbajal Llosa
Jefe de Tecnologías de la Información - CAC ILO

Fecha: 14/09./2021

UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

LISTA DE COTEJO

Nombres del especialista: Omar Ernesto Gil Cuba

Institución donde labora: Banco Ripley

Cargo en la institución: Analista de Riesgo y Seguridad de la Información

Trabajó en alguna Caja Municipal? (Nombre de la institución y cargo): Sí, Caja Trujillo y cargo Analista de Seguridad de Información y Continuidad Negocio

Autor del Instrumento: Alan Pierre Salinas Tomapasca

N°	PREGUNTA	APRECIACIÓN SI	APRECIACIÓN NO	APORTES Y/O SUGERENCIAS
1	¿Considera que la autenticación multifactorial debe ser una característica para un modelo de ciberseguridad en tiempos de transformación digital?	X		Porque no dependerá de una única contraseña
2	¿Considera que la protección del endpoint fuera del perímetro debe ser una característica para un modelo de ciberseguridad en tiempo de transformación digital?	X		Porque integra todos los puntos de acceso.
3	¿Un modelo de ciberseguridad en tiempos de transformación digital debe tener la capacidad de integrar sus soluciones de seguridad en el diseño de su arquitectura para una mejor protección y visibilidad de toda la red?	X		
4	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe adoptar estrategias de Threat Hunting para la detección proactiva de amenazas avanzadas?	X		
5	¿El análisis del comportamiento del usuario debe ser una característica para un modelo de ciberseguridad en tiempos de transformación digital?	X		
6	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital solo debe desconfiar del tráfico proveniente desde internet y confiar plenamente en todo el tráfico interno?		X	porque debe desconfiar del tráfico interno también.
7	¿Un modelo de ciberseguridad en tiempos de transformación digital debe adaptarse a un ciclo continuo de gestión de la ciberseguridad y el riesgo?	X		
8	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe hacerle frente a los malware únicamente a través del análisis basado en firmas?		X	también a los que no tiene firma.
9	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe utilizar ejercicios de Red Team para simular ciberataques avanzados?	X		
10	¿A nivel organizacional, considera que una estructura piramidal que comprenda los niveles Estratégicos, operacionales y tácticos para la gestión de la ciberseguridad en toda la organización fortalecería el modelo?	X		
11	¿A nivel organizacional, considera que deben existir secciones dedicadas exclusivamente a ver temas de ciberseguridad, tanto de lado de Seguridad de la información, como de tecnologías de la información?	X		
12	¿Considera que el modelo Zero Trust, basado en desconfiar de todo el tráfico y verificarlo todo, cumpliría con las exigencias de la transformación digital y de la coyuntura actual?	X		

Omar Gil Cuba.

Nombre y Firma

Fecha: .../...../.....

UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

LISTA DE COTEJO

Nombres del especialista: Ricardo Ramirez Quevedo

Institución donde labora: Caja Trujillo

Cargo en la institución: Analista de Seguridad de la Información y Continuidad del Negocio

Trabajó en alguna Caja Municipal? (Nombre de la institución y cargo):
Caja Municipal de Sullana – Analista de Seguridad de la Información / Caja Trujillo – Analista de Seguridad de la Información y Continuidad del Negocio.

Autor del Instrumento: Alan Pierre Salinas Tomapasca

N°	PREGUNTA	APRECIACIÓN		APORTES Y/O SUGERENCIAS
		SI	NO	
1	¿Considera que la autenticación multifactorial debe ser una característica para un modelo de ciberseguridad en tiempos de transformación digital?	X		
2	¿Considera que la protección del endpoint fuera del perímetro debe ser una característica para un modelo de ciberseguridad en tiempo de transformación digital?	X		Se debe considerar inclusive el enfoque BYOD, para el modelo de Ciberseguridad considerando el entorno de las organizaciones.
3	¿Un modelo de ciberseguridad en tiempos de transformación digital debe tener la capacidad de integrar sus soluciones de seguridad en el diseño de su arquitectura para una mejor protección y visibilidad de toda la red?	X		
4	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe adoptar estrategias de Threat Hunting para la detección proactiva de amenazas avanzadas?	X		
5	¿El análisis del comportamiento del usuario debe ser una característica para un modelo de ciberseguridad en tiempos de transformación digital?	X		
6	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital solo debe desconfiar del tráfico proveniente desde internet y confiar plenamente en todo el tráfico interno?		X	Muchos de los incidentes de ciberseguridad a nivel global han sido materializados por eventos que surgen desde la red interna.
7	¿Un modelo de ciberseguridad en tiempos de transformación digital debe adaptarse a un ciclo continuo de gestión de la ciberseguridad y el riesgo?	X		
8	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe hacerle frente a los malware únicamente a través del análisis basado en firmas?		X	
9	¿Considera que un modelo de ciberseguridad en tiempos de transformación digital debe utilizar ejercicios de Red Team para simular ciberataques avanzados?	X		El modelo de Ciberseguridad debe considerar tato ejercicios de Red Team (a fin que se puedan identificar posibles brechas de seguridad) como de Blue Team, haciendo un reforzamiento al equipo de seguridad informática que se encuentra trabajando para y desde la empresa, a fin que pueda tener un mejor entendimiento de los diversos tipos de ataque y tener un mejor enfoque para la respuesta a incidentes.
10	¿A nivel organizacional, considera que una estructura piramidal que comprenda los niveles Estratégicos, operacionales y tácticos para la gestión de la ciberseguridad en toda la organización fortalecería el modelo?	X		

11	¿A nivel organizacional, considera que deben existir secciones dedicadas exclusivamente a ver temas de ciberseguridad, tanto de lado de Seguridad de la información, como de tecnologías de la información?	X		La ciberseguridad debe considerar la mejor estrategia para el accionar ante los incidentes que se presentan en el entorno, esto implica la sinergia óptima entre ambos frentes (Seguridad de la Información y Tecnologías de la Información)
12	¿Considera que el modelo Zero Trust, basado en desconfiar de todo el tráfico y verificarlo todo, cumpliría con las exigencias de la transformación digital y de la coyuntura actual?	X		

Nombre y Firma Ricardo Ramirez Quevedo

Fecha:07/09/2021

Anexo 4 – Juicio de expertos

UNIVERSIDAD PRIVADA DEL NORTE

UNIVERSIDAD PRIVADA DEL NORTE
ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

JUICIO DE EXPERTO SOBRE LA PERTINENCIA, RELEVANCIA Y CLARIDAD DE LA PROPUESTA MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

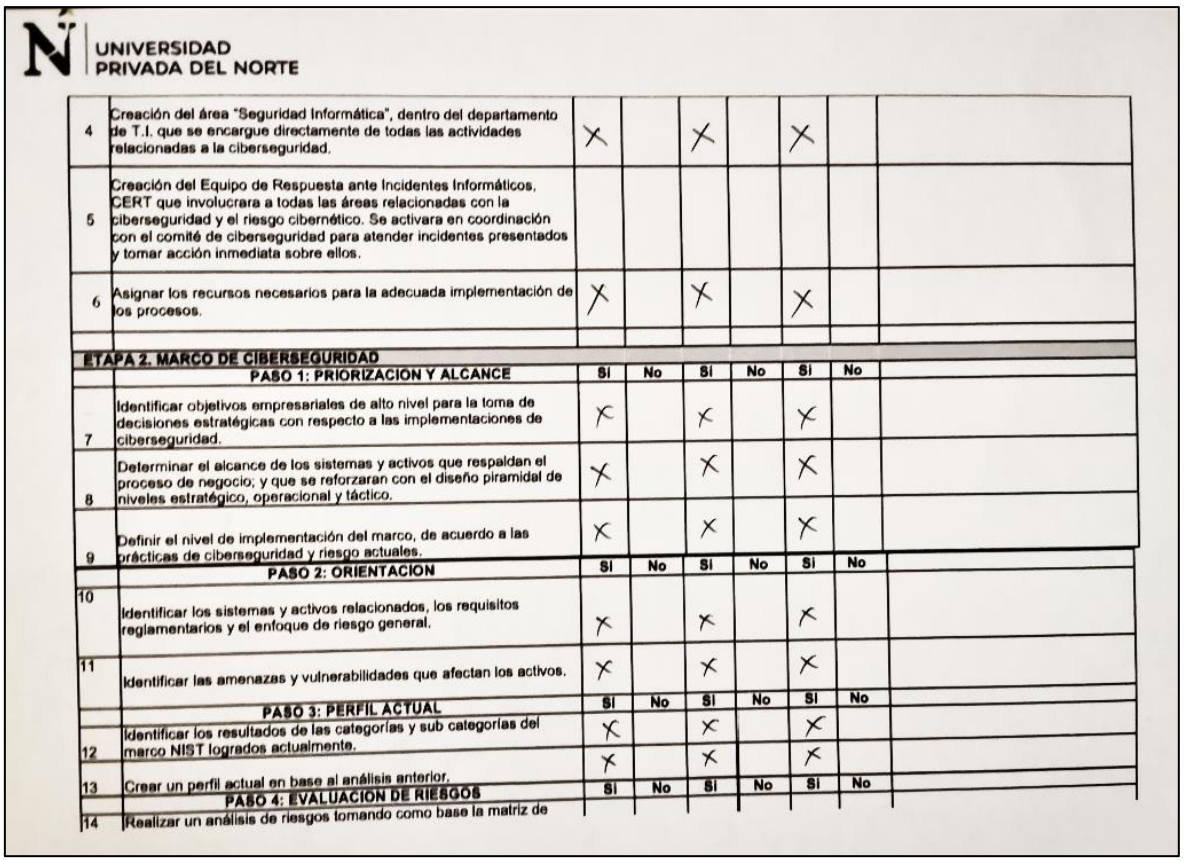
INSTRUCCIONES:

Coloque en cada casilla un aspa correspondiente al aspecto cualitativo de cada ítem y alternativa de respuesta, según los criterios que a continuación se detallan.

[1]**Pertinencia:** El ítem corresponde a la fase o etapa establecida.
[2]**Relevancia:** El ítem es apropiado para representar al componente o fase o etapa establecida.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

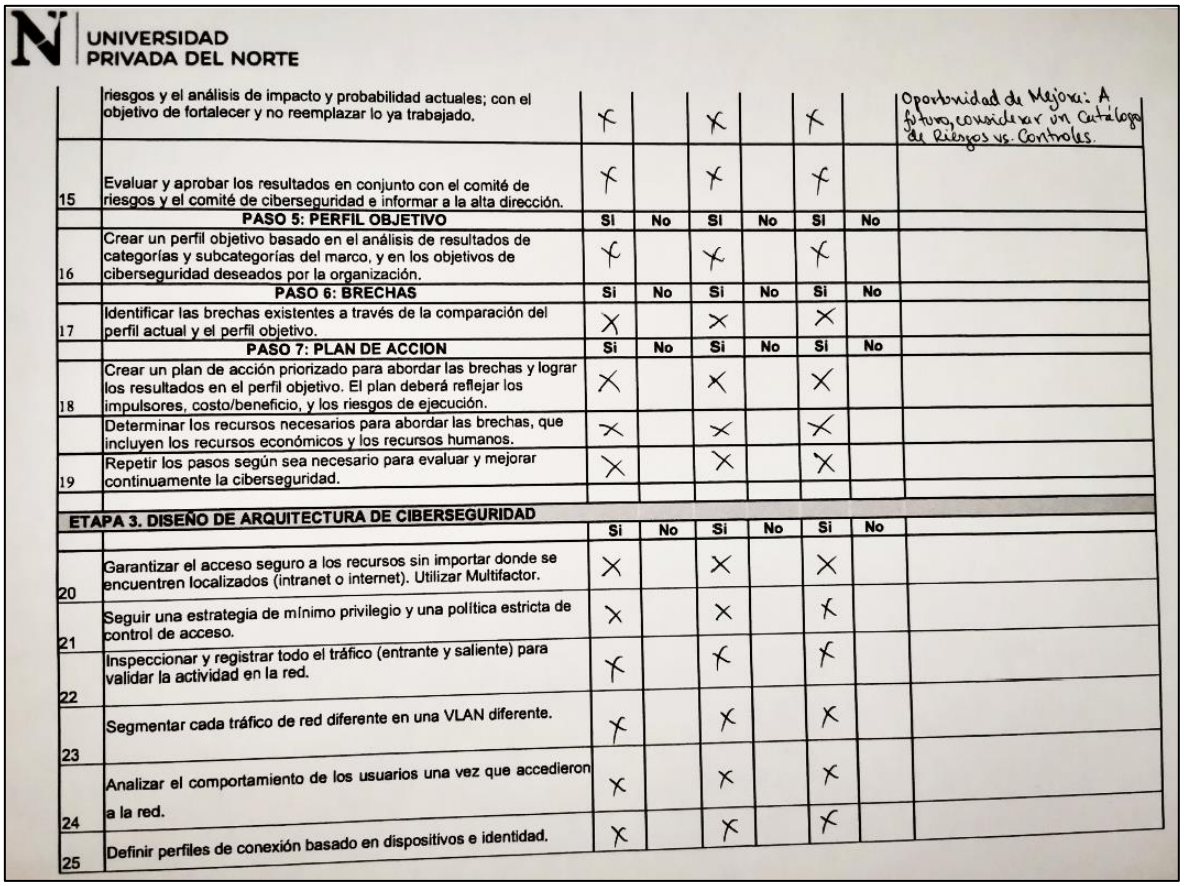
Las etapas a evaluar son: Contexto organizacional, marco de ciberseguridad, diseño de arquitectura de ciberseguridad y cultura en ciberseguridad. En la casilla de sugerencias puede sugerir el cambio o mejora a cada actividad.

Nº	ETAPA / FASE/ACTIVIDAD	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
ETAPA 1. CONTEXTO ORGANIZACIONAL								
	CONTEXTO ORGANIZACIONAL	Si	No	Si	No	Si	No	
1	Definir el flujo de información y de toma de decisiones sobre la base de una estructura piramidal a través de la creación de tres niveles: Estratégico, Operacional y táctico que soporte el modelo y la gestión de ciberseguridad.	X		X		X		
2	Creación del "Comité de ciberseguridad", el cual se encargará de asesorar a la alta dirección en el análisis y la definición de la Política General de Ciberseguridad; proponer acciones para superar las brechas encontradas; evaluar la correcta implementación y funcionamiento del marco de ciberseguridad; entre otras.	X		X		X		
3	Reestructurar el departamento de seguridad de la información, creando las siguientes secciones que dependerán directamente del oficial de seguridad: sección de Seguridad de la información, sección de continuidad del negocio y sección de ciberseguridad.	X		X		X		



UNIVERSIDAD PRIVADA DEL NORTE

4	Creación del área "Seguridad Informática", dentro del departamento de T.I. que se encargue directamente de todas las actividades relacionadas a la ciberseguridad.	X		X		X		
5	Creación del Equipo de Respuesta ante Incidentes Informáticos, CERT que involucrara a todas las áreas relacionadas con la ciberseguridad y el riesgo cibernético. Se activara en coordinación con el comité de ciberseguridad para atender incidentes presentados y tomar acción inmediata sobre ellos.							
6	Asignar los recursos necesarios para la adecuada implementación de los procesos.	X		X		X		
	ETAPA 2. MARCO DE CIBERSEGURIDAD							
	PASO 1: PRIORIZACIÓN Y ALCANCE	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	Identificar objetivos empresariales de alto nivel para la toma de decisiones estratégicas con respecto a las implementaciones de ciberseguridad.	X		X		X		
8	Determinar el alcance de los sistemas y activos que respaldan el proceso de negocio, y que se reforzaran con el diseño piramidal de niveles estratégico, operacional y táctico.	X		X		X		
9	Definir el nivel de implementación del marco, de acuerdo a las prácticas de ciberseguridad y riesgo actuales.	X		X		X		
	PASO 2: ORIENTACIÓN	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	Identificar los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general.	X		X		X		
11	Identificar las amenazas y vulnerabilidades que afectan los activos.	X		X		X		
	PASO 3: PERFIL ACTUAL	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	Identificar los resultados de las categorías y sub categorías del marco NIST logrados actualmente.	X		X		X		
13	Crear un perfil actual en base al análisis anterior.	X		X		X		
	PASO 4: EVALUACIÓN DE RIESGOS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
14	Realizar un análisis de riesgos tomando como base la matriz de							



UNIVERSIDAD PRIVADA DEL NORTE

	riesgos y el análisis de impacto y probabilidad actuales; con el objetivo de fortalecer y no reemplazar lo ya trabajado.	X		X		X		Oportunidad de Mejora: A futuro, considerar un Catálogo de Riesgos vs. Controles.
15	Evaluar y aprobar los resultados en conjunto con el comité de riesgos y el comité de ciberseguridad e informar a la alta dirección.	X		X		X		
	PASO 5: PERFIL OBJETIVO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	Crear un perfil objetivo basado en el análisis de resultados de categorías y subcategorías del marco, y en los objetivos de ciberseguridad deseados por la organización.	X		X		X		
	PASO 6: BRECHAS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
17	Identificar las brechas existentes a través de la comparación del perfil actual y el perfil objetivo.	X		X		X		
	PASO 7: PLAN DE ACCION	**Si**	**No**	**Si**	**No**	**Si**	**No**	
18	Crear un plan de acción priorizado para abordar las brechas y lograr los resultados en el perfil objetivo. El plan deberá reflejar los impulsores, costo/beneficio, y los riesgos de ejecución.	X		X		X		
	Determinar los recursos necesarios para abordar las brechas, que incluyen los recursos económicos y los recursos humanos.	X		X		X		
19	Repetir los pasos según sea necesario para evaluar y mejorar continuamente la ciberseguridad.	X		X		X		
	ETAPA 3. DISEÑO DE ARQUITECTURA DE CIBERSEGURIDAD							
		Si	**No**	**Si**	**No**	**Si**	**No**	
20	Garantizar el acceso seguro a los recursos sin importar donde se encuentren localizados (intranet o internet). Utilizar Multifactor.	X		X		X		
21	Seguir una estrategia de mínimo privilegio y una política estricta de control de acceso.	X		X		X		
22	Inspeccionar y registrar todo el tráfico (entrante y saliente) para validar la actividad en la red.	X		X		X		
23	Segmentar cada tráfico de red diferente en una VLAN diferente.	X		X		X		
24	Analizar el comportamiento de los usuarios una vez que accedieron a la red.	X		X		X		
25	Definir perfiles de conexión basado en dispositivos e identidad.	X		X		X		

UNIVERSIDAD PRIVADA DEL NORTE

26	Validar que las soluciones tecnológicas puedan integrarse entre sí, para garantizar acciones preventivas y proactivas; así como también, conseguir mayor visibilidad en toda la red.	X		X		X		
ETAPA 4. CULTURA EN CIBERSEGURIDAD								
		Si	No	Si	No	Si	No	
27	Comunicar constantemente a los trabajadores sobre las nuevas metodologías y técnicas empleadas en un ciberataque.	X		X		X		
28	Incluir dentro del proceso de inducción para nuevos colaboradores una correcta capacitación sobre las políticas de ciberseguridad de la organización.	X		X		X		
29	Implementar programas de capacitaciones y evaluaciones continuas para los colaboradores en materia de ciberseguridad.	X		X		X		
30	Desarrollar un programa formal de entrenamiento en materia de ciberseguridad debidamente documentado, y actualizarlo con frecuencia para incluir en él información sobre nuevos vectores de ataque y otros riesgos.	X		X		X		
31	Conseguir el compromiso de la alta dirección para que respaldas las acciones tomadas.	X		X		X		

En resumen, Ud. diría que la metodología propuesta es: **Viable [X]** **Viable después de corregir [ ]** **No viable [ ]**

Apellidos y nombres del experto: Alvarado Jacinto, Arnaldo Martín **DNI:** 43490242

Grado Académico: Ingeniero de Sistemas **Especialidad del evaluador:** Seguridad de la Información / Continuidad de Negocio / Ciberseg

Institución: Caja Trujillo **Cargo Ejercido en la Institución:** Analista de Seguridad de la Información y Continuidad del Negocio

Julio de 2021

Firma

Ing. Arnaldo Alvarado Jacinto, ISO 27001 LI
CIP Nº 129037. ISO 27032 LCM.

UNIVERSIDAD PRIVADA DEL NORTE

UNIVERSIDAD PRIVADA DEL NORTE
ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

JUICIO DE EXPERTO SOBRE LA PERTINENCIA, RELEVANCIA Y CLARIDAD DE LA PROPUESTA MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

INSTRUCCIONES:

Coloque en cada casilla un aspa correspondiente al aspecto cualitativo de cada ítem y alternativa de respuesta, según los criterios que a continuación se detallan.

[1]**Pertinencia:** El ítem corresponde a la fase o etapa establecida.
[2]**Relevancia:** El ítem es apropiado para representar al componente o fase o etapa establecida.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Las etapas a evaluar son: Contexto organizacional, marco de ciberseguridad, diseño de arquitectura de ciberseguridad y cultura en ciberseguridad. En la casilla de sugerencias puede sugerir el cambio o mejora a cada actividad.

Nº	ETAPA / FASE/ACTIVIDAD	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
ETAPA 1. CONTEXTO ORGANIZACIONAL								
	CONTEXTO ORGANIZACIONAL	Si	No	Si	No	Si	No	
1	Definir el flujo de información y de toma de decisiones sobre la base de una estructura piramidal a través de la creación de tres niveles: Estratégico, Operacional y táctico que soporte el modelo y la gestión de ciberseguridad.	✓		✓		✓		
2	Creación del "Comité de ciberseguridad", el cual se encargará de asesorar a la alta dirección en el análisis y la definición de la Política General de Ciberseguridad; proponer acciones para superar las brechas encontradas; evaluar la correcta implementación y funcionamiento del marco de ciberseguridad; entre otras.	✓		✓		✓		
3	Reestructurar el departamento de seguridad de la información, creando las siguientes secciones que dependerán directamente del oficial de seguridad: sección de Seguridad de la información, sección de continuidad del negocio y sección de ciberseguridad.	✓		✓		✓		La entidad evalua su estructura y determinará si unifica o maneja independiente a Dpto. S.I.

UNIVERSIDAD PRIVADA DEL NORTE

4	Creación del área "Seguridad Informática", dentro del departamento de T.I. que se encargue directamente de todas las actividades relacionadas a la ciberseguridad.	✓		✓		✓		Necesario independizar funciones para una correcta gestión. Con sus perfiles definidos.
5	Creación del Equipo de Respuesta ante Incidentes Informáticos, CERT que involucrara a todas las áreas relacionadas con la ciberseguridad y el riesgo cibernético. Se activara en coordinación con el comité de ciberseguridad para atender incidentes presentados y tomar acción inmediata sobre ellos.	✓		✓		✓		
6	Asignar los recursos necesarios para la adecuada implementación de los procesos.	✓		✓		✓		
ETAPA 2. MARCO DE CIBERSEGURIDAD								
	PASO 1: PRIORIZACION Y ALCANCE	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	Identificar objetivos empresariales de alto nivel para la toma de decisiones estratégicas con respecto a las implementaciones de ciberseguridad.	✓		✓		✓		
8	Determinar el alcance de los sistemas y activos que respaldan el proceso de negocio; y que se reforzaran con el diseño piramidal de niveles estratégico, operacional y táctico.	✓		✓		✓		
9	Definir el nivel de implementación del marco, de acuerdo a las prácticas de ciberseguridad y riesgo actuales.	✓		✓		✓		
	PASO 2: ORIENTACION	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	Identificar los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general.	✓		✓		✓		Necesario contar con una política de actualización de inventarios periódica.
11	Identificar las amenazas y vulnerabilidades que afectan los activos.	✓		✓		✓		
	PASO 3: PERFIL ACTUAL	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	Identificar los resultados de las categorías y sub categorías del marco NIST logrados actualmente.	✓		✓		✓		
13	Crear un perfil actual en base al análisis anterior.	✓		✓		✓		
	PASO 4: EVALUACION DE RIESGOS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
14	Realizar un análisis de riesgos tomando como base la matriz de							

UNIVERSIDAD PRIVADA DEL NORTE

	riesgos y el análisis de impacto y probabilidad actuales; con el objetivo de fortalecer y no reemplazar lo ya trabajado.	✓		✓		✓		
15	Evaluar y aprobar los resultados en conjunto con el comité de riesgos y el comité de ciberseguridad e informar a la alta dirección.	✓		✓		✓		
	PASO 5: PERFIL OBJETIVO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	Crear un perfil objetivo basado en el análisis de resultados de categorías y subcategorías del marco, y en los objetivos de ciberseguridad deseados por la organización.	✓		✓		✓		
	PASO 6: BRECHAS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
17	Identificar las brechas existentes a través de la comparación del perfil actual y el perfil objetivo.	✓		✓		✓		
	PASO 7: PLAN DE ACCION	**Si**	**No**	**Si**	**No**	**Si**	**No**	
18	Crear un plan de acción priorizado para abordar las brechas y lograr los resultados en el perfil objetivo. El plan deberá reflejar los impulsores, costo/beneficio, y los riesgos de ejecución.	✓		✓		✓		
19	Determinar los recursos necesarios para abordar las brechas, que incluyen los recursos económicos y los recursos humanos.	✓		✓		✓		
20	Repetir los pasos según sea necesario para evaluar y mejorar continuamente la ciberseguridad.	✓		✓		✓		
ETAPA 3. DISEÑO DE ARQUITECTURA DE CIBERSEGURIDAD								
		Si	**No**	**Si**	**No**	**Si**	**No**	
21	Garantizar el acceso seguro a los recursos sin importar donde se encuentren localizados (intranet o internet). Utilizar Multifactor.	✓		✓		✓		
22	Seguir una estrategia de mínimo privilegio y una política estricta de control de acceso.	✓		✓		✓		Política debe estar asociada a una matriz de accesos.
23	Inspeccionar y registrar todo el tráfico (entrante y saliente) para validar la actividad en la red.	✓		✓		✓		Acompañar con reportes de monitoreo
24	Segmentar cada tráfico de red diferente en una VLAN diferente.	✓		✓		✓		
25	Analizar el comportamiento de los usuarios una vez que accedieron a la red.	✓		✓		✓		Integrar la trazabilidad de los accesos.
26	Definir perfiles de conexión basado en dispositivos e identidad.	✓		✓		✓		Integrar listas blancas de accesos.

UNIVERSIDAD PRIVADA DEL NORTE

27	Validar que las soluciones tecnológicas puedan integrarse entre sí, para garantizar acciones preventivas y proactivas; así como también, conseguir mayor visibilidad en toda la red.	✓		✓		✓		Necesario para garantizar un correcto control integral inmediato.
ETAPA 4. CULTURA EN CIBERSEGURIDAD								
		Si	**No**	**Si**	**No**	**Si**	**No**	
28	Comunicar constantemente a los trabajadores sobre las nuevas metodologías y técnicas empleadas en un ciberataque.	✓		✓		✓		Sensibilizar y concientizar continuamente.
29	Incluir dentro del proceso de inducción para nuevos colaboradores una correcta capacitación sobre las políticas de ciberseguridad de la organización.	✓		✓		✓		
30	Implementar programas de capacitaciones y evaluaciones continuas para los colaboradores en materia de ciberseguridad.	✓		✓		✓		
31	Desarrollar un programa formal de entrenamiento en materia de ciberseguridad debidamente documentado, y actualizarlo con frecuencia para incluir en él información sobre nuevos vectores de ataque y otros riesgos.	✓		✓		✓		
32	Conseguir el compromiso de la alta dirección para que respaldas las acciones tomadas.	✓		✓		✓		Muy necesario para mantener en el tiempo el compromiso

En resumen, Ud. diría que la metodología propuesta es: **Viable [✓]** **Viable después de corregir [ ]** **No viable [ ]**

Apellidos y nombres del experto: Plasencia Cabanillas Juan Carlos **DNI:** 41425380

Grado Académico: Titulado Ing. Electrónica **Especialidad del evaluador:** Diplomado en Seguridad de la Información y Auditoría de Sistemas de Información

Institución: Caja Trujillo **Cargo Ejercido en la Institución:** Coordinador de Canales Tecnológicos

Julio de 2021

Firma

UNIVERSIDAD PRIVADA DEL NORTE

UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

JUICIO DE EXPERTO SOBRE LA PERTINENCIA, RELEVANCIA Y CLARIDAD DE LA PROPUESTA MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

INSTRUCCIONES:

Coloque en cada casilla un aspa correspondiente al aspecto cualitativo de cada ítem y alternativa de respuesta, según los criterios que a continuación se detallan.

[1]**Pertinencia:** El ítem corresponde a la fase o etapa establecida.
[2]**Relevancia:** El ítem es apropiado para representar al componente o fase o etapa establecida.
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Las etapas a evaluar son: Contexto organizacional, marco de ciberseguridad, diseño de arquitectura de ciberseguridad y cultura en ciberseguridad. En la casilla de sugerencias puede sugerir el cambio o mejora a cada actividad.

N°	ETAPA / FASE/ACTIVIDAD	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
ETAPA 1. CONTEXTO ORGANIZACIONAL								
	CONTEXTO ORGANIZACIONAL	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Definir el flujo de información y de toma de decisiones sobre la base de una estructura piramidal a través de la creación de tres niveles: Estratégico, Operacional y táctico que soporte el modelo y la gestión de ciberseguridad.		X	X		X		
2	Creación del "Comité de ciberseguridad", el cual se encargará de asesorar a la alta dirección en el análisis y la definición de la Política General de Ciberseguridad; proponer acciones para superar las brechas encontradas; evaluar la correcta implementación y funcionamiento del marco de ciberseguridad; entre otras.	X		X			X	Enfocarse mas a una política de gestión y control de la seguridad
3	Reestructurar el departamento de seguridad de la información, creando las siguientes secciones que dependerán directamente del oficial de seguridad: sección de Seguridad de la información, sección de continuidad del negocio y sección de ciberseguridad.		X		X		X	La ciberseguridad impacta transversalmente tanto a la SI y CN, también a TI, por lo que deberían reforzar en ambas,

UNIVERSIDAD PRIVADA DEL NORTE

4	Creación del área "Seguridad Informática", dentro del departamento de T.I. que se encargue directamente de todas las actividades relacionadas a la ciberseguridad.	X		X		X		
5	Creación del Equipo de Respuesta ante Incidentes Informáticos, CERT que involucrara a todas las áreas relacionadas con la ciberseguridad y el riesgo cibernético. Se activara en coordinación con el comité de ciberseguridad para atender incidentes presentados y tomar acción inmediata sobre ellos.	X		X		X		
6	Asignar los recursos necesarios para la adecuada implementación de los procesos.	X		X			X	Especificar los procesos a fin.
ETAPA 2. MARCO DE CIBERSEGURIDAD								
	PASO 1: PRIORIZACION Y ALCANCE	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	Identificar objetivos empresariales de alto nivel para la toma de decisiones estratégicas con respecto a las implementaciones de ciberseguridad.	X		X			X	Alinear los objetivos estratégico empresariales con los objetivos estratégicos de l Ciberseguridad
8	Determinar el alcance de los sistemas y activos que respaldan el proceso de negocio; y que se reforzaran con el diseño piramidal de niveles estratégico, operacional y táctico.		X	X		X		
9	Definir el nivel de implementación del marco, de acuerdo a las prácticas de ciberseguridad y riesgo actuales.	X		X		X		
	PASO 2: ORIENTACION	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	Identificar los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general.	X		X		X		
11	Identificar las amenazas y vulnerabilidades que afectan los activos.	X		X			X	Debe considerarse en una matriz de riesgos
	PASO 3: PERFIL ACTUAL	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	Identificar los resultados de las categorías y sub categorías del marco NIST logrados actualmente.	X		X		X		
13	Crear un perfil actual en base al análisis anterior.	X			X	X		
	PASO 4: EVALUACION DE RIESGOS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
14	Realizar un análisis de riesgos tomando como base la matriz de							

UNIVERSIDAD PRIVADA DEL NORTE

	riesgos y el análisis de impacto y probabilidad actuales; con el objetivo de fortalecer y no reemplazar lo ya trabajado.	X		X			X	Objetivo de mapear y controlar periódicamente la exposición al riesgo
15	Evaluar y aprobar los resultados en conjunto con el comité de riesgos y el comité de ciberseguridad e informar a la alta dirección.	X		X		X		
	PASO 5: PERFIL OBJETIVO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	Crear un perfil objetivo basado en el análisis de resultados de categorías y subcategorías del marco, y en los objetivos de ciberseguridad deseados por la organización.	X		X		X		
	PASO 6: BRECHAS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
17	Identificar las brechas existentes a través de la comparación del perfil actual y el perfil objetivo.	X		X		X		
	PASO 7: PLAN DE ACCION	**Si**	**No**	**Si**	**No**	**Si**	**No**	
18	Crear un plan de acción priorizado para abordar las brechas y lograr los resultados en el perfil objetivo. El plan deberá reflejar los impulsores, costo/beneficio, y los riesgos de ejecución.	X		X		X		
	Determinar los recursos necesarios para abordar las brechas, que incluyen los recursos económicos y los recursos humanos.	X		X		X		
19	Repetir los pasos según sea necesario para evaluar y mejorar continuamente la ciberseguridad.	X		X		X		
ETAPA 3. DISEÑO DE ARQUITECTURA DE CIBERSEGURIDAD								
		Si	**No**	**Si**	**No**	**Si**	**No**	
20	Garantizar el acceso seguro a los recursos sin importar donde se encuentren localizados (intranet o internet). Utilizar Multifactor.	X		X		X		
21	Seguir una estrategia de mínimo privilegio y una política estricta de control de acceso.	X		X		X		
22	Inspeccionar y registrar todo el tráfico (entrante y saliente) para validar la actividad en la red.	X		X		X		
23	Segmentar cada tráfico de red diferente en una VLAN diferente.	X		X		X		
24	Analizar el comportamiento de los usuarios una vez que accedieron a la red.	X		X		X		
25	Definir perfiles de conexión basado en dispositivos e identidad.	X		X		X		

UNIVERSIDAD PRIVADA DEL NORTE

26	Validar que las soluciones tecnológicas puedan integrarse entre sí, para garantizar acciones preventivas y proactivas; así como también, conseguir mayor visibilidad en toda la red.	X		X		X		
ETAPA 4. CULTURA EN CIBERSEGURIDAD								
		Si	**No**	**Si**	**No**	**Si**	**No**	
27	Comunicar constantemente a los trabajadores sobre las nuevas metodologías y técnicas empleadas en un ciberataque.	X		X		X		
28	Incluir dentro del proceso de inducción para nuevos colaboradores una correcta capacitación sobre las políticas de ciberseguridad de la organización.	X		X		X		
29	Implementar programas de capacitaciones y evaluaciones continuas para los colaboradores en materia de ciberseguridad.	X		X		X		
30	Desarrollar un programa formal de entrenamiento en materia de ciberseguridad debidamente documentado, y actualizarlo con frecuencia para incluir en él información sobre nuevos vectores de ataque y otros riesgos.	X		X		X		
31	Conseguir el compromiso de la alta dirección para que respaldas las acciones tomadas.	X		X		X		

En resumen, Ud. diría que la metodología propuesta es: **Viable [X]** **Viable después de corregir [ ]** **No viable [ ]**

Apellidos y nombres del experto: CARBAJAL LLOSA, OMAR FRANCISCO **DNI:** 18198118

Grado Académico: MAESTRO - INGENIERO **Especialidad del evaluador:** Ingeniería de Computación y Sistemas

Institución: CMAC SANTA / CAC ILO **Cargo Ejercido en la Institución:** Jefe de Tecnologías de la Información

Julio de 2021

Ms. Ing. Omar Francisco Carbajal Llosa
Jefe de Tecnologías de la Información - CAC ILO
Firma

UNIVERSIDAD PRIVADA DEL NORTE

UNIVERSIDAD PRIVADA DEL NORTE
ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

JUICIO DE EXPERTO SOBRE LA PERTINENCIA, RELEVANCIA Y CLARIDAD DE LA PROPUESTA MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

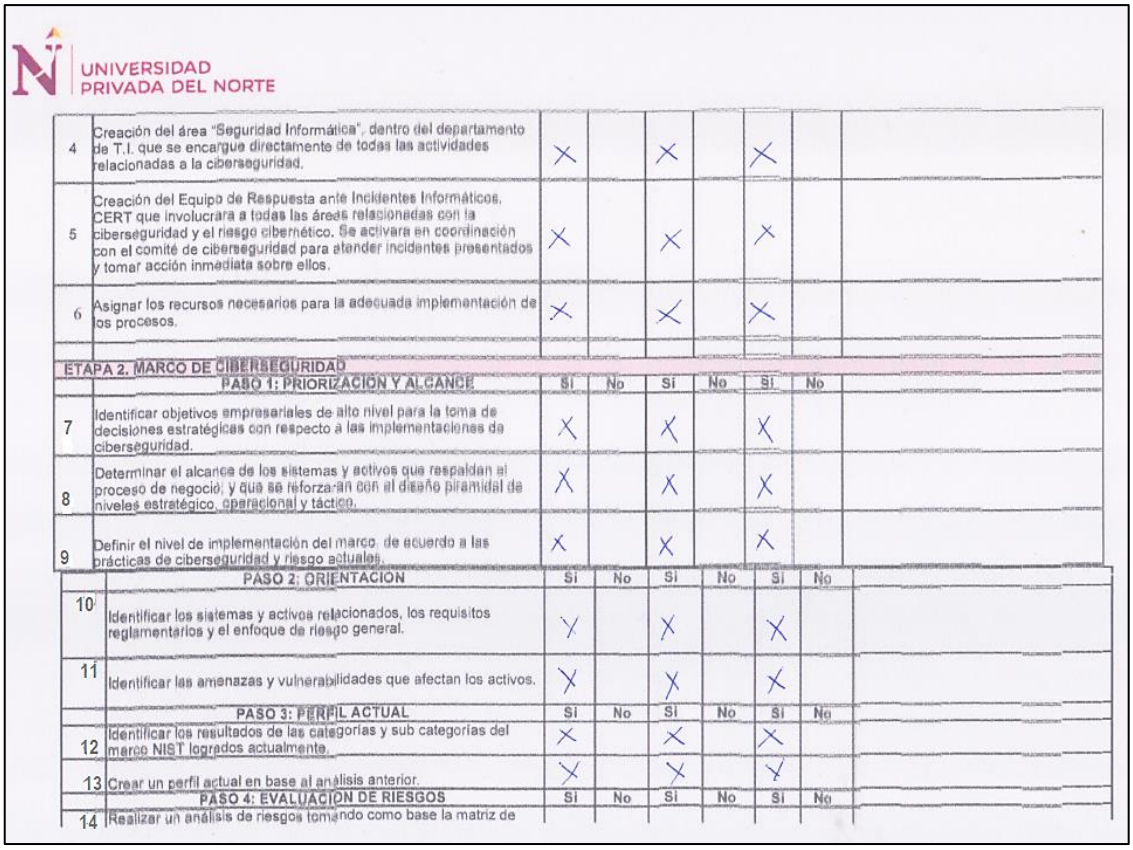
INSTRUCCIONES:

Coloque en cada casilla un aspa correspondiente al aspecto cualitativo de cada ítem y alternativa de respuesta, según los criterios que a continuación se detallan.

[1]Pertinencia: El ítem corresponde a la fase o etapa establecida.
[2]Relevancia: El ítem es apropiado para representar al componente o fase o etapa establecida.
[3]Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

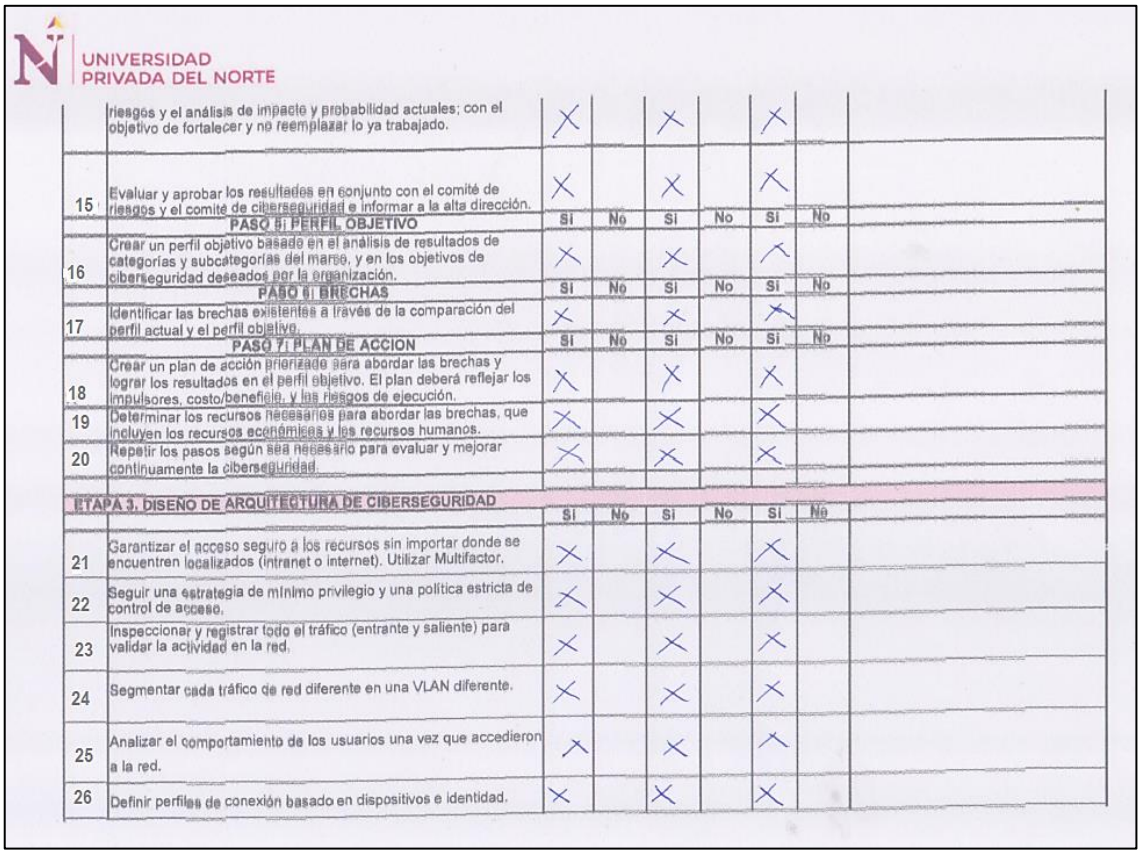
Las etapas a evaluar son: Contexto organizacional, marco de ciberseguridad, diseño de arquitectura de ciberseguridad y cultura en ciberseguridad. En la casilla de sugerencias puede sugerir el cambio o mejora a cada actividad.

Nº	ETAPA / FASE/ACTIVIDAD	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
ETAPA 1. CONTEXTO ORGANIZACIONAL								
	CONTEXTO ORGANIZACIONAL	Si	No	Si	No	Si	No	
1	Definir el flujo de información y de toma de decisiones sobre la base de una estructura piramidal a través de la creación de tres niveles: Estratégico, Operacional y táctico que soporte el modelo y la gestión de ciberseguridad.	X		X		X		
2	Creación del "Comité de ciberseguridad", el cual se encargará de asesorar a la alta dirección en el análisis y la definición de la Política General de Ciberseguridad; proponer acciones para superar las brechas encontradas; evaluar la correcta implementación y funcionamiento del marco de ciberseguridad; entre otras.	X		X		X		
3	Reestructurar el departamento de seguridad de la información, creando las siguientes secciones que dependerán directamente del oficial de seguridad: sección de Seguridad de la información, sección de continuidad del negocio y sección de ciberseguridad.		X		X		X	Misma política para independientes.



UNIVERSIDAD PRIVADA DEL NORTE

4	Creación del área "Seguridad Informática", dentro del departamento de T.I. que se encargue directamente de todas las actividades relacionadas a la ciberseguridad.	X		X		X		
5	Creación del Equipo de Respuesta ante Incidentes Informáticos, CERT que involucrara a todas las áreas relacionadas con la ciberseguridad y el riesgo cibernético. Se activara en coordinación con el comité de ciberseguridad para atender incidentes presentados y tomar acción inmediata sobre ellos.	X		X		X		
6	Asignar los recursos necesarios para la adecuada implementación de los procesos.	X		X		X		
	ETAPA 2. MARCO DE CIBERSEGURIDAD							
	PASO 1: PRIORIZACIÓN Y ALCANCE	Si	No	Si	No	Si	No	
7	Identificar objetivos empresariales de alto nivel para la toma de decisiones estratégicas con respecto a las implementaciones de ciberseguridad.	X		X		X		
8	Determinar el alcance de los sistemas y activos que respaldan el proceso de negocio, y que se reforzaran con el diseño piramidal de niveles estratégico, operacional y táctico.	X		X		X		
9	Definir el nivel de implementación del marco, de acuerdo a las prácticas de ciberseguridad y riesgo actuales.	X		X		X		
	PASO 2: ORIENTACIÓN	Si	No	Si	No	Si	No	
10	Identificar los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general.	X		X		X		
11	Identificar las amenazas y vulnerabilidades que afectan los activos.	X		X		X		
	PASO 3: PERFIL ACTUAL	Si	No	Si	No	Si	No	
12	Identificar los resultados de las categorías y sub categorías del marco NIST logrados actualmente.	X		X		X		
13	Crear un perfil actual en base al análisis anterior.	X		X		X		
	PASO 4: EVALUACIÓN DE RIESGOS	Si	No	Si	No	Si	No	
14	Realizar un análisis de riesgos tomando como base la matriz de							



UNIVERSIDAD PRIVADA DEL NORTE

	riesgos y el análisis de impacto y probabilidad actuales; con el objetivo de fortalecer y no reemplazar lo ya trabajado.	X		X		X		
15	Evaluar y aprobar los resultados en conjunto con el comité de riesgos y el comité de ciberseguridad e informar a la alta dirección.	X		X		X		
	PASO 5: PERFIL OBJETIVO	Si	No	Si	No	Si	No	
16	Crear un perfil objetivo basado en el análisis de resultados de categorías y subcategorías del marco, y en los objetivos de ciberseguridad deseados por la organización.	X		X		X		
	PASO 6: BRECHAS	Si	No	Si	No	Si	No	
17	Identificar las brechas existentes a través de la comparación del perfil actual y el perfil objetivo.	X		X		X		
	PASO 7: PLAN DE ACCION	Si	No	Si	No	Si	No	
18	Crear un plan de acción priorizado para abordar las brechas y lograr los resultados en el perfil objetivo. El plan deberá reflejar los impulsores, costo/beneficio, y los riesgos de ejecución.	X		X		X		
19	Determinar los recursos necesarios para abordar las brechas, que incluyen los recursos económicos y los recursos humanos.	X		X		X		
20	Repetir los pasos según sea necesario para evaluar y mejorar continuamente la ciberseguridad.	X		X		X		
	ETAPA 3. DISEÑO DE ARQUITECTURA DE CIBERSEGURIDAD							
		Si	No	Si	No	Si	No	
21	Garantizar el acceso seguro a los recursos sin importar donde se encuentren localizados (intranet o internet). Utilizar Multifactor.	X		X		X		
22	Seguir una estrategia de mínimo privilegio y una política estricta de control de acceso.	X		X		X		
23	Inspeccionar y registrar todo el tráfico (entrante y saliente) para validar la actividad en la red.	X		X		X		
24	Segmentar cada tráfico de red diferente en una VLAN diferente.	X		X		X		
25	Analizar el comportamiento de los usuarios una vez que accedieron a la red.	X		X		X		
26	Definir perfiles de conexión basado en dispositivos e identidad.	X		X		X		

UNIVERSIDAD PRIVADA DEL NORTE

27	Validar que las soluciones tecnológicas puedan integrarse entre sí, para garantizar acciones preventivas y proactivas; así como también, conseguir mayor visibilidad en toda la red.	X		X		X		
ETAPA 4. CULTURA EN CIBERSEGURIDAD		Si	No	Si	No	Si	No	
28	Comunicar constantemente a los trabajadores sobre las nuevas metodologías y técnicas empleadas en un ciberataque.	X		X		X		
29	Incluir dentro del proceso de inducción para nuevos colaboradores una correcta capacitación sobre las políticas de ciberseguridad de la organización.	X		X		X		
30	Implementar programas de capacitaciones y evaluaciones continuas para los colaboradores en materia de ciberseguridad.	X		X		X		
31	Desarrollar un programa formal de entrenamiento en materia de ciberseguridad debidamente documentado, y actualizarlo con frecuencia para incluir en él información sobre nuevos vectores de ataque y otros riesgos.	X		X		X		
32	Conseguir el compromiso de la alta dirección para que respaldas las acciones tomadas.	X		X		X		

En resumen, Ud. diría que la metodología propuesta es: Viable [X] Viable después de corregir [ ] No viable [ ]

Apellidos y nombres del experto: Gil Cuba Omar Ernesto DNI: 18207811

Grado Académico: Bachiller Especialidad del evaluador: Ingeniería de Sistemas

Institución: Caja Trujillo Cargo Ejercido en la Institución: Analista de Seguridad de Información y Cont. Negocio

Julio de 2021

Omar Gil Cuba

Firma

UNIVERSIDAD PRIVADA DEL NORTE

UNIVERSIDAD PRIVADA DEL NORTE

ESCUELA DE POST GRADO Y ESTUDIOS CONTINUOS

JUICIO DE EXPERTO SOBRE LA PERTINENCIA, RELEVANCIA Y CLARIDAD DE LA PROPUESTA MODELO DE CIBERSEGURIDAD PARA CAJAS MUNICIPALES EN TIEMPOS DE TRANSFORMACION DIGITAL – UN NUEVO ENFOQUE

INSTRUCCIONES:

Coloque en cada casilla un aspa correspondiente al aspecto cualitativo de cada ítem y alternativa de respuesta, según los criterios que a continuación se detallan.

[1]**Pertinencia:** El ítem corresponde a la fase o etapa establecida.

[2]**Relevancia:** El ítem es apropiado para representar al componente o fase o etapa establecida.

[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Las etapas a evaluar son: Contexto organizacional, marco de ciberseguridad, diseño de arquitectura de ciberseguridad y cultura en ciberseguridad. En la casilla de sugerencias puede sugerir el cambio o mejora a cada actividad.

N°	ETAPA / FASE/ACTIVIDAD	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
ETAPA 1. CONTEXTO ORGANIZACIONAL								
	CONTEXTO ORGANIZACIONAL	Si	No	Si	No	Si	No	
1	Definir el flujo de información y de toma de decisiones sobre la base de una estructura piramidal a través de la creación de tres niveles: Estratégico, Operacional y táctico que soporte el modelo y la gestión de ciberseguridad.	X		X		X		

UNIVERSIDAD PRIVADA DEL NORTE

2	Creación del "Comité de ciberseguridad", el cual se encargará de asesorar a la alta dirección en el análisis y la definición de la Política General de Ciberseguridad; proponer acciones para superar las brechas encontradas; evaluar la correcta implementación y funcionamiento del marco de ciberseguridad; entre otras.		X	X		X		Se debe tener en cuenta que según la ISO/IEC 27032 La Ciberseguridad se encuentra embebido dentro de la Seguridad de la Información, motivo por el Cual inclusive según la Resolución SBS 504 - 2021 se considera la creación del "Comité de Seguridad de la Información y Ciberseguridad". En ese sentido, se debería crear un comité considerando ambos frentes.
3	Reestructurar el departamento de seguridad de la información, creando las siguientes secciones que dependerán directamente del oficial de seguridad: sección de Seguridad de la información, sección de continuidad del negocio y sección de ciberseguridad.	X		X		X		
4	Creación del área "Seguridad Informática", dentro del departamento de T.I. que se encargue directamente de todas las actividades relacionadas a la ciberseguridad.	X		X		X		
5	Creación del Equipo de Respuesta ante Incidentes Informáticos, CERT que involucrara a todas las áreas relacionadas con la ciberseguridad y el riesgo cibernético. Se activará en coordinación con el comité de ciberseguridad para atender incidentes presentados y tomar acción inmediata sobre ellos.	X		X		X		
6	Asignar los recursos necesarios para la adecuada implementación de los procesos.	X		X		X		
ETAPA 2. MARCO DE CIBERSEGURIDAD								
	PASO 1: PRIORIZACION Y ALCANCE	**Si**	**No**	**Si**	**No**	**Si**	**No**	
7	Identificar objetivos empresariales de alto nivel para la toma de decisiones estratégicas con respecto a las implementaciones de ciberseguridad.	X		X		X		
8	Determinar el alcance de los sistemas y activos que respaldan el proceso de negocio; y que se reforzaran con el diseño piramidal de niveles estratégico, operacional y táctico.	X		X		X		

UNIVERSIDAD PRIVADA DEL NORTE

9	Definir el nivel de implementación del marco, de acuerdo a las prácticas de ciberseguridad y riesgo actuales.	X		X		X		
	PASO 2: ORIENTACION	**Si**	**No**	**Si**	**No**	**Si**	**No**	
10	Identificar los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general.	X		X		X		
11	Identificar las amenazas y vulnerabilidades que afectan los activos.	X		X		X		Se deben especificar activos de información que están interconectados al ciberespacio.
	PASO 3: PERFIL ACTUAL	**Si**	**No**	**Si**	**No**	**Si**	**No**	
12	Identificar los resultados de las categorías y sub categorías del marco NIST logrados actualmente.	X		X		X		
13	Crear un perfil actual en base al análisis anterior.	X		X		X		
	PASO 4: EVALUACION DE RIESGOS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
14	Realizar un análisis de riesgos tomando como base la matriz de riesgos y el análisis de impacto y probabilidad actuales; con el objetivo de fortalecer y no reemplazar lo ya trabajado.	X		X		X		
15	Evaluar y aprobar los resultados en conjunto con el comité de riesgos y el comité de ciberseguridad e informar a la alta dirección.	X		X		X		
	PASO 5: PERFIL OBJETIVO	**Si**	**No**	**Si**	**No**	**Si**	**No**	

UNIVERSIDAD PRIVADA DEL NORTE

16	Crear un perfil objetivo basado en el análisis de resultados de categorías y subcategorías del marco, y en los objetivos de ciberseguridad deseados por la organización.	X		X		X		
	PASO 6: BRECHAS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
17	Identificar las brechas existentes a través de la comparación del perfil actual y el perfil objetivo.	X		X		X		
	PASO 7: PLAN DE ACCION	**Si**	**No**	**Si**	**No**	**Si**	**No**	
18	Crear un plan de acción priorizado para abordar las brechas y lograr los resultados en el perfil objetivo. El plan deberá reflejar los impulsores, costo/beneficio, y los riesgos de ejecución.	X		X		X		
	Determinar los recursos necesarios para abordar las brechas, que incluyen los recursos económicos y los recursos humanos.	X		X		X		
19	Repetir los pasos según sea necesario para evaluar y mejorar continuamente la ciberseguridad.	X		X		X		
ETAPA 3. DISEÑO DE ARQUITECTURA DE CIBERSEGURIDAD								
		Si	**No**	**Si**	**No**	**Si**	**No**	
20	Garantizar el acceso seguro a los recursos sin importar donde se encuentren localizados (intranet o internet). Utilizar Multifactor.	X		X		X		La definición del diseño de la Arquitectura de Ciberseguridad debería considerar modelos de Arquitectura de Seguridad Empresarial como por ejemplo SABSA o TOGAF, después de definir las capas de seguridad se pueden considerar los controles a aplicar.
21	Seguir una estrategia de mínimo privilegio y una política estricta de control de acceso.	X		X		X		
22	Inspeccionar y registrar todo el tráfico (entrante y saliente) para validar la actividad en la red.	X		X		X		
23	Segmentar cada tráfico de red diferente en una VLAN diferente.	X		X		X		
24	Analizar el comportamiento de los usuarios una vez que accedieron a la red.	X		X		X		
25	Definir perfiles de conexión basado en dispositivos e identidad.	X		X		X		

UNIVERSIDAD PRIVADA DEL NORTE

26	Validar que las soluciones tecnológicas puedan integrarse entre sí, para garantizar acciones preventivas y proactivas; así como también, conseguir mayor visibilidad en toda la red.	X		X		X		
ETAPA 4. CULTURA EN CIBERSEGURIDAD								
		Si	**No**	**Si**	**No**	**Si**	**No**	
27	Comunicar constantemente a los trabajadores sobre las nuevas metodologías y técnicas empleadas en un ciberataque.	X		X		X		
28	Incluir dentro del proceso de inducción para nuevos colaboradores una correcta capacitación sobre las políticas de ciberseguridad de la organización.	X		X		X		
29	Implementar programas de capacitaciones y evaluaciones continuas para los colaboradores en materia de ciberseguridad.	X		X		X		
30	Desarrollar un programa formal de entrenamiento en materia de ciberseguridad debidamente documentado, y actualizarlo con frecuencia para incluir en él información sobre nuevos vectores de ataque y otros riesgos.	X		X		X		
31	Conseguir el compromiso de la alta dirección para que respaldas las acciones tomadas.	X		X		X		

En resumen, Ud. diría que la metodología propuesta es: Viable [X] Viable después de corregir [ ] No viable [ ]

Apellidos y nombres del experto: Ricardo Ramirez Quevedo DNI: 43976393

Grado Académico: Ingeniero de Sistemas Especialidad del evaluador: Seguridad de la Información y Ciberseguridad

Institución: Caja Trujillo Cargo Ejercido en la Institución: Analista de Seguridad de la Información y Continuidad del Negocio

Firma

Julio de 2021