Universidad de Lima
Facultad de Ingeniería
Carrera de Ingeniería de Sistemas

IOC – INTRUSION OPERATION CENTER

Trabajo de suficiencia profesional para optar el Título Profesional
de Ingeniero de Sistemas

Juan Gabriel Lazo Canazas
Código 20030986

Asesor

Carlos Martin Torres Paredes

Lima – Perú
Febrero de 2021

UNIVERSIDAD DE LIMA
MCMLXV
SCIENTIA ET PRAXIS

IOC – INTRUSION OPERATION CENTER

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

Debido al constante crecimiento del cibercrimen, los ataques e intrusiones informáticas y de la necesidad por las principales empresas de los distintos sectores por proteger su infraestructura informática, se ha generado una necesidad por una forma eficiente de obtener alertas tempranas a las vulnerabilidades existentes a lo largo de toda la infraestructura telemática de la organización y en sus distintos niveles lógicos.

El presente documento describe al sistema bautizado como IOC – Intrusion Operation Center o Centro de Operaciones de Intrusión, un sistema automatizado de alertas tempranas para vulnerabilidades multinivel y multiplataforma, con el objetivo de apoyar de una forma eficiente a la mitigación de riesgos que podrían conllevar a una intrusión exitosa en la infraestructura informática de una organización.

El enfoque en el que trabaja el sistema es netamente proactivo y pretende informar en cortos periodos de tiempo sobre vulnerabilidades halladas para acortar el tiempo de respuesta a la mitigación, sobre todo en aquellos activos críticos para los procesos de negocio de la organización.

Palabras clave:

Ciberseguridad, gestión de vulnerabilidades, ciberamenazas, cibercrimen, sistema de alerta temprana, hacking, pentesting

ABSTRACT

Due to the constant growth in cybercrime, attacks, computer intrusions and the need for companies of different sectors to protect their computer infrastructure, a need has been generated for an efficient way of obtaining early alerts to existing vulnerabilities throughout the entire telematics infrastructure of the organization and at its different logical levels.

The following document describes the IOC Project – Intrusion Operation Center, an automatic vulnerability early detection system that works on different layers and platforms. The project's main objective is to support and enhance the vulnerability management and mitigation process, in order to decrease the risk ratio that could lead to a successful intrusion on the company's digital assets.

The system's approach is preventive and proactive, trying at every step to inform as quickly as possible when a new vulnerability is found in order to increase the efficiency on the response and mitigation tasks, mainly on the organization's critical and most valuable assets.

Keywords:

Cybersecurity, vulnerability management, cyberthreats, cybercrime, early alert system, hacking, pentesting

CAPÍTULO I: INTRODUCCIÓN

En la actualidad es incuestionable que una empresa opere de forma eficiente y tenga posibilidad de escalar sin un brazo tecnológico que apoye los diferentes procesos de la empresa.

La información es desde hace años, activo fundamental de empresas, instituciones y gobiernos. Esta, procesada mediante distintas tecnologías y sistemas, permite que se ofrezcan un sinfín de servicios de relevancia tanto para la parte interna de la empresa, como para la del lado de sus clientes o proveedores.
Este incremento en uso de tecnología provoca el aumento de complejidad de las redes y sistemas, así como la hiper conectividad hacia redes privadas y públicas.

Como consecuencia de todo lo mencionado, se incrementa también el riesgo de que algún sistema o su información, vea impactada sus propiedades de confidencialidad, integridad o disponibilidad. A mayor cantidad de sistemas, tecnologías, plataformas, aplicaciones, etc., mayor la superficie tecnológica que hay que resguardar ante posibles eventualidades maliciosas ocasionadas por externos.

Todas las empresas hoy en día están siendo atacadas miles de veces diariamente y desde hace mucho tiempo se sabe que los sistemas no siempre son seguros y que muchas organizaciones se encuentran frecuentemente amenazadas por grupos de hackers o incluso gobiernos que desean la información contenida en sus sistemas.

Al día de hoy han sido vulneradas empresas tan grandes y de segmentos varios como Equifax, Maersk, Linkedin, Twitter, Swift o incluso YouPorn. De amenazas cibernéticas o ciberataques no se escapan ni las instituciones gubernamentales más grandes y seguras como la NSA – National Security Agency.

Nos encontramos entonces ante un escenario donde sin importar las medidas de seguridad implementadas, habrá u ocurrirá algún tipo de ataque o intrusión que tenga éxito a cierta medida y para la cual debemos estar preparados. No se trata entonces de

preocuparnos por “si nos van a atacar” sino más bien “¿qué debemos hacer una vez que recibamos el ataque?” o tratar de integrar un enfoque proactivo para tratar de eliminar al mínimo aquellas vulnerabilidades que podrían representar un riesgo a la información y procesos de la empresa.

El proyecto busca mejorar el tiempo de respuesta de la mitigación de vulnerabilidades de infraestructura, sistemas operativos, aplicaciones y protocolos de comunicación en una organización. De tal forma que cuando los cibercriminales representen una amenaza real, tengan la menor posibilidad de ataque en la organización. El enfoque proactivo que se persigue se realiza mediante la implementación de un sistema de alerta temprana, diseñado, integrado y mejorado por el área de I+D+i de la empresa ENHACKE desde el año 2018 y colocado ya en distintos clientes en segmentos de alto valor en el mercado Peruano y en una empresa Europea a modo de prueba para la mejora continua del proyecto.

En el presente documento se brindan algunos detalles del sistema y cómo busca apoyar en la disminución de los índices de intrusiones exitosas en sistemas críticos en las empresas.

CAPÍTULO II: FUNDAMENTOS TEÓRICOS

En este apartado se brindará de forma general, distintos conceptos necesarios para la comprensión de la tecnología y la implementación del proyecto en cuestión.

2.1 Enfoques de ciberseguridad

Existen distintos enfoques de ciberseguridad en la actualidad, utilizados por las empresas según su tamaño, industria, apetito de riesgo y nivel de presupuesto. Los enfoques no son excluyentes, sino más bien son utilizados en forma complementaria para tratar de minimizar el riesgo de exposición a ciberataques y dependerán de la postura de la organización, su grado de madurez en ciberseguridad y la estrategia de TI y negocios prevista por la empresa. Los enfoques pueden ser categorizados según:

- Tipo de postura o acción: defensiva u ofensiva.
- Alcance para proteger o analizar de la infraestructura informática de la organización: interna o externa, también llamada perimetral.

A continuación, se describen estos enfoques.

2.1.1 Ciberseguridad defensiva

Las empresas que utilizan este enfoque buscan proteger sus activos de información de mayor criticidad utilizando lo que se llama protección por resguardo. Es decir, se busca aplicar distintos controles que protejan la información a distintos niveles. Un ejemplo claro de esto podría ser el de un firewall o cortafuegos en una red local o externa y que busquen resguardar una serie de servidores.

El concepto clave en este enfoque es que se busca proteger el activo con algún control, usualmente digital.

2.1.2 Ciberseguridad ofensiva

Este enfoque busca el aseguramiento final de los activos, pero probando la seguridad tanto de los sistemas, como de aquellos controles que los protegen. Estas pruebas o análisis ofensivos buscan hallar vulnerabilidades o debilidades en los sistemas de información o de protección, con el objetivo de encontrar oportunidades de mejora.

Como es presumible, este tipo de enfoque trabaja de la mano y es complementario al descrito en el punto 2.1.1.

2.1.3 Ciberseguridad perimetral

Cuando se menciona la ciberseguridad perimetral de una organización, se refiere principalmente a los controles o mecanismos de protección implementados para proteger la parte externa de la infraestructura tecnológica de una organización. Esta parte externa es la que comúnmente se halla de cara a internet y es accesible públicamente.

2.1.4 Ciberseguridad interna

Cuando se menciona la ciberseguridad interna de una organización, se refiere principalmente a la serie de controles o mecanismos de protección implementados para proteger la infraestructura tecnológica interna de la organización. Esta es la que se encuentra en la red local organizacional, también denominada red LAN corporativa.

Incluye la red de servidores locales, los terminales de los usuarios, dispositivos IoT (Internet of Things) de la empresa como cámaras o sensores de producción y dispositivos de comunicación como switches, routers o telefonía VoIP (Voice over IP).

2.2 Tipos de equipos

La necesidad por ciberseguridad en las organizaciones ha llevado a que se generen nuevos perfiles profesionales, especializados en temas muy concretos de la ciberseguridad.

Inicialmente se hablaba solamente de los hackers éticos, perfil que ha sufrido una evolución debido al grado de subespecialización requerida para procesos específicos de la organización, como lo son, la defensa, el ataque y la orientación a negocio. A continuación, se mencionan los tres más comunes en la actualidad.

2.2.1 Red team

El equipo profesional denominado como red team o de bandera roja, tiene como función principal realizar pruebas a la infraestructura tecnológica de la empresa, bajo un enfoque netamente ofensivo. Su objetivo es tratar de simular ataques de terceros maliciosos que intenten impactar contra la confidencialidad, integridad o disponibilidad de los sistemas o la información contenida en estos.

2.2.2 Blue team

El equipo profesional denominado como blue team o de bandera azul, tiene como función principal realizar la protección de la infraestructura tecnológica de la organización, utilizando el enfoque de ciberseguridad defensiva. Sus tareas principales son las de implementación de controles de ciberseguridad, monitorización de seguridad y respuesta a incidentes.

2.2.3 Purple team

El equipo profesional denominado como purple team o de bandera púrpura, tiene como función principal proponer niveles de protección adecuados según el perfil de atacante que podría ser una amenaza para la organización. El profesional de este equipo buscaría aterrizar los controles, con el conocimiento también de la parte atacante, para que estos sean sensatos para el negocio, el nivel de presupuesto, la amenaza real y la industria en la que se desarrolla la organización.

A diferencia de un profesional del equipo de bandera roja o read team, el integrante de un equipo de bandera púrpura comprende los ataques y las técnicas utilizadas para llevarlos a cabo, pero sus funciones tienen énfasis especial en analizar si los controles impuestos por el equipo de bandera azul son necesarios, efectivos y eficientes.

2.3 Tipos de test de intrusión

Como se mencionó en el punto 2.1.2, algunas empresas realizan pruebas ofensivas para medir su ciberseguridad y encontrar nuevas brechas o vulnerabilidades que podrían ser explotadas por cibercriminales o terceros maliciosos. Estas pruebas se realizan bajo distintas modalidades o niveles, explicados a continuación.

2.3.1 Caja negra

Son pruebas ofensivas que simulan de la forma más real, un posible ataque por un cibercriminal o un grupo de estos que tienen por objetivo llegar a generar intrusión en algún nivel de la infraestructura informática de la organización. Estas pruebas, para tratar de generar un escenario real, se realizan sin contar con ningún tipo de información acerca de la organización o de su infraestructura.

2.3.2 Caja gris

Estas pruebas comprenden ataques e intentos de intrusión a la infraestructura de la organización como se explicó en el punto anterior, pero con la diferencia que se cuenta con cierto nivel de información acerca de la infraestructura informática de la organización, usualmente direcciones IP, objetivos o información sobre los dispositivos a ser analizados.

2.3.3 Caja blanca

En este nivel de pruebas, se realizan ataques, pero contando con una amplia lista de detalles e información sobre la infraestructura informática de la organización, la tecnología y los procedimientos con los que se trabajan. En este nivel se puede llegar incluso a tener como punto de inicio del análisis, el código fuente de la aplicación web, móvil o los parámetros de configuración de la infraestructura a ser analizada.

2.4 Tecnologías aplicables

En el presente apartado se detallan algunas tecnologías que se utilizan actualmente en los distintos enfoques de ciberseguridad descritos anteriormente y que servirán para comprender mejor la idoneidad del proyecto.

2.4.1 Tecnologías de centralización de eventos

También conocidos como sistemas de correlación de eventos o SIEM – Security Information Events Manager. Tienen como principal objetivo reunir toda la información de registro o logs de los distintos dispositivos de seguridad y redes de la infraestructura informática de la organización, para procesar y mostrar lo más relevante. Este tipo de solución brinda información para tomar acciones de forma reactiva y responder ante intentos de ataque que se puedan llevar a cabo.

2.4.2 Tecnologías de respuesta a incidentes

Existe una gran variedad de soluciones que brindan algún tipo de respuesta a incidentes automatizada bajo una forma reactiva, es decir, como respuesta a una eventualidad establecida o incidente de ciberseguridad. La característica principal de este tipo de tecnología es que pueda responder a eventos previamente definidos en forma de reglas.

Mientras mejor establecidas sean estas reglas, mejor capacidad de respuesta tendrá el sistema.

2.4.3 Tecnologías de inteligencia de eventos

En los últimos años se ha visto la aparición de tecnologías que se apoyan en el análisis de grandes cantidades de información proporcionada por la misma infraestructura tecnológica de la organización y que ayuda a realizar inteligencia de red, sobre todo en eventos pasados, brindando de esta forma la capacidad de analizar eventos pasados con niveles de detalle increíbles.

Este tipo de tecnologías utilizan lo que llaman información inteligente de red (smart network data) para plasmar en algún tipo de plantilla o firma, el contenido de red de un ataque específico llevándose a cabo en algún lugar de la infraestructura de la organización, de tal forma que esta firma de paquete de red sirve para buscar en toda la información recolectada y almacenada previamente, con el objetivo de encontrar patrones de flujo de comunicación con cierto grado de similitud para poder identificar ataques que se llevaron a cabo en el pasado pero que no fueron detectados porque aún no se sabía de dicho comportamiento, ataque o comunicación maliciosa en la red.

2.4.4 Tecnologías de computación en la nube

El uso de servicios en la nube, proveedores de plataformas o infraestructuras en internet es hoy indiscutible tanto por empresas como por usuarios finales. Servicios de procesamiento en la nube como los proporcionados por AWS, AZURE, GOOGLE CLOUD, DIGITAL OCEAN, OVH, entre otros ofrecen un sinfín de posibilidades para obtener infraestructura especializada con un precio muy accesible y con muchas características de personalización.

2.5 Conceptos adicionales

En el presente apartado se detallan algunos conceptos adicionales que pueden ayudar a la comprensión del proyecto, ya que están estrechamente relacionados con la ciberseguridad y el estado actual de este campo.

2.5.1 Intrusión informática

Es muy común pensar en el hacking o el cibercrimen como un evento fortuito y poco común. Usualmente es relacionado con el fraude bancario (clonación de tarjetas o robo de dinero de cuentas bancarias) o con el robo de cuentas de redes sociales o email, siendo esto solamente una parte muy pequeña de lo que ocurre corporativamente. Una intrusión informática exitosa en una organización puede ocurrir incluso si esta tiene sistemas de seguridad implementados y un equipo que vela por la seguridad. Esto por el grado de complejidad que representa proteger tanto la red interna como externa (cara a internet) de los cibercriminales y la gran cantidad de detalles y factores a tener en cuenta para el aseguramiento de red y corporativo.

Una intrusión informática puede permanecer varias semanas o meses sin ser detectada en la infraestructura de la organización. Según IBM en su informe del costo de una vulneración de datos, el tiempo promedio para identificar y contener una vulneración de datos es de 280 días, mientras el ahorro logrado en caso la organización logre contener la intrusión en menos de 200 días, tiene un promedio de 1 millón de dólares (IBM, 2020).

Para una mejor comprensión de donde puede suceder una intrusión, se listan algunos de los objetivos utilizados comúnmente por los cibercriminales para el ataque:

- Servidores de la red corporativa interna
- Servidores de la red corporativa externa o cara a internet
- Terminales de los usuarios (desktops o laptops)
- Dispositivos inteligentes o IoT
- Dispositivos móviles (tablets o celulares) de los usuarios
- Infraestructura en la nube
- Servicios online corporativas utilizados por la organización (redes sociales, servicios de correo, almacenamiento, trabajo colaborativo, procesamiento de información o análisis de datos en la nube, entre otros)

2.5.2 Advanced Persistent Threat (APT)

Una amenaza persistente avanzada se da cuando un grupo de cibercriminales o agentes especializados de gobierno tiene como fin la intrusión a ciertos objetivos específicos, usualmente alguna industria en algún grupo de países previamente decididos.
Estas oleadas de ataques complejas o avanzadas se dan durante un tiempo prolongando (de ahí el nombre de amenaza persistente).

En los últimos años estos ataques se han hecho tan comunes y conocidos que han sido reconocidos distintos grupos de ataque, algunos incluso relacionados a ciertos países por los intereses geopolíticos que tienen.

Quizás el primero y más reconocido por marcar el inicio de este tipo de ataques de alta complejidad, alcance específico y persistencia en el tiempo, es el ataque que se realizó a las plantas de tratamiento de uranio de Irán, con el objetivo de retrasar su carrera de preparación nuclear. Para esto se creó un malware con el único objetivo de replicarse hasta hallar los controladores que se hacían cargo de las centrífugas de tratamiento de uranio para modificar su funcionamiento y lectura de datos.

El ataque no solo se llevó a cabo, sino que tuvo éxito e Irán reportó tener problemas en sus plantas y tuvieron que retrasar su agenda por un aproximado de dos años. El ataque fue atribuido a Estados Unidos, quien trabajó en conjunto con Israel.

2.5.3 Movimiento lateral

Las organizaciones que cuentan con una infraestructura informática amplia suelen ser mucho más complejas a la hora de proteger o desarrollar un plan de ciberseguridad apropiado, esto por la variedad de factores que se debe tener en cuenta a la hora de implementar un plan de ciberseguridad. Esta complejidad abre paso a que no exista una sola falencia o vulnerabilidad en la red corporativa, sino varias y a distintos niveles.

Dichas vulnerabilidades usualmente son aprovechadas una por una en ciberataques, una vez que algún tipo de intrusión haya ocurrido. El movimiento lateral es justamente el salto entre dispositivos, terminales o servidores aprovechando distintas vulnerabilidades en cada uno de estos, una vez dentro de la red corporativa.

2.5.4 Impactos organizacionales

Como se mencionó antes, usualmente el cibercrimen y el hacking está muy asociado al fraude bancario por clonación de tarjetas o robo de cuentas de redes sociales, sin embargo, corporativamente la intrusión y en algunos casos la divulgación de la información sensible, tienen distintas consecuencias que pueden tener distintos niveles de impacto en la organización, todos con algún nivel de pérdida económica. Se listan algunos a continuación:

- Robo de dinero: Por medio de ataques de suplantación y toma de control de cuentas de correo o identidad digital.
- Pérdida de reputación: Por la divulgación del ataque o información sensible de la organización.
- Multas: Las organizaciones que se encuentran reguladas por distintas entidades (dependiendo del rubro e industria en la que se desarrollan) deben cumplir ciertas normativas que son incumplidas al ser comprobada la intrusión o divulgación de información. Como consecuencia de este incumplimiento, se incurre en multas bastante cuantiosas.
- Secuestro de información: Una vez que la intrusión es exitosa por parte de los cibercriminales, éstos pueden elegir secuestrar la información aplicando métodos de cifrado muchas veces militar que impide el acceso y uso de la información por parte de la organización. Para poder recuperar el acceso a los datos, los cibercriminales piden un rescate que puede ir desde algunas decenas de miles de dólares a un par de millones de dólares.
- Extorsión: Ya se han dado algunos casos también en la que las empresas son extorsionadas para no ver sus datos expuestos públicamente.

2.5.5 Vectores de ataque más comunes

Para un mejor entendimiento de las distintas amenazas y ataques de las que podría ser víctima una organización, se listan a continuación los vectores de ataque más comunes.

- Ataques a nivel web: Uno de los vectores más utilizados por los cibercriminales debido a la alta presencia de aplicaciones web que puede tener una organización actualmente. En esta categoría se pueden encontrar los ataques de inyección de

código (HTML, SQL y de código de lado servidor), robo de sesión, interceptación de los datos, entre otros.

- Ataques de infraestructura: Sea esta interna o externa, tienen por objetivo explotar las distintas vulnerabilidades que puedan tener los servidores de la organización, sus sistemas operativos o su implementación.
- Ataques orientados a clientes: En esta categoría se pueden incluir todos los ataques que tienen por objetivo la intrusión no a un servidor de la organización sino a uno de sus empleados o usuarios, sin importar su posición en la jerarquía organizacional. Este tipo de intrusiones tiene como finalidad encontrar un punto débil de entrada e información que pueda ser utilizada en algún ataque posterior de mayor magnitud. La mayor cantidad de los ataques en esta categoría se dan por ingeniería social, es decir tratando de engañar al usuario por medio de correo, páginas web con ofrecimientos falsos, mensajería, sistemas de colaboración o teletrabajo, redes inalámbricas, entre otros.
- Ataques de denegación de servicio: Este tipo de ataque suele tomarse como una categoría independiente debido a que hay distintas formas de provocar indisponibilidad en un recurso digital de la organización. La forma más usual se da a través de miles de consultas y requerimientos simultáneos al recurso afectado desde distintos puntos de origen, causando su ralentización. También existen distintos métodos que no necesitan mucha potencia de consulta sino por el contrario, algo mínimo de procesamiento, pero si una vulnerabilidad específica que puede colgar o dejar inutilizable el servicio o recurso en cuestión.

CAPÍTULO III: FUNDAMENTACIÓN DEL PROYECTO

3.1 Fundamentación de la deseabilidad del proyecto

En el siguiente apartado se detallan distintos factores que ayudaron a guiar a la evolución del proyecto y de las necesidades que cubriría este en ambientes o escenarios corporativos y gubernamentales.

3.1.1 Estado del cibercrimen

Como resultado de la globalización, la evolución tecnológica, económica, la hiper conectividad y la masividad de la información disponible en la actualidad, no hay negocio que busque subsistir y escalar sin apoyo de un brazo tecnológico.

El incremento de la conectividad de las redes, la introducción de los dispositivos IoT y la gran capacidad de procesamiento posible, han permitido que tecnologías innovadoras como la inteligencia artificial, big data y cloud computing prosperen.

Toda esta revolución tecnológica, como todo, tiene aspectos positivos y negativos. Dentro de las partes negativas o complejas, se podría mencionar que, dados estos grandes avances, cada vez hay menos gente que sepa ampliamente sobre distintos aspectos de la tecnología y todo tiende a ser más especializado aún. Este incremento de complejidad hace también más difícil la gestión apropiada de la ciberseguridad, y habilita que existan mayores posibilidades de error a la hora de desarrollar una tecnología, implementarla, configurarla o incluso utilizarla.

En los siguientes puntos se describe cual es la situación actual del cibercrimen, como se ven afectadas las empresas por el aumento de cibercrimen bajo esta nueva coyuntura y las motivaciones de sus atacantes. El objetivo es establecer la necesidad por herramientas complementarias de ciberseguridad para mejorar los índices de riesgos.

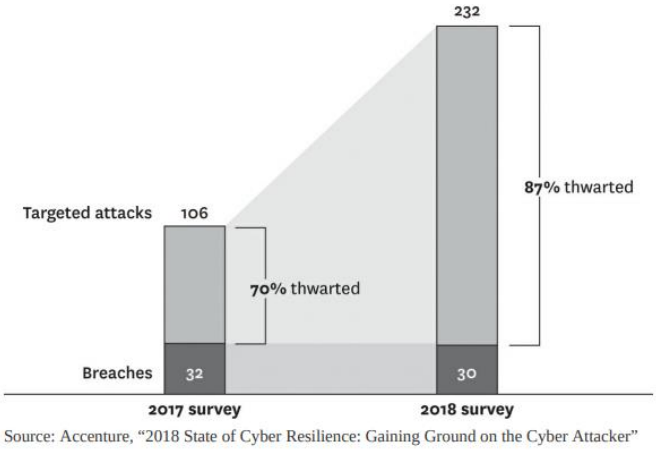
3.1.1.1 Situación actual del cibercrimen global

Según Scott Berinato y Matt Perry, la buena noticia es que las compañías están deteniendo ataques más que nunca, lamentablemente, la mala es que los ataques están incrementándose también (Berinato y Perry, 2019).

En el informe de estado de ciber resiliencia de Accenture, se trata el tema del incremento de ataques y como se muestra claramente en la Figura 3.1, si bien se está detectando un mayor porcentaje de ataques con respecto al año anterior, en proporción, el cibercrimen también incrementó cuantiosamente (Accenture, 2018).

Figura 3. 1

Incremento del cibercrimen y de la detección de ataques



Nota: De *Estado de ciber resiliencia*, por Accenture, 2018 (https://www.accenture.com/_acnmedia/PDF-76/Accenture-2018-state-of-cyber-resilience.pdf#zoom=50)

Verizon en su reporte data breach investigation report (véase Figuras 3.2 y 3.3), toma en cuenta el último año para sus muestras, intervalo en el cual considera para su análisis 157,525 incidentes de ciberseguridad ocurridos en distintas organizaciones a lo largo de 16 industrias distintas y cuatro regiones del mundo (Verizon, 2020).

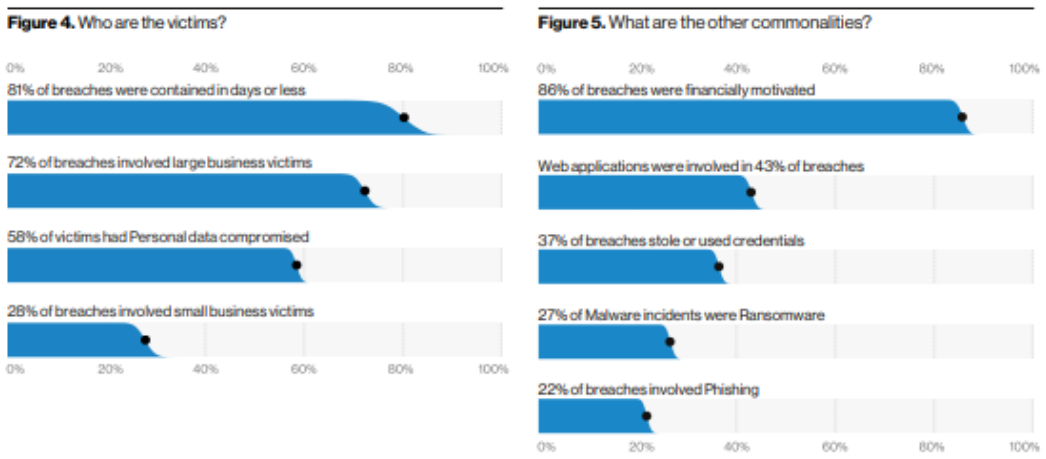
Figura 3. 2

¿Qué tácticas son utilizadas y quien está detrás de los ataques?

Nota: De *Data Breach Investigations Report*, por Verizon, 2020 (https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/)

Figura 3. 3

¿Quiénes son las víctimas y que otros aspectos en común se encuentran?



Nota: De *Data Breach Investigations Report*, por Verizon, 2020 (https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/)

El mensaje es claro en este último informe:

- El cibercrimen incrementa año a año
- Los ataques en su mayoría son generados externamente, es decir a la infraestructura cara a internet de la organización
- Las motivaciones de dichos ataques son en su mayoría financieras

- Mas del 80% de las brechas son contenidas en días, aunque algunas veces un día sea suficiente para tener un impacto económico y reputacional de grandes magnitudes.

3.1.1.2 Situación actual del cibercrimen para la región Latinoamérica

Potencias como Estados Unidos, Rusia y China tienen principal interés en países en vías de desarrollo por el grado de inversión a mediano y largo plazo que puede haber en estos países. Esto trae como resultado crecimiento económico en distintos segmentos e industrias y como se mencionó antes, viene de la mano de tecnología.

En el informe de Verizon se menciona bajo una parte específica de análisis a la región LAC – Latin American and Caribean, donde mencionan que en la región tienen 87 incidentes analizados, de los cuales 14 tuvieron fuga de información publicada y divulgada en forma confirmada.

Para la región, el 91% de los ataques ocurre en forma de denegación de servicio, software malicioso y ataques hacia aplicaciones web.

La mayor cantidad de incidentes tienen una procedencia externa (93%), es decir utilizando internet como medio de ataque y tuvieron fines económicos como motivación principal de ataque.

Dentro de estos casos los 2 más resaltantes mediáticamente fueron los casos del Banco de Crédito del Perú (véase Figura 3.4) y de la cadena de cines Cineplanet (véase Figura 3.5). Ambas organizaciones vieron información sensible publicada en mercado negro y en páginas o foros de hacking, a la venta al mejor postor.

Figura 3. 4
Noticia de ataque realizado al banco BCP

Nota: De *BCP reconoce que sufrió ataque informático en el 2018*, por Diario El Comercio, 2019 (https://elcomercio.pe/economia/negocios/bcp-reconoce-que-sufrio-ataque-informatico-en-el-2018-banco-de-credito-del-peru-nndc-noticia/)

Figura 3. 5
Noticia de ataque realizado a Cineplanet

Nota: De *Datos de cinéfilos peruanos quedan expuestos tras filtración de cadena Cineplanet*, por Diario Gestión, 2020 (https://gestion.pe/tecnologia/cineplanet-datos-de-miles-de-cinefilos-peruanos-quedan-expuestos-tras-filtracion-por-cadena-cineplanet-noticia/)

3.1.1.3 Atacantes y sus motivaciones

Existen 3 tipos de atacantes, categorizados por su motivación:

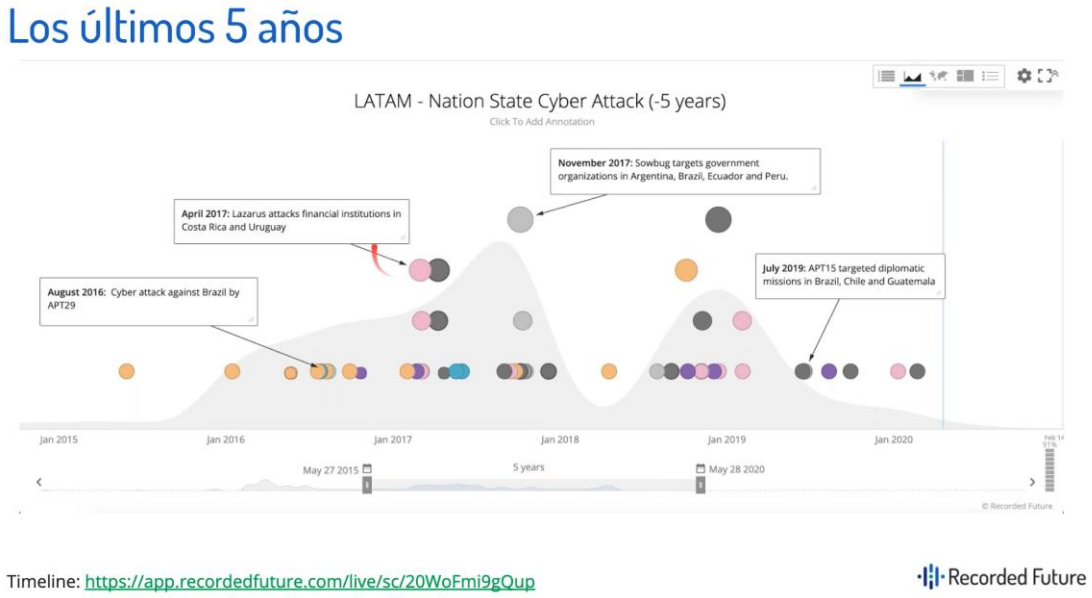
- Atacantes patrocinados por su gobierno

Este tipo de atacantes pertenecen a unidades militares, parte de servicios de inteligencia y llevan a cabo operaciones bajo órdenes militares del gobierno de dicho país. Dado el éxito de las operaciones de ciberespionaje de este tipo, cada año crece su financiamiento por parte del gobierno, por lo que no se espera que este tipo de ataques disminuya.

Los objetivos a ser atacados son variados y corresponden a los intereses de información o control que podría tener geopolíticamente un país sobre otro (véase Figura 3.6). Estos objetivos pueden ser empresas, instituciones de gobierno o personas de

relevancia para sus campañas de recolección de información. En algunos casos los ataques pueden llegar a generar daños físicos como los realizados hacia la infraestructura crítica de Ucrania o ataques contra sistemas de control industrial SCADA.

Figura 3. 6
Ataques patrocinados por gobiernos en los últimos 5 años



Nota: De *Nation State Cyber Attack (-5 years)*, por Recorded Future, 2020 (https://www.recordedfuture.com/)

- Atacantes con motivos financieros

Según los informes mencionados en el punto 3.1.1.1, la mayor cantidad de ataques se llevan a cabo por motivos financieros. Se llevan a cabo ataques de distintos tipos y orientados a distintos sectores empresariales e industriales.

Dentro de los más afectados, por la cantidad de exposición o de superficie de ataque, aquellos segmentos de alto valor como lo son el financiero, minería, infraestructuras críticas y energía.

Las formas de ataque más usuales por este tipo de atacantes son: Ransomware, exfiltración de información, extorsión por información sensible, reventa en mercado negro.

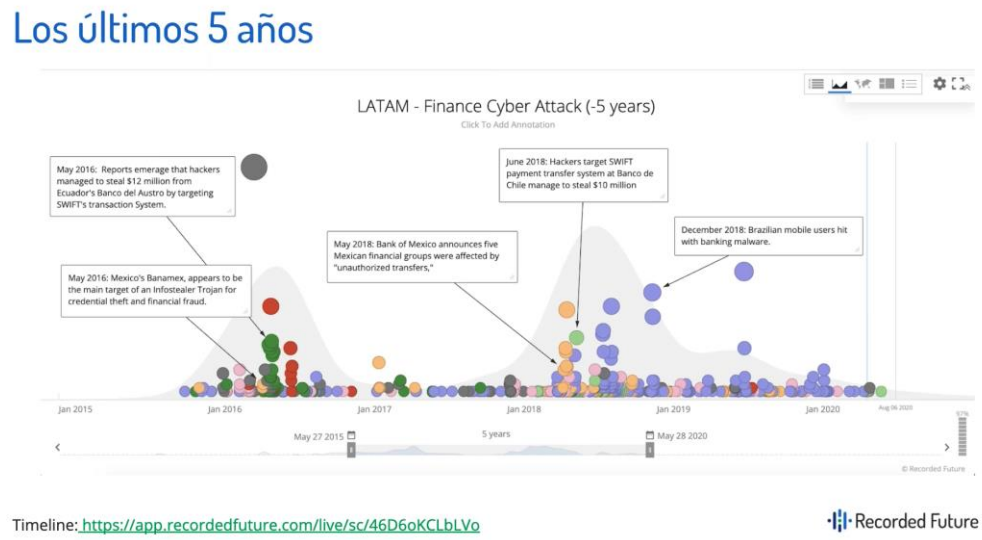
Los atacantes en estos casos pueden ser cibercriminales, grupos de cibercrimen organizado o incluso gobiernos que buscan de esta forma financiar parte de sus campañas de inteligencia y armamentista. Un claro ejemplo de esto se puede observar de los ataques del grupo Lazarus, que supuestamente es de Corea del Norte y que tiene dos unidades de ataque: 121, encargada de llevar a cabo operaciones de inteligencia y 180, a cargo de

realizar ataques grandes que tengan como objetivo extracción u obtención de grandes sumas de dinero. Para tener una mejor idea de la magnitud de este tipo de eventos o cibercrimen organizado por un estado para obtener fondos, podríamos referirnos al ataque que se le hizo al banco de Bangladesh en el año 2016 y que tuvo como consecuencia de este ataque, extracción de dinero por una suma aproximada a los 100 millones de dólares.

En Latinoamérica los ataques al segmento financiero de mayor impacto se dieron mediante la campaña de hacking al sistema SWIFT, donde se hizo extracción de varios millones de dólares a distintos bancos que sufrieron de la intrusión (véase Figura 3.7).

Figura 3. 7

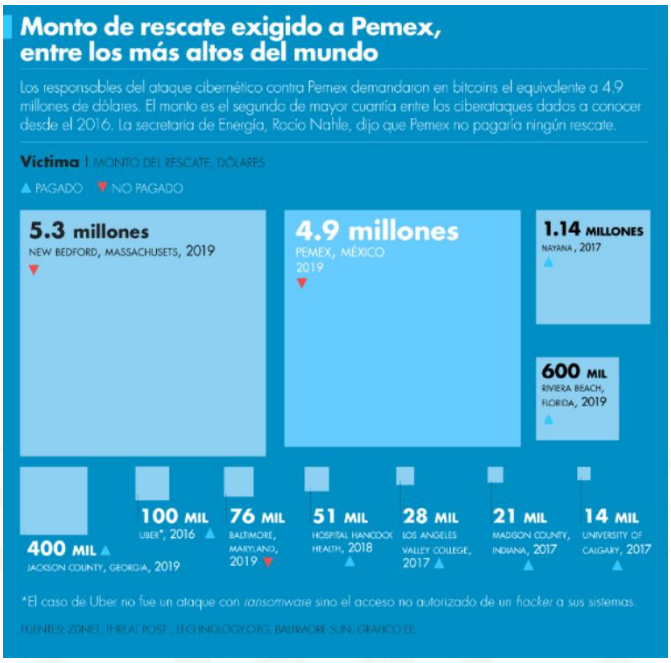
Ciberataques al segmento financiero latinoamericano en los últimos 5 años



Nota: De *Finance Cyber Attack (-5 years)*, por Recorded Future, 2020 (https://www.recordedfuture.com/)

El año pasado, la petrolera mexicana PEMEX sufrió un ataque de tipo Ransomware por el cual fue víctima de extorsión digital por un monto aproximado de 5 millones de dólares (véase Figura 3.8).

Figura 3. 8
Ataque realizado a PEMEX - Petróleos Mexicanos



Nota: De *El rescate por el hackeo a Pemex es el segundo mayor por ransomware)*, por Diario El Economista, 2019 (https://www.recordedfuture.com/)

- Hacktivistas

Este tipo de atacante dice no perseguir fines económicos, sino más bien políticos o ideológicos. El ejemplo más claro es el del grupo Anonymous, que recientemente en el presente año nuevamente tuvo presencia mediática por realizar ataques informáticos para desvelar detalles allegados a la muerte del ciudadano George Floyd en Estados Unidos.

3.1.1.4 Nueva coyuntura: Pandemia COVID-19

En marzo del 2020 la Policía Europea publicó un informe en el que se analizan los factores que harían más fácil que usuarios naturales y corporativos caigan en fraudes, estafas y actos de cibercrimen. Estos factores son:

- Alta demanda por bienes específicos y que se hacen difíciles de hallar
- Movilidad limitada por temas de cuarentena
- Incremento de estadía en casa utilizando tecnologías desde el hogar
- Incremento de miedo y ansiedad por el cambio generado por la pandemia

Estos factores están siendo utilizados y explotados actualmente por cibercriminales para poder acceder a datos de usuarios y empresas.

El Buró Federal de Investigaciones (Federal Bureau of Investigation; FBI), a través de su centro de denuncias de cibercrimen, sostuvo que el cibercrimen por la pandemia se ha cuadruplicado desde el mes de marzo, esto sin tomar en cuenta aquellas empresas que no reportan el ciberataque.

Es necesario mencionar también que, por la pandemia, se verá una contracción económica grande tanto a nivel empresarial como gubernamental, por lo que habrá ajustes en los gastos y la disponibilidad de presupuesto para ciberseguridad podría ser menor, a pesar de que el cibercrimen está en aumento, por lo que son ideales aquellas soluciones que puedan ofrecer altos niveles de efectividad y calidad por un precio accesible.

3.1.2 Estándares y normativas de ciberseguridad

La necesidad por ciberseguridad no ha pasado desapercibida en las industrias que generan altos niveles de ingresos, puesto que son a su vez las más atacadas. Existen distintos estándares y normativas de seguridad de la información que en los últimos años han realizado adiciones para tomar en cuenta el aspecto específico de la ciberseguridad.

- Serie ISO 27000 e ISO 27032
- Superintendencia de Banca y Seguros (SBS) G140
- Payment Card Industry – Data Security Estándar (PCI-DSS), Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago
- General Data Protection Regulation (GDPR), Regulación General de Protección de Datos
- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), Marco de trabajo de Ciberseguridad del Instituto Nacional de Estándares y Tecnología
- Center for Internet Security Controls (CIS Controls), Controles del Centro de Seguridad para Internet

NIST Cybersecurity Framework y CIS Controls se encuentran orientados netamente a un enfoque de ciberseguridad según industria, estados de madurez de la organización y niveles de presupuesto.

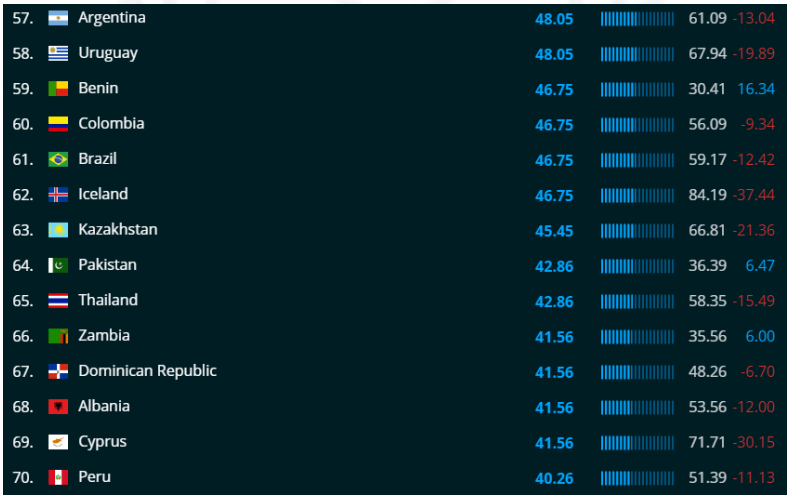
Actualmente existe ya una propuesta de reglamento para la gestión de la seguridad de la información y ciberseguridad dispuesta por la Superintendencia de Banca y Seguros y que plantea hacerse obligatorio para todo el segmento financiero el próximo año. Puede ver la prepublicación del reglamento en el Anexo 1.

3.1.3 Estrategias de ciberseguridad nacional

El incremento del riesgo no solo por el cibercrimen, sino también del ciberespionaje industrial y gubernamental, tuvo como consecuencia en los últimos años que muchos países generen sus estrategias de ciberseguridad nacional. En la región Latinoamérica ya varios países cuentan con una. En el caso de Perú, se tiene una Política Nacional de Ciberseguridad que plantea generar capacidades técnicas, legislativas y de formación para enfrentar las nuevas amenazas consecuencia de la digitalización e hiper conectividad (Anexo 2). Esta política de ciberseguridad vino acompañada de una ley de ciberdefensa que brinda un brazo legislativo para poder articular las estrategias propuestas (Anexo 3).

Adicionalmente, existen organizaciones independientes que, bajo análisis de distintos factores, sitúan a los países según sus niveles de ciberseguridad. Este es el caso del índice de ciberseguridad nacional, establecido por el centro e-Governance Academy de Estonia. En la Figura 3.9 el Perú se sitúa en el puesto 70.

Figura 3. 9
Índice Nacional de Ciberseguridad



Nota: De *National Cybersecurity Index – E-Governance Academy*, por NCSI, 2020 (https://ncsi.ega.ee/ncsi-index/)

Es pertinente mencionar también que Perú ha caído 4 puestos solamente durante la cuarentena. Esto no debido a que hayan decaído los esfuerzos de ciberseguridad en el país, sino a que el número de intrusiones informáticas y ciberataques exitosos han aumentado por el incremento de cibercrimen bajo esta coyuntura sin precedentes.

3.1.4 Servicios de ciberseguridad en el mercado

Actualmente existe una amplia variedad de productos y servicios de ciberseguridad, algunos son completamente complementarios y en muchos otros casos traslapan ciertas características o beneficios entre ellos.

Se listarán los servicios con mayor cantidad de oferta en el mercado de la ciberseguridad:

- Servicios y productos de diagnóstico
    - Auditorías y análisis de brecha
    - **Servicios de ethical hacking:** Servicio que tiene por objetivo simular ataques externos e internos como si de un grupo de hackers se tratase. Este tipo de servicios busca evidenciar vulnerabilidades en la infraestructura interna y la de cara a internet de la organización, antes de que lo hagan los verdaderos atacantes.
    - **Análisis de vulnerabilidades:** Servicio que suele brindarse a modo básico con una herramienta específica según los requerimientos del cliente, con el objetivo de identificar vulnerabilidades en los sistemas implementados por la organización. Los hallazgos reportados por la herramienta no siempre son 100% reales, por lo que hay una tasa importante de falsos positivos que deben ser confirmados por un analista posteriormente.
- Servicios de aseguramiento
    - Implementación de soluciones
    - Configuración e implementación de metodologías y buenas prácticas
    - **Monitorización de incidentes:** Servicio que busca estar siempre alerta, mediante un equipo profesional que monitoriza los activos más críticos de la organización, de tal forma que detecten los ataques que se llevan a cabo

para mitigarlos o en peor de los casos, detectar lo antes posible los que ya se llevaron a cabo y fueron exitosos, para iniciar las medidas de respuesta a incidentes.

- Servicios post ataque
    - Informática forense
    - Respuesta a incidentes

Se resaltaron y detallaron los servicios de ethical hacking y monitorización porque son justamente los que se alinean y complementan con el tema de este proyecto.

3.1.5 Aseguramiento actual vs intrusiones exitosas

Las empresas tratan de prevenir los ciberataques por medio de una mezcla de servicios entre los definidos anteriormente en las categorías de diagnóstico y aseguramiento. Analizaremos los dos servicios detallados anteriormente.

- **Servicios de ethical hacking:** En algunas organizaciones grandes como en caso de los bancos, cuentan con un pequeño equipo que hace este tipo de pruebas, con la desventaja de que este equipo no siempre está actualizado con las últimas técnicas y métodos de ataque, lo que disminuye la efectividad de las pruebas. En la actualidad, este tipo de procesos son parte de programas de gestión de vulnerabilidades dentro de la empresa. Lo más frecuente es que las organizaciones lo tercericen, pero al ser un servicio muy especializado y que requiere un conjunto de habilidades profesionales muy específicas tiende a ser costoso, lo que hace que la empresa solamente decida llevar a cabo este servicio una o dos veces al año.

  En los últimos años, con el incremento de ciberataques y con la intención de reducir la brecha entre vulnerabilidades y mitigación, las organizaciones empezaron a incrementar sus presupuestos de ciberseguridad y con esto, a solicitar más servicios de ethical hacking por año. Es el caso de empresas que por regulaciones como PCI-DSS necesitan llevar a cabo por lo menos 4 procesos de ethical hacking al año.

- **Monitorización de incidentes:** Las organizaciones suelen tercerizar esto mediante la contratación de un SOC o Centro de Operaciones de Seguridad, ellos se encargan de implementar una serie de tecnologías que permiten la visualización

casi total de la infraestructura para poder hacer seguimiento de todo en tiempo real. El problema es que la cantidad de servidores puede llegar a ser grande y la información que estos generan, aún mayor. Es por ello que en los últimos dos años se viene llevando a cabo una actualización a los SOC de segunda generación, que incluyen mucha automatización. El enfoque que suelen tomar este tipo de servicios es el reactivo, es decir, responder cuando el ataque sucede o cuando ya se llevó a cabo.

Lo sorprendente es que a pesar de que muchas empresas lleven a cabo varios procesos de ethical hacking al año y de contar con servicios profesionales muy capaces de monitorización de incidencias, aún así siguen teniendo intrusiones exitosas con exfiltración de datos. Es el caso de empresas de la talla como Equifax, Maersk, Linkedin, Yahoo, Uber, Deloitte, entre otras. Debido a esto es que se está buscando constantemente hallar métodos proactivos, eficientes y cada vez más automatizados para evidenciar las vulnerabilidades y mitigarlas lo antes posible.

3.1.6 Retos actuales y futuros de la ciberseguridad en las empresas

Dicho todo lo anterior, las empresas tienen varios retos por delante y estos justamente pueden ser factores críticos para que un programa de ciberseguridad corporativo sea exitoso, se detallan a continuación estos.

- **Procesos:** Las empresas deben hallar la forma de empezar a integrar nuevas políticas y procedimientos de ciberseguridad en su trabajo diario a lo largo de toda la organización. En un entorno latinoamericano, la ciberseguridad aún es vista como un lujo más que como una necesidad. En parte porque aún no hay una conciencia fuerte sobre su importancia y por la falta de profesionales de niveles ejecutivos que cuenten con el conocimiento, que puedan comandar y dirigir un apropiado Plan Director de Ciberseguridad como parte de una estrategia alineada a los objetivos de negocio de la organización.

  La gran ola de ciberataques en la región Latinoamérica y lo mediáticos que son está cambiando este concepto, pero aún hay organizaciones que no cuentan con áreas de seguridad de la información y al no estar reguladas, tienen un crecimiento tecnológico mientras van evolucionando, pero dejando de lado la ciberseguridad.

- **Personas:** Un factor muy importante por el cual muchas de las empresas tienen dificultad para implementar sus áreas de ciberseguridad dentro de la empresa es

la falta de personal profesional capacitado y que cuente con las habilidades técnicas necesarias. Es por esto que se espera una escasez de profesionales. El principal problema en este tema en particular es que se necesita mucho conocimiento técnico y que no es adquirible rápidamente.

- **Tecnología:** El reto en este punto no es pequeño, existen decenas de soluciones muy buenas pero que tienen un costo muy elevado para un entorno económico latinoamericano, dejando de lado aquellas empresas que no pueden soportar un alto nivel de presupuesto en ciberseguridad. Si, existen las opciones de desarrollo libre, pero estas necesitan más conocimiento del proyecto, gente con conocimientos muy bien fundamentados y en constante capacitación, lo que a la vez encarece el proyecto.

Los tres puntos mencionados anteriormente como retos son justamente los que dan lugar a una necesidad por una tecnología de bajo coste en comparación a otras herramientas, que sea automatizada y que permita realizar simulaciones de ethical hacking con poco esfuerzo y en grandes cantidades para poder reducir los tiempos de respuesta a las mitigaciones de vulnerabilidades descubiertas. El proyecto que se presenta en este documento pretende justamente ser una solución propuesta para estos retos y para aminorar el nivel de riesgo con respecto a las amenazas de creciente cibercrimen a nivel mundial, Latinoamérica y Perú.

3.2 Fundamentación de la factibilidad del proyecto

En este apartado se hablará sobre la tecnología en sí que hace que el proyecto sea posible. La tecnología disponible, las distintas opciones disponibles según el enfoque u objetivo a cumplir, lo que ofrece el proyecto tecnológicamente y como lo ha venido ofreciendo comercialmente.

3.2.1 Soluciones actuales de ciberseguridad

3.2.1.1 Preventivos o de detección de vulnerabilidades

También llamados scanners de vulnerabilidades, existen en el mercado ya desde hace varios años una variada gama de herramientas para la detección de vulnerabilidades a distintos niveles, algunas ven específicamente una parte o una de las capas de OSI específicamente; lo hacen muy detalladamente y otras ven varias capas del modelo, pero

de forma general. Si se pueden categorizar muy fácilmente por la forma de adquisición ya que algunas son licenciadas y otras, de formato abierto o más conocido como herramientas opensource.

Es preciso especificar que no necesariamente por ser una herramienta opensource es de menor calidad que alguna de pago, ya que muchas de estas herramientas abiertas tienen ya bastantes años de evolución y una comunidad bastante bien establecida.

Se muestran en la Tabla 3.1, algunas herramientas conocidas para la consultoría, en la categoría detección de vulnerabilidades.

Tabla 3. 1

Herramientas para la detección de vulnerabilidades

Objetivo	Herramientas Licenciadas	Herramientas Opensource
Detección de vulnerabilidades de infraestructura y sistema operativo	Nessus, Nexpose, Metasploit Pro	OpenVas
Detección de vulnerabilidades en plataformas o aplicaciones web y web services	Acunetix, Appscan, Netssparker, Burpsuite Pro	OwaspZAP, Burpsuite Community, Wapiti, W3AF, Arachni, Nikto

3.2.1.2 Reactivos o de detección de amenazas y ataques

Las herramientas en esta categoría focalizan sus esfuerzos en un análisis en tiempo real en distintas partes del flujo de información de datos en una red corporativa, con el objetivo de reconocer patrones anómalos y sospechosos mediante distintos métodos. Su trabajo principal es reconocer un ataque o intento de este y tratar de alarmar de la mejor manera y en algunos casos específicos y bien configurados, reaccionar también, véase Tabla 3.2.

Tabla 3. 2

Soluciones para la detección de amenazas y ataques

	Herramientas
Licenciadas	Palo Alto Networks, UTM Fortinet, UTM Checkpoint, UTM Cisco
Opensource	OPNSense, Sophos XG Firewall, PFSense, NG Firewall

3.2.1.3 Centralizadores o correlacionadores de logs y eventos

Dada la evolución e incremento en complejidad de las redes corporativas, se ha visto también a lo largo de los últimos años, la aparición de distintos mecanismos o soluciones de ciberseguridad para distintas capas y niveles. Adicionalmente, los mismos dispositivos de red, servidores y terminales de usuarios se han visto dotados de características de

registro de eventos de ciberseguridad para una mejor gestión y análisis de la ciberseguridad.

Todos y cada uno de estos dispositivos, sean de seguridad o no, generan altas cantidades de información en tiempo real mientras hacen uso de la red. Esta información no se puede analizar de forma eficiente en poco tiempo y con recursos humanos reducidos. Es decir, sería una tarea muy desgastadora en tiempo y esfuerzo.

Los dispositivos de esta categoría se enfocan en concentrar toda esta información, analizarla y brindar información de valor sobre esta. Se les llama correlacionadores porque generan correlación entre muchos pedazos de información, encontrando relaciones que permiten una rápida toma de decisiones a nivel de ciberseguridad (véase Tabla 3.3). Los más conocidos son:

Tabla 3. 3

Herramientas de centralización o correlación de registros

	Herramientas
Licenciadas	IBM QRadar, Splunk, Paper Trail, Loggly
Opensource	Elasticsearch, Logstash, Kibana, Graylog

3.2.1.4 Arquitectura e infraestructura para las soluciones

Dependiendo del tipo de solución que se va a implementar y los objetivos a analizar o proteger, estas herramientas se pueden implementar tanto en ambientes on premise o en nube. Se detallan a continuación algunos factores a tener en cuenta para su elección.

- On Premise: Muchas de las herramientas descritas, sobre todo en la parte de correlacionadores de eventos son muy consumidoras de RAM y de procesamiento, por lo que hace falta un servidor que tenga alta disponibilidad de hilos de tareas en paralelos y una cantidad de RAM por encima de los 16GB como mínimo. A su vez, es recomendable que, a la hora de hacer la implementación de la solución, no se realicen sus configuraciones por defecto
- Nube: La implementación en nube presenta ventajas muy grandes por la capacidad de personalización que ofrece en la infraestructura y por el costeo por procesamiento y almacenamiento dinámico. No es recomendable en entornos donde la velocidad o ancho de banda sea reducida o donde los dispositivos de red interna puedan generar cuellos de botella al tratar de canalizar toda la información hacia el componente en la nube.

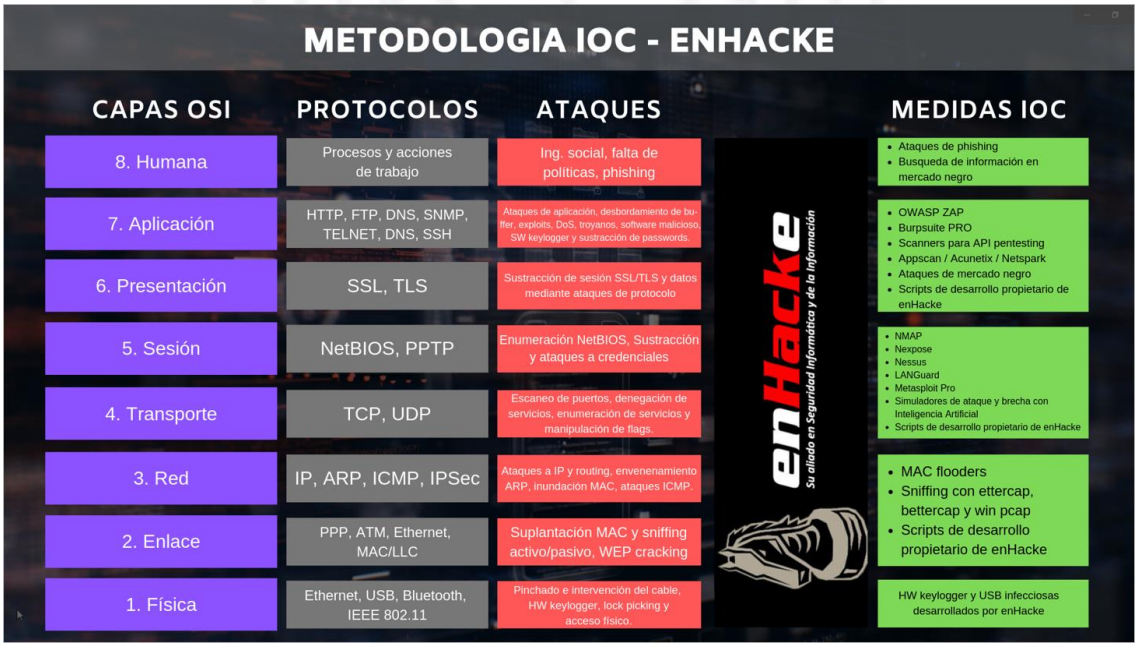
Ejemplos de proveedores para la nube pueden ser: AWS, Azure, OVH o Digital Ocean.

3.2.2 Tecnologías a utilizar en el proyecto

El objetivo del Intrusion Operation Center (IOC) es el de unificar distintas herramientas libres y licenciadas también si así lo quiere el cliente, de tal forma que se pueda automatizar gran parte del proceso de ethical hacking mediante las herramientas preventivas o de detección de vulnerabilidades descritas en el punto 3.2.1.1. Como ya se mencionó anteriormente algunas herramientas se desempeñan mejor al analizar cierta parte de la comunicación en la red y en una capa específica.

A continuación, se muestra una imagen en la que se muestra como en la empresa de ciberseguridad ENHACKE se fue integrando cada una de las herramientas para lograr este cometido. Hay que mencionar también que a las 7 capas de OSI se le adicionó la capa humana, dado que se quería tener identificados los riesgos también en esa capa para mejoras posteriores. Cada una de las capas del modelo OSI tiene protocolos con los que se trabaja, formas de ataque personalizadas, herramientas y métodos para analizar la existencia de vulnerabilidades en dicha capa, así como protecciones y formas de aseguramiento (véase Figura 3.10).

Figura 3. 10
Capas OSI, protocolos, ataques y herramientas por capa.



(Enhacke, 2020)

En la Tabla 3.4 se muestran las tecnologías y herramientas que se utilizan para el proyecto.

Tabla 3. 4

Tecnologías y herramientas utilizadas en el proyecto

	Tecnologías / Herramientas		
	Licenciadas	**Opensource**	**Propietarias enHacke**
Detección de vulnerabilidades de infraestructura y sistema operativo	Nessus, Nexpose	OpenVAS, Nmap	Scripts nse, scripts Python
Detección de vulnerabilidades en plataformas o aplicaciones web y web services		Owasp ZAP, Burpsuite Community	Scripts
Correlación de logs o registros		ElasticSearch, Logstash, Kibana, Greylog	
Infraestructura para implementación	Servidor: HP, Dell Nube: AWS		

3.2.3 Experiencia con clientes

Para realizar pruebas de concepto iniciales se llevó a cabo una fase embrionaria en la que solamente se probaron scripts desarrollados en Python y que brindaban una funcionalidad limitada para un alcance personalizado del cliente. Estas pruebas se realizaron tanto en las oficinas de España como en Perú. Al ver el correcto funcionamiento de esta fase, se procedió a incluir la ejecución de estos scripts dentro de los servicios de ethical hacking hacia clientes, para obtener feedback de ellos. Los resultados fueron positivos y nos permitieron escalar la solución. Más detalle al respecto se comenta en el capítulo siguiente.

3.2.4 Modelo de negocio

3.2.4.1 Segmento de clientes

El servicio está orientado principalmente a empresas que deban tener cumplimiento a algún estándar o normativa como SBS-140, PCI-DS o alguna exigencia internacional por parte de su matriz. Industrias dentro de este rango: financieras, banca, seguros, mineras, energía y gubernamentales.

Algo a remarcar con la tecnología implementada es que es modular y por lo

tanto personalizable. Si hay alguna empresa de alto valor que requiera una parte básica del sistema, es posible y rápido de redefinir el alcance según sus necesidades y tamaño de infraestructura informática.

3.2.4.2 Propuesta de valor

El proyecto IOC – Intrusion Operation Center inicialmente fue concebido como un producto que podría ser operado por las mismas áreas de ciberseguridad de las empresas.

A la hora de realizar las pruebas iniciales, nos dimos cuenta de los retos y dificultades que enfrenta una empresa al tratar de obtener personal, capacitarlo, entender la herramienta y empezar a ser efectivo con esta luego de una curva de aprendizaje.

Es por esto que la propuesta de valor cambió en una segunda etapa de solo producto a producto ofrecido como servicio gestionado. En este escenario la herramienta es implementada en la organización y es gestionada por enHacke, quien se encarga de su funcionamiento óptimo, de obtener los informes y más importante de generar análisis adicionales que permita tomar mejores decisiones a la empresa. Las características principales son:

- Novedad: por el nuevo enfoque de tomar el servicio y como unifica distintos niveles de análisis con distintas herramientas y métodos
- Personalización: altamente personalizable para prestar más atención a aquellas redes o servidores que representen mayor riesgo para la empresa para que se encuentren mejor observados y por ende asegurados. La personalización en este punto va también al lado del negocio, para no interrumpir o sobrecargar los servidores utilizados en fechas especiales como por ejemplo campañas de ventas, marketing, cyberdays o cierres contables.
- Ayuda a hacer el trabajo: en vez de tener varios analistas que tengan que hacer mucho trabajo operativo o de contratar distintos servicios en el año, este sistema ofrecido como servicio, ayuda a automatizar y agilizar el proceso de ethical hacking que se realiza, en distintas capas, bajo distintos enfoques, siendo esto lo óptimo para tener una gestión de vulnerabilidades óptima.
- Precio: el precio es muchísimo más bajo comparado a herramientas internacionales orientadas a mercados americanos o europeos, cuentan con la misma robustez que estas a una fracción del precio.

- Reducción de costes: permite reducir cuantiosamente los costos, debido a que no es necesario comprar una herramienta, un curso y un designar un analista para que se encargue de esto, por mucho menos y con mayor eficiencia y conocimiento especializado, se obtiene una herramienta con servicio de última generación.
- Reducción de riesgos: el enfoque multi capa que se brinda con la herramienta permite ver las vulnerabilidades desde distintos ángulos: protocolos de red, puertos, servicios, flujo de datos de red, sistema operativo y aplicación. Esta forma de gestionar las vulnerabilidades minimiza el riesgo ante amenazas potencialmente explotables por terceros maliciosos.

3.2.4.3 Relación con los clientes

Actualmente los clientes de estos segmentos se los capta por varias estrategias que se desarrollan en conjunto con el área de marketing.

- Adquisición de clientes por área de ventas
- Presencia en ferias nacionales o internacionales
- Demostraciones de la solución como parte de servicios más pequeños, sin generar costos adicionales

Para mejorar los índices de experiencia y satisfacción del cliente se analizaron las características ofrecidas por marcas de productos y servicios de consultoría internacionales. Se agregaron estas características al producto:

- Mantenimiento gratuito por un año
- Informes mensuales personalizados como servicio
- Bolsa de hora de asesoría técnica personalizada para la mitigación de vulnerabilidades
- Capacitación constante

3.2.4.4 Canal de distribución

Las ventas se realizan por acercamiento con el cliente ya sea porque se pone en contacto en alguno de nuestros canales (web, ferias, recomendación, área de ventas y desde este año: resellers).

El proyecto cuenta de las siguientes partes para que su funcionamiento sea óptimo:

- Servidor: dependiendo del alcance del proyecto puede ser un servidor físico y/o un servidor en la nube. Estos se utilizan exclusivamente para el cliente en todo el tiempo de vida del contrato.
- Analista de parte del cliente: se define un interlocutor oficial para poder establecer una comunicación fluida con el cliente y sus áreas de: redes & infraestructura, sistemas, seguridad de la información, ciberseguridad y riesgos.
- Procedimientos: Mediante un análisis del cliente y del alcance del proyecto se establecen una serie de procedimientos de trabajo e interacción con el sistema IOC.
- Jefe de proyecto o especialista de cuenta: Un especialista de enHacke es designado para analizar el proyecto de implementación y para hacer seguimiento con el analista a lo largo de la vida útil del servicio.
- Analista de parte de enHacke: Un analista se encarga de hacer las personalizaciones al sistema como parte de requerimientos mensuales que puede ir haciendo el cliente. Tiene también la responsabilidad de reportar vulnerabilidades críticas a su superior para poder activar los procedimientos de respuesta y mitigación.

3.2.4.5 Actividades clave

Las principales actividades para que el cliente tenga una experiencia satisfactoria y que brinde valor real a sus operaciones diarias de aseguramiento y mitigación de riesgos son:

- Fase de implementación
    - Reuniones de levantamiento de información
    - Definición de alcance de infraestructura
    - Pruebas de visibilidad y conectividad
    - Implementación
    - Personalización
    - Adiestramiento de la solución
- Fase de servicio
    - Personalización por eventualidades

- Verificación de vulnerabilidades y eliminación de falsos positivos
- Reportes mensuales
- Vulnerabilidades críticas que deben ser reportadas bajo un procedimiento de emergencia

3.2.4.6 Recursos clave

Para que el producto pueda ofrecerse con características óptimas a los clientes, dependerá básicamente de la tecnología donde es implementado y del personal que realice la implementación, por lo que se han definido como recursos clave los siguientes:

- Servidores físicos o en la nube
- Jefe de proyecto y analista
- Sistema personalizado

3.2.4.7 Socios claves

Los socios estratégicos o claves son aquellos que brindarían la infraestructura para realizar la implementación y aquellos revendedores que apoyen en la introducción al mercado de la solución. Por estas razones se eligen como socios claves a los siguientes:

- Proveedor de servidor en caso sea uno físico (Dell o HP)
- Proveedor de servicios en la nube (AWS)
- Resellers

3.2.4.8 Estructura de costes

Para la realización exitosa de este proyecto, los costos se pueden dividir en costos tecnológicos y de recursos humanos calificados. Se han definido los siguientes:

- Servidor
- Jefe de proyecto
- Analista

3.2.4.9 Flujo de ingresos

Los ingresos se dan mediante un modelo de suscripción anual, donde se le pide al cliente que realice el pago por el año entero por adelantado.

3.2.5 Oportunidades del proyecto actual

Si bien el producto ahora es ofrecido como servicio gestionado, las cualidades del sistema en sí tienen muchas características para crecer y que se planea ir implementando a lo largo del 2021 y 2022. Algunas de las características son:

- Predicción de vulnerabilidades por métodos de correlación y análisis de bigdata, con clientes del mismo segmento e infraestructura similar
- Automatización de mecanismos de mitigación
- Predicción de ataques en la parte reactiva si adicionalmente el cliente cuenta con un SOC – Security Operations Center.

Adicionalmente es necesario mencionar que este proyecto no es solamente un concepto, sino que ya tuvo una fase embrionaria y de validación con clientes. Ha tenido una evolución y muchas de las características implementadas desde esa primera fase, se han ido realizando gracias a la colaboración y feedback de nuestros clientes.

3.3 Beneficios esperados

Se muestra a continuación la utilidad esperada de implementación bajo dos escenarios distintos: clientes que escogen servidor físico (véase Tabla 3.5) y clientes que escogen servidor en la nube (véase Tabla 3.6). Adicionalmente se cumple lo siguiente para el cálculo:

- Se toma en cuenta que es un solo cliente y que se decide por una u otra opción.
- El costo de jefe de proyecto y de analista se ha llevado al cálculo anual y bajo un enfoque por horas mensuales, ya que ambos perfiles mantienen 4 clientes en paralelo.
- Se tiene en cuenta que el cliente tiene una infraestructura informática mediana

3.3.1 Escenario con servidor físico

Tabla 3. 5

Utilidad si la implementación se realiza en servidor físico

		1 año
Ingreso		
	Suscripción anual	95 000
Egreso		
	Servidor	10 000
	Jefe de proyecto (40 hh / mes)	15 000
	Analista (40 hh / mes)	12 000
	Total de egresos	37 000
Utilidad		**58 000**

Nota. Los valores están expresados en soles peruanos.

3.3.2 Escenario con servidor en nube

Tabla 3. 6

Utilidad si la implementación se realiza en servidor en nube

		1 año
Ingreso		
	Suscripción anual	70 000
Egreso		
	Servidores AWS	4 000
	Jefe de proyecto (40 hh / mes)	15 000
	Analista (40 hh / mes)	12 000
	Total de egresos	31 000
Utilidad		**39 000**

Nota. Los valores están expresados en soles peruanos.

3.4 Financiamiento obtenido

Dado el avance y evolución del proyecto, así como su aceptación por parte de clientes reales, el proyecto recibió financiamiento de una de las empresas del grupo por 30,000.00 euros para el desarrollo de la 2da fase.

CAPÍTULO IV: DEFINICIÓN DEL PROYECTO

4.1 Definición del proyecto

El proyecto presentado en este documento, bautizado como IOC – Intrusion Operation Center, es un producto ofrecido al cliente como servicio gestionado y que tiene como objetivo disminuir los riesgos de exposición a ciberataques y facilitar al cliente encontrar vulnerabilidades antes de la materialización de un ataque, mediante un sistema de alerta temprana de vulnerabilidades que actúa analizando constantemente la infraestructura informática crítica de la organización.

El sistema puede ser implementado ya sea On Premise, es decir instalado en la propia empresa con un servidor físico o en cloud mediante servicios de Amazon Web Services, dependiendo del alcance del servicio y tipo de infraestructura con la que cuente el cliente. En ambos casos el servidor viene incluido en el servicio.

El sistema ofrece reducir los tiempos de mitigación y respuesta ante evidencia de vulnerabilidades, disminuir riesgos y eliminar carga de trabajo por parte de las áreas internas de auditoría o ciberseguridad, mediante del uso automatizado de las herramientas del sistema.

4.2 Objetivos del proyecto

4.2.1 Objetivo general

Disminuir los riesgos por ciberataques hacia la infraestructura informática del cliente.

4.2.2 Objetivos específicos

- Determinar la infraestructura informática total de la organización
- Definir los segmentos internos, externos, nube pública y privada
- Definir los activos de mayor importancia y relevancia para los procesos críticos de la organización

- Diseñar una serie de reglas personalizadas para que los procesos y sus sistemas puedan ser analizados sin percances
- Diseñar la estrategia de implementación
- Llevar a cabo la implementación con los ajustes y personalizaciones necesarias
- Validar el buen funcionamiento del sistema, así como de su sistema de reportes

4.3 Beneficios esperados

- Beneficios obtenidos por los clientes

  Los clientes que ya han probado la solución no solo han encontrado vulnerabilidades no mapeadas antes, sino que a partir del mes 3 han empezado a reaccionar de forma más eficiente ante la mitigación de dichas vulnerabilidades.

  Con la consultoría adicional incluida en el servicio, dos de nuestros clientes se encuentran en vías de conseguir su certificación PCI-DSS (Payment Card Industry – Data Security Standard, Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago) este año.

- Beneficios económicos para la empresa

  A continuación, en la Tabla 4.1, se muestra el flujo de caja para 5 años tomando en consideración un escenario pesimista en el que solamente se coloca una venta el primer año y cada año siguiente se aumenta en uno el número de clientes.

  Este flujo de caja representa los ingresos obtenidos por las ventas colocadas cada año y los egresos realizados para poder ofrecer el servicio haciendo uso de la plataforma IOC a los clientes.

  Adicionalmente se le agregan como gastos adicionales un desarrollador que tenga como única misión mejorar el sistema y agregarle mayores funcionalidades y características al sistema y un presupuesto de marketing solamente para posicionar el producto con un incremento del 30% anual para captar más clientes y mejorar el posicionamiento de la marca.

Tabla 4. 1

Flujo de caja

	Año					
	0	**1**	**2**	**3**	**4**	**5**
Ingresos						
Ventas		95 000	190 000	285 000	380 000	475 000
Cantidad		1	2	3	4	5
Precio		95 000	95 000	95 000	95 000	95 000
Aporte de capital	100 000					
Egresos						
Servidor		10 000	20 000	30 000	40 000	50 000
Jefe de proyecto		15 000	30 000	45 000	60 000	75 000
Analista		12 000	24 000	36 000	48 000	60 000
Desarrollador		48 000	48 000	48 000	48 000	48 000
Marketing		20 000	26 000	33 800	43 940	57 122
Total egresos		105 000	148 000	192 800	239 940	290 122
Flujo del año	**-100 000**	**-10 000**	**42 000**	**92 200**	**140 060**	**184 878**

Nota. Los valores están expresados en soles peruanos.

Con los mismos datos del cuadro anterior, se muestra en la Tabla 4.2 de forma resumida el flujo de caja, un costo de oportunidad del 10% y el VAN y TIR resultante, demostrando que el proyecto es viable económicamente.

Tabla 4. 2

Cálculo de VAN y TIR

	Año					
	0	**1**	**2**	**3**	**4**	**5**
Inversión inicial	100 000					
Flujo de caja	-100 000	-10 000	42 000	92 200	140 060	184 878
COK	**10%**					
VAN	**205 349**					
TIR	**46%**					
Beneficio / Costo	**3**					

Nota. Los valores están expresados en soles peruanos.

4.4 Segmento de Mercado

- **Orientación de mercado**

El servicio tiene una orientación primaria hacia empresas que requieren demostrar cumplimiento hacia ciertos organismos reguladores, específicamente en el segmento financiero, donde la exigencia por normas de cumplimiento es mayor. Regulaciones o normas como: SBS G-140 y en algunos casos PCI-DSS

- Bancos
- Financieras
- Cajas
- Cooperativas
- Seguros

- **Tareas u obligaciones del cliente**

El cliente final es el oficial de seguridad de la información o en caso exista la función en la empresa, el oficial de ciberseguridad. Sus principales tareas son:

- Monitorizar amenazas que pongan en riesgo los procesos críticos de la organización
- Hallar vulnerabilidades en la infraestructura informática de la organización
- Evaluar y gestionar los riesgos que se puedan presentar por vulnerabilidades o incidentes de ciberseguridad
- Parchar o mitigar las vulnerabilidades halladas
- Reportar al directorio sobre el estado de ciberseguridad en la empresa, así como la cantidad de ataques o incidencias que hubieron en un periodo de tiempo a informar

- **Frustraciones y alegrías del cliente**

Debido a los constantes ataques por parte de cibercriminales, la mayoría de las empresas han sufrido o están al borde de sufrir un ciberataque con intrusión exitosa. Ya no se trata de si atacarán o no, sino de cuándo tendrán éxito.

El equipo encargado de la ciberseguridad en la empresa se encuentra en constante preocupación y su principal reto es tener bajo constante observación miles de computadoras y cientos de servidores. Lo peor es que siempre atacan donde uno menos lo espera. De ahí la frustración y en algunos casos, al hacer la investigación del incidente se revelan datos que llevan a hacer creer al equipo que la intrusión no fue de hace unos días como fue detectado inicialmente, sino que los cibercriminales llevan en la infraestructura semanas o hasta meses haciendo de las suyas.

Por otro lado, a pesar de que los presupuestos para el tema de ciberseguridad aumentan cada año, siempre es ajustado por el precio tan elevado de los servicios y productos que se deben adquirir para asegurar la infraestructura.

4.5 Roles y responsabilidades del equipo del proyecto

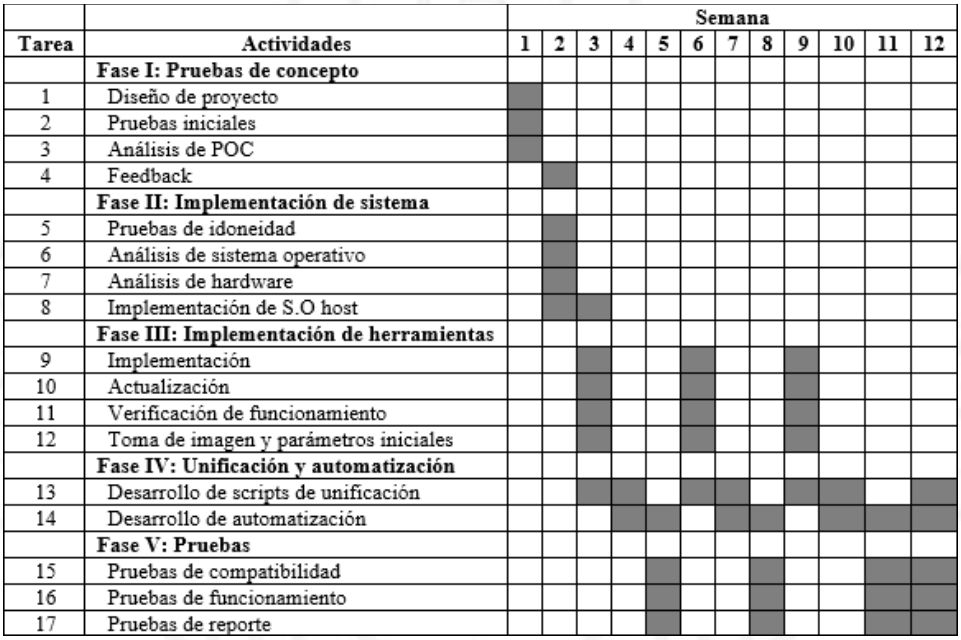
- Jefe de proyecto:
    - Definir el alcance de la infraestructura informática del cliente.
    - Diseña la estrategia de implementación
    - Durante el servicio ve el desempeño del analista
    - Durante el servicio, si se activa el procedimiento de vulnerabilidad crítica, debe ejecutar procedimientos para avisar al cliente
    - Recolecta feedback del cliente para posibles mejoras
- Analista: Trabaja en conjunto con el jefe de proyecto y el cliente para llevar a cabo:
    - La definición de segmentos críticos dentro de la infraestructura informática interna y externa
    - La definición de activos de importancia
    - Levantamiento de información para personalización de reglas
    - Implementa el servicio
    - Durante el servicio, se encarga de velar por la ejecución y correcto funcionamiento del sistema y sus herramientas
    - Recoge los análisis semanales y ve si hay alguna vulnerabilidad descubierta con criticidad alta. De ser así lo reporta al jefe de proyecto
- Desarrollador
    - Crea una lista de mejoras según feedback de clientes
    - Prioriza las mejoras
    - Crea módulos pequeños de prueba y junto a los desarrolladores, jefes de proyecto y analistas, hacen una pequeña prueba de concepto
    - Realizar mejoras

- Analista de marketing
    - Analiza la respuesta de los clientes ante el producto
    - Aplica técnicas para mejorar la venta y ofrecimiento del producto junto al equipo de marketing de la empresa

4.6 Cronograma

Figura 4. 1

Cronograma del proyecto



Tarea	Actividades	Semana											
		1	2	3	4	5	6	7	8	9	10	11	12
	Fase I: Pruebas de concepto												
1	Diseño de proyecto												
2	Pruebas iniciales												
3	Análisis de POC												
4	Feedback												
	Fase II: Implementación de sistema												
5	Pruebas de idoneidad												
6	Análisis de sistema operativo												
7	Análisis de hardware												
8	Implementación de S.O host												
	Fase III: Implementación de herramientas												
9	Implementación												
10	Actualización												
11	Verificación de funcionamiento												
12	Toma de imagen y parámetros iniciales												
	Fase IV: Unificación y automatización												
13	Desarrollo de scripts de unificación												
14	Desarrollo de automatización												
	Fase V: Pruebas												
15	Pruebas de compatibilidad												
16	Pruebas de funcionamiento												
17	Pruebas de reporte												

4.7 Recursos y presupuesto

A continuación, en la Tabla 4.3, se muestra un estimado para echar a andar el proyecto. Como servidor se toma una versión básica que servirá de pruebas y que tiene menor costo que el que se entregaría al cliente. Adicionalmente se separa un fondo para un programador especializado en caso sea requerido.

Tabla 4. 3

Presupuesto para llevar a cabo desarrollo del proyecto

Item	Recurso	Cantidad	Costo / Mes	Costo anual
1	Jefe de proyecto	1	4 000	48 000
2	Analista de ciberseguridad / programación	1	3 000	36 000
3	Programador especializado consultivo	1		10 000
4	Servidor	1	6 000	6 000
			Total	**100 000**

Nota. Los valores están expresados en soles peruanos.

CAPÍTULO V: DESARROLLO DEL PROYECTO

A lo largo de este capítulo se lleva a cabo la metodología de Design Thinking para poder afinar la idea de producto o servicio a la que se quiere llegar, partiendo de la idea de que hay algunas necesidades no cubiertas por la oferta actual de mercado en el campo de ciberseguridad. El objetivo de la metodología es poder conocer al cliente, sus necesidades o requerimientos reales y poder brindar una solución a estos, a partir de un prototipo que nos ayudará a comprobar que el producto o servicio aborda directamente las penas o tareas que el cliente requiere realizar y de esta manera evaluar la idoneidad del producto.

5.1 Empatizar

En el presente apartado se explicarán y analizarán distintos puntos y temas que nos permitirán comprender mejor al usuario y posible cliente, de tal forma que podamos empatizar con él y lograr entender sus necesidades y problemas reales a ser resueltos.

Se explicará el problema actual que enfrentan muchas empresas en distintos segmentos e industrias, pero focalizándose obviamente en el segmento aplicable para el presente proyecto, como fue definido antes: banca, financieras, cajas, cooperativas y seguros. A su vez también se explicará el enfoque de solución disponible en el mercado en la actualidad.

Por último, conoceremos más al usuario dentro de este contexto problema / solución, con el objetivo de aprender más sobre sus necesidades reales a la hora de ejecutar sus tareas y funciones de trabajo.

5.1.1 El problema

En el capítulo III – Fundamentación del proyecto, más específicamente en el punto 3.1.1 se habla sobre el estado del cibercrimen a nivel global y el incremento en los últimos años. En la actualidad y debido a la pandemia, se ha dado un incremento del cibercrimen llegando a duplicarse o triplicarse las cifras de reportes por ciberataques en algunos países.

Latinoamérica y Perú no han sido excepción y también se ha visto parte del

incremento de ataques informáticos. Tan solo en el último año han sucedido los siguientes ataques de renombre e impacto mediático:

- Pemex (noviembre 2019)

  La empresa Petróleos Mexicanos sufrió el ataque a varios servidores centrales en los cuales les aplicaron secuestro de información. Los cibercriminales pidieron 4 millones de dólares por el rescate y devolución de la información (Diario El Economista, 2019).

  Impacto en: Imagen, multas y penalidades, productividad.

- Banco de Crédito del Perú (diciembre 2019)

  El banco reconoció haber sido víctima de una intrusión en el 2018 por la que se filtró información de clientes (Diario Gestión, 2019).

  Impacto en: imagen, incumplimiento regulatorio, multas o penalidades, pérdida de clientes.

- Cineplanet (enero 2020)

  La cadena de cines tuvo un ataque informático que terminó en la filtración masiva de información de clientes (contraseñas, información de pago, documentos de identidad, entre otros datos) (C|NET en español, 2020).

  Impacto en: imagen, multas o penalidades por incumplir la Ley de Protección de Datos Personales y pérdida de clientes.

- Diario Expreso (junio 2020)

  La plataforma web del diario fue víctima de intrusión informática, por la cual los cibercriminales tomaron control del servidor y su información, dejando la página indisponible por varias horas (Diario Expreso, 2020)

  Impacto en: imagen, reputación y productividad.

El problema que tienen las empresas para controlar este tipo de ataques puede verse desde varios frentes o enfoques, pero se podrían resumir en dos aspectos principales:

- Incapacidad para asegurar la infraestructura informática de la organización

- Incapacidad para reconocer o detectar los ataques o intentos de intrusión que se llevan a cabo en la infraestructura informática de la organización

Ambas incapacidades son las que se toman como análisis en el presente proyecto. La oportunidad detectada de la solución propuesta va alineada justamente a una de ellas, la incapacidad para asegurar rápidamente la infraestructura informática antes de que los ataques se materialicen.

5.1.2 Soluciones actuales

Como se explica en el punto 3.2.1. Soluciones actuales de ciberseguridad, existen distintas formas de intentar abordar el problema de las intrusiones o ataques en desarrollo por parte de cibercriminales. A continuación, se muestran las tablas comparativas 5.1 y 5.2, que permiten ver las principales características de cada solución en su enfoque.

Tabla 5. 1

Características de detección de vulnerabilidades en infraestructura, sistema operativo o aplicaciones

		Tipo de vulnerabilidad						
	Herramienta o solución	S.O	Servicios	Flujo de datos	Aplicación	B.D	Web	Automatización de tareas
Detección de vulnerabilidades (enfoque preventivo)	Nessus	X	X			X		X
	Nexpose	X	X		X	X		X
	Metasploit Pro	X	X			X		X
	Openvas	X	X					X
	Acunetix				X	X	X	X
	Appscan				X	X	X	X
	Owasp zap			X	X	X	X	
	BurpSuite			X				
	Nikto				X			
Monitorización y/o detección de ataques o intrusiones (enfoque reactivo)	Palo alto Fortinet Checkpoint Cisco F5 Sophos Firewall PF Sense NG Firewall							

Tabla 5. 2

Características de detección de intrusión o ataques en infraestructura, sistema operativo o aplicaciones

	Herramienta o solución	Filtrado de tráfico	Detección de ataques en red	Detección de ataques en aplicación web	Anti Denegación de Servicio (DoS)	Automatización de la monitorización
Detección de vulnerabilidades (enfoque preventivo)	Nessus Nexpose Metasploit Pro Openvas Acunetix Appscan Owasp zap BurpSuite Nikto					
Monitorización y/o detección de ataques o intrusiones (enfoque reactivo)	Palo alto	X	X	X	X	X
	Fortinet	X	X	X		X
	Checkpoint	X	X	X	X	X
	Cisco	X	X	X		X
	F5	X	X	X	X	X
	Sophos Firewall	X	X			X
	PF Sense	X				
	NG Firewall	X				

Los objetivos al presentar ambos cuadros son:

- Mostrar que las herramientas utilizadas por cada enfoque (detección de vulnerabilidades y detección de ataques) son distintas y especializadas en su enfoque
- Mostrar que, a diferencia de las herramientas de detección de ataques, las herramientas de detección de vulnerabilidades disponibles se especializan en algunas categorías de vulnerabilidades, no en todas.

En el segundo cuadro se puede ver que hay soluciones automatizadas que cubren un amplio espectro de actividades. Esto se ha podido lograr por la unificación de módulos en los conocidos UTMs (Unified Threat Management – gestión unificada de amenazas). Sin embargo, no sucede lo mismo en el campo del análisis de vulnerabilidades porque las herramientas son diseñadas para una parte muy específica (infraestructura, sistema operativo, flujo de información o capa de aplicación), es por esto que, si bien las herramientas tienen incluidas algunas opciones de automatización de las tareas, estas las

realizan solamente en su alcance y no se presenta una solución que busque automatizar las distintas herramientas bajo un solo dominio.

5.1.3 Perfil del cliente

Se realizaron entrevistas a clientes de distintos segmentos, especialmente de aquellos que eran los que se encontraban alineados con este proyecto.

Los factores que se consideraron para obtener un perfil aproximado de cliente ideal fueron:

- Empresas que tengan la obligación de cumplir con lineamientos de seguridad de la información y/o ciberseguridad porque se lo pide la matriz (siendo el caso de multinacionales).
- Empresas que tengan la obligación de cumplir con estándares o regulaciones nacionales o internacionales como: PCI-DSS, SBS G-140.

Las industrias que encajan más con este perfil son: financieras, banca, seguros, mineras, energía y gubernamentales.

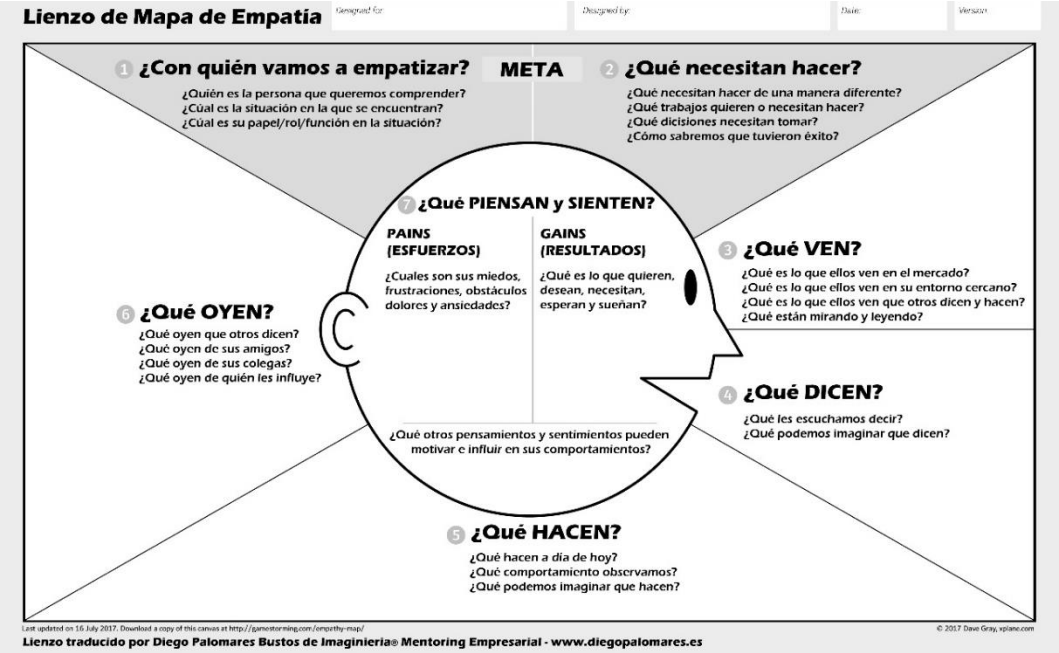
El perfil específico de la industria sería:

Empresa de una industria específica (mencionada anteriormente) con más de 300 trabajadores, regulada por algún organismo o estándar y que tenga la necesidad obligatoria de cumplir con implementaciones y estrategias de ciberseguridad para la mitigación del riesgo.

5.1.4 Conociendo al cliente – Mapa de empatía

Para conocer mejor al cliente se elaboraron una serie de preguntas tomando en cuenta el lienzo de mapa de empatía (véase Figura 5.1). Estas tienen por objetivo conocer más acerca de las obligaciones, dolores y beneficios del cliente.

Figura 5. 1
Lienzo de mapa de empatía



(David Gray, 2017) (Alexander Ostelwalder e Yves Pigneur, 2010)

Adicionalmente y con el objetivo de poder comprender a mayor detalle las necesidades reales del cliente y así empatizar con él, se tomaron preguntas propuestas por el Business Model Canvas en la sección específica de Value Proposition. Los formularios originales de preguntas pueden ser consultados en los anexos 4, 5 y 6 u obtenerse libremente de la sección recursos libres de la página oficial de strategyzer.com.

Estas preguntas están orientadas directamente al cliente, a sus tareas por cumplir, sus frustraciones o esfuerzos y los éxitos o beneficios que quiere lograr.

- Tareas / obligaciones / responsabilidades
    - Funcionales (acerca de las tareas concretas)
        - Cuéntame acerca de tus responsabilidades
        - ¿Qué retos encuentras en tu día a día?
        - ¿Cuál es la tarea que no puedes dejar de hacer en tu trabajo sino la empresa se ve directamente impactada o te despiden?
        - ¿Cómo describirías un día normal y un día difícil?
        - ¿Qué necesitas cumplir que te toma mucho tiempo de coordinación?
        - ¿Qué tareas realizas para cumplir tus responsabilidades?
    - Sociales (ej: impresionar a amigos)

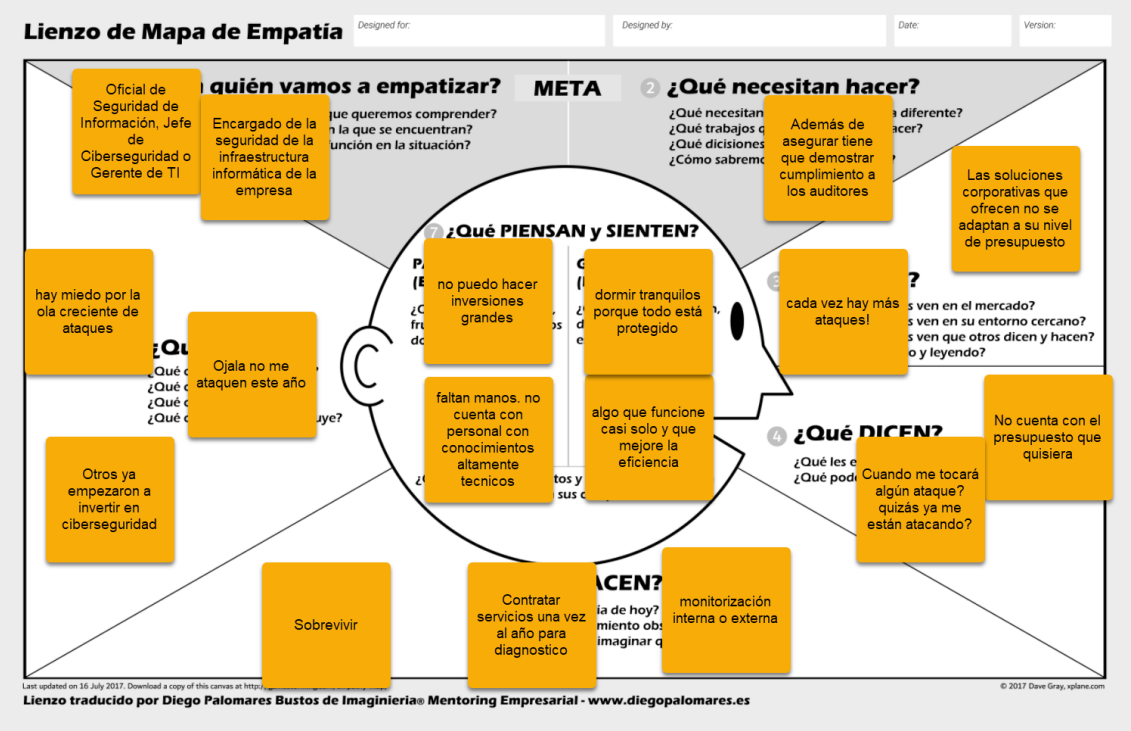
        - ¿Cómo describirías una gestión exitosa de tu trabajo?
        - ¿Cuéntame, a quién le dirías si hicieras las cosas perfectamente?
        - ¿Cómo quieres ser percibido por la industria y clientes?
    - Emocionales (ej: piece of mind)
        - ¿Qué sentirías en un día difícil?
        - ¿Qué sentirías cuando todo va bien?
        - ¿Qué te haría sentir realizado?
        - ¿Cómo te quisieras sentir?
- Dolores o esfuerzos (que tiene el cliente al hacer sus tareas)
    - ¿Qué te hace sentir mal?
    - ¿Cómo sería un día difícil?
    - ¿Qué retos encuentras en tu día a día?
- Beneficios
    - ¿Con qué soñaría tu área?
    - ¿Qué consecuencia socialmente positiva desearía tu área usuaria o empresa?
    - ¿Cómo mide tu área el éxito o el fracaso?
    - ¿Cuáles son tus aspiraciones?

Como resultado de las entrevistas, se obtuvo información valiosa. Las respuestas a las preguntas realizadas nos permitieron conocer mucho más de cerca al cliente y fue posible comprender más acerca de:

- Sus funciones, tareas y responsabilidades de trabajo
- Cuales son aquellas actividades o tareas que le representan un esfuerzo, dolor o incomodidad
- Que piensan, sienten, ven, oyen o hacen al hacer su trabajo

A continuación, en la Figura 5.2, se muestra el lienzo de Mapa de Empatía con la información recabada.

Figura 5. 2
Lienzo de mapa de empatía llenado



5.2 Definir

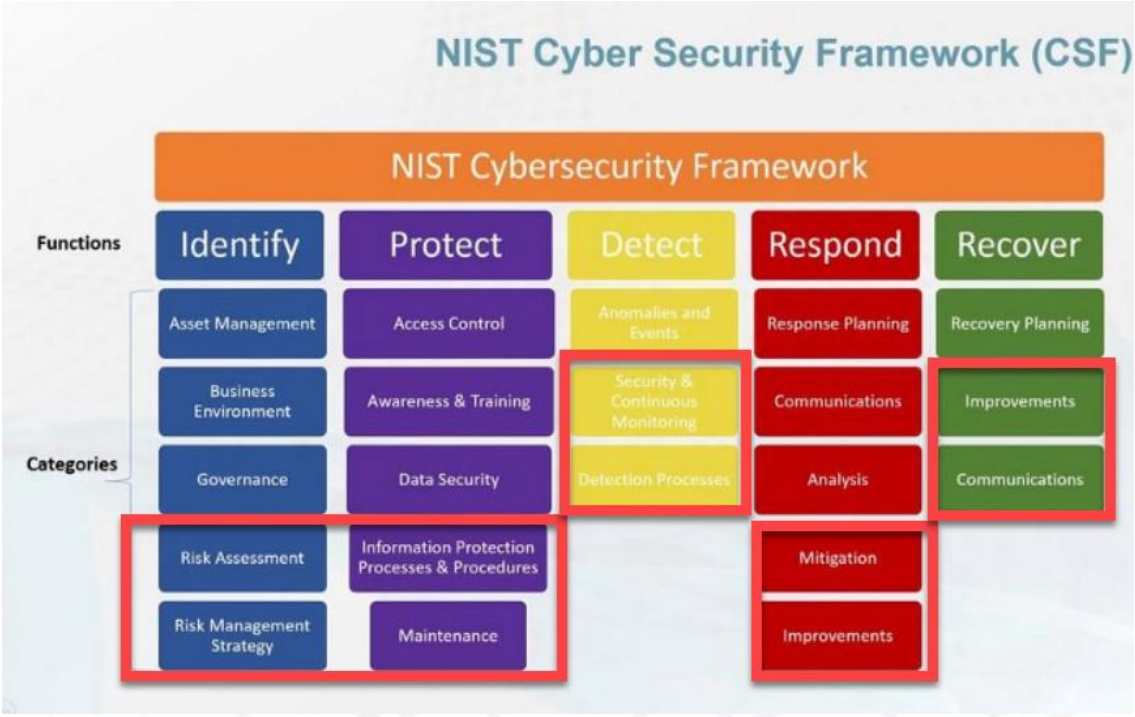
5.2.1 Journey del cliente

En este apartado se muestra el ciclo de vida de tareas del cliente desde un punto de vista netamente de ciberseguridad. Para esto se utilizará el marco de trabajo de ciberseguridad establecido por NIST – National Institute of Standards and Technology. El objetivo es mostrar el flujo de pensamiento de un usuario o cliente típico en sus labores o funciones ejecutadas mensualmente.

Del marco de trabajo de ciberseguridad de NIST se han escogido solamente aquellos procesos que tienen relación específicamente con el proyecto presentado en el presente documento (véase Figura 5.3). A continuación, en la Figura 5.4 se muestra el journey del cliente, tomando en cuenta dichos procesos a ser utilizados para el análisis.

Figura 5. 3

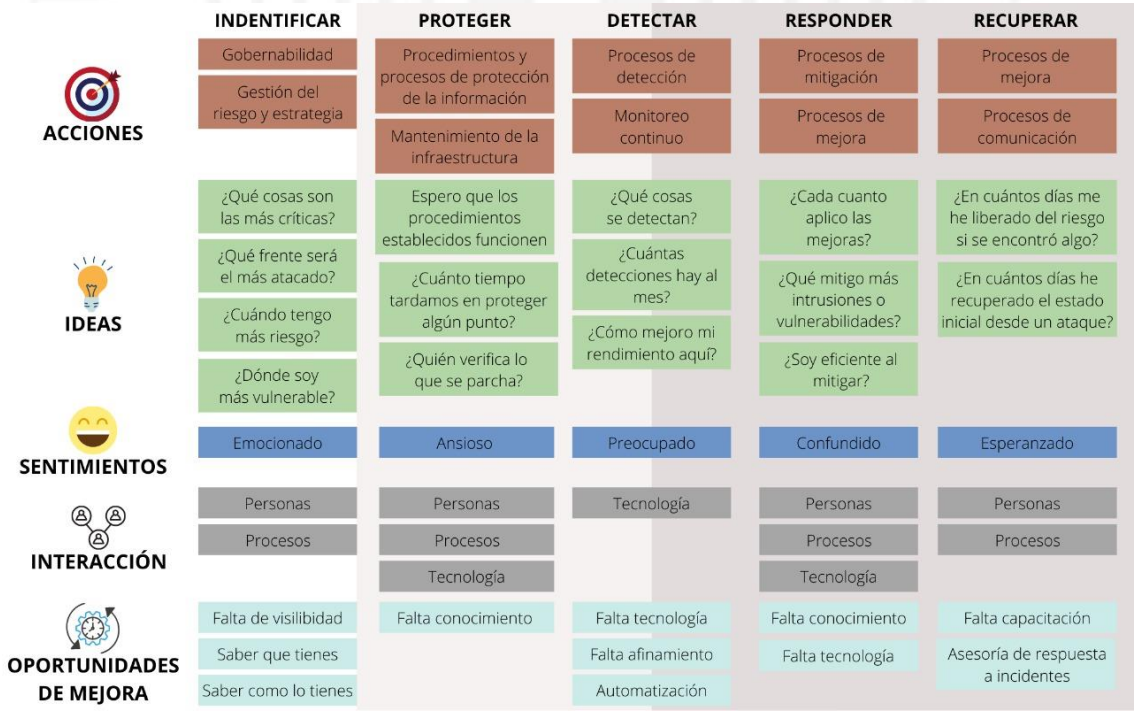
Marco de trabajo de ciberseguridad de NIST



(National Institute of Standards and Framework's Cybersecurity Framework, 2014)

Figura 5. 4

Journey del cliente



(Design Thinking, 2018)

5.2.2 Punto de vista del cliente - Point of View (POV)

El cliente tiene preocupaciones por la seguridad de su información y de su infraestructura informática, sobre todo por el incremento del cibercrimen a nivel mundial. Quiere buscar una forma eficiente que apoye su estrategia actual, que no necesite reinventar toda el área y que permita definitivamente acelerar su trabajo y hacerlo más eficiente.

Actualmente hace muchas cosas manualmente, otras las realiza una sola vez al año en servicios de diagnóstico que, si bien dan información, no son las más adecuadas para la toma de decisiones en cada mes del año y por último hay procesos que no lleva a cabo por falta de conocimiento y especialización de su equipo.

Los sistemas de monitorización que tiene muchas veces son de funcionalidad y conectividad, más no necesariamente de seguridad o eventos de ciberseguridad, por lo que tiene una clara necesidad de visibilidad del riesgo de su red en tiempo real y aquello que podría estar previniendo antes de que suceda un ataque.

5.3 Idear

En este apartado se mostrará la fase de ideación, en la cual se toma todo el conocimiento adquirido sobre las necesidades y problemas reales del cliente y mediante dinámicas de colaboración y lluvia de ideas de propuestas de solución, se generan posibles formas de ayudar al cliente a resolver sus problemas.

5.3.1 Lluvia de ideas

- Ofrecer una cantidad mayor de servicios de ethical hacking a los clientes
- Ofrecer un analista capacitado para que trabaje en forma permanente dentro de las instalaciones del cliente haciendo las pruebas y análisis con mayor frecuencia
- Brindar capacitaciones más detalladas al cliente para elevar su nivel de conocimiento en cuanto a la resolución de problemas
- Automatizar uno de los programas
- Que las herramientas escaneen todo y que los registros lleguen a Enhacke para su análisis y reporte
- Proteger más los servidores con monitorización extra

- Centralizar los registros o resultados de las herramientas para análisis
- Automatizar los programas y centralizar sus resultados

5.3.1.1 Idea ganadora

Luego de haber analizado las necesidades y problemas del usuario según las preguntas y el mapa de empatía realizado, se resaltaron las siguientes características:

- Preocupación por crecimiento de cibercrimen y alza en ataques
- Presupuesto ajustado
- Existen muchas tareas (escaneos internos, análisis de vulnerabilidades, estado de los puertos, disponibilidad de servicios, seguimiento de mitigación) y poco personal con el conocimiento técnico necesario

Es por ello que se cree que hay cabida si se ofrece una solución que pueda automatizar gran parte de estas tareas y realizarlas de manera eficiente, con poco personal y con un precio competitivo.

De la lluvia de ideas, las que tuvieron más votos y estaban más alineadas con las necesidades del usuario, fueron:

- Automatizar uno de los programas (análisis de red, puertos y vulnerabilidades de servicios, sistema operativo o web)
- Centralizar los registros o resultados de las herramientas para análisis

Uniendo ambas ideas, se decide automatizar la mayor cantidad de programas posibles (análisis de puertos, servicios y vulnerabilidades a distintos niveles) y centralizar sus resultados para una gestión más rápida.

Tomando esta nueva idea como central, se realizó una nueva lluvia de ideas que obtuvo como puntos principales:

- Automatizar los programas de consola ya sea en powershell o bash según el tipo de herramienta
- Automatizar programas de más alto nivel con scripts de Python

- Utilizar un lenguaje de reporte común como XML para que todas las herramientas tengan un mismo tipo de reporte que sea más fácil de tratar
- Utilizar librerías disponibles para el graficado y representación de la información recolectada por las herramientas

5.3.2 Solución propuesta

Lo que se propone es mejorar el proceso de aseguramiento de la infraestructura reduciendo los tiempos de respuesta de detección de vulnerabilidades y permitiendo calificar de mejor manera los riesgos en la infraestructura informática de la organización.

La solución propuesta busca unificar varias herramientas de detección de vulnerabilidades que tienen distintos alcances, en un espacio común, fácil de gestionar y comprender, en forma centralizada para así agilizar el tiempo de respuesta en los procesos de respuesta a incidencias por vulnerabilidades ubicadas (véase Tabla 5.3).

Tabla 5. 3

Características de detección de vulnerabilidades de distintas herramientas unificadas por un sistema centralizado – IOC

		Tipo de vulnerabilidad						
	Herramienta o solución	S.O	Servicios	Flujo de datos	Aplicación	B.D	Web	Automatización de tareas
Detección de vulnerabilidades (enfoque preventivo)	Nessus	X	X			X		X
	Nexpose	X	X		X	X		X
	Metasploit Pro	X	X			X		X
	Openvas	X	X					X
	Acunetix				X	X	X	X
	Appscan				X	X	X	X
	Owasp zap			X	X	X	X	
	BurpSuite			X				
	Nikto				X			
	IOC	Openvas	Nessus	Burpsuite	Owasp zap	Acunetix	Owasp Zap	X
Monitorización y/o detección de ataques o intrusiones (enfoque reactivo)	Palo alto Fortinet Checkpoint Cisco F5 Sophos Firewall PF Sense NG Firewall							

Nota. Las herramientas con las que inicialmente se trabaja en el sistema IOC fueron seleccionadas por contar con la mejor relación calidad – precio.

5.4 Prototipar

El objetivo de la fase de prototipeo es validar las ideas y conceptos que se tienen sobre la forma en la que cubriremos o ayudaremos en las necesidades del cliente y poder realizar estas comprobaciones de una forma rápida y con bajo coste.
Para este proyecto se llevaron a cabo dos fases de prototipo:

- Alfa: super básica y que representaba el menor esfuerzo posible, pero a la vez una forma rápida de comprobar incógnitas propuestas inicialmente.
- Beta: una leve mejora sobre la fase alfa que ya no solamente validaba funcionalidad, sino que también buscaba mejorar la interacción y sentir del usuario con la herramienta.

5.4.1 Prototipado fase ALFA

Para comprobar si la idea ganadora iba por buen camino y ver si realmente aporta y es de utilidad con los problemas del usuario, se realizó un prototipo funcional con características mínimas.

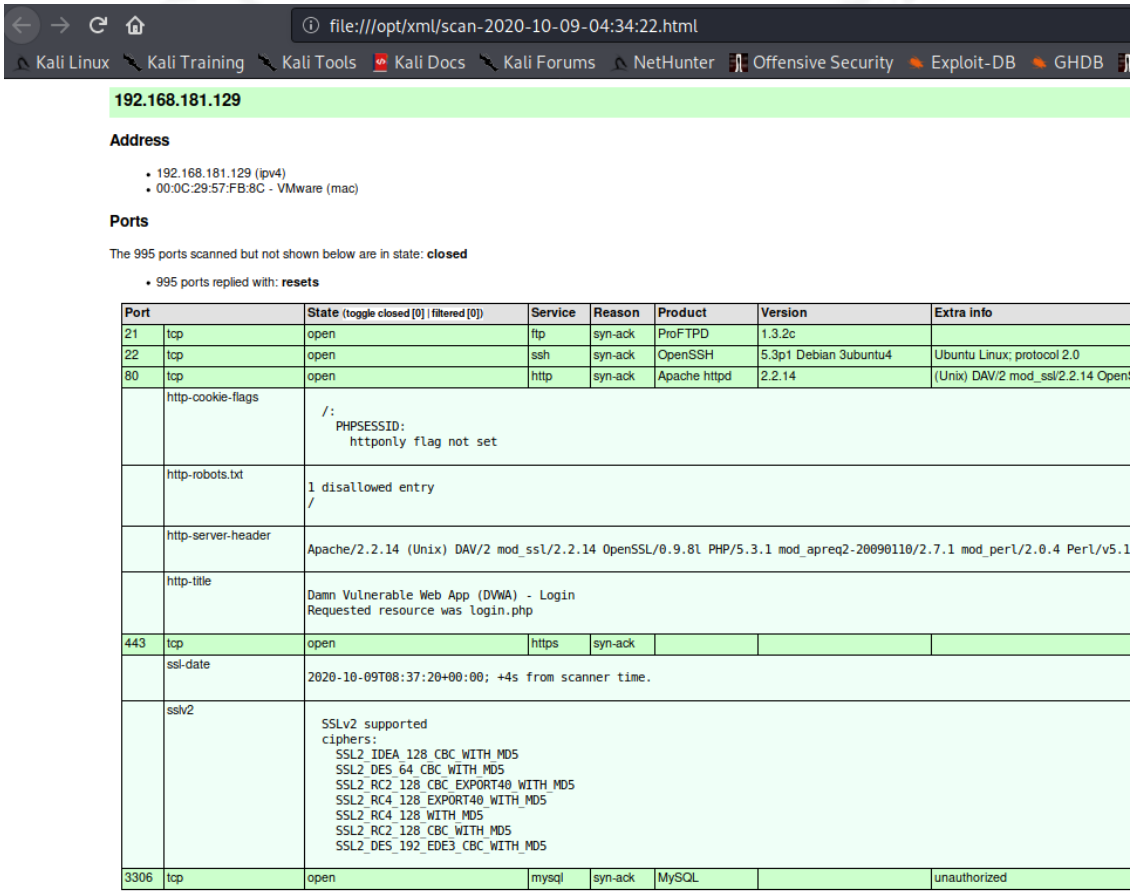
5.4.1.1 Características del prototipo

- Qué hace: El prototipo trata de hacer escaneos automatizados de nivel básico hacia un segmento específico de red, recaba la información y la entrega en un informe humanizado. Todo esto programado de forma automática para que el usuario solamente vea los reportes.
- Como está hecho: Módulos y scripts en Bash y Python que, mediante una serie de librerías, invocan a una herramienta con distintos parámetros para obtener la información y procesarla. Posteriormente con el uso de otra herramienta, también integrada en el script, permitirá volcar la información recopilada en un archivo tipo informe visualizable por el usuario (véase Figuras 5.5. y 5.6).

Figura 5. 5
Ejecución de sistema IOC en su versión alfa

```
kali@kali:~/Desktop/IOC$ sudo bash ioc_alfa.sh
Bienvenido al sistema de automatización de verificaciones de puertos y vulnerabilidades
1) Escaneo a un servidor (solo IP)
2) Escaneo a lista de servidores (archivo txt)
¿Qué deseas escanear? 1
Ingrese una ip: 192.168.181.129
0. Solo esta vez
1. Diario
2. Semanal
3. Mensual
Elija frecuencia: 0
Iniciando escaneo ...
```

Figura 5. 6
Visualización de reporte generado por la herramienta



5.4.1.2 Conceptos que se quieren probar

- Es posible invocar una herramienta de escaneo y automatizarla mediante un lenguaje de programación o scripting de alto nivel.
- Es posible invocar una herramienta de reporte y automatizar resultados obtenidos de otra herramienta

- Es posible automatizar y agendar ambos procesos: escaneo y reporte para que el usuario tenga el menor esfuerzo posible.
- La automatización de estos procesos ayuda al usuario en las tareas que realiza.
- La automatización de los resultados ayuda al usuario en la toma de decisiones tempranas sobre ciberseguridad.

5.4.1.3 Resultados

Todo lo que se quiso probar en esta fase del análisis fue comprobado de manera exitosa, tal como se explica en la Tabla 5.4 y en las Figuras 5.7-5.12.

Tabla 5. 4

Análisis de conceptos para probar

Conceptos por probar	Análisis	Resultado
Invocar una herramienta de escaneo y automatizarla mediante un lenguaje de programación de alto nivel	Para esta fase alfa, se utilizó scripting en bash y Python para invocar a Nmap y agendar escaneos según decisión del usuario	Comprobado
Invocar una herramienta de reporte y automatizar resultados obtenidos de otra herramienta	El script invoca una herramienta que permite traducir el resultado del escaneo a un formato HTML visualizable y comprensible por el usuario	Comprobado
Automatizar y agendar ambos procesos: escaneo y reporte, para que el usuario tenga el menor esfuerzo posible	El script invoca a la herramienta cron para agendar el proceso de escaneo elegido por el usuario y de esa forma automatizarlo	Comprobado
Automatización de estos procesos ayuda al usuario en las tareas que realiza	Las tareas de visibilidad de puertos y servicios forman parte de tareas rutinarias que suelen hacerse con cierta frecuencia de forma manual	Comprobado
Automatización ayuda en la toma de decisiones tempranas sobre ciberseguridad	Dado que estas tareas ahora pueden ser automatizadas, el tiempo entre cada escaneo puede ser menor, lo que incrementa la visibilidad y capacidad de responder ante cambios en los puertos y servicios	Comprobado

Figura 5. 7
Código inicial y de bienvenida al programa

```
#!/bin/sh
date=`date +%F-%T`

#inicio de programa
#IOC version de prueba - alfa

echo "Bienvenido al sistema de automatización de verificaciones de
puertos y vulnerabilidades"
echo "1) Escaneo a un servidor (solo IP)"
echo "2) Escaneo a lista de servidores (archivo txt)"
read -p "¿Qué deseas escanear? " option
```

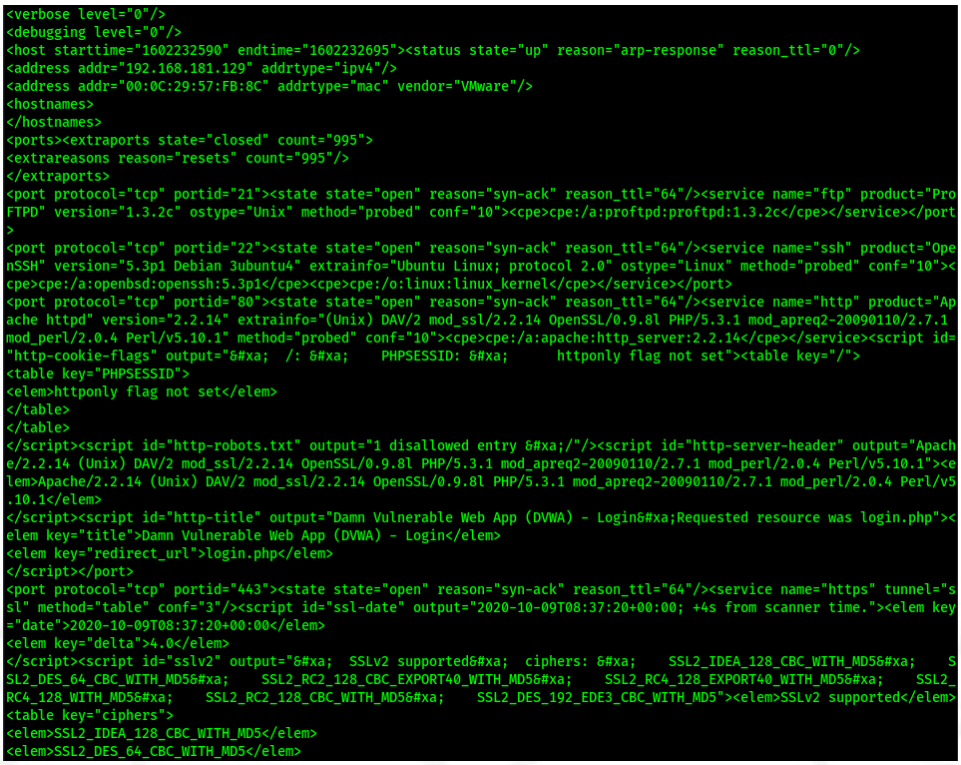
Figura 5. 8
Código para establecer y automatizar frecuencia de escaneo

```
#Funcion que realiza la programacion de los escaneos
scheduleNmap() {
    echo "0. Solo esta vez"
    echo "1. Diario"
    echo "2. Semanal"
    echo "3. Mensual"
    read -p "Elija frecuencia: " frequency

    if [ $frequency -eq "0" ]; then
        echo "Iniciando escaneo ..."
        bash $1
        echo "Escaneo finalizado ..."
    fi
    if [ $frequency -eq "1" ]; then
        echo "@daily root $1" >> /etc/crontab
        echo "Escaneo automatizado diariamente"
    fi
    if [ $frequency -eq "2" ]; then
        echo "@weekly root $1" >> /etc/crontab
        echo "Escaneo automatizado semanalmente"
    fi
    if [ $frequency -eq "3" ]; then
        echo "@monthly root $1" >> /etc/crontab
        echo "Escaneo automatizado mensualmente"
    fi
}
```

Figura 5. 9

Ejemplo de resultado de escaneo en formato XML listo para ser importado



```
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1602232590" endtime="1602232695"><status state="up" reason="arp-response" reason_ttl="0"/>
<address addr="192.168.181.129" addrtype="ipv4"/>
<address addr="00:0C:29:57:FB:8C" addrtype="mac" vendor="VMware"/>
<hostnames>
</hostnames>
<ports><extraports state="closed" count="995">
<extrareasons reason="resets" count="995"/>
</extraports>
<port protocol="tcp" portid="21"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="ftp" product="Pro
FTPD" version="1.3.2c" ostype="Unix" method="probed" conf="10"><cpe>cpe:/a:proftpd:proftpd:1.3.2c</cpe></service></port
>
<port protocol="tcp" portid="22"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="ssh" product="Ope
nSSH" version="5.3p1 Debian 3ubuntu4" extrainfo="Ubuntu Linux; protocol 2.0" ostype="Linux" method="probed" conf="10"><
cpe>cpe:/a:openbsd:openssh:5.3p1</cpe><cpe>cpe:/o:linux:linux_kernel</cpe></service></port>
<port protocol="tcp" portid="80"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="http" product="Ap
ache httpd" version="2.2.14" extrainfo="(Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1
mod_perl/2.0.4 Perl/v5.10.1" method="probed" conf="10"><cpe>cpe:/a:apache:http_server:2.2.14</cpe></service><script id=
"http-cookie-flags" output="&#xa;  /: &#xa;    PHPSESSID: &#xa;      httponly flag not set"><table key="/">
<table key="PHPSESSID">
<elem>httponly flag not set</elem>
</table>
</table>
</script><script id="http-robots.txt" output="1 disallowed entry &#xa;/"/><script id="http-server-header" output="Apach
e/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1"><e
lem>Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5
.10.1</elem>
</script><script id="http-title" output="Damn Vulnerable Web App (DVWA) - Login&#xa;Requested resource was login.php"><
elem key="title">Damn Vulnerable Web App (DVWA) - Login</elem>
<elem key="redirect_url">login.php</elem>
</script></port>
<port protocol="tcp" portid="443"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="https" tunnel="s
sl" method="table" conf="3"/><script id="ssl-date" output="2020-10-09T08:37:20+00:00; +4s from scanner time."><elem key
="date">2020-10-09T08:37:20+00:00:00</elem>
<elem key="delta">4.0</elem>
</script><script id="sslv2" output="&#xa;  SSLv2 supported&#xa;  ciphers: &#xa;    SSL2_IDEA_128_CBC_WITH_MD5&#xa;    S
SL2_DES_64_CBC_WITH_MD5&#xa;    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5&#xa;    SSL2_RC4_128_EXPORT40_WITH_MD5&#xa;    SSL2_
RC4_128_WITH_MD5&#xa;    SSL2_RC2_128_CBC_WITH_MD5&#xa;    SSL2_DES_192_EDE3_CBC_WITH_MD5"><elem>SSLv2 supported</elem>
<table key="ciphers">
<elem>SSL2_IDEA_128_CBC_WITH_MD5</elem>
<elem>SSL2_DES_64_CBC_WITH_MD5</elem>
```

Figura 5. 10

Resultados convertidos exitosamente a formato HTML

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	ProFTPD	1.3.2c	
22	tcp	open	ssh	syn-ack	OpenSSH	5.3p1 Debian 3ubuntu4	Ubuntu Linux; protocol 2.0
80	tcp	open	http	syn-ack	Apache httpd	2.2.14	(Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
	http-cookie-flags	/: PHPSESSID: httponly flag not set					
	http-robots.txt	1 disallowed entry /					
	http-server-header	Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1					
	http-title	Damn Vulnerable Web App (DVWA) - Login Requested resource was login.php					
443	tcp	open	https	syn-ack			
	ssl-date	2020-10-09T08:37:20+00:00; +4s from scanner time.					
	sslv2	SSLv2 supported ciphers: SSL2_IDEA_128_CBC_WITH_MD5 SSL2_DES_64_CBC_WITH_MD5 SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 SSL2_RC4_128_EXPORT40_WITH_MD5 SSL2_RC4_128_WITH_MD5 SSL2_RC2_128_CBC_WITH_MD5 SSL2_DES_192_EDE3_CBC_WITH_MD5					
3306	tcp	open	mysql	syn-ack	MySQL		unauthorized

Figura 5. 11
Ejecución del programa en su versión alfa, programando semanalmente la tarea de escaneo

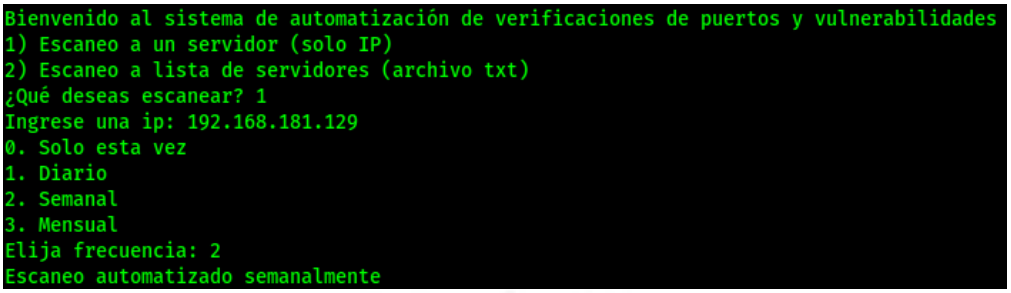
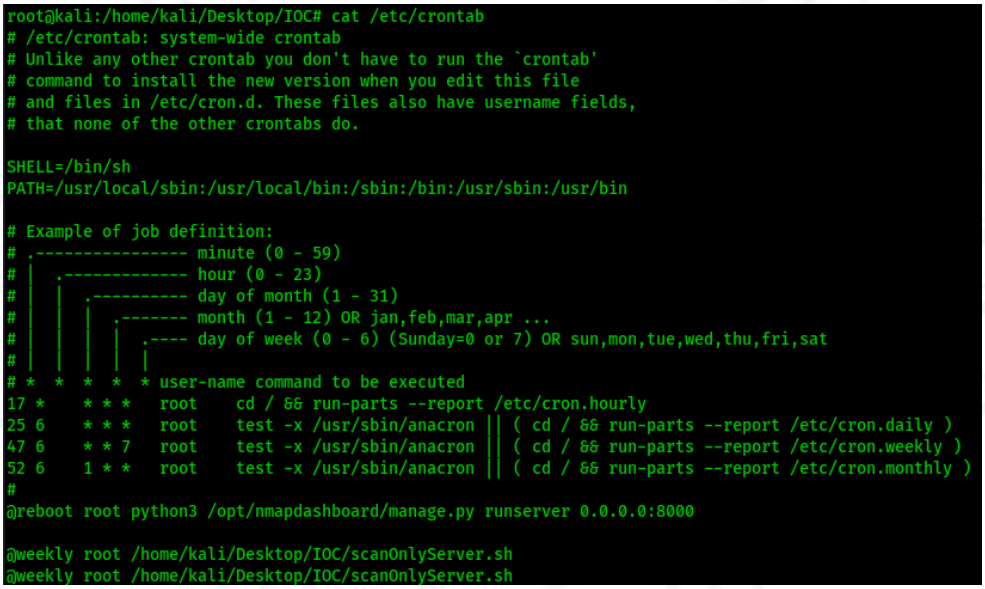


Figura 5. 12
Consulta a la agenda del sistema para corroborar ejecución exitosa del programa



5.4.2 Prototipado fase BETA

En este apartado se mostrará la segunda fase de prototipeo, en la cual se muestra ya una evolución a la solución (Figuras 5.13-5.21), pues se le agrega:

- Integración con más herramientas como las de mapeo visual de red, integración de resultados y consultas embebidas a la base de datos de vulnerabilidades CVE.
- Interfaz visual (GUI de usuario)
- Sistema de reporte

Nota: Como escenario de prueba para la correcta ejecución de la herramienta, esta fue realizada en un ambiente con algunas máquinas virtuales que la herramienta podía escanear y demostrar sus capacidades.

5.4.2.1 Pantalla o recorrido de partes más importantes del producto

Figura 5. 13
Bienvenida al sistema

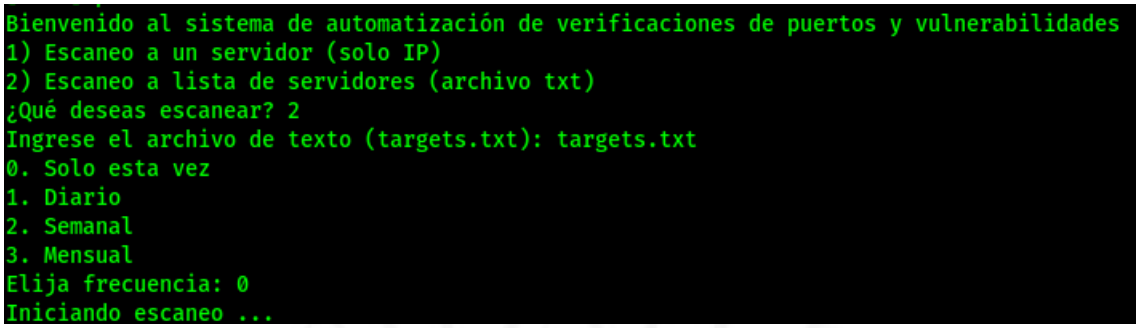


Figura 5. 14
Visualización de lista de objetivos o servidores elegidos

Figura 5. 15
Visualización de contenido de archivo crontab de tareas agendadas

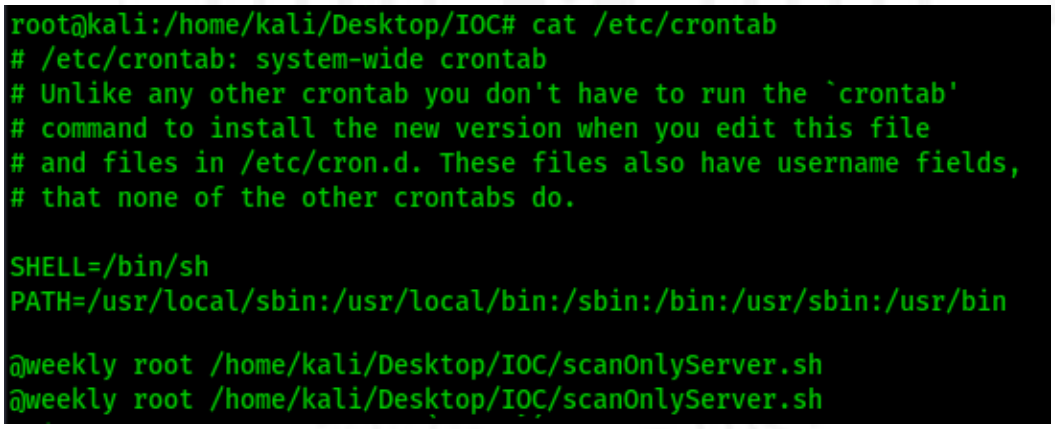


Figura 5. 16
Listado de archivos de reporte en formatos html y xml

```
root@kali:/home/kali/Desktop/IOC# ls -la /opt/xml
total 112
drwxr-xr-x 2 root root  4096 Oct  9 06:27 .
drwxr-xr-x 6 root root  4096 Sep 19 22:14 ..
-rw-r--r-- 1 root root 14263 Oct  2 22:12 scan-2020-10-02+22:10:10.xml
-rw-r--r-- 1 root root 14631 Oct  2 22:23 scan-2020-10-02+22:15:08.html
-rw-r--r-- 1 root root 14558 Oct  2 22:16 scan-2020-10-02+22:15:08.xml
-rw-r--r-- 1 root root 14631 Oct  2 22:25 scan-2020-10-02+22:25:01.html
-rw-r--r-- 1 root root  4627 Oct  5 00:00 scan-2020-10-02+22:25:01.xml
-rw-r--r-- 1 root root 11451 Oct  9 04:38 scan-2020-10-09-04:34:22.html
-rw-r--r-- 1 root root  8981 Oct  9 04:38 scan-2020-10-09-04:34:22.xml
-rw-r--r-- 1 root root  4520 Oct  9 06:27 scan-2020-10-09-06:25:30.xml
```

Figura 5. 17
Reportes visualizados desde interfaz gráfica web

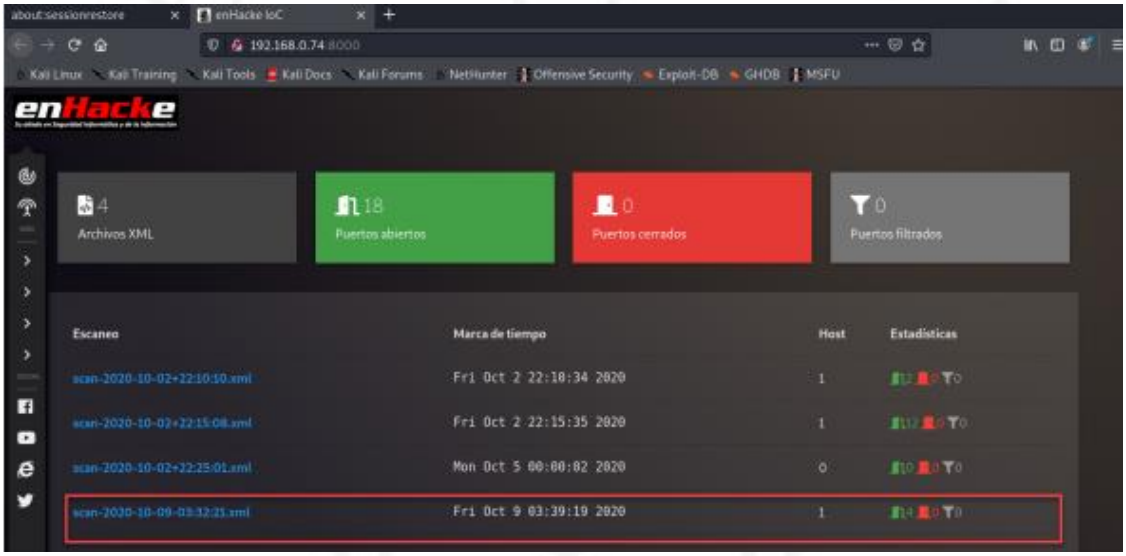


Figura 5. 18
Visualización de componentes de red e información obtenida en escaneo

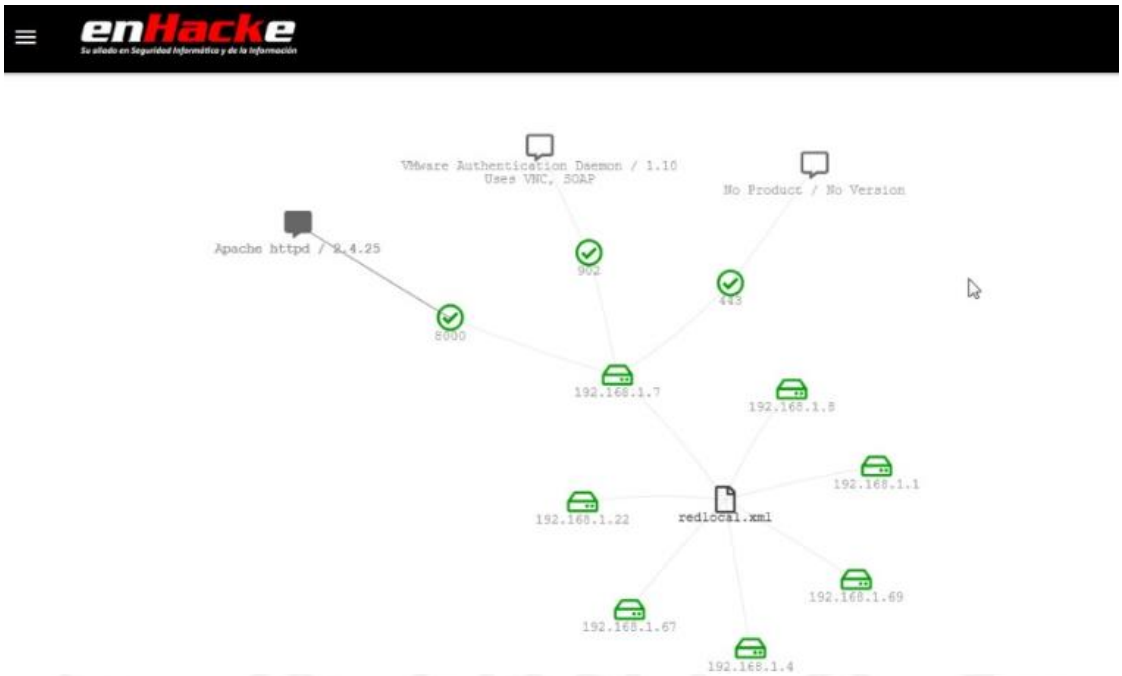


Figura 5. 19
Interfaz de integración de resultados

Para las pruebas de escaneo se utilizó como máquina de objetivo de pruebas, un sistema virtualizado de Linux que tenía algunas configuraciones por defecto y algunos servicios sin actualizar, incrementando así las vulnerabilidades para que el sistema pueda reconocerlas.

Figura 5. 20

Integración con verificación de vulnerabilidades

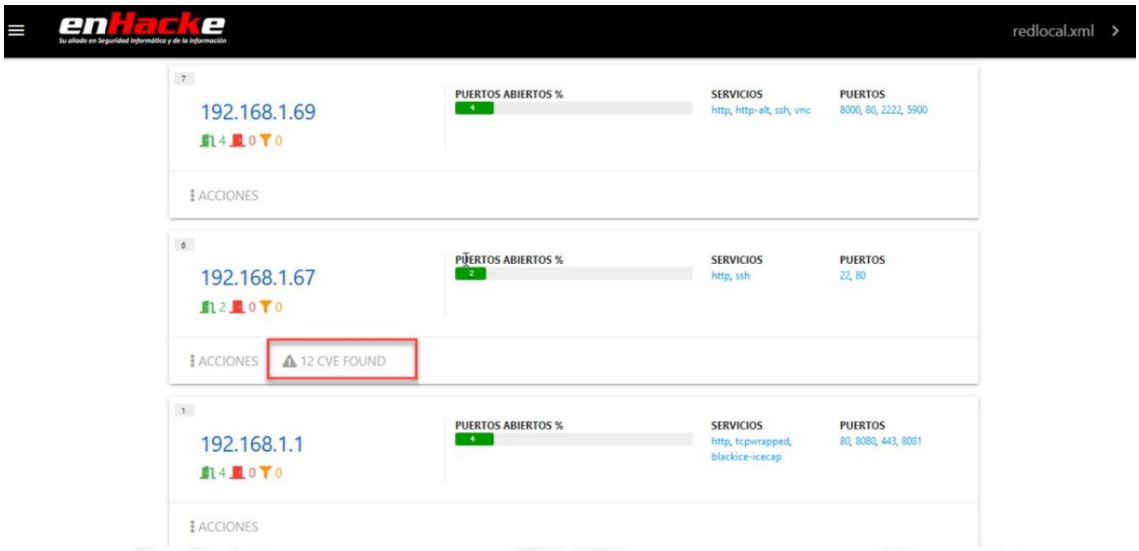
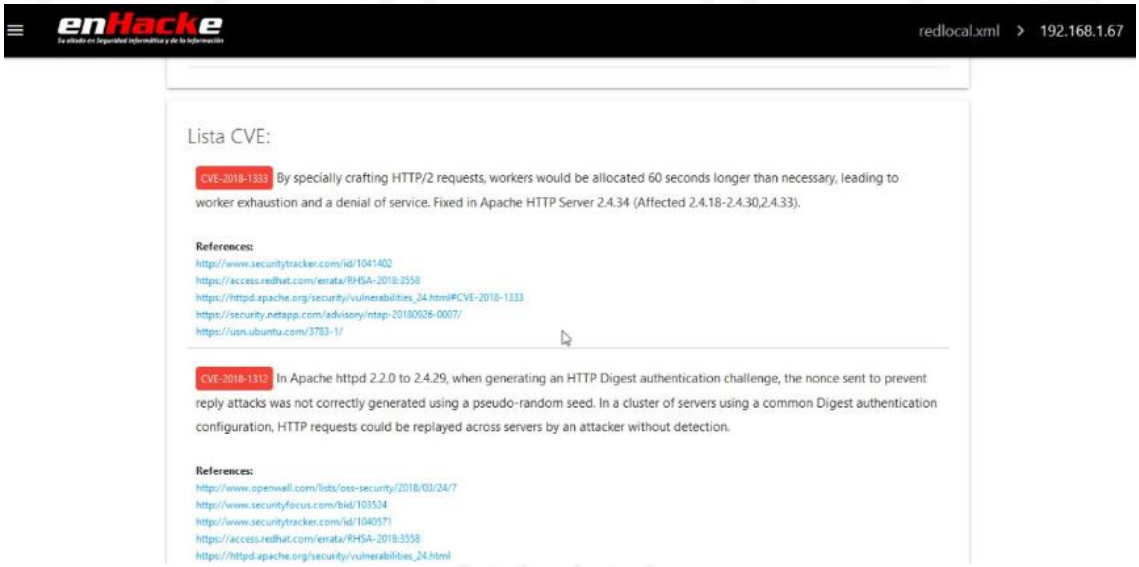


Figura 5. 21

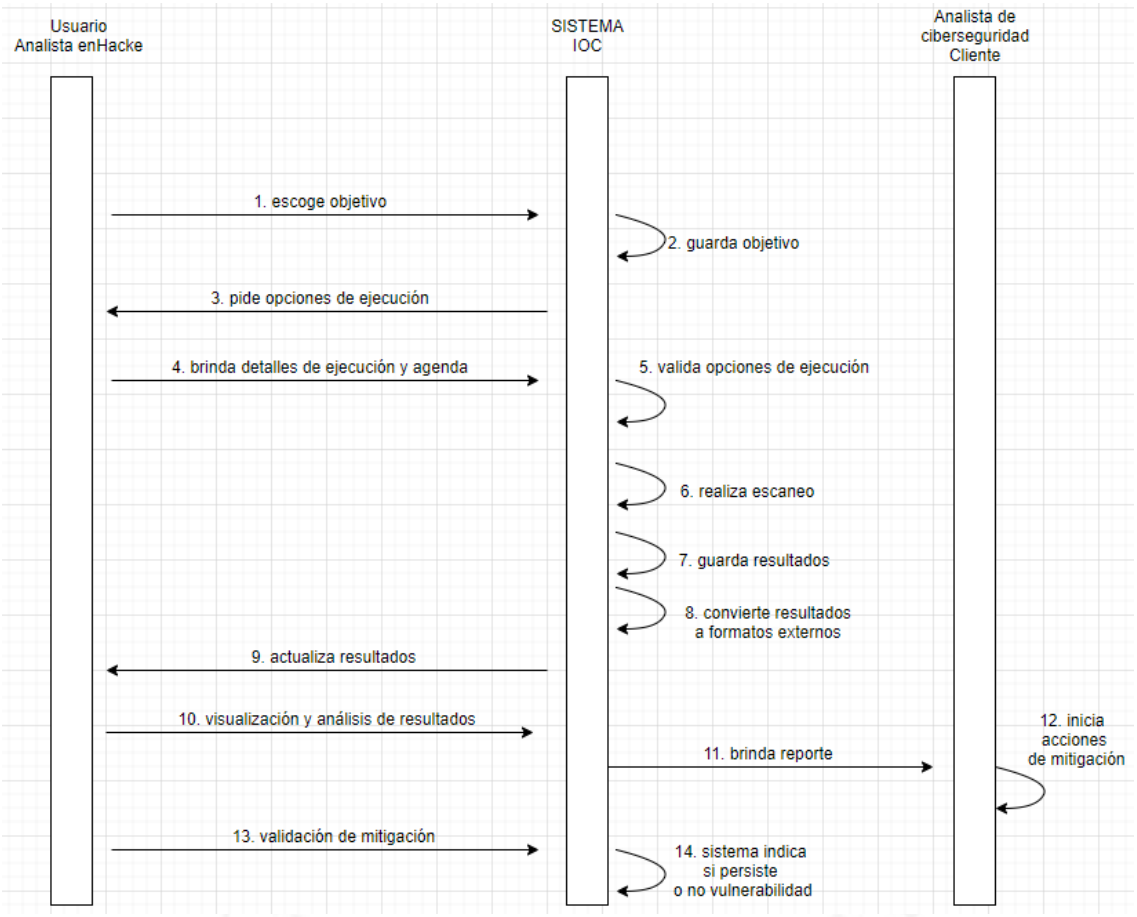
Consulta de vulnerabilidades a fuentes abiertas de CVE - Common Vulnerabilities and Exposures



5.4.3 Diseño funcional de la solución

A continuación, en la Figura 5.22 se muestra el detalle del flujo de acciones e interacciones entre el usuario que gestiona la plataforma, el sistema IOC y el analista de ciberseguridad del cliente, encargado de ser el puente de comunicación con las distintas áreas tecnológicas de la empresa.

Figura 5. 22
Diagrama de interacción y flujo



Como se puede observar en el diagrama, el sistema IOC solo necesita información inicial para luego automatizar varios de sus procesos, dejando libre tanto al usuario analista de enHacke (encargado de utilizar la plataforma), como al analista de ciberseguridad de la empresa cliente, que solo espera a los reportes para iniciar acciones de mitigación en coordinación con las áreas que se vean involucradas en los informes.

5.4.4 Arquitectura de la solución

En este apartado se mostrará una arquitectura básica en ambas opciones, local y nube. En ambos casos se requiere de servidores virtualizados tanto Windows como Linux, ya que serán repositorios de las distintas herramientas que luego se comunicarán con el sistema IOC y su plataforma web. En la Tabla 5.5 se presentan las características necesarias aproximadas para ambos escenarios (véase Figuras 5.23 y 5.24).

Tabla 5. 5

Características de infraestructura

Recurso	Infraestructura en la nube	Infraestructura on Premise
Memoria RAM	RAM asignada por cada máquina desplegada	32GB de RAM
Plataforma operativa	Plataforma de gestión AWS	VMWare ESXi
Sistemas virtualizados	Linux y Windows	Linux y Windows
Tarjetas de red	Tarjetas lógicas virtualizadas	Distintas tarjetas de red físicas y lógicas

Figura 5. 23

Representación gráfica de la infraestructura en la nube

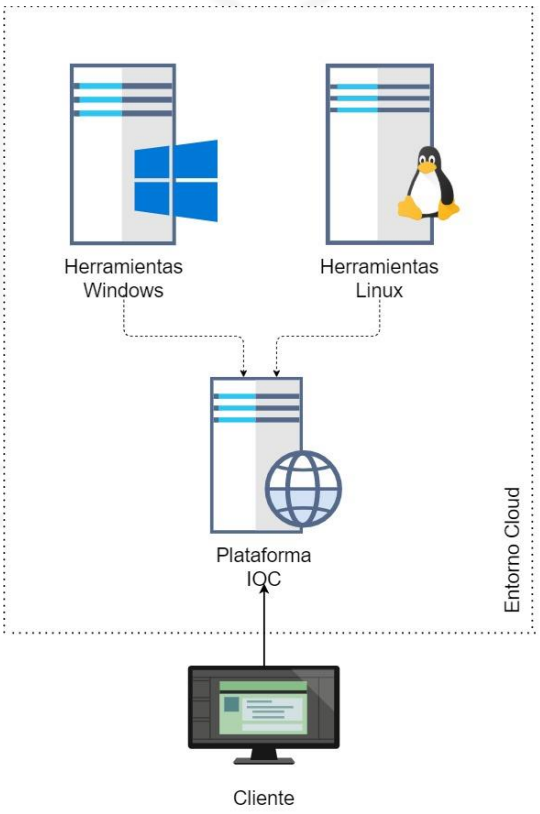
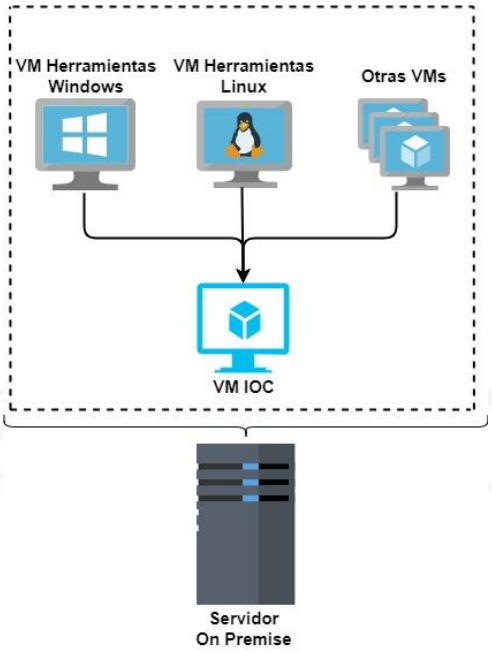


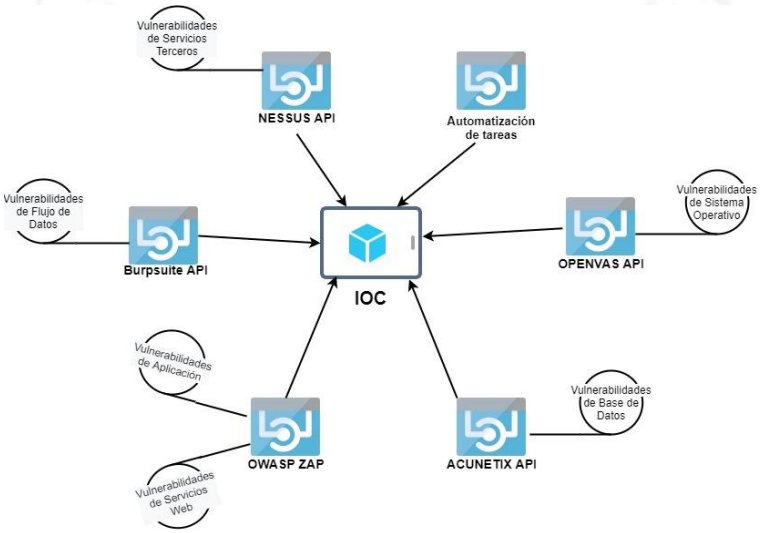
Figura 5. 24
Representación gráfica de la infraestructura en servidor físico



5.4.5 Diseño técnico de la solución

Para que el sistema funcione correctamente, se apoya en la interacción con otras herramientas que le permiten proveer capacidades avanzadas de análisis a lo largo de distintas capas y enfoques explicadas anteriormente. La relación entre cada una de las herramientas y la plataforma integradora son centralizadas. A su vez, se cuenta con un módulo de automatización de tareas que provee a la plataforma de la gestión del resto de las herramientas (véase Figura 5.25).

Figura 5. 25
Representación gráfica de interacción con distintas herramientas



5.5 Evaluar

Para poder comprobar que el prototipo sí apoyó en la verificación de las necesidades del cliente y en cómo eran satisfechas o mitigadas por el prototipo, se realizaron una lista de conceptos a probar para la fase alfa, que tenía el objetivo básico de corroborar que era posible integrar herramientas y que esta integración le ayudaba en algo al cliente, y para la fase beta que tenía como objetivo incrementar la eficiencia en los procesos o tareas del usuario, así como mejorar su experiencia de interacción con la plataforma. Estas características justamente irían escalando conforme la herramienta vaya incrementando su desarrollo.

5.5.1 Conceptos a probar por fase

Como se puede apreciar en la Tabla 5.6, todos los conceptos de prueba fueron analizados y comprobados.

Tabla 5. 6

Conceptos para probar en fases ALFA y BETA

Fase	Conceptos para probar	Análisis	Resultado
Alfa	Invocar una herramienta de escaneo y automatizarla mediante un lenguaje de programación de alto nivel	Para esta fase alfa, se utilizó scripting en bash y Python para invocar a Nmap y agendar escaneos según decisión del usuario	Comprobado
	Invocar una herramienta de reporte y automatizar resultados obtenidos de otra herramienta	El script invoca una herramienta que permite traducir el resultado del escaneo a un formato HTML visualizable y comprensible por el usuario	Comprobado
	Automatizar y agendar ambos procesos: escaneo y reporte, para que el usuario tenga el menor esfuerzo posible	El script invoca a la herramienta cron para agendar el proceso de escaneo elegido por el usuario y de esa forma automatizarlo	Comprobado
	Automatización de estos procesos ayuda al usuario en las tareas que realiza	Las tareas de visibilidad de puertos y servicios forman parte de tareas rutinarias que suelen hacerse con cierta frecuencia de forma manual	Comprobado
	Automatización ayuda en la toma de decisiones tempranas sobre ciberseguridad	Dado que estas tareas ahora pueden ser automatizadas, el tiempo entre cada escaneo puede ser menor, lo que incrementa la visibilidad y capacidad de responder ante cambios en los puertos y servicios	Comprobado
Beta	Integración con otras herramientas brinda más información relevante para el cliente	El sistema ahora ofrece cuadros de relación de infraestructura, visualización de puertos, servicios y vulnerabilidades	Comprobado
	La interfaz gráfica facilita la comprensión de la información	Los gráficos ofrecidos se brindan de forma amigable y bien categorizados para mejor comprensión por parte del cliente	Comprobado

(continúa)

(continuación)

Fase	Conceptos para probar	Análisis	Resultado
Beta	El sistema automatiza aún más los procesos de escaneo y visualización de información	El sistema está ahora configurado para centralizar toda la información no solo del último escaneo, sino de los anteriores también	Comprobado
	Es posible juntar la información obtenida con herramientas externas de gestión de vulnerabilidades	El sistema provee interacción con fuentes abiertas de base de datos de vulnerabilidades CVE	Comprobado
	Se puede exportar a un formato de informe aún más amigable	El sistema brinda la opción de exportar el informe a formato PDF con toda la información normalizada y convertida para una fácil visualización	Comprobado

5.5.2 Resultados de experiencia de usuario

En el cuadro presentado a continuación se explica y detalla el ahorro de tiempo que hay en cada una de las tareas del usuario, como se realizaban originalmente y como se realizan después de la implementación del sistema IOC. Es importante remarcar que el impacto en tiempo y eficiencia es enorme, sobre todo si la organización cuenta con recursos humanos limitados (véase Tabla 5.7).

Tabla 5. 7

Comparativa de tareas antes vs. Después

Tarea	Como se realizaba	Duración de proceso antes	Como la realiza con la herramienta	Duración de proceso con sistema implementado
Escaneo	Con herramientas y en forma manual, por segmentos	El proceso era repetitivo, tedioso y manual, por lo que tomaba un par de semanas cada vez	Proceso ahora automatizado, se puede agendar diaria, semanal o mensualmente	Una vez elegidos los objetivos, los procesos de escaneos se ejecutan automáticamente. Toma uno o dos días elegir los objetivos según uso de red o negocio
Verificación y comparación	Analizando los resultados y comparándolos con resultados anteriores	Los informes al ser independientes, en distintos repositorios y diferentes formatos, no eran fácilmente analizables ni comparables, por lo que tomaba entre una y dos semanas dependiendo de la cantidad de objetivos	Todos los resultados están centralizados para fácil acceso	Dependiendo de la cantidad de objetivos, puede llegar a tomar una semana así son varias redes
Investigación de vulnerabilidades	Si la herramienta le daba algún mensaje de vulnerabilidad, esta se buscaba en internet	La búsqueda o investigación de vulnerabilidades consumía mucho tiempo. Dependiendo de la cantidad de vulnerabilidades y de apoyo que pudiese recibir de otros analistas, entre semanas o un par de meses.	Acceso al repositorio de vulnerabilidades según los resultados que brinden las herramientas de escaneo	Las vulnerabilidades más críticas están mapeadas en la base de datos abierta de Common Vulnerabilities and Exposures (CVE), por lo que la integración permite saber de primera mano si hay resultados críticos con tan solo un par de horas o días si el informe incluye personalización por parte del equipo enHacke.
Comunicación de vulnerabilidades	Se desarrollaba un informe en Excel y este era enviado a infraestructura, redes y TI	Dependiendo de la cantidad de información, hasta una semana	Informe automatizado para enviar	El informe es altamente técnico pero personalizable por el equipo enHacke, este puede acomodarse a lo que requiere el cliente de tal forma que el analista solo requiera comprenderlo y enviarlo a las áreas pertinentes
Seguimiento de mitigación	Llamadas y reuniones para ver como iban respecto a la mitigación	Este era un cuello de botella, porque el analista no podría hacer seguimiento con las áreas y volver a realizar el escaneo y análisis, muchas veces tenía que esperar confirmación de las otras áreas	La herramienta al estar lanzando escaneos en forma automatizada (debido a los procesos agendados), le permite saber si se hizo la mitigación o no y permite un mejor seguimiento	El analista cuenta con información actualizada siempre, dependiendo de como agendó las tareas

CONCLUSIONES

- Con este proyecto se propone un enfoque adicional a las ya tradicionales tareas de ciberseguridad en las que se detectan los ataques e intentos de intrusión de manera reactiva. Las tareas preventivas de auditoría, pentesting y ethical hacking que se vienen llevando a cabo en las organizaciones en los últimos años no siempre son suficientes para obtener un diagnóstico acotado y actualizado sobre las vulnerabilidades presentes en la infraestructura tecnológica de la organización. Si bien son tareas que se llevan a cabo un par de veces al año, su periodicidad genera una brecha de conocimiento actualizado sobre los potenciales puntos a ser utilizados en ataques por los cibercriminales o terceros maliciosos.
- La automatización inteligente es un factor clave que no sólo genera valor en este proyecto, sino en los cientos o miles de proyectos que se encuentran llevándose a cabo en la actualidad. El hecho de poder ejecutar inteligentemente tareas repetitivas ayuda a los analistas en áreas de ciberseguridad o seguridad de la información a enfocarse mejor en temas prioritarios como la estrategia de ciberseguridad, la mitigación de vulnerabilidades y prevención ante amenazas.
- Las pruebas de prototipado realizadas nos permiten comprobar que un sistema de este tipo y bajo un enfoque totalmente preventivo, no solo tiene cabida dentro de las actividades de trabajo de un área corporativa de ciberseguridad, sino que permite además realizar estas tareas de forma eficiente.
- Uno de los retos a la hora de realizar implementaciones de sistemas de este tipo es el de la cambiante infraestructura de redes en las organizaciones. Ya no solo definido por una infraestructura interna y externa, sino por la expansión hacia las ahora conocidas como redes híbridas, donde los límites antes claramente definidos, se diluyen entre el interno, externo, cloud y redes de dispositivos IoT. Este cambio de panorama representa una mayor dificultad para la implementación de sistemas de seguimiento que otorguen visibilidad en cuanto a vulnerabilidades en cada uno de los distintos segmentos de red de la organización.

RECOMENDACIONES

- En proyectos de ciberseguridad en los que se desea innovar o mejorar procesos, se recomienda hacer uso de Python como lenguaje de mejora. Esto debido a la gran cantidad de librerías disponibles no solamente para manejo de archivos y gestión de sistema, sino para networking, machine learning y ciberseguridad misma. La aceptación que ha tenido Python en la comunidad de ciberseguridad ha tenido como consecuencia la evolución y tecnificación de muchos proyectos que se comparten libremente para poder analizar y aprender de estos.
- Se podría utilizar machine learning en el futuro con el objetivo de poder mapear o identificar patrones en las vulnerabilidades que se van obteniendo o en el comportamiento a la hora de encontrar puertos recientemente abiertos.
- Siempre es recomendable, antes de embarcarse en algún proyecto, realizar pruebas de concepto iniciales y pequeñas que permitan comprobar que lo que se quiere lograr en el futuro tendrá al menos un camino o posibilidad.
- Se podría expandir la inteligencia del proyecto mediante el análisis de las vulnerabilidades que se van encontrando en la infraestructura del cliente, si se hace un análisis correlacionando los vectores de ataque de MITRE (Anexo 7).

GLOSARIO DE TÉRMINOS

- **NSA:** National Security Agency. Agencia de Seguridad Nacional de Estados Unidos de America.
- **AWS:** Amazon Web Services. Servicios de alquiler de infraestructura en la nube de Amazon.
- **IoT:** Internet of Things. Se le dan este nombre a todos los dispositivos de uso casero, industrial o comercial, que tienen conectividad con internet ya sea para su gestión o para envío de información. Un claro ejemplo son las refrigeradoras que tienen ahora conectividad wifi para brindar mayores prestaciones a los usuarios.
- **NIST Cybersecurity Framework:** Marco de trabajo de ciberseguridad propuesto por NIST, Instituto Nacional de Estándares y Tecnología, que brinda un método y una serie de controles para medir, asegurar y avanzar en la estrategia de ciberseguridad corporativa o gubernamental.
- **ISO 27000:** Conjunto de estándares de seguridad de la información.
- **ISO 27032:** Documentación para la gestión de la ciberseguridad.
- **SBS G140:** Circular emitida por la Superintendencia de Banca y Seguros sobre la Gestión de la Seguridad de la Información.
- **PCI-DSS:** Payment Card Industry – Data Security Standard. Es el estándar de seguridad de datos para la industria de tarjetas de pago. En su documentación contiene información y una serie de controles y recomendaciones para cumplir con el aseguramiento de la infraestructura que compromete el procesamiento o almacenamiento de información sensible de tarjetahabientes.
- **GDPR:** General Data Protection Regulation, regulación europea de protección de datos generales de los usuarios.
- **CIS Controls:** Controles provistos por el Centro de Seguridad para Internet que contienen las buenas prácticas priorizadas para su implementación corporativamente.

- **SOC:** Security Operations Center o Centro de Operaciones de Seguridad está compuesto por tecnología, profesionales y procedimientos que tienen por objetivo resguardar la infraestructura tecnológica de la organización.
- **CVE:** Common Vulnerabilities and Exposures, es una base de datos que centraliza toda la información sobre vulnerabilidades de ciberseguridad en las distintas plataformas y componentes de tecnología disponibles en la actualidad.
- **MITRE ATT&CK:** Base de conocimiento orientada a mostrar a nivel técnico las distintas formas de ataque y técnicas utilizadas por terceros maliciosos en ciberataques en la actualidad.
- **Script:** Conjunto de comandos en un archivo diseñados para ser ejecutados como un programa y con uno o varios objetivos en mente.
- **Scripting:** Codificación en algún lenguaje de alto nivel y haciendo uso de scripts.
- **Bash:** Lenguaje de órdenes y comandos para Unix / Linux.
- **NMAP:** Herramienta de análisis de red que permite realizar escaneos de puertos y servicios.
- **CRON:** Administrador de procesos que permite agendar la ejecución de estos en forma personalizada.
- **On Premise:**

REFERENCIAS

Accenture. (2018). 2018 State of Cyber Resilience: Gaining Ground on the Cyber Attacker (Rep.).

Berinato, S., & Perry, M. (2019). Cybersecurity: Insights you need from Harvard Business Review.

C|NET en español. (2020, Enero 27). Filtración en Perú expuso información de clientes de una cadena de cines. Recuperado de https://www.cnet.com/es/noticias/peru-fuga-datos-cineplanet/

Diario El Economista. (2019, Noviembre 17). El rescate por el hackeo a Pemex es el segundo mayor por ransomware. Recuperado de https://www.eleconomista.com.mx/empresas/El-rescate-por-el-hackeo-a-Pemex-es-el-segundo-mayor-por-ransomware-20191115-0035.html

Diario Expreso. (2020, Junio 30). Hackeo masivo de web de EXPRESO. Recuperado de https://www.expreso.com.pe/destacado-portada/hackeo-masivo-de-web-de-expreso/

Diario Gestión. (2019, Diciembre 03). BCP reconoce que se filtró información de clientes en un ataque cibernético de 2018. Recuperado de https://gestion.pe/tu-dinero/bcp-reconoce-que-se-filtro-informacion-de-clientes-en-un-ataque-cibernetico-de-2018-nndc-noticia/?ref=gesr

IBM. (2020). Informe del costo de una vulneración de datos 2020 (Rep.).

Verizon. (2020). Data Breach Investigation Report 2020 (Rep.).

BIBLIOGRAFÍA

Center for Internet Security. (2019). CIS Controls, Version 7.1 (Publication).

Framework for Improving Critical Infrastructure Cybersecurity. (2018). Version 1.1. National Institute of Standards and Technology. https://doi.org/10.6028/nist.cswp.04162018

Graham, J., Olson, R., & Howard, R. (2016). Cyber Security Essentials. Auerbach Publications.Cybersecurity essentials

Osterwalder, A., & Pigneur, Y. (2010). Business model generation: A handbook for visionaries, game changers, and challengers. Hoboken, NJ: Wiley.

Stallings, W. (2019). Effective cybersecurity: Understanding and using standards and best practices. Upper Saddle River, NJ: Addison-Wesley.

ANEXOS

Anexo 1: Norma SBS para ciberseguridad

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

PREPUBLICACIÓN

Resolución S.B.S.
Nº -2020
La Superintendenta de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones

CONSIDERANDO:

Que, el Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado mediante la Resolución SBS N° 272-2017, incorpora disposiciones que tienen por finalidad que las empresas supervisadas cuenten con una gestión de riesgos y gobierno corporativo adecuados;

Que, mediante el Reglamento para la Gestión del Riesgo Operacional, aprobado mediante la Resolución SBS N° 2116-2009, se incluyen disposiciones que las empresas deben cumplir en la gestión efectiva del riesgo operacional;

Que, mediante la Resolución SBS Nº 11699-2008 y sus modificatorias, se aprobó el Reglamento de Auditoria Interna;

Que, mediante la Resolución SBS Nº 17026-2010 y sus modificatorias, se aprobó el Reglamento de Auditoria Externa;

Que, esta Superintendencia emitió la Circular G-140-2009 con la finalidad de establecer criterios mínimos para una adecuada gestión de la seguridad de la información;

Que, resulta necesario actualizar la normativa sobre gestión de seguridad de la información vía la aprobación de un reglamento, complementario al Reglamento para la Gestión del Riesgo Operacional, tomando en cuenta los estándares y buenas prácticas internacionales, entre los que se encuentran los publicados por el National Institute of Standards and Technology y la familia de estándares ISO/IEC 27000 sobre seguridad de la información, así como la creciente interconectividad y mayor adopción de canales digitales para la provisión de los servicios del sistema financiero, de seguros y privado de pensiones, y que ante este contexto es necesario que las empresas de dichos sistemas supervisados fortalezcan sus capacidades para el manejo de incidentes de ciberseguridad y procesos de autenticación;

Que, para recoger las opiniones del público, se dispone la prepublicación del proyecto de resolución sobre la materia en el portal electrónico de la Superintendencia, al amparo de lo dispuesto en el Decreto Supremo Nº 001-2009-JUS;

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

PREPUBLICACIÓN

Con el visto bueno de las Superintendencias Adjuntas de Banca y Microfinanzas, de Administradoras Privadas de Fondos de Pensiones, de Seguros, de Riesgos, de Conducta de Mercado e Inclusión Financiera y de Asesoría Jurídica; y,

En uso de las atribuciones conferidas por los numerales 7 y 9 del artículo 349 de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley N° 26702 y sus modificatorias, y el inciso d) del artículo 57 de la Ley del Sistema Privado de Administración de Fondos de Pensiones, cuyo Texto Único Ordenado es aprobado por Decreto Supremo N° 054-97-EF;

RESUELVE:

Artículo Primero.- Aprobar el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, según se indica a continuación:

REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Alcance

1.1. El presente Reglamento es de aplicación a las empresas señaladas en los artículos 16 y 17 de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas, al igual que las referidas en los párrafos 1.2 y 1.3.

1.2. También es de aplicación al Banco de la Nación, al Banco Agropecuario, a la Corporación Financiera de Desarrollo (COFIDE), al Fondo MIVIVIENDA S.A., y a las Derramas y Cajas de Beneficios bajo control de la Superintendencia, en tanto no se contrapongan con las normativas específicas que regulen el accionar de dichas instituciones.

1.3. Es de aplicación a las empresas corredoras de seguros de acuerdo con lo dispuesto en la Quinta Disposición Complementaria Final del presente Reglamento.

Artículo 2. Definiciones

Para efectos de la aplicación del presente Reglamento deben considerarse las siguientes definiciones:

a) **Activo de información**: Información o recurso que lo soporta, definido y gestionado como una sola unidad de acuerdo con las necesidades de negocios y los requerimientos legales, de manera que pueda ser entendida, compartida y usada eficazmente. Es de valor para la empresa, tiene vulnerabilidades asociadas y un ciclo de vida.

b) **Amenaza**: Evento que puede afectar adversamente la operación de las empresas y sus activos de información, mediante el aprovechamiento de una vulnerabilidad.

c) **Autenticación**: Para fines de esta norma, es el conjunto de políticas, procesos y procedimientos, que permiten verificar de manera digital que una entidad sea quien dice ser, para lo cual hace uso de las credenciales y los factores de autenticación. La autenticación puede usar uno, dos o más factores de autenticación independientes, tal que, en términos de la tecnología utilizada, el acceso sin autorización a uno de ellos no compromete la fiabilidad de los otros factores.

d) **Canal digital**: Medio empleado por las empresas para proveer servicios en línea, como internet, teléfonos móviles, cajeros automáticos, terminales de puntos de atención, y otros cuyo almacenamiento, procesamiento y transmisión se realiza mediante la representación de datos en bits.
e) **Ciberseguridad**: Conjunto de políticas, procesos, procedimientos y recursos utilizados por la organización para proteger los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes en el ciberespacio; el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.
f) **Credencial**: Conjunto de datos que es generado y asignado a una entidad para fines de autenticación.
g) **Directorio**: Directorio u órgano equivalente.
h) **Entidad**: Elemento que tiene una identidad en un sistema, lo cual la hace separada y distinta de cualquier otra en dicho sistema. .
i) **Evento**: Un suceso o serie de sucesos que puede ser interno o externo a la empresa, originado por la misma causa, que ocurre durante el mismo periodo de tiempo, según lo definido en el Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos vigente.
j) **Factores de autenticación**: Aquellos factores empleados para verificar la identidad de una entidad, que pueden consistir en:
   - Algo que solo la entidad conoce, y sobre lo cual la empresa ha establecido medidas para asegurar su confidencialidad y evitar su divulgación a terceros no autorizados.
   - Algo que solo la entidad posee, y sobre lo cual la empresa ha establecido medidas para evitar su replicación y uso por terceros no autorizados.
   - Algo que la entidad es, y sobre lo cual la empresa ha establecido medidas para evitar su revelación y uso por terceros no autorizados, así como para asegurar una muy baja probabilidad de que un tercero no autorizado sea autenticado.

   Su uso puede reforzarse con la adopción de otros factores relacionados a algo que la entidad regularmente realiza, como el patrón de comportamiento o de ubicación de una entidad.
k) **Identidad**: Una colección de atributos que definen de forma exclusiva a una persona o entidad.
l) **Incidente:** Evento que se ha determinado que tiene un impacto sobre la organización y que requiere de acciones de respuesta y recuperación.
m) **Información**: Datos que pueden ser procesados, distribuidos y almacenados, y representados en cualquier medio electrónico, digital, óptico, magnético u otros, que son el elemento fundamental de los activos de información.
n) **Servicios en nube**: Infraestructura tecnológica que permite el acceso de red ubicuo, a conveniencia y bajo demanda, a un conjunto compartido de recursos informáticos configurables que se pueden habilitar y suministrar rápidamente, con mínimo esfuerzo de gestión o interacción con los proveedores de servicios.
o) **Reglamento**: Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.
p) **Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos:** Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado por la Resolución SBS Nº 272-2017.
q) **Superintendencia**: Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.
r) **Vulnerabilidad**: Debilidad que expone a los activos de información ante amenazas que pueden originar incidentes con afectación a los mismos activos de información, y a otros de los que forma parte o con los que interactúa.

Artículo 3. Sistema de gestión de seguridad de la información y Ciberseguridad (SGSI-C)
3.1. El sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) es el conjunto de políticas, procesos, procedimientos, roles y responsabilidades, diseñados para identificar y proteger los activos de información, así como detectar y responder ante eventos de seguridad y ciberseguridad.

3.2. El sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) implica, cuando menos, los siguientes objetivos:

a) Confidencialidad: La información sólo es disponible para entidades o procesos autorizados; incluyendo las medidas para proteger la información personal y la información propietaria;
b) Disponibilidad: Asegurar acceso y uso oportuno a la información; e,
c) Integridad: Asegurar el no repudio de la información y su autenticidad, y evitar su uso inapropiado, modificación o destrucción, así como que esta sea precisa y completa.

Artículo 4. Proporcionalidad del sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C)
4.1. El sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) de la empresa debe ser proporcional al tamaño, la naturaleza y la complejidad de sus operaciones.

4.2. Las disposiciones descritas en el Capítulo II, Subcapítulos I, II, III y IV del presente Reglamento son de aplicación obligatoria a las siguientes empresas (Régimen General):

a) Empresa Bancaria;
b) Empresa Financiera;
c) Caja Municipal de Ahorro y Crédito - CMAC;
d) Caja Municipal de Crédito Popular - CMCP;
e) Caja Rural de Ahorro y Crédito - CRAC;
f) Empresa de Seguros y/o Reaseguros;
g) Empresa de Transporte, Custodia y Administración de Numerario;
h) Administradora Privada de Fondos de Pensiones;
i) Empresa Emisora de Tarjetas de Crédito y/o de Débito;
j) Empresa Emisora de Dinero Electrónico; y
k) El Banco de la Nación.

4.3. Las disposiciones descritas en el Capítulo II, Subcapítulo V del presente Reglamento son de aplicación obligatoria a las siguientes empresas (Régimen Simplificado):

a) Banco de Inversión;
b) Entidad de Desarrollo a la Pequeña y Micro Empresa – EDPYME;
c) Empresa de Transferencia de Fondos;
d) Derrama y Caja de Beneficios bajo control de la Superintendencia;
e) La Corporación Financiera de Desarrollo –COFIDE;
f) El Fondo MIVIVIENDA S.A.;
g) El Fondo de Garantía para Préstamos a la Pequeña Industria –FOGAPI; y,
h) El Banco Agropecuario.

4.4. Las empresas señaladas en el Artículo 1, no listadas en los párrafos 4.2 o 4.3 anteriores del presente Reglamento, podrán establecer un sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) conforme a las disposiciones de este Reglamento.

4.5. Las disposiciones descritas en el Capítulo II, Subcapítulo VI (Régimen Reforzado) del presente Reglamento son de aplicación obligatoria a las empresas sujetas a un requerimiento de

patrimonio efectivo por riesgo de concentración de mercado, de acuerdo con lo señalado en el Reglamento para el requerimiento de patrimonio efectivo adicional. Asimismo, la Superintendencia puede incluir a otras empresas cuando la complejidad de sus operaciones o los riesgos en ciberseguridad ameriten mayor control.

Artículo 5. Responsabilidades del directorio

El directorio es responsable de aprobar y facilitar las acciones requeridas para contar con un SGSI-C apropiado a las necesidades de la empresa y su perfil de riesgo, entre ellas:

a) Aprobar las principales políticas y lineamientos para la implementación del SGSI-C y su mejora continua.
b) Asignar los recursos técnicos, de personal, financieros requeridos para su implementación y adecuado funcionamiento.
c) Aprobar la organización, roles y responsabilidades para el SGSI-C, incluyendo las medidas de difusión y capacitación periódica que contribuyan a un mejor conocimiento de los riesgos involucrados.

Artículo 6. Responsabilidades de la gerencia

6.1 La gerencia general es responsable de tomar las medidas necesarias para implementar el SGSI-C de acuerdo a las disposiciones del directorio y lo dispuesto en este Reglamento, proveer los recursos necesarios y una organización para cumplir con sus responsabilidades.

6.2 Los gerentes de las unidades de negocios y de apoyo son responsables de apoyar el buen funcionamiento del SGSI-C y gestionar los riesgos asociados a la seguridad de la información y Ciberseguridad en el marco de sus funciones.

Artículo 7. Funciones del comité de riesgos

7.1. Adicionalmente a las funciones que se han dispuesto que el Comité de Riesgos de las empresas asuman por parte de la normativa de la Superintendencia, se encuentran las siguientes vinculadas a la seguridad de la información y ciberseguridad:
   a) Aprobar el plan estratégico del SGSI-C y recomendar acciones a seguir.
   b) Aprobar el plan de capacitación a fin de garantizar que el personal, la plana gerencial y el directorio cuenten con competencias necesarias en seguridad de la información y Ciberseguridad.
   c) Fomentar la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención.

7.2. Para el cumplimiento de las funciones indicadas en el párrafo 7.1, la empresa puede constituir un Comité Especializado en Seguridad de la Información y Ciberseguridad (CSIC). El CSIC se debe encontrar conformado por al menos tres (3) miembros, uno de los cuales debe ser un miembro del directorio que no desempeñe cargo ejecutivo en la empresa, quien lo preside. Asimismo, también deben ser miembros de este Comité el Jefe de la Unidad de Riesgos, el Jefe de la Unidad de Tecnología de la Información y quien desempeñe la Función de Seguridad de Información y Ciberseguridad. Asimismo, el CSIC se rige por las disposiciones sobre comités del directorio del Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos. En caso de no existir un Comité de Riesgos o un CSIC, las funciones antes indicadas son asignadas al directorio.

Artículo 8. Función de Seguridad de Información y Ciberseguridad

8.1. Las empresas deben contar con una función independiente de seguridad de información y ciberseguridad respecto de las áreas de tecnología o sistemas de información, cuyo nivel y relación jerárquica será definido por el directorio a propuesta del Comité de Riesgos, con excepción de las empresas incluidas en el Régimen simplificado del Reglamento, establecido en el Artículo 4 del presente Reglamento. Son responsabilidades de la función de seguridad de la información y ciberseguridad:

1. Proponer el Plan estratégico del SGSI-C y desarrollar los planes operativos.
2. Implementar y manejar las operaciones diarias necesarias para el funcionamiento efectivo del SGSI-C.
3. Implementar procesos de autenticación para controlar el acceso a la información y sistema que utilice la empresa, y a los servicios que provea.
4. Informar al Comité de Riesgos periódicamente sobre los riesgos que enfrenta la empresa en materia de seguridad de información y Ciberseguridad.
5. Informar sobre los incidentes de seguridad al Comité de Riesgos o CSIC, según los lineamientos que este establezca, y a las entidades gubernamentales que lo requieran de acuerdo con la normativa vigente
6. Evaluar las amenazas de seguridad en las estrategias de continuidad del negocio que la empresa defina y proponer medidas de mitigación de riesgos, así como informar al Comité de Riesgos o CSIC.
7. En general realizar lo necesario para dar debido cumplimiento a lo dispuesto en el presente Reglamento.

8.2. La empresa debe contar con un equipo de trabajo de manejo de incidentes de Ciberseguridad, el cual debe implementar el plan y los procedimientos para gestionarlos, conformado por representantes de las áreas que permitan prever en ellos los aspectos legales, técnicos y organizacionales, de forma consistente con los requerimientos del programa de ciberseguridad establecidos en este Reglamento.

Artículo 9. Información a la Superintendencia

Como parte de los informes periódicos sobre gestión del riesgo operacional requeridos por el Reglamento para la Gestión del Riesgo Operacional, emitido por la Superintendencia, las empresas deben incluir información sobre la gestión de la seguridad de la información.

CAPÍTULO II
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD (SGSI-C)

SUBCAPÍTULO I
REGIMEN GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN y CIBERSEGURIDAD (SGSI-C)

Artículo 10. Objetivos y requerimientos del SGSI-C

Son objetivos del SGSI-C los siguientes:

1. Identificar los activos de información, analizar las amenazas y vulnerabilidades asociadas a estos, y formular programas y medidas que busquen reducir la posibilidad de incidentes en los siguientes aspectos:

a) El diseño de nuevos productos y procesos, cambios operativos y asociados a transformación digital.
b) Las relaciones con terceros, en el sentido más amplio, incluyendo proveedores de servicios, empresas con las que se tiene relaciones de subcontratación y en general toda relación con terceros.
c) Los proyectos nuevos o en curso.
d) Las obligaciones de seguridad de la información que se derivan de disposiciones legales, regulatorias, normas internas y de acuerdos contractuales.
e) Toda actividad que exponga sus activos de información por causa interna o externa.

2. Monitorear el alcance y la efectividad de los controles internos, y contar con capacidades de detección, respuesta y recuperación ante incidentes sobre los activos de información de la empresa.

3. Establecer la relación existente con los planes de emergencia, crisis y de continuidad establecidos según lo previsto en la normativa correspondiente.

Artículo 11. Alcance del SGSI-C
El alcance del SGSI-C debe incluir las funciones y unidades organizacionales, las ubicaciones físicas existentes, la infraestructura tecnológica y de comunicaciones, así como el perímetro de control asociado a las relaciones con terceros, que estén bajo responsabilidad de la empresa, conforme a las disposiciones establecidas sobre subcontratación en el Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos.

Artículo 12. Medidas mínimas de seguridad de la información a adoptar por las empresas
Las empresas deben adoptar las siguientes medidas mínimas de seguridad de información:

1. Controles de acceso físico y lógico:
   a) Implementar protocolos de seguridad de la información aplicables en el reclutamiento e incorporación del personal, ante cambio de puesto y terminación del vínculo laboral.
   b) Prevenir el acceso no autorizado a la información, así como a los sistemas, equipos e instalaciones mediantes los cuales es procesada, transmitida o almacenada, sea de manera presencial o remota.
   c) Implementar procesos de autenticación para controlar el acceso a los activos de información; y en particular, para el acceso a los servicios provistos a usuarios por canales digitales, los procesos de autenticación deben cumplir los requisitos establecidos en el Subcapítulo III del presente Reglamento.
   d) Prevenir la pérdida, el daño, el robo o el compromiso de los activos de información y la interrupción de las operaciones de la empresa.
   e) Utilizar criptografía para el almacenamiento y transmisión de datos, en función a la evaluación de amenazas de conocimiento público en el ámbito técnico.
   f) Revisar periódicamente las políticas de control de accesos existentes y monitorear su efectividad.

2. Seguridad en las operaciones:
   a) Asegurar y prever el funcionamiento continuo de las instalaciones de procesamiento, almacenamiento y transmisión de información.

b) Mantener la operación de los sistemas informáticos acorde a procedimientos previamente establecidos.
c) Controlar los cambios en el ambiente operativo de sistemas, y mantener segregado el ambiente productivo.
d) Restringir la instalación de software en los sistemas operativos; prevenir la explotación de las vulnerabilidades de seguridad de la información; y minimizar el impacto de las actividades de auditoría en los sistemas operacionales.
e) Contar con protocolos de respuesta y recuperación ente eventos de malware; habilitar y probar copias de respaldo de información, software y elementos que faciliten su restablecimiento.
f) Monitorear las operaciones de la infraestructura tecnológica, para lo cual debe contar con registros de auditoría de la actividad de usuarios, operadores y administradores de sistemas, así como registros de errores e incidentes.

3. Seguridad en las comunicaciones:
   a) Implementar y mantener la seguridad de redes de comunicaciones acorde a la información que por ella se trasmite y las amenazas a las que se encuentra expuesta.
   b) Asegurar que las redes de comunicaciones y servicios de red son gestionados y controlados para proteger la información.
   c) Segregar los servicios de información disponibles, usuarios y sistemas en las redes de la empresa.
   d) Implementar protocolos seguros y controles de seguridad para la transferencia de información, desde y hasta redes internas o externas.
   e) Asegurar que el acceso remoto, y que la interconexión que se utilice a través de redes propias y de terceros cuenta con controles acorde a las amenazas de seguridad existentes.
   f) Monitorear y revisar regularmente la efectividad y funcionamiento de los controles de seguridad de redes.

4. Adquisición, desarrollo y mantenimiento de sistemas:
   a) Implementar y mantener la seguridad en los servicios y sistemas informáticos acorde a la información que se procese y amenazas a las que se encuentren expuestos.
   b) Asegurar que se incluyan prácticas de seguridad de la información en la planificación, desarrollo, implementación, operación, soporte y desactivación en los servicios y sistemas informáticos.
   c) Asegurar que se incluyan prácticas de pruebas funcionales en los servicios y sistemas informáticos, así como aquellas que permitan validar la seguridad de estos.
   d) Implementar y verificar el cumplimiento de procedimientos que incluyan prácticas de desarrollo seguro de servicios y sistemas informáticos.
   e) Implementar controles que aseguren la integridad de las transacciones que son ejecutadas en los servicios y sistemas informáticos.
   f) Monitorear y revisar regularmente la efectiva aplicación de prácticas seguras en la adquisición, desarrollo y mantenimiento de servicios y sistemas informáticos.

5. Servicios provistos por terceros:
   a) Evaluar las amenazas y vulnerabilidades de seguridad de la información en la provisión de bienes y servicios, o en la relación con terceros, según sea aplicable.
   b) Establecer requerimientos de seguridad de la información consistentes con las políticas del SGSI-C, cuando corresponda, incorporándolos en los acuerdos suscritos.

c) Establecer los roles y responsabilidades sobre seguridad de la información con los proveedores, según sea aplicable.
d) Monitorear la provisión de servicios de terceros, y evaluar los riesgos que afectan la seguridad de la información ante eventuales cambios, según corresponda.
e) Contar con una estrategia de salida de los servicios a cargo del proveedor, de forma que la información de la empresa pueda ser migrada a un proveedor distinto o a las instalaciones y recursos de la empresa.
f) Asegurar que la información en custodia del proveedor puede ser eliminada definitivamente ante la resolución del acuerdo contractual.
g) Cuando se trate de la provisión del servicio de procesamiento de datos, debe cumplir adicionalmente los requerimientos establecidos en el Subcapítulo IV del presente Reglamento.

6. Gestión de incidentes de seguridad de la información:
   a) Implementar procedimientos para la gestión de incidentes de seguridad la información, y cuando se trate de incidentes en el ciberespacio, estos procedimientos deben incluir las responsabilidades del equipo de manejo de incidentes de ciberseguridad, de acuerdo a lo señalado en numeral 8.1 del Artículo 8 del presente Reglamento; así también, intercambiar información cuando corresponda, conforme al Artículo 17 del presente Reglamento.
   b) Implementar una metodología para clasificar eventos, incidentes de seguridad de la información y de ciberseguridad.
   c) Implementar mecanismos de reporte interno de incidentes de acuerdo con lo señalado en el Artículo 8 del presente Reglamento, y a la Superintendencia conforme al Artículo 16 del presente Reglamento.
   d) Identificar las posibles limitaciones y mejoras en la gestión de incidentes de seguridad de la información luego de la ocurrencia de estos.
   e) Mantener información que permita realizar las investigaciones forenses.

Artículo 13. Actividades planificadas
En el marco del Plan estratégico del SGSI-C, la empresa debe mantener planes operativos, por lo menos para los siguientes fines:

a) Identificar los activos de información, analizar las amenazas y vulnerabilidades asociadas a estos, y tomar medidas para reducir la posibilidad de incidentes.
b) Someter el SGSI-C a evaluaciones, revisiones y pruebas periódicas para determinar su efectividad, mediante servicios internos y externos, y en función al nivel de complejidad y amenazas sobre los activos de información asociados. En función a los resultados que obtenga, debe incorporar las mejoras o adoptar los correctivos.
c) Atender las necesidades de capacitación y difusión, según corresponda a los roles y funciones en la organización, en materia de seguridad de la información y ciberseguridad para asegurar la efectividad del SGSI-C.
d) Desarrollar el programa de ciberseguridad, según sea aplicable el Subcapítulo IV.

SUBCAPÍTULO II
CIBERSEGURIDAD

Artículo 14. Programa de ciberseguridad

14.1. Toda empresa que cuente con presencia en el ciberespacio debe contar con un programa específico de gestión de incidentes de ciberseguridad (PG-C), aplicable a las operaciones, procesos y otros activos de información asociados.

14.2. El PG-C debe prever un diagnóstico de las capacidades para gestionar un incidente, respecto a un marco de referencia internacional de ciberseguridad, que evalúe por lo menos las siguientes funciones:

a) Identificación de los activos de información.
b) Protección frente a las amenazas a los activos de información.
c) Detección de la ocurrencia de incidentes.
d) Respuesta con medidas que reduzcan el impacto de los incidentes.
e) Recuperación de las actividades de negocio, y capacidades o servicios afectados.

Artículo 15. Reporte de incidentes de ciberseguridad

15.1 La empresa debe reportar a la Superintendencia, en cuanto advierta, la ocurrencia de un incidente de ciberseguridad que tenga un efecto verificado o presumible de:

a) Pérdida o hurto de información de la empresa o de clientes.
b) Fraude internos o externos.
c) Impacto negativo en la imagen y reputación de la empresa.
d) Interrupción de operaciones.

15.2 La Superintendencia, mediante norma de carácter general, establece el contenido mínimo, formato y protocolos adicionales a utilizar en dicho reporte.

Artículo 16. Intercambio de información de ciberseguridad

16.1 La empresa debe procurar contar con información que le permita tomar acción oportuna frente a las amenazas de ciberseguridad y para el tratamiento de las vulnerabilidades.

16.2 Al intercambiar información relativa a ciberseguridad, la empresa debe suscribir acuerdos con otras empresas del sector o con terceros que resulten relevantes, de forma bipartita, grupal o gremial. El intercambio debe realizarse acorde a criterios previamente establecidos para mantener la confidencialidad de la información y reducir el contenido mínimo necesario, sin que con ello se pierda la utilidad de la información para tomar las acciones preventivas o reactivas.

16.3 Mediante norma de carácter general, la Superintendencia podrá establecer requerimientos específicos para que se incorporen en el intercambio de información de ciberseguridad.

SUBCAPÍTULO III
AUTENTICACIÓN

Artículo 17. Implementación de los procesos autenticación

17.1 La empresa debe implementar procesos de autenticación, conforme a la definición establecida en este Reglamento, para controlar el acceso a los servicios que provea a sus usuarios por canales digitales, previo a lo cual debe evaluar formalmente y tomar medidas sobre:

a) La combinación de factores de autenticación que serán admitidos.
b) Requerimientos criptográficos aceptados, basados en software o en hardware, y sus prestaciones de confidencialidad o integridad esperadas.
c) Plazos y condiciones en las que será obligatorio requerir a la entidad volver a autenticarse, lo que incluye y no se limita a casos por periodo de inactividad o sesiones de uso prolongado de sistemas.
d) Línea base de controles de seguridad de la información requerida, lo que incluye, y no se restringe, al número límite de intentos de autenticación, la prevención de ataques de interceptación y manipulación de mensajes, reproducción de mensajes de autenticación y suplantación.
e) Lineamientos para la retención de registros de auditoría para la detección de amenazas conocidas y eventos de seguridad de la información.

17.2 Los procesos de autenticación deben ser reevaluados siempre que se presenten cambios en la tecnología que los soportan, o tras el descubrimiento de nuevas vulnerabilidades que pueda afectarlos.

17.3 La empresa debe mantener y proteger los registros detallados de lo actuado en cada habilitación y uso del proceso de autenticación, incluyendo información de identificación, credencial asignada, así como los datos de cada operación y los intentos de autenticación.

17.4 La empresa debe contar con los registros de auditoría, herramientas y procedimientos para detectar y remediar los intentos de uso no autorizado de credenciales; así también, implementar el monitoreo de transacciones que permita tomar medidas de reducción de posibilidad de operaciones fraudulentas, que incorpore los escenarios de fraude ya conocidos, y el robo o compromiso de los elementos utilizados para la autenticación.

Artículo 18. Inscripción y gestión de credenciales

Para la habilitación de la autenticación de una entidad para el acceso a servicios provistos por canal digital, la empresa debe:

a) Recabar la información necesaria para determinar la validez de la identidad de la entidad y corroborarla con un registro de identificación reconocido por el marco legal vigente, o un repositorio bajo responsabilidad de la empresa. Cuando corresponda debe cumplir con los requisitos de debida diligencia en el conocimiento del cliente, establecidos en el Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo.
b) Para reducir la posibilidad de suplantación de identidad cuando se efectúe lo requerido en el literal anterior por canal digital, la verificación de identidad deberá requerir del uso de dos factores de autenticación, donde por lo menos uno de los cuales debe ser biométrico.
c) Emitir y asignar una credencial a una entidad para la validación de su identificación; además de su emisión, prever procedimientos para su suspensión, reemplazo, renovación y revocación, así también asegurar en todo momento su confidencialidad e integridad.

Artículo 19. Autenticación reforzada para operaciones por canal digital

Para aquellas operaciones que se realicen a través de un canal digital que implique una transferencia de fondos, un pago, la solicitud de un trámite o la contratación de un producto o servicio, modificación de los límites y condiciones en los que se proveen los servicios, y otros que pueden originar una operación fraudulenta u otro abuso en perjuicio del cliente, debe requerirse una autenticación reforzada, que debe contar por lo menos con lo siguiente:

a) Utilizar dos o más factores de autenticación, de los cuales por lo menos dos no podrán ser de ubicación o comportamiento.
b) Lo indicado en el literal a) debe resultar en la generación de un código de autenticación, mediante métodos criptográficos, a partir de los datos específicos de cada operación.
c) Dicho código de autenticación debe utilizarse por única vez para realizar la operación para la que fue generada, no podrá derivarse de él alguno de los factores de autenticación, algún dato de la operación u otro código de autenticación posterior. Su uso y transmisión debe realizarse con controles para prevenir su captura y manipulación no autorizadas, así como el límite a intentos fallidos en el proceso de autenticación.

Artículo 20. Exenciones de autenticación reforzada para operaciones por canal digital
Están exentas del requisito de autenticación reforzada indicado en el artículo 19 del presente Reglamento, las siguientes operaciones realizadas por canal digital:

a) La consulta de información de estados de cuenta, saldos de cuenta, historial de operaciones y movimientos de cuentas; salvo que sea efectuado por primera vez o luego de un periodo sin uso, según lo definido por la empresa.
b) Las operaciones de pago, pagos periódicos o transferencia hacia un beneficiario registrado previamente por el cliente como beneficiario de confianza, de acuerdo con las condiciones de su autorización, salvo a partir de que el cliente excluya a un anterior beneficiario de confianza o modifique las condiciones del pago periódico.
c) Las operaciones de micropago conforme se define en la regulación vigente sobre tarjetas de crédito y débito.

SUBCAPÍTULO IV
PROVISIÓN DE SERVICIOS DE PROCESAMIENTO DE DATOS

Artículo 21. Provisión de servicios de procesamiento de datos a las empresas
Los requisitos establecidos en el numeral 5 del artículo 12 son de aplicación a la provisión de servicios de procesamientos de datos a las empresas. Además, cuando se trate de servicios en nube, es de aplicación también el artículo 22, y cuando sea procesamiento principal y provisto desde el exterior, es de aplicación también el artículo 23.

Artículo 22. Servicios de procesamiento de datos en nube
Las empresas que utilicen servicios de procesamiento de datos en nube deben:

a) Implementar procedimientos para la administración de operaciones y configuraciones del procesamiento en la nube, así como servicios de soporte ante casos de falla, indisponibilidad o incidentes de ciberseguridad.
b) Gestionar las amenazas y vulnerabilidades en el uso de interfaces de programación de aplicaciones (API, por sus siglas en inglés) y otros servicios similares suministrados por el proveedor de nube.
c) Contar con evidencia de que el proveedor de procesamiento mantiene vigente las certificaciones ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018 relevantes a la zona o región desde donde se provee el servicio.

Artículo 23. Autorización de provisión de procesamiento principal de datos en el exterior o en la nube

23.1 Cuando el procesamiento principal de datos se realice fuera del país o en la nube la empresa debe solicitar autorización previa de esta Superintendencia, de acuerdo a los requisitos señalados en el Anexo A del Reglamento.

23.2 La autorización que conceda esta Superintendencia es específica al proveedor del servicio y, al país y ciudad desde el que se recibe, así como a las condiciones generales que fueron objeto de la autorización, por lo que de existir modificaciones en ellas, se requiere de un nuevo procedimiento de autorización ante la Superintendencia.

23.3 Los servicios de procesamiento principal de datos o en la nube autorizados a ser provistos desde el exterior deben ser sometidos anualmente a un examen de auditoría independiente, realizado por una sociedad auditora externa o una firma nacional o extranjera, que acredite contar con el conocimiento y experiencia requerida, debiendo remitir a ésta Superintendencia el reporte SOC 2 tipo 2 resultante de una evaluación realizada conforme a las secciones AT-C 105 y AT-C 205 del estándar de auditoría SSAE 18, emitidos por el Instituto Americano de Contadores Públicos Certificados (AICPA), o el ISAE 3000, emitido por el Consejo de Normas Internacionales de Auditoría y Aseguramiento (IAASB). El alcance periodo del servicio es de doce meses, a cubrir con reportes de por lo menos 6 meses.

SUBCAPÍTULO V
RÉGIMEN SIMPLIFICADO DEL SGSI-C

Artículo 24. Sistema simplificado de gestión de seguridad de la información

24.1 El SGSI-C es responsabilidad de directorio que, para la implementación del régimen simplificado de gestión de seguridad de la información, debe:

a) Aprobar las políticas y lineamientos.
b) Asignar los recursos técnicos, de personal y financieros requeridos para su implementación y adecuado funcionamiento.
c) Aprobar la organización, roles y responsabilidades para las medidas de difusión y capacitación periódica.

24.2 El régimen simplificado de gestión de seguridad de la información requiere la planificación y ejecución de las siguientes actividades, acorde a una periodicidad definida por el directorio, que por lo menos debe ser anual:

a) Identificar con las unidades de negocio y de apoyo, cuál es la información de mayor importancia, por las obligaciones legales, regulatorias o contractuales existentes, y por la necesidad de operar.
b) Identificar los dispositivos que se conectan a la red interna y todo software que se encuentre instalado en la infraestructura.
c) Identificar las cuentas de usuario y en particular las que poseen privilegios alternativos con posibilidad de adicionar software a la infraestructura.
d) Priorizar y cerrar las brechas de seguridad identificadas mediante las acciones detalladas en el numeral previo.
e) Configurar e implementar una línea base de seguridad en sistemas operativos y aplicaciones utilizadas. Identificar y evaluar la habilitación de las funciones de seguridad integradas en los sistemas operativos.

f) Desarrollar una campaña de orientación para la adopción de prácticas seguras dirigida a los empleados, plana gerencial y de dirección.

24.3 En caso provea servicios a usuarios por canales digitales que implique una transferencia de fondos, un pago, la solicitud de un trámite o la contratación de un producto o servicio, modificación de los límites y condiciones en los que se proveen los servicios, y otros que pueden originar una operación fraudulenta u otro abuso en perjuicio del cliente, debe requerirse una autenticación reforzada, la empresa deberá implementar las disposiciones establecidas en el Subcapítulo III del Capítulo II.

24.4 En caso utilice servicios significativos provistos por terceros, la empresa debe implementar las disposiciones establecidas en el numeral 5 del artículo 12 y, cuando se trate del procesamiento de datos, las indicadas en el Subcapítulo IV del Capítulo II.

24.5 La empresa debe mantener un programa de ciberseguridad, conforme al Subcapítulo II del Capítulo II, con un alcance que por lo menos incluya los servicios indicados en los párrafos 24.3 y 24.4. del presente artículo.

SUBCAPÍTULO VI
DISPOSICIONES ADICIONALES APLICABLES A EMPRESAS CON CONCENTRACIÓN DE MERCADO

Artículo 25. Requerimientos adicionales para empresa con concentración de mercado

25.1 El directorio debe designar a un director como responsable de velar por la efectividad del sistema de gestión de seguridad de la información, lo que incluye el desarrollo del plan estratégico del SGSI-C.

25.2 La empresa debe someter periódicamente una evaluación independiente el alcance y efectividad del SGSI-C.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- La empresa puede contar con un marco especializado para la gestión de los riesgos asociados a la seguridad de la información, que deber ser integrado en lo que corresponda en la gestión del riesgo operacional, conforme a los lineamientos establecidos en el Artículo 22° del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos.

Segunda.- Los informes a los que se refieren los literales g) y h) del Artículo 12°, y el artículo 27° del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos deben incluir la evaluación de los riesgos asociados a la seguridad de la información.

Tercera- En caso de eventos que afecten la continuidad operativa y que tengan como causa probable un incidente de ciberseguridad, es aplicable lo señalado en el Artículo 15 del Reglamento para la Gestión de la Continuidad del Negocio, sobre Reporte de Eventos de Interrupción significativa.

Cuarta.- Sin perjuicio de lo señalado en el Artículo 4 del presente Reglamento, la Superintendencia puede disponer el cambio de régimen, del sistema de gestión de seguridad de la información y la ciberseguridad, que una empresa debe cumplir.

Quinta.- La aplicación del presente Reglamento se extiende a las empresas corredoras de seguros del segmento 1, según segmentación establecida en el artículo 36 del Reglamento para la Supervisión y Control de los Corredores y Auxiliares de Seguros aprobado por la Resolución SBS N° 809-2019, sobre la base de las siguientes consideraciones.

1. Se les aplica el Régimen Simplificado del Sistema de Gestión y Seguridad de la Información y Ciberseguridad con excepción de los párrafos 24.4 y 24.5 del artículo 24.
2. En el caso de los párrafos 24.1 y 24.2 del artículo 24, las empresas corredoras desarrollarán las actividades requeridas, de acuerdo al tamaño y volumen de sus operaciones.
3. En el caso del párrafo 24.3 del artículo 24, aplica solo cuando la empresa corredora desarrolle con alguna compañía de seguros, sistemas que involucren la contratación de seguros y pago.
4. Finalmente, dependiendo del nivel de riesgo al que se encuentre expuesta la empresa corredora en aspectos de seguridad de información o de ciberseguridad, la Superintendencia podrá realizar requerimientos adicionales señalados en el presente Reglamento.

Anexo 2: Política nacional de ciberseguridad

POLÍTICA NACIONAL DE CIBERSEGURIDAD

Objetivo

Proteger la infraestructura de información, los datos e información del Estado y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las propuestas legislativas, y en general la normatividad relacionada con la seguridad de la información o ciberseguridad comprendida en esta Política, identificando los recursos involucrados y las partidas presupuestales correspondientes.

Mantener la Política Nacional de Ciberseguridad actualizada, a efectos de asegurar su vigencia y por ende su eficacia, promoviendo la participación de las entidades de sector público y privado, así como representantes de la sociedad civil y la academia.

I. Alcance

La presente Política se aplica a todas las entidades de la Administración Pública a que hace referencia el Artículo I del Título Preliminar de la Ley N° 27444, así como a todos sus recursos y procesos sean estos internos o externos.

II. Referencias Internacionales

La presente Política cuenta con los siguientes marcos de referencia:

- Resolución Ministerial N° 246-2007-PCM, que aprueba la Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática, o la que haga sus veces.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática, o la que haga sus veces.
- Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.

III. Marco Normativo

- Constitución Política del Perú.
- Decreto Legislativo N° 604.
- Ley N° 29158: Ley Orgánica del Poder Ejecutivo.

- Ley Nº 27658: Ley Marco de Modernización de la Gestión del Estado.
- Ley Nº 27806: Ley Transparencia y Acceso a la Información Pública.
- Ley N° 27444: Ley de Procedimiento Administrativo General.
- Ley N° 27269: Ley de Firmas y Certificados Digitales.
- Ley N° 27291: Ley que modifica el código civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica.
- Ley N° 28493: Ley que regula el uso del Correo Electrónico comercial no solicitado (SPAM).
- Ley N° 29733: Ley de Protección de Datos Personales.
- Ley N° 28530: Ley de Promoción de Acceso a Internet para personas con discapacidad y adecuación del espacio físico en cabinas públicas de internet.
- Ley N° 29904: Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica.
- Ley N° 30096 y su modificatoria Ley 30171: Ley de Delitos Informáticos.
- Decreto Legislativo N° 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses.
- Decreto Supremo N° 022-2017-PCM, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.
- Decreto Supremo N° 066-2011-PCM: Aprueba el "Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0".
- Decreto Supremo N° 004-2013-PCM: Aprueba la Política Nacional de Modernización de la Gestión Pública.
- Decreto Supremo N° 081-2013-PCM: Aprueba la Política Nacional de Gobierno Electrónico 2013-2017.
- Resolución Ministerial N° 179-2004-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2004 Tecnología de la Información. "Procesos del Ciclo de Vida del Software, 1ª Edición" en entidades del Sistema Nacional de Informática.
- Resolución Ministerial N° 246-2007-PCM, que aprueba la Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 197-2011-PCM, que establece fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información".
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

- Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.

IV. Términos y Definiciones

a) Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

- *Confidencialidad*: Garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- *Integridad*: Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.
- *Disponibilidad*: Garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deben considerarse los conceptos de:

- *Autenticidad*: Asegurar que la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- *Auditabilidad*: Definir que todos los eventos de un sistema puedan ser registrados para su control posterior.
- *Protección a la duplicación*: Asegurar que una transacción sólo se realice una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- *No repudio*: Evitar que una entidad que haya enviado o recibido información o intercambiado datos, alegue ante terceros que no los envió o no los recibió.
- *Legalidad*: Cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- *Confiabilidad de la Información*: Que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

- *Información*: Toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- *Sistema de Información*: Conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- *Tecnología de la Información*: Hardware y software operados por la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
- *Propietario de la Información*: Persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.

b) Evaluación de Riesgos

Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma; la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

c) Tratamiento de Riesgos

Proceso de selección e implementación de medidas para modificar el riesgo.

d) Gestión de Riesgos

Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo.

NOTA. La gestión de riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

e) Comité de Seguridad de la Información

Colegiado integrado por representantes de todas las áreas sustantivas de la entidad, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

f) Responsable de Seguridad de la Información

Persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la entidad que así lo requieran.

g) Incidente de Seguridad

Evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de quebrar los mecanismos de seguridad existentes.

h) Riesgo

Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.

i) Amenaza

Causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

j) Vulnerabilidad

Debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

k) Control

Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal.

V. Política Nacional de Ciberseguridad

1. ***Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el de la ciberseguridad, creando un entorno y las condiciones necesarias que permitan brindar protección en el ciberespacio.***

   Para lograr este objetivo es necesario involucrar a todos los sectores y entidades del Estado con responsabilidad en el campo de ciberseguridad y ciberdefensa, creando un ambiente participativo en el que participen representantes del sector privado, sociedad y la academia, donde cada quien aporte y actúe a propósitos comunes, estrategias concertadas y esfuerzos coordinados. Asimismo, es de vital importancia crear conciencia y sensibilizar a la población respecto de la importancia de la seguridad de la información (ciberseguridad); así como, fortalecer los niveles de cooperación y colaboración internacional en aspectos de ciberseguridad y ciberdefensa; apoyar investigaciones relacionadas con ataques informáticos y proteger a la ciudadanía de las consecuencias de estos ataques.

2. ***Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en materia de ciberseguridad dentro de la Administración Pública.***

   Este objetivo permitirá generar y fortalecer las capacidades existentes en materia de seguridad cibernética, con el propósito de afrontar las amenazas que atentan contra los propósitos planteados.

   Inicialmente, se capacitará a los funcionarios y servidores que estén directamente involucrados en la atención y manejo de incidentes cibernéticos. Gradualmente se extenderá esta capacitación a las demás entidades del Estado. Entre los planes de capacitación, el Pe-CERT con el apoyo del Comité Interamericano Contra el Terrorismo (CICTE) de la OEA, entre otros, elaborará un Plan de Capacitación para los demás funcionarios y servidores del Estado, así como programas de sensibilización y concienciación para los ciudadanos en general. De la misma forma, el Ministerio del Interior (MININTER) buscará la implementación gradual de asignaturas en seguridad de la información, ciberseguridad y ciberdefensa (teórico-prácticas) en las escuelas de formación y de capacitación de oficiales y suboficiales.

3. ***Desarrollar un Plan de sensibilización y capacitación a todos los ciudadanos respecto a la Ciberseguridad.***

   Se busca que la sociedad civil tome consciencia sobre la ciber-seguridad, identificar posibles vulnerabilidades o amenazas y tomar acciones oportunas para su seguridad.

   El Plan contará con una Estrategia de difusión que incluya la organización de conferencias para instituciones educativas (de nivel primario a universitario), y tareas de divulgación entre ciudadanos y otras entidades públicas y privadas del país.

   Así mismo, se realizarán foros que permitan intercambiar opiniones y experiencias entre todas las entidades públicas y privadas, sociedad civil y academia, con el objeto de compartir las mejores prácticas en Ciberseguridad y Ciberdefensa.

   Parte de la sensibilización en temas de Seguridad de la Información, radica en socializar la Normatividad vigente, como la Ley N° 27933 de Protección de Datos Personales, que ampara a todos los ciudadanos y la Ley N° 30096 modificada por la Ley N° 30171 – Ley de Delitos Informáticos, entre otros.

4. ***Fortalecer la legislación en materia de ciberseguridad, la cooperación internacional y propiciar la adhesión del Perú a los diferentes organismos internacionales en esta temática.***

   Este objetivo busca desarrollar las herramientas jurídicas necesarias para una efectiva y eficiente prevención, investigación y judicialización de los delitos informáticos.

   Así, se propenderá por la expedición de la normatividad necesaria para dar cumplimiento a los tratados internacionales sobre ciberseguridad, ciberdelincuencia, en la medida que hagan parte del bloque de constitucionalidad, así como por la debida reglamentación de lo dispuesto en la legislación nacional. Las entidades responsables de la ciberseguridad y ciberdefensa deberán buscar y evaluar la participación en diferentes redes y mecanismos internacionales de cooperación (Consejo de Europa, OEA y Forum Of Incident Response Security Teams - FIRST), que permitan preparar al país para afrontar los crecientes desafíos del entorno internacional en el área de ciber-seguridad, así como responder de una forma más eficiente a incidentes y delitos de seguridad cibernética.

   De manera especial el Perú deberá gestionar la adhesión al Convenio de Ciberdelincuencia suscrito en Budapest el 23 de noviembre del 2001, adhesión que permitirá combatir la ciber-delincuencia de manera coordinada y globalizada, lo cual a su vez, se orienta al cumplimiento del Compromiso al que se arribó en la Cumbre Mundial sobre Sociedad de la información en Túnez 2005, enmarcados dentro de los Objetivos de Desarrollo del Milenio, (ahora denominados Objetivos de Desarrollo Sostenible), que disponen incrementar la confianza y la seguridad en cuanto a la utilización de las Tecnologías de la Información y de la Comunicación (TIC), y a su vez, se encuentra dentro de los alcances de lo establecido en el Política Nacional de Gobierno Electrónico 2013-2017, aprobada mediante Decreto Supremo N° 081-2013-PCM , y en plena concordancia con la Ley de Delitos Informáticos aprobada mediante Ley N° 30096, modificada mediante Ley N° 30171.

5. ***Afianzar la integración y coordinación eficaz, entre las diversas Coordinadoras de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública y el sector privado.***

   Según lo establecido en la Resolución Ministerial N° 360-2009-PCM, se hace necesario que cada Ministerio o la que haga sus veces, coordine con el Pe-CERT, para hacer cumplir sus objetivos.

   Es importante que dicha coordinación se realice permanentemente y que la misma tenga un carácter de prioridad ante cualquier amenaza que vulnere la seguridad de la Nación.

6. **Elaborar un Plan de Acción Nacional en Ciberseguridad**

   Este Plan deberá realizarse de forma multisectorial y multidisciplinaria, entre representantes de las entidades del sector público, sector privado, sociedad y la academia.

7. **Crear el Comité Nacional de Ciberseguridad**

   Este Comité tendrá como parte de sus funciones, el velar por el fiel cumplimiento de las políticas y lineamientos que se establezcan respecto a la Ciberseguridad.

   El Comité está conformado por las siguientes entidades:

   1. Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno Digital (SEGDI)
   2. Poder Judicial
   3. Dirección Nacional de Inteligencia (DINI)
   4. Ministerio de Defensa (MINDEF)
   5. Ministerio del Interior (MININTER)
   6. Policía Nacional del Perú (PNP)
   7. Asociación de Gobiernos Regionales
   8. Sociedad Nacional de Industrias (SNI)
   9. Cámara de Comercio de Lima (CCL) (OBS)
   10. Cámara Nacional de Comercio, Producción, Turismo y Servicios – PERUCÁMARAS
   11. Colegio de Abogados de Lima (CAL)
   12. Colegio de Ingenieros del Perú (CIP)
   13. NAP (Network Access Point) Peru
   14. Confederación Nacional de Institucionales Empresariales Privadas (CONFIEP)
   15. Asociación de Bancos del Perú (ASBANC)
   16. Asociación para el Fomento de la Infraestructura Nacional (AFIN)
   17. Red Científica Peruana (RCP)
   18. Otros (Definir)

Anexo 3: Ley de ciberdefensa

2. La organización política determina los requisitos y el número de sus postulantes a candidatos de acuerdo con su normativa interna.
3. Los candidatos en las elecciones internas deben tener, al menos, seis (6) meses de afiliación a la organización política por la que deseen postular con anterioridad a la fecha de realización de las elecciones primarias.
4. Las elecciones internas solo admiten la participación de afiliados a la organización política.

Para continuar con su participación en el proceso electoral, la organización política debe obtener al menos el 1,5% de los votos válidamente emitidos en las elecciones primarias.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los cinco días del mes de agosto de dos mil diecinueve.

PEDRO C. OLAECHEA ÁLVAREZ CALDERÓN
Presidente del Congreso de la República

KARINA BETETA RUBÍN
Primera Vicepresidenta del Congreso de la República

AL SEÑOR PRESIDENTE DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiséis días del mes de agosto del año dos mil diecinueve.

MARTÍN ALBERTO VIZCARRA CORNEJO
Presidente de la República

SALVADOR DEL SOLAR LABARTHE
Presidente del Consejo de Ministros

1801519-4

LEY Nº 30999

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

LA COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY DE CIBERDEFENSA

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto
La presente ley tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley.

Artículo 2. Finalidad
Defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

Artículo 3. Ámbito de aplicación
El ámbito de aplicación de la norma se circunscribe a la ejecución de operaciones de ciberdefensa en y mediante el ciberespacio frente a las amenazas o los ataques que afecten la seguridad nacional.

Artículo 4. Definición
Entiéndase por ciberdefensa a la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional.

Artículo 5. Órganos ejecutores
Las Fuerzas Armadas, que están constituidas por el Ejército, la Marina de Guerra y la Fuerza Aérea, y el Comando Conjunto de las Fuerzas Armadas son instituciones con calidad de órganos ejecutores del Ministerio de Defensa.

TÍTULO II

DE LA CIBERDEFENSA

CAPÍTULO I

LAS CAPACIDADES DE CIBERDEFENSA Y LAS OPERACIONES EN Y MEDIANTE EL CIBERESPACIO

Artículo 6. De las capacidades de ciberdefensa
Es el uso de conocimiento, habilidades y medios para realizar operaciones en y mediante el ciberespacio a fin de asegurar su empleo por las fuerzas propias.

Artículo 7. De las operaciones militares en el ciberespacio
Es el eficiente y eficaz empleo de las capacidades de ciberdefensa por parte de los órganos ejecutores del Ministerio de Defensa, de acuerdo a sus funciones y en el ámbito de sus respectivas competencias, contra las amenazas o los ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

Artículo 8. De la planificación y ejecución de las operaciones en el ciberespacio
La planificación y ejecución de las operaciones de ciberdefensa a cargo del Comando Conjunto de las Fuerzas Armadas responde al mandato conferido en la Constitución Política del Perú, así como al cumplimiento de las responsabilidades asignadas en las leyes que regulan su naturaleza jurídica, competencias, funciones y estructura orgánica, las disposiciones contenidas en la presente ley, y los tratados y acuerdos internacionales de los que el Perú es parte y resulten aplicables.

CAPÍTULO II

DEL USO DE LA FUERZA EN Y MEDIANTE EL CIBERESPACIO

Artículo 9. Del uso de la fuerza por las Fuerzas Armadas
El uso de la fuerza por la Fuerzas Armadas en y mediante el ciberespacio se sujeta a las disposiciones contenidas en el artículo 51 de la Carta de las Naciones Unidas y el presente dispositivo legal, y está regido por las normas del Derecho Internacional de los Derechos Humanos y del Derecho Internacional Humanitario que sean aplicables.

Artículo 10. De la legítima defensa
Toda amenaza o ataque en y mediante el ciberespacio que ponga en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales, da lugar al ejercicio del derecho de legítima defensa.

Artículo 11. Requisitos para el ejercicio del uso de la fuerza
El ejercicio del derecho de legítima defensa en el contexto de las operaciones de ciberdefensa está sujeto a los principios de legalidad, necesidad y oportunidad.
En el caso de conducir una operación de respuesta en y mediante el ciberespacio que contenga un ataque deliberado, debe realizarse de acuerdo a ley.

CAPÍTULO III

DE LA SEGURIDAD DE LOS ACTIVOS CRÍTICOS NACIONALES Y RECURSOS CLAVES

Artículo 12. Del control y de la protección de los activos críticos nacionales y recursos claves
El Comando Conjunto de las Fuerzas Armadas está a cargo de la ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores y/o del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia sea sobrepasada, a fin de mantener las capacidades nacionales, en el ámbito de la seguridad nacional.

Artículo 13. De los protocolos de escalamiento, coordinación, intercambio y activación
La Presidencia del Consejo de Ministros, en su calidad de miembro del Consejo de Seguridad y Defensa Nacional, establece los protocolos de escalamiento, coordinación, intercambio y activación para lo indicado en la presente ley.
Esta función se ejerce a través de la Secretaría de Gobierno Digital en su calidad de ente rector del Sistema Nacional de Informática y de la seguridad digital en el país, quien emite los lineamientos y las directivas correspondientes.

Artículo 14. Modificación del artículo 32 del Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital
Modifícase el artículo 32 del Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, el cual queda redactado de la siguiente manera:

"Artículo 32.- Gestión del Marco de Seguridad Digital del Estado Peruano
El Marco de Seguridad Digital del Estado Peruano tiene los siguientes ámbitos:

a. Defensa: El Ministerio de Defensa (MINDEF), en el marco de sus funciones y competencias, dirige, norma, supervisa y evalúa las normas en materia de ciberdefensa.
[...]."

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Reglamentación en materia de ciberdefensa
La Presidencia del Consejo de Ministros, en coordinación con el Ministerio de Defensa, aprueba el reglamento de la presente ley, en un plazo máximo de noventa (90) días, contados a partir del día siguiente de su publicación en el diario oficial El Peruano.

SEGUNDA. Modificaciones a normas de las Fuerzas Armadas en materia de ciberdefensa
El Ministerio de Defensa, en un plazo de noventa (90) días, contados a partir de la fecha de entrada en vigencia de la presente ley, presenta las modificaciones, derogaciones e incorporaciones a las normas correspondientes a las Fuerzas Armadas en materia de la presente ley.

TERCERA. Recursos críticos de Internet
Se reconoce a las entidades que gestionen recursos críticos de Internet (nombres de dominio, números IP y protocolos) en su naturaleza de entidades vinculadas a la ciberdefensa, debiendo mantener mecanismos de comunicación de incidentes que pudieran afectar la capacidad de ciberdefensa nacional.

CUARTA. Desarrollo de currículos de educación superior en materia de ciberdefensa
La Presidencia del Consejo de Ministros, en su calidad de ente rector en materia de seguridad digital, coordina con el Ministerio de Defensa y el Ministerio de Educación la pertinencia del desarrollo de contenidos especializados en materia de seguridad digital, que incluye la ciberdefensa, en las instituciones de educación superior universitaria y tecnológica, a nivel de pregrado y postgrado. Para ello, establece instrumentos de cooperación interinstitucional con entidades del sector privado, la academia, la sociedad civil y la comunidad técnica.

QUINTA. Aplicación de recursos especiales
Los procesos para las capacidades de ciberdefensa deben considerarse dentro del alcance de la aplicación de los artículos 30 y 31 del Decreto Legislativo 1141.

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogatoria
Deróganse o déjense en suspenso, según el caso, las disposiciones legales y reglamentarias que se opongan a lo establecido por la presente ley o limiten su aplicación, con la entrada en vigencia de la presente ley.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los nueve días del mes de agosto de dos mil diecinueve.

PEDRO C. OLAECHEA ÁLVAREZ CALDERÓN
Presidente del Congreso de la República

KARINA BETETA RUBÍN
Primera Vicepresidenta del Congreso de la República

AL SEÑOR PRESIDENTE DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiséis días del mes de agosto del año dos mil diecinueve.

MARTÍN ALBERTO VIZCARRA CORNEJO
Presidente de la República

SALVADOR DEL SOLAR LABARTHE
Presidente del Consejo de Ministros

1801519-5

PODER EJECUTIVO

PRESIDENCIA DEL CONSEJO DE MINISTROS

Modifican el Anexo N° 01 "Fondos destinados para la prevención de inundaciones pluviales, fluviales y movimiento de masas y entidades ejecutoras" que forma parte del Plan y dictan diversas disposiciones

RESOLUCIÓN DE DIRECCIÓN EJECUTIVA N° 00074-2019-RCC/DE

Lima, 26 de agosto de 2019

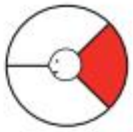
VISTOS: El Acuerdo N° 1 de la Sexagésima Primera Sesión de Directorio de la Autoridad para la Reconstrucción con Cambios, el Informe N° 494-2019-RCC/GPE y el Informe N° 532-2019-RCC/GL;

CONSIDERANDO:

Que, la Ley N° 30556 aprueba disposiciones de carácter extraordinario para las intervenciones del Gobierno Nacional frente a desastres y dispone la creación de la Autoridad para la Reconstrucción con Cambios (en adelante la Autoridad), como una entidad adscrita a la Presidencia del Consejo de Ministros, de carácter excepcional y temporal, encargada de liderar e implementar el Plan Integral para la Reconstrucción con Cambios;

Anexo 4: Guía de entrevista a cliente - tareas y responsabilidades

Customer Jobs



Trigger Questions

Jobs describe the things your customers are trying to get done in their work or in their life. A customer job could be the tasks they are trying to perform and complete, the problems they are trying to solve, or the needs they are trying to satisfy.

Use the following trigger questions to help you think of different potential customer jobs:

1. What is the one thing that your customer couldn't live without accomplishing? What are the stepping stones that could help your customer achieve this key job?
2. What are the different contexts that your customers might be in? How do their activities and goals change depending on these different contexts?
3. What does your customer need to accomplish that involves interaction with others?
4. What tasks are your customers trying to perform in their work or personal life? What functional problems are your customers trying to solve?
5. Are there problems that you think customers have that they may not even be aware of?
6. What emotional needs are your customers trying to satisfy? What jobs, if completed, would give the user a sense of self-satisfaction?
7. How does your customer want to be perceived by others? What can your customer do to help themselves be perceived this way?
8. How does your customer want to feel? What does your customer need to do to feel this way?
9. Track your customer's interaction with a product or service throughout its lifespan. What supporting jobs surface throughout this life cycle? Does the user switch roles throughout this process?

Strategyzer
www.strategyzer.com/vpd

Anexo 5: Guía de entrevista a cliente - dolencias y retos

Customer Pains

Trigger Questions

Pains describe anything that annoys your customers before, during, and after trying to get a job done or simply prevents them from getting a job done. Pains also describe risks, that is, potential bad outcomes, related to getting a job done badly or not at all.

Use the following trigger questions to help you think of different potential customer pains:

1. How do your customers define too costly? Takes a lot of time, costs too much money, or requires substantial efforts?
2. What makes your customers feel bad? What are their frustrations, annoyances, or things that give them a headache?
3. How are current value propositions under performing for your customers? Which features are they missing? Are there performance issues that annoy them or malfunctions they cite?
4. What are the main difficulties and challenges your customers encounter? Do they understand how things work, have difficulties getting certain things done, or resist particular jobs for specific reasons?
5. What negative social consequences do your customers encounter or fear? Are they afraid of a loss of face, power, trust, or status?
6. What risks do your customers fear? Are they afraid of financial, social, or technical risks, or are they asking themselves what could go wrong?
7. What's keeping your customers awake at night? What are their big issues, concerns, and worries?
8. What common mistakes do your customers make? Are they using a solution the wrong way?
9. What barriers are keeping your customers from adopting a value proposition? Are there upfront investment costs, a steep learning curve, or other obstacles preventing adoption?

Strategyzer
www.strategyzer.com/vpd

Anexo 6: Guía de entrevista a cliente - beneficios y ganancias

Customer Gains

Trigger Questions

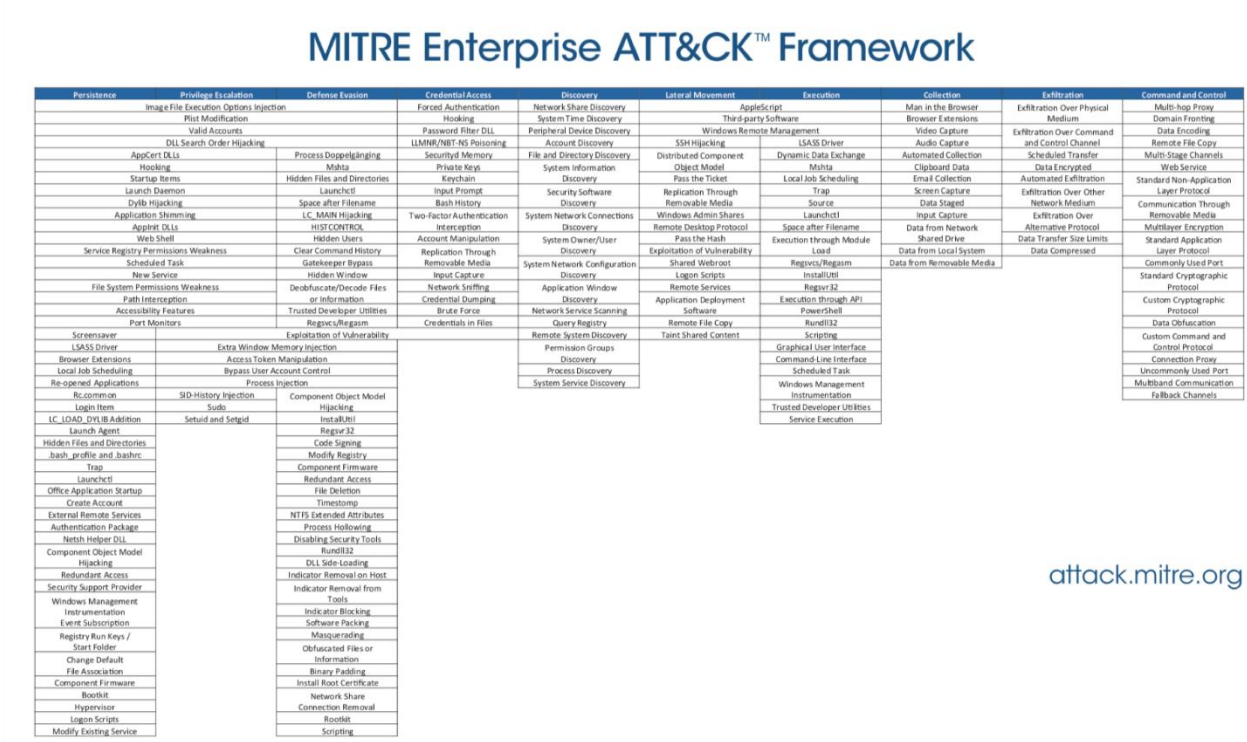
Gains describe the outcomes and benefits your customers want. Some gains are required, expected, or desired by customers, and some would surprise them. Gains include functional utility, social gains, positive emotions, and cost savings.

Use the following trigger questions to help you think of different potential customer gains:

1. Which savings would make your customers happy? Which savings in terms of time, money, and effort would they value?
2. What quality levels do they expect, and what would they wish for more or less of?
3. How do current value propositions delight your customers? Which specific features do they enjoy? What performance and quality do they expect?
4. What would make your customers' jobs or lives easier? Could there be a flatter learning curve, more services, or lower costs of ownership?
5. What positive social consequences do your customers desire? What makes them look good? What increases their power or their status?
6. What are customers looking for most? Are they searching for good design, guarantees, specific or more features?
7. What do customers dream about? What do they aspire to achieve, or what would be a big relief to them?
8. How do your customers measure success and failure? How do they gauge performance or cost?
9. What would increase your customers' likelihood of adopting a value proposition? Do they desire lower cost, less investment, lower risk, or better quality?

Strategyzer
www.strategyzer.com/vpd

Anexo 7: Marco de trabajo MITRE ATT&CK



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Image File Execution Options Injection			Forced Authentication	Network Share Discovery	AppleScript		Man in the Browser	Exfiltration Over Physical Medium	Multi-hop Proxy
Plist Modification			Hooking	System Time Discovery	Third-party Software		Browser Extensions		Domain Fronting
Valid Accounts			Password Filter DLL	Peripheral Device Discovery	Windows Remote Management		Video Capture	Exfiltration Over Command and Control Channel	Data Encoding
DLL Search Order Hijacking			LLMNR/NBT-NS Poisoning	Account Discovery	SSH Hijacking	LSASS Driver	Audio Capture		Remote File Copy
AppCert DLLs		Process Doppelgänging	Securityd Memory	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Scheduled Transfer	Multi-Stage Channels
Hooking		Mshta	Private Keys	System Information Discovery		Mshta	Clipboard Data	Data Encrypted	Web Service
Startup Items		Hidden Files and Directories	Keychain		Pass the Ticket	Local Job Scheduling	Email Collection	Automated Exfiltration	Standard Non-Application Layer Protocol
Launch Daemon		Launchctl	Input Prompt	Security Software Discovery	Replication Through Removable Media	Trap	Screen Capture	Exfiltration Over Other Network Medium	
Dylib Hijacking		Space after Filename	Bash History			Source	Data Staged		Communication Through Removable Media
Application Shimming		LC_MAIN Hijacking	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Launchctl	Input Capture	Exfiltration Over Alternative Protocol	
AppInit DLLs		HISTCONTROL			Remote Desktop Protocol	Space after Filename	Data from Network Shared Drive		Multilayer Encryption
Web Shell		Hidden Users	Account Manipulation	System Owner/User Discovery	Pass the Hash	Execution through Module Load	Data from Local System	Data Transfer Size Limits	Standard Application Layer Protocol
Service Registry Permissions Weakness		Clear Command History	Replication Through Removable Media		Exploitation of Vulnerability		Data from Removable Media	Data Compressed	
Scheduled Task		Gatekeeper Bypass		System Network Configuration Discovery	Shared Webroot	Regsvcs/Regasm			Commonly Used Port
New Service		Hidden Window	Input Capture		Logon Scripts	InstallUtil			Standard Cryptographic Protocol
File System Permissions Weakness		Deobfuscate/Decode Files or Information	Network Sniffing	Application Window Discovery	Remote Services	Regsvr32			
Path Interception			Credential Dumping		Application Deployment Software	Execution through API			Custom Cryptographic Protocol
Accessibility Features		Trusted Developer Utilities	Brute Force	Network Service Scanning		PowerShell			Data Obfuscation
Port Monitors		Regsvcs/Regasm	Credentials in Files	Query Registry	Remote File Copy	Rundll32			
Screensaver		Exploitation of Vulnerability		Remote System Discovery	Taint Shared Content	Scripting			Custom Command and Control Protocol
LSASS Driver	Extra Window Memory Injection			Permission Groups Discovery		Graphical User Interface			Connection Proxy
Browser Extensions	Access Token Manipulation					Command-Line Interface			Uncommonly Used Port
Local Job Scheduling	Bypass User Account Control			Process Discovery		Scheduled Task			Multiband Communication
Re-opened Applications	Process Injection			System Service Discovery		Windows Management Instrumentation			Fallback Channels
Rc.common	SID-History Injection	Component Object Model Hijacking				Trusted Developer Utilities			
Login Item	Sudo					Service Execution			
LC_LOAD_DYLIB Addition	Setuid and Setgid	InstallUtil							
Launch Agent		Regsvr32							
Hidden Files and Directories		Code Signing							
.bash_profile and .bashrc		Modify Registry							
Trap		Component Firmware							
Launchctl		Redundant Access							
Office Application Startup		File Deletion							
Create Account		Timestomp							
External Remote Services		NTFS Extended Attributes							
Authentication Package		Process Hollowing							
Netsh Helper DLL		Disabling Security Tools							
Component Object Model Hijacking		Rundll32							
Redundant Access		DLL Side-Loading							
Security Support Provider		Indicator Removal on Host							
Windows Management Instrumentation Event Subscription		Indicator Removal from Tools							
Registry Run Keys / Start Folder		Indicator Blocking							
Change Default File Association		Software Packing							
Component Firmware		Masquerading							
Bootkit		Obfuscated Files or Information							
Hypervisor		Binary Padding							
Logon Scripts		Install Root Certificate							
Modify Existing Service		Network Share Connection Removal							
		Rootkit							
		Scripting							

Proyecto_profesional-2020-IOC_v10

INFORME DE ORIGINALIDAD

4%	3%	1%	1%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	www.asis.org.pe Fuente de Internet	1%
2	Submitted to Universidad de Lima Trabajo del estudiante	1%
3	Cristina Torres Machí. "Optimización heurística multiobjetivo para la gestión de activos de infraestructuras de transporte terrestre.", Universitat Politecnica de Valencia, 2015 Publicación	<1%
4	repositorio.ulima.edu.pe Fuente de Internet	<1%
5	Submitted to UNAPEC Trabajo del estudiante	<1%
6	iapp.org Fuente de Internet	<1%
7	oa.upm.es Fuente de Internet	<1%
8	www.tdx.cat	