UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster universitario en Seguridad Informática

Proceso para Definir y Establecer un Centro de Operaciones de Seguridad (SOC) en una Organización Financiera

Trabajo Fin de Máster

Presentado por: Román Torres, María José

Director/a: Rubio Blanco, José Antonio

Ciudad: Guayaquil

Fecha: 23 de enero de 2019

Índice de Contenido

Índice de Tablas

Índice de Ilustraciones

Resumen del Trabajo

Debido a la necesidad de las Organizaciones del sector Financiero de garantizar la seguridad de la información de sus Clientes en los diferentes servicios que se ofrece, es común en las Organizaciones invertir tiempo, dinero, entre otros recursos, en definir procesos que ayuden a detectar, prevenir y solventar posibles fallos de seguridad en los servicios y sistemas que se administran dentro de la Organización, para esto es necesario contar con un área especializada en las actividades relacionadas con la Seguridad de la Información que tendrán que ejecutarse diariamente. Este trabajo se enfocará en los puntos principales que una Organización debe tomar en cuenta para poder establecer los procesos de un Centro de Operaciones de Seguridad (SOC por sus siglas en inglés) con personal especializado en la materia y el uso de herramientas adecuadas para poder gestionar la Seguridad de la Información de toda la Organización tanto de sus empleados como de sus clientes.

Palabras Claves:

Centro de Operaciones de Seguridad; SOC; Seguridad; Operaciones de Seguridad; Procesos de Seguridad; Detección de Intrusos; Seguridad de Redes.

CAPÍTULO I

1. Introducción

1.1. Motivación

Los sistemas de información han evolucionado exponencialmente durante las últimas décadas y paralelamente también las amenazas contra la seguridad de los mismos, hoy en día, la seguridad de la información es considerada un proceso continuo fundamental para la mayoría de las Empresas de diversas industrias, sectores y tamaños, por lo cual es esencial poder garantizar los servicios principales de la seguridad de la información (confidencialidad, integridad y disponibilidad de la información). En la actualidad la Información es considerada el principal activo para cualquier Organización, incluso se podría considerar a la información como un activo estratégico, cierto tipo de información puede ser más sensible que otras. La información que es considerada como sensible tendría un valor clave dentro de los procesos y para poder ser gestionada es común definir niveles para clasificar la Información según el tipo de confidencialidad de la misma. Entre las clasificaciones más utilizadas por las Organizaciones se puede mencionar los siguientes niveles:

Nivel	Clasificación de la Información	Descripción
4	**Confidencial**	Información que posee un nivel alto de confidencialidad, cuya revelación podría ocasionar pérdidas económicas y afectar la reputación de la empresa, como por ejemplo estados financieros, información sensible de clientes, entre otros.
3	**Restringido y/o Privado**	Información que posee un nivel intermedio de confidencialidad como por ejemplo las listas de proveedores, nómina de empleados, entre otros.
2	**Uso Interno**	Información que posee un nivel bajo de confidencialidad como por ejemplo documentos de políticas internas en la Organización
1	**Uso Público**	Información que puede ser accedida por todas las personas internas o externas a la Organización

Tabla 1. Niveles de Clasificación de la Información

Considerando que la información que es considerada como sensible estaría dentro de los niveles 2, 3 y 4 antes mencionados, se busca implementar controles en los procesos y actividades de la Organización para garantizar la seguridad de dichos niveles de información.

Entre los principales objetivos que se buscan lograr en la gestión de la seguridad de la información es poder evitar que personal no autorizado tenga acceso a la información sensible de la Organización y pueda comprometerla, en el caso de que la información llegara a estar comprometida de cualquier manera podría afectar gravemente los servicios que la Organización ofrece, lo que conllevaría a un daño en su imagen, en la confianza de sus clientes y inclusive podría ocasionar pérdidas en sus ingresos económicos. Para poder evitar este tipo de riesgos es necesario definir e implementar controles y procesos que ayuden a garantizar la seguridad de la información, considerando todas las actividades, activos, sistemas y/o herramientas que la Organización maneje. Un análisis realizado durante el 2018 sobre los tipos de información más vulnerables para los atacantes, que existe hoy en día dentro de las organizaciones muestra que la información de tipo “Confidencial” como puede ser estados financieros, información de clientes o de empleados, etc.; se encuentra encabezando la lista con un 57% siendo considerada como el tipo de información más vulnerable (CA Technologies, 2018), ver anexo VIII.

Actualmente la mayoría de las Organizaciones manejan información personal o privada de sus clientes y empleados, la cual es una de las primeras motivaciones detrás de los ataques informáticos es el crimen cibernético, como se puede observar en el siguiente cuadro estadístico del mes de Septiembre del año 2018:

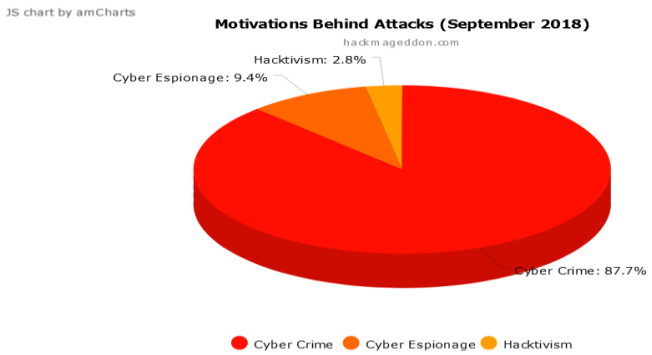


Figura 1. Cuadro Estadístico “Motivaciones detrás de Ataques (Septiembre 2018)” (Passeri, 2018)

Las Organizaciones que pertenecen al sector Financiero además de administrar datos personales de sus clientes, gestionan la información financiera de los mismos como por ejemplo: cuentas bancarias, inversiones financieras, préstamos, tarjetas de créditos, entre

otros. Por dicha razón las Organizaciones dentro del sector Financiero es uno de los principales objetivos para delincuentes informáticos para ejecutar ataques. Hasta septiembre del 2018 se observa que el 10.4% de la distribución de los objetivos de ataques corresponde a instituciones financieras y seguros privados, estando dentro de los 5 primeros objetivos de ataques, ver anexo IX.

Entre las principales técnicas y herramientas utilizadas por los cibercriminales para realizar los ataques a las Organizaciones del sector financiero se encuentran las siguientes:

Técnica de Ataque	Descripción
Denegación de Servicio (DoS)	Es una técnica de ataque contra una red o servicio informático que busca que el recurso sea inaccesible para usuarios autorizados. Por lo general provoca perdida de la conexión al servicio o sobrecarga del recurso informático atacado que ocasiona que el servicio no esté disponible.
Explotación de Vulnerabilidades en sus servicios web	Consiste en realizar un análisis del servicio web al que se va atacar para detectar posibles vulnerabilidades de programación y/o configuración, entre otros; por el cual podrían vulnerar el sistema y tener acceso no autorizado y comprometer el servicio.
Código malicioso en dispositivos de Puntos de Ventas (PoS) o Cajeros Automáticos (ATM)	Esta técnica explota vulnerabilidades en estos dispositivos utilizados por los clientes de las instituciones financieras para comprometer el funcionamiento del mismo y de esta manera obtener información bancaria relacionada con las tarjetas que posee el cliente.
Herramienta de Ataques Dirigidos	Se trata de utilizar herramientas especializadas para poder ejecutar ataques como por ejemplo del tipo Phishing para obtener información bancaria de los clientes. La técnica de Phishing es una las más utilizadas por los cibercriminales para robar información
Watering Hole	Es una técnica relativamente nueva que consiste en comprometer sitios web que sean visitados por empleados de la institución financiera para poder infectar sus máquinas con algún tipo de malware y de esta manera ingresar a la red interna de la institución

Tabla 2. Técnicas utilizadas por Cibercriminales en Instituciones Financieras.

Considerando que el sector financiero siempre está evolucionando sus servicios y herramientas al igual que la tecnología que utiliza, asimismo, las técnicas de ataques de los cibercriminales también evolucionan adaptándose a estos cambios, es elemental que los

procesos y controles de seguridad que se utilicen sean capaces de adaptarse y/o evolucionar paralelamente y que cubran todas las necesidades de la Organización.

Para optimizar los procesos de detección y respuesta frente amenazas es necesario establecer un enfoque de seguridad diferente al tradicional, el cual se basaría en utilizar toda la información disponible relacionada con las actividades que se realizan en la Organización, esta información puede proceder de fuentes internas (como procesos internos, sistemas, dispositivos tecnológicos, etc.) o externas (como servicios que utilizan los clientes) para poder detectar posibles amenazas existentes y prevenir amenazas futuras.

Tratar de implementar mecanismos de defensa apropiados para mitigar los riesgos de seguridad es una es uno de los retos del personal responsable de la seguridad en la Organización, es por esto que uno de los primordiales objetivos en las instituciones del sector Financiero es contar con proceso adecuado para la gestión de las Operaciones de la Seguridad de la Información y el monitoreo constante de las actividades que se realizan diariamente, con lo cual se lograría prevenir, evitar, reducir e inclusive detectar los posibles ataques a los que pueden estar expuestos.

1.2. Solución de la Problemática

La mayoría de las actividades diarias que se ejecutan dentro de las Instituciones Financieras son a través de sistemas informáticos de esta manera los procesos son más ágiles, sencillos y estructurados, sin embargo, para conseguir la protección de dichos procesos es importante que la Seguridad de la Información sea parte fundamental dentro de la cultura organizacional, y de esta manera poder establecer procesos seguros, en los que se debe definir los siguientes puntos:

- Recursos y activos de información utilizados por el proceso
- Personal y recursos que tendrá acceso a la información del proceso
- Personal y recursos que podrá modificar la información del proceso
- Dueño del proceso y la información, entre otros.

Actualmente la mayoría de las herramientas y sistemas de información que se encuentran en el mercado vienen con controles de seguridad incorporados para proteger la información que procesa, a pesar de esto es necesario contar con un esquema de seguridad general dentro de la Organización, el cual tienen como objetivo satisfacer las necesidades del negocio y definir los lineamientos y medidas de seguridad que los recursos informáticos deben de

cumplir basándose en estándares y mejores prácticas reconocidas a nivel mundial, de esta manera se puede garantizar a los clientes la seguridad y protección de su información.

Por este motivo la implementación de un Centro de Operaciones de Seguridad (SOC por sus siglas en inglés – *Security Operation Center*) dentro de las instituciones financieras es elemental para poder brindar seguridad a la Organización y sus servicios. La principal función de un SOC es el monitoreo constante de las actividades que ejecutan los recursos informáticos dentro de la Organización con el objetivo de prevenir y/o evitar incidentes de seguridad, y en el caso de ocurrir disponer de un proceso de respuesta ágil y adecuado.

Entre los principales servicios internos que ofrece un SOC a la Organización se menciona:

Servicio del SOC	Objetivo
Prevención de Incidentes	Este servicio se enfoca en todas las actividades a realizar para evitar que incidentes de seguridad y amenazas se materialicen y afecten el funcionamiento normal de los servicios de la Organización.
Detección de Amenazas	Su objetivo principal es detectar cualquier tipo de amenaza que se presente en la Organización y poder realizar acciones mitigantes para evitar su materialización.
Corrección y Respuesta ante Incidentes	Este servicio engloba todas las acciones y medidas ejecutadas para solventar un incidente de manera ágil y correcta dentro de los tiempos de respuestas definidos en el esquema de seguridad de la empresa.

Tabla 3. Servicios de un Centro de Operaciones de Seguridad (SOC)

Basándose en lo previamente expuesto se puede concluir que es de suma importancia que todas las Organizaciones en especial las del sector Financiero por la naturaleza de la información que manejan, se enfoquen en implementar un SOC, con lo cual ayudara a incrementar la seguridad de la Organización y disminuir el riesgo de las amenazas contra la seguridad de la información.

Debido a que hoy en día no existe un estándar que trate exclusivamente a la implementación de un SOC dentro del sector Financiero, este trabajo de fin de máster busca establecer un proceso para la implementación de un Centro de Operaciones de Seguridad dentro de las instituciones financieras, basándose en las mejores prácticas que actualmente son utilizadas a nivel mundial.

1.3. Estructura del Trabajo

Con el entendimiento de que es indispensable tener a la seguridad como uno de los principales protagonistas dentro de todos los procesos y actividades de la Organización del sector Financiero, para de esta manera poder prevenir posibles amenazas que puedan poner en riesgo la funcionalidad de los servicios y llegar a perjudicar a sus clientes, es necesario mantener un proceso oportuno de detección de ataques y en conjunto con un proceso adecuado de respuesta ante incidentes de seguridad que puedan materializarse. Es por ello que en las organizaciones deben siempre considerar a la seguridad de sus activos de información como uno de los principales requisitos a exigir en todo los procesos.

El presente trabajo de fin de Máster abarcará todos los aspectos que son necesarios considerar para definir e implementar un Centro de Operaciones de Seguridad, de esta manera el trabajo proporcionará un proceso para la implementación un SOC dentro de una Organización en el sector Financiero, con el cual podrá mejorar el rendimiento de los procesos de detección y respuesta ante las amenazas.

Este documento se encuentra conformado por 4 capítulos que detallaran los fundamentos, normativas, estándares y mejores prácticas que son necesarias considerar para poder definir e implementar un Centro de Operaciones de Seguridad que ayude a mitigar el riesgo de los ataques a los que se encuentra expuesta la Organización. A continuación una breve descripción de los capítulos del trabajo:

- Capítulo I. Introducción: Este capítulo expone la problemática existente sobre la necesidad de considerar a la seguridad en cada actividad dentro de las organizaciones, adicional a esto se definirá la justificación de porque es necesario implementar un Centro de Operaciones de Seguridad dentro de las empresas.
- Capítulo II. Estado del Arte: En este capítulo se detalla la situación actual de la seguridad de la información, sus principales preocupaciones y los índices de seguridad con los que se encuentra las empresas. También se desglosa la importancia de la seguridad de la información en las instituciones financieras y cuáles son las principales amenazas a las que se exponen diariamente.
- Capítulo III. Objetivos y Metodología del Trabajo: Este capítulo desglosa los principales objetivo que se busca cumplir en la realización del presente trabajo de fin de máster.
- Capítulo IV. Marco Teórico: En este capítulo se detallará a rasgos breves los principales conceptos que deben considerarse para poder hondar en el campo de la

seguridad informática previamente a la implementación de Centro de Operaciones de Seguridad (SOC).

- Capítulo V. Centro de Operaciones de Seguridad SOC: Este capítulo se enfocará en los puntos relevantes que se deben tomar en cuenta al momento de diseñar y definir un Centro de Operaciones de Seguridad dentro de una organización, como por ejemplo: sus principales funciones y aspectos, la triada de operaciones de seguridad (personas, procesos y tecnologías).
- Capítulo VI. Lineamiento de Seguridad estipulados en la Resolución SB-2018-771: El capítulo se analiza los requerimientos de seguridad de la información, estipulados por la Superintendencia de Bancos del Ecuador para ser cumplidos por las instituciones financieras. Adicionalmente, se analiza la resolución SB-2018-771 versus el estándar internacional ISO/IEC 27000 para la gestión de la seguridad de la información.
- Capítulo VII. Normas y Estándares Internacionales con lineamientos aplicables a un SOC: En este capítulo se detallará de manera breve cuales son los puntos definidos en estándares y normas internacionales que pueden ser aplicables dentro de un SOC.
- Capítulo VIII. Conclusiones del trabajo.

CAPÍTULO II

2. Contexto y Estado del Arte

2.1. Estado actual de la Seguridad de la Información

Entre las preocupaciones habituales que tienen los Gerentes Generales de las instituciones (puede ser pequeña, mediana o grande) de los diferentes sectores comerciales, es llegar a conocer el estado actual y real sobre la seguridad de su empresa, de esta manera podrán saber con exactitud qué tan expuesto se encuentran ante el riesgo de ser el objetivo de ataque de un cibercriminal.

Hoy en día existe muchas fuentes de información que nos ayuda a entender cuál es el estado general de la seguridad en las empresas, para el presente apartado nos enfocaremos en el estudio realizado por la empresa ESET (empresa dedicada a la seguridad y protección antivirus) para conocer el estado de la seguridad de la información en los países de Latinoamérica durante el año 2017 (ESSET, 2018).

En el ámbito de la seguridad de la información existe muchas preocupaciones para los responsables de la seguridad dentro de las empresas independiente del tamaño de la misma, durante el transcurso del 2017 se observó que los tipos de preocupaciones más frecuentes son las siguientes:

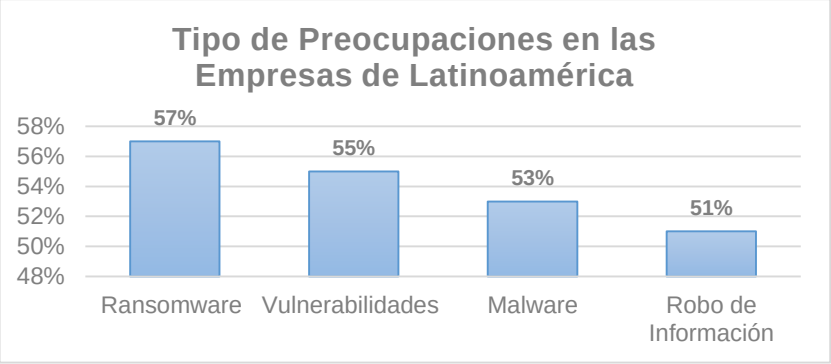


Figura 2. Cuadro estadístico del porcentaje de empresas según los tipos de preocupaciones relacionadas con la seguridad de la información

Para tener un mayor entendimiento de estos tipos de preocupaciones a continuación se presenta una breve descripción de cada una:

- Ransomware

  Es un tipo de programa considerado dañino que puede infectar un computador, servidor, dispositivo móvil, entre otros; el cual tiene como objetivo restringir el acceso a los usuarios a ciertos documentos, archivos, carpetas y/o unidades de disco dentro del sistema infectado, por medio de técnicas fuertes de cifrado. Una vez restringido el acceso pide un valor de "rescate" para que el usuario pueda volver a tener acceso a los archivos, usualmente el valor a pagar es en criptomoneda.
- Vulnerabilidades

  Se considera como vulnerabilidad los puntos débiles de cualquier sistema de información o dispositivo tecnológico, que permitirán a los atacantes comprometer la información.
- Malware

  Es cualquier programa o código malicioso cuyo objetivo es contaminar el funcionamiento normal y correcto de un sistema de información y/o dispositivo tecnológico y recopilar información que será utilizada por el atacante.
- Robo de Información

  Es el acto de apropiarse de información privada de terceras personas para poder utilizarla de forma ilegal y no autorizada.

Según estas estadísticas el Ransomware encabeza la lista de las preocupaciones en el ámbito de la seguridad, gracias a la rentabilidad monetaria que esta técnica ofrece a sus atacantes, muchas empresas son target de estos tipos de ataques. Debido a que el Ransomware es un tipo de Malware, una de las formas para poder infectar un sistema es por medio del uso de código malicioso que estará camuflado en un programa el cual va almacenarse en la maquina victima para que posteriormente el Ransomware pueda activarse, por esos es importante tener implementado una gestión de protección para la información y los activos en los que reside para de esta manera poder reducir el riesgo de infección.

Durante el 2017 se presentaron varios incidentes de seguridad de infección por Malware en Latinoamérica, se observa que los países con el índice de infección más alto, de este tipo son Ecuador y Venezuela con un 22%, y El Salvador y Paraguay con el índice más bajo con un 13%:

Adicional a las infecciones por código malicioso también se presentaron otro tipo de incidentes de seguridad que fueron reportados por las empresas participantes en el estudio durante ell

2017, del cual el 10% reportaron incidentes que atentan contra la disponibilidad de los servicios de la empresa y un 11% reportaron incidentes de acceso no autorizado a sistemas o bases de datos de la empresa, ver anexo X.

Otra forma bastante utilizada por los atacantes para obtener información de sus víctimas es utilizando Ingeniería Social, esta técnica está evolucionando constantemente y hasta el día de hoy se usa con bastante frecuencia, como por ejemplo los ataques de Phishing para las Bancas Virtuales de las Instituciones Financieras de esta manera se puede obtener información de credenciales y dispositivos de seguridad que poseen los clientes. Desde el 2013 hasta el 2017 se observa el siguiente comportamiento de incidentes reportados relacionados con ingeniería social:

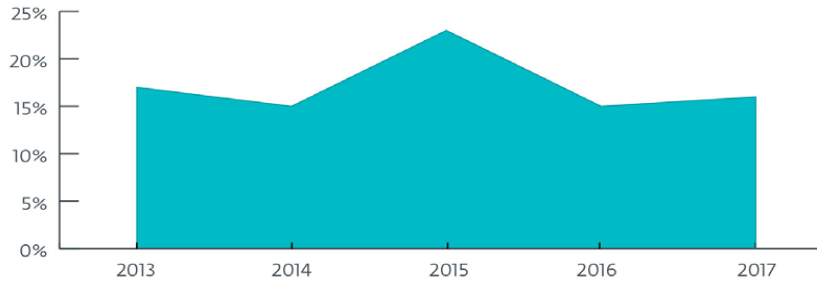


Figura 3. Tendencia de Incidentes reportados relacionados con Ingeniería Social

En la actualidad existen una amplia gama de amenazas que atentan contra la seguridad de los sistemas de información de las empresas, por ello es primordial para las empresas de cualquier tipo de tamaño, establecer controles de seguridad que minimicen el riesgo de infección. De acuerdo al tamaño de la Organización pueden variar los tipos de controles de seguridad, como por ejemplo las empresas pequeña debido a que poseen una menor capital de inversión por lo general utilizan controles de seguridad basados en la tecnología, como herramientas o soluciones de TI, para proteger sus servicios, sin embargo, carecen de controles de seguridad basados en gestión de seguridad (políticas, procesos, planes, etc.) que se hayan sido definidos en la empresa, por lo general este tipo de controles basados en políticas son más utilizados por las empresas grandes o multinacionales. En el estudio realizado por ESSET durante el 2017 (ESSET, 2018), se observa que el porcentaje de empresas pequeñas que carecen de controles de seguridad supera al porcentaje de empresas de tamaño grandes:

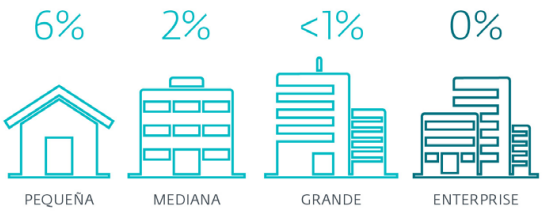


Figura 4. Porcentaje de empresas que carecen de controles de seguridad según su tamaño

Esto se debe a que las empresas de tamaño grande tienen actividades y procesos más estructurados basados en estándares, normativas y mejores prácticas que aconsejan la gestión de la seguridad de la información es uno de los principales requisitos en la actualidad, de igual manera este tipo de empresas posee un mayor presupuesto económico para poder invertir en la gestión de la seguridad y herramientas especializadas.

Entre las empresas que utilizan controles basados en la gestión de la seguridad, se observa la adopción de los siguientes tipos:

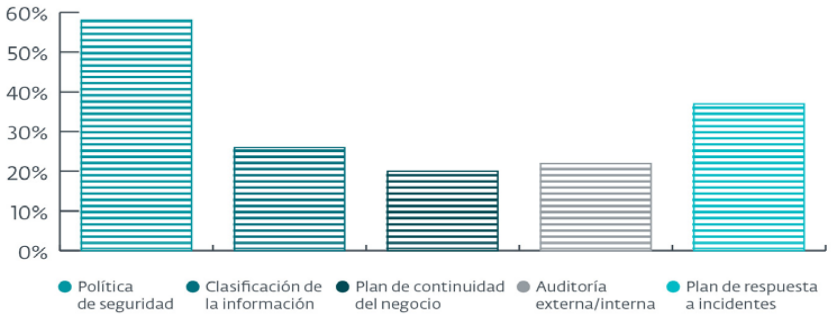


Figura 5. Estadística de adopción de tipo de controles basados en la gestión de la seguridad

El control de “Política de Seguridad” es uno de los más utilizados por las empresas, porque por medio de este se establecen todos los lineamientos y pautas de seguridad con los que los empleados deben cumplir, estas políticas siempre están alineadas directamente con la estrategia del negocio para poder cumplir con los requisitos de la empresa.

Estos tipos de controles son parte del proceso integral de la gestión de la seguridad y para poder administrarlos, monitorearlos y evaluarlos es necesario que dentro de las empresas se encuentre definida un área exclusivamente dedicada a la gestión de seguridad, sin embargo, en general al menos un 10% de las empresas no cuentan con este tipo de áreas; la gestión de la seguridad es realizada por otras área o personal no especializado en la materia. Esta manera de gestionar la seguridad de la información puede generar un conflicto de intereses

debido a que en ciertos casos el mismo personal de TI es el encargado de implementar controles de seguridad y evaluarlos, cuando las mejores prácticas recomiendan que el área de seguridad de la información no sea parte del área de TI, sino un ente independiente que supervise y monitoree las actividades de las demás áreas.

Un análisis de las empresas de Latinoamérica que cuentan con un área especializada para la gestión de la seguridad de la información, muestra que la tendencia no supera el 15% de las empresas examinadas durante los tres últimos años, el crecimiento anual muestra un ligero incremento (ESSET, 2018):

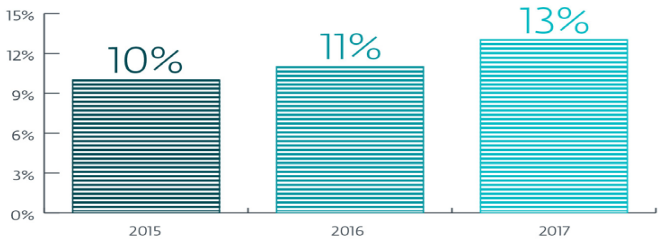


Figura 6. Porcentaje de Empresas que cuentan con un área especializada para la gestión de la Seguridad de la Información

Cada año más empresas, independiente de su tamaño y sector, reconocen la importancia de invertir en un proceso de gestión de la seguridad de la información adecuado, lo que involucra la definición e implementación de un área especializada que realice la verificación de las actividades dentro de la Organización para poder prevenir y evitar posibles ataques a los que se encuentre expuestos. Los Centro de Operaciones de Seguridad (SOC) cada día son más útiles y necesarios dentro de las empresas, porque a través de ellos se realizara el monitoreo y evaluación de todas las actividades para poder correlacionar eventos, predecir ataques y evitar infecciones, contar con personal especializado en la materia y procesos correctamente definidos ayudaran a aumentar la seguridad de la empresa y de sus servicios, es por esto que el presente trabajo se enfocará en los puntos principales que hay que tomar en cuenta al momento de definir un proceso para la implementación de un SOC.

2.2. Seguridad de la Información en Instituciones Financieras

Para las Instituciones financieras es elemental mantener una relación de confianza con sus Clientes, debido a que son los Clientes los que entregan parte de su patrimonio económico a este tipo de Instituciones para que sea administrado y resguardado. Es por esto que la confianza guarda una relación directa con la seguridad que debe establecerse en todas las actividades realizadas en el sector financiero.

Antes del uso de sistemas de información para la gestión de los procesos y operaciones dentro de Instituciones Financieras, la seguridad se enfocaba a nivel físico, implementando mecanismos de seguridad para evitar el acceso o modificación no autorizada de documentos físicos del Banco o Clientes, acceso a las bóvedas donde se encontraba el dinero almacenado, entre otros. Sin embargo, con la evolución de la forma de procesar información y el uso de sistemas de información, donde los documentos físicos son transformados a información lógica que se almacena en una base de datos (Evans, 2015), convirtiendo a la Información como uno de los Activos más importante para cualquier Organización independientemente del sector al cual pertenezca.

Los cibercriminales amenazan a los clientes de las entidades financieras por medio de ataques para obtener credenciales para acceder a bancas virtuales y realizar transacciones bancarias no autorizadas, para poder evitar estos tipos de ataques las instituciones del sector financiero tienen que constantemente mejorar sus controles de seguridad en todos los servicios que interactúen con los clientes y también en toda su infraestructura tecnológica. Una de las formas más utilizadas por los atacantes para obtener información son los engaños utilizando de Ingeniería Social, por medio de técnicas como malware o Phishing logran recopilar información de clientes como credenciales de acceso, id de sesión, dispositivos de seguridad, entre otros; para poder ser utilizada luego.

Actualmente los ataques no son solamente contra los clientes de entidades financieras, sino también contra la propia entidad, buscando manipular sus sistemas o procesos para transferir grandes sumas de dinero a bancos fuera del país. Las instituciones financieras se expone a múltiples frentes de ataques, pero los más comunes son los ataques contra los clientes y contra la infraestructura de la propia Organización (Wueest, 2017).

2.2.1. Ataques contra los clientes de Instituciones Financieras

Son los ataques que tienen como target los clientes de las Instituciones financieras, su principal objetivo es el robo de información como credenciales, cuentas bancarias, dispositivos de seguridad, ID de sesión, entre otros. Esta información será utilizada por los cibercriminales para realizar transacciones bancarias ilegales y fraudulentas. Entre las técnicas de ataques más utilizados se puede mencionar:

- Fraude en tarjetas de crédito
  Consiste en el robo de la información de la tarjeta de crédito o débito del cliente, para posteriormente clonarla y ser utilizada por el atacante de manera ilegal.
- Troyanos financieros

Es un tipo de malware que tiene como objetivo infectar la computadora o dispositivo del cliente para obtener información de cuentas bancarias electrónicas.

- Phishing
  Es la técnica más utilizada por los atacantes, en la que simulan el sitio web o banca virtual de la Institución Financiera para que los clientes accedan con sus credenciales y así robar la información de acceso, con la cual podrán realizar transacciones fraudulentas.
- Ingeniería social
  Es una forma de obtener información personal o privada a través de la manipulación de los clientes, una de las técnicas de ataque a clientes de instituciones financieras, más usadas dentro de la Ingeniería Social es el Phishing.
- Fraude en bancas móviles
  Dentro de esta categoría se presentan varios tipos de ataques que pueden utilizar los cibercriminales contra los clientes de las instituciones financieras que realizan sus transacciones bancarias por medio de dispositivos móviles. Entre las técnicas más utilizadas se puede mencionar:
  - Vishing Telefónico la cual se realiza por medio de mensajes de texto que envía el atacante a los clientes para que ingresen a sitios fraudulentos y obtener información de sus cuentas bancarias
  - Descarga de aplicaciones con bancas móviles falsas para capturar los datos de acceso del cliente.
  - Smishing es una técnica que utiliza mensajes SMS para solicitar a los clientes información confidencial a los clientes en nombre de la institución financiera.

2.2.2. *Ataques contra las Instituciones Financieras*

En estos tipos de ataques los cibercriminales tienen como target la Institución Financiera, tienen como objetivo vulnerar los sistemas, dispositivo o infraestructura de la empresa para poder comprometer los servicios y la información que maneja, esta clase de ataques atenta contra los principios de la seguridad de la información (integridad, disponibilidad y confidencialidad). Hoy en día existen muchas técnicas y vectores de ataques que pueden utilizar los cibercriminales contra las instituciones financieras, entre las más conocidas tenemos las siguientes:

- DDOS (Denegación de Servicios Distribuidos)
  Esta técnica de ataque consiste en afectar la disponibilidad de un servicio, servidor o infraestructura de la empresa, por medio del envío de una cantidad excesiva de

peticiones que afecten inhabiliten el objetivo. Este ataque puede realizarse de diferentes formas, como por ejemplo:

  - Saturando el ancho de banda del servidor de la empresa para que el servicio no se encuentre disponible.
  - Agotar los recursos de procesamiento del servidor o infraestructura para impedir que el servicio responda al tráfico legítimo.

- Blackmailing

  En esta técnica el atacante ha vulnerado la seguridad de la empresa y ha obtenido información sensible de sus clientes, el objetivo de este ataque es pedir a la institución financiera un valor a pagar para evitar que el atacante haga pública dicha información.

- Ataques contra los ATM y POS

  Estos ataques tienen como objetivo vulnerar la seguridad de los ATM (cajeros automáticos) y POS (dispositivos de ventas) de las instituciones financieras con la finalidad de robar información de los clientes o tener acceso a las funcionalidades de estos dispositivos y poder realizar actividades no autorizadas.

- Ataques comunes utilizados por los Hackers para vulnerar la seguridad de la infraestructura tecnológica de las instituciones financieras.

2.2.3. Enfoque para la protección en Instituciones Financieras

Considerando que las instituciones financieras son uno de los targets más populares entre los cibercriminales es necesario que la organizaciones de este sector adopten un enfoque de gestión de seguridad multicapas que ayude a minimizar el riesgo de infección tanto dentro de la organización como de los servicios que son utilizados por los clientes.

Un enfoque de seguridad multicapas puede ser aplicar un ciclo de vida para la defensa contra amenazas, el cual se encamina en prevenir, detectar, analizar y responder contra las amenazas de la actualidad. Este ciclo de vida debe ser aplicado en todos los servidores, redes y endpoints de la infraestructura tecnológica, puede ser física, virtual o en la nube (MacMillan, 2014). Ver Anexo XI.

Una de las etapas más importantes en este ciclo de vida es la de “Prevenir”, debido a que poder prevenir infecciones futuras ayudará a disminuir considerablemente el riesgo que las amenazas se materialicen, algunas formas de conseguir esto es realizando evaluaciones continuas de la infraestructura de la organización, monitorean todas las actividades, tratar posibles vulnerabilidades en los sistemas de información, establecer controles basados en la gestión de la seguridad de la información, entre otros.

2.2.4. Entidades Regulatorias en el Sector Financiero Ecuatoriano

En empresas que administran información sensible y críticas de clientes, como lo son las del sector Financiero, la gestión de la seguridad de la información es un proceso elemental que ayudará a disminuir el impacto de posibles riesgos que atenten contra los sistemas de información, considerando también la implementación de controles que cumplan con los lineamientos establecidos en normativas y regulaciones propias del País. Los Gobiernos de cada País emiten resoluciones formales de normativas y regulaciones que puedan garantizar que las actividades y decisiones tomadas por las Instituciones Financieras no puedan generar un riesgo mayor que impacte contra los ciudadanos y su bienestar económico (Evans J. D., 2015).

En Ecuador desde 1927, las operaciones bancarias de las empresas dentro del sector Financiero se encuentran reguladas por un Organismo de Control denominado Superintendencia de Bancos del Ecuador más conocida por sus siglas SBE, la cual es la encargada de supervisar y controlar las diferentes actividades que realizan las instituciones del sector financiero, de seguridad social, públicas y privadas (Superintendencia de Bancos del Ecuador, s.f.).

La Superintendencia de Bancos del Ecuador emite normativas formales que detalla los lineamientos que tienen implementar todas las Instituciones Financieras reguladas del País para las diferentes actividades y áreas que se encuentran dentro del Sector Financiero. Para la supervisión y control de las operaciones de las instituciones es realizado mediante visita in situ en las que se evalúa el grado de cumplimiento por parte de las Instituciones en base a las normativas establecidas por el Organismos de Control, tomando en cuenta entre las operaciones importante la Gestión de la Seguridad de la Información dentro de la Institución Financiera.

El Organismo de Control dentro del Libro I "*Normas Generales para las Instituciones del Sistema Financiero*" del Título X "*De la Gestión y Administración de Riesgos*" en Capítulo V "*De la Gestión del Riesgo Operativo*" se encuentra la sección VII dentro de la cual se define los lineamientos mínimos y obligatorios a cumplir por las Instituciones Financieras, relacionados con la Gestión de la Seguridad de la Información, la cual tiene como referencia el estándar internacional ISO/IEC 27000 (Resolución No. SB.2018.771, 2018).

El incumplimiento de las normativas regulatorias definidas por el Organismo de Control conllevaría a la Institución Financiera a obtener multas y sanciones sobre sus operaciones lo cual afectaría la imagen de la organización y la confianza de sus clientes.

Considerando la importancia que tiene la gestión de la seguridad dentro de las Instituciones Financieras tanto por el lado de la seguridad de sus servicios y clientes, y por el lado legal con el cumplimiento de regulaciones normativas de la Superintendencia de Bancos por parte del sector financiero, es necesario contar dentro de la Organización con un Centro de Operaciones de Seguridad que supervise y monitoree todas las actividades internas en los diferentes recursos que se mantienen para poder identificar amenazas y prevenir incidentes, en el caso de que los incidentes ocurran contar con proceso adecuado para la gestión de los mismos de manera ágil y oportuna. De esta manera se estaría cumpliendo con lo exigido por la entidad de control gubernamental de Ecuador.

2.3. Conclusiones del Contexto

La Seguridad de la Información es un proceso crítico dentro de toda Organización, incluso más para las que se encuentran dentro del sector Financiero por ser las más propensas en ser atacadas por cibercriminales.

Hoy en día muchas son cada vez más las organizaciones que se preocupan por establecer controles de seguridad tecnológicos que ayuden a aumentar el nivel de protección de su información y servicios, sin embargo, la gestión de seguridad sigue siendo un proceso que no es implementado por algunas empresas, por diferentes motivos: tamaño de la organización, falta de presupuesto económico, falta de personal especializado entre otros. Para poder conseguir un nivel de seguridad óptimo no basta con la aplicación de controles de seguridad basados en tecnología (dispositivos y herramientas), es necesario dar un enfoque a nivel de la gestión de la seguridad de la información, implementando controles basados en la gestión y monitorear las actividades, analizarlas y observar cómo interactúan entre sí.

Pero para poder lograr esto es esencial contar con un área especializada para que se dedique exclusivamente a las tareas del ciclo de vida para la defensa contra las amenazas, es por esto que la definición e implementación de un Centro de Operaciones de Seguridad dentro de una Institución Financiera es elemental para garantizar los principios de la seguridad de la información (integridad, confidencialidad y disponibilidad) en todos los sistemas, dispositivos e infraestructura de la Organización.

Un Centro de Operaciones de Seguridad no solo ayudará a la organización a aumentar el nivel de protección de sus servicios y activos de información, sino que incrementará el rendimientos de sus procesos internos, debido a que se considerará a la seguridad como un requisito principal dentro del diseño de cada proceso, producto, sistemas, herramienta o

servicio que sea utilizado dentro de la empresa, inclusive hasta en los servicios con los que interactúan sus clientes.

Cabe recalcar que disponer de un área con personal especializado en seguridad dentro de las Instituciones Financieras actualmente no es una elección a la ligera, las entidades de control como lo es la Superintendencia de Bancos del Ecuador estipulan lineamientos explícitos con los que debe cumplir cualquier organización del sistema financiero relacionados con la seguridad de la información, siendo este un punto importante a considerar en la definición e implementación de un Centro de Operaciones de Seguridad en una institución financiera.

CAPÍTULO III

3. Objetivos y Metodología del Trabajo

3.1. Objetivo General

Proponer un proceso para la definición e implementación de un Centro de Operaciones de Seguridad (SOC) en las instituciones del sector Financiero basándose en estándares y mejores prácticas relacionadas con la seguridad reconocidas a nivel mundial, para poder garantizar la protección de todos los activos de información y servicios de la empresa incluyendo los servicios que interactúan con sus clientes.

3.2. Objetivos Específicos

En este presente trabajo se establecen los siguientes objetivos específicos:

- Definir los requisitos necesarios que se deben considerar al momento de definir un SOC dentro de una Organización.
- Identificar roles y funciones que deberán poseer el personal especializado que trabaje dentro de un SOC.
- Plantear servicios y soluciones que podrían ser utilizadas para ejecutar las actividades diarias dentro de un SOC.
- Proponer métricas para la evaluación del desempeño y efectividad de las funciones que realiza un SOC dentro de una Organización.
- Analizar los lineamientos de seguridad que se encuentran detallados en los estándares y mejores prácticas actuales que se encuentran relacionadas con las funciones de un SOC.

3.3. Metodología del Trabajo

Este trabajo se lo realizará utilizando técnicas de investigación documental para poder realizar la recolección de fuente de referencia Bibliográfica, White Papers, Reportes actuales y sitios web de interés relacionados con el tema, que permitirán establecer los hecho relevantes relacionados con las generalidades y antecedentes de la línea del tema desarrollado, el marco teórico del trabajo y las fases que intervendrá para la propuesta del proceso de definición e implementación de un SOC.

También se abarcará en la investigación la información para el análisis y comparación de algunos estándares internacional como ISO/IEC 27001 y mejores prácticas para comprobar que lineamientos pueden ser aplicables en la gestión de un SOC dentro de una organización financiera, incluyendo información relevante para la definición de métricas para la evaluación del proceso propuesto.

Con esta técnica utilizada se podrá obtener información suficiente y relevante para poder analizar y proponer el proceso de implementación de un SOC dentro de instituciones financieras.

CAPÍTULO IV

4. Marco Teórico

4.1. Marco Teórico

Para poder desglosar los puntos importantes que deben ser considerados para el diseño e implementación de un Centro de Operaciones de Seguridad (SOC) es necesario primero conocer los conceptos de los términos fundamentales sobre la seguridad de la información que se encuentran relacionados con el funcionamiento y gestión de un SOC.

A continuación se desglosan la descripción de los términos más relevantes para el presente trabajo.

4.1.1. Seguridad de la Información

El activo considerado como principal para cualquier tipo de organización es la “Información”, debido a su importancia y sensibilidad es necesario que cuente con medidas de protecciones adecuadas y robustas para evitar que sea comprometida en cualquier ámbito del negocio.

Este tipo de activo puede presentarse de muchas maneras: impreso, lógico, escrito o almacenado en diferentes dispositivos informáticos, entre otros. Es por esto que todos los medios que en los que se generé, procese, gestione o almacene la información debe cumplir con requerimientos de seguridad para poder garantizar su protección.

Tal cual como lo indica el estándar internacional ISO 17799, la Seguridad de la Información consiste en proteger a la información de un amplio rango de posibles amenazas que pueden atentar contra la continuidad del negocio, de esta manera se podría minimizar el riesgo comercial y maximizar el retorno de las inversiones, de igual manera, la seguridad reside en poder preservar la confidencialidad, integridad y disponibilidad de la Información, sin dejar de lado otra propiedades como lo son la autenticidad, responsabilidad, no-repudiación y confiabilidad (ISO/IEC, 2005).

4.1.2. Propiedades de la Seguridad de la Información

Desde el punto de vista gráfico se podría ilustrar las propiedades o servicios con los que debe cumplir la seguridad de la información, de la siguiente manera:

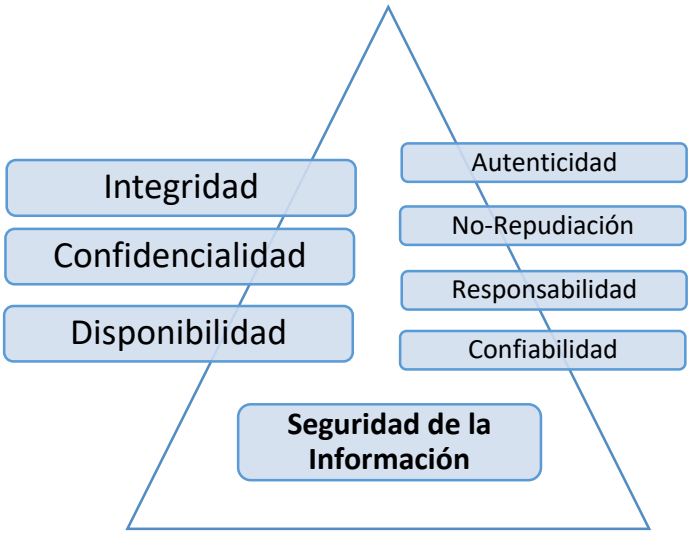


Figura 7. Definición de la Seguridad de la Información según el estándar ISO/IEC 17799

A continuación se desglosará de manera breve la descripción de cada una de estas propiedades que deben considerarse para poder alcanzar la meta principal en la seguridad de la información (Vieites, 2014).

Dentro de las propiedades antes mencionadas existen 3 que son más nombradas en el campo de la seguridad de la información, las cuales son: Integridad, Confidencialidad y Disponibilidad.

- Integridad: Esta propiedad garantiza que un mensaje o archivo de información no ha sido modificado desde su punto de origen y durante su transmisión por medio de una red informática. Este tipo de servicio ayuda a detectar posibles modificaciones o eliminación de datos que sean parte del mensaje original.
- Confidencialidad: Esta propiedad garantiza que los mensajes almacenados en un equipo tecnológico, dispositivo de almacenamiento o enviados por medio de una red informática solo puedan ser leídos por destinatarios autorizados, esto quiere decir que en caso de ser accedido por terceras personas no autorizadas el mensaje original sea incomprensible para ellos.
- Disponibilidad: Esta propiedad garantiza que los sistemas de información e infraestructura tecnológica funcione de manera correcta y se encuentre disponible para ser accedida por usuarios autorizados, por esto es necesario desarrollar e implementar sistemas robustos que puedan ser capaces de enfrentar ataques o interferencias de personal no autorizado.

Sin embargo, existen otras propiedades que son muy comunes e importantes considerar dentro de la seguridad de la información:

- Autenticidad: Esta propiedad ayuda a verificar que el emisor de un mensaje es realmente la persona correcta que originó dicho mensaje, asimismo, esto se puede aplicar a los equipos o dispositivos tecnológicos que tratan de acceder a determinadas redes o servicios de TI para comprobar su identidad.
- No-Repudiación: Esta propiedad consiste en poder implementar un mecanismo probatorio que ayude a demostrar que un determinado usuario generó y envió un mensaje para de esta forma dicho usuario no pueda negar esta acción posteriormente del envío del mensaje. Este mecanismo también puede ser utilizado para el usuario destinatario del mensaje.
- Responsabilidad: Esta propiedad o servicio también es conocido como Auditabilidad, el cual permite registrar y monitorizar el uso de distintos recursos tecnológicos por parte de usuarios previamente conectados y autorizados, de esta manera poder detectar situaciones sospechosas que podría permitir que posibles amenazas se materialicen.
- Confiabilidad: Esta propiedad es la que garantiza que las propiedades antes mencionadas se cumplen de manera correcta en los activos de información.

4.1.3. Objetivos y Controles de la Seguridad de la Información

La Seguridad de la Información está enfocada como una disciplina que se encuentra en constante evolución, debido a que es aplicada sobre los sistemas de información y dispositivos tecnológicos de las empresas. Este campo tiene como principal meta permitir que una organización, independiente de su naturaleza, cumpla con todos sus objetivos de negocio o misión, desarrollando e implementando sistemas de información que tomen en cuentan todas las amenazas y riesgos relativos a los que se encuentran expuestos las TIC de la organización, empleados, clientes, etc. (Areitio, 2008).

En el ámbito de la seguridad de la información existen muchos objetivos que deben lograr cumplirse para poder garantizar la protección de los datos, entre los cuales están:

- ✓ Asegurar el correcto uso de los recursos tecnológicos y sistemas de información de la organización por parte los usuarios.
- ✓ Identificar la mayoría de los riesgos de seguridad a los que se encuentra expuesto la organización.
- ✓ Diseñar e implementar procesos adecuados que ayuden a minimizar los riesgos de amenazas y problemas de seguridad, asimismo, como detectar y gestionar incidentes de seguridad que se puedan presentar.

- ✓ Mantener mecanismos de recuperación de los sistemas de información y recursos tecnológicos en caso de presentarse incidentes de seguridad que atenten con la continuidad del negocio.
- ✓ Garantizar el cumplimiento del marco legal establecido por el gobierno al cual se encuentra sujeto la organización.
- ✓ Cumplir con todos los requerimientos expuestos en los contratos con los clientes de la organización.

Desde el punto de vista organizacional existen cuarto planos que deben considerarse para poder alcanzar los objetivos de la seguridad de la información: técnico, legal, humano y organizativo (Vieites, 2014). En estos planos es necesario diseñar e implementar controles que ayuden a alcanzar los objetivos antes descritos:

1. Plano Humano: Es el plano que abarca todo el recurso humano con el que cuenta la organización para poder realizar sus actividades diarias, para este plano se debería diseñar controles relacionados con los empleados:
   - Impartir educación y capacitación sobre la seguridad de la información al personal de la Organización.
   - Asignación de responsabilidades del personal relacionadas con la seguridad de la información.
   - Procesos de control y monitoreo de las actividades de los empleados.
2. Plano Legal: Es el plano que está enfocado en todas la clausulas y normativas legales con la que debe cumplir la organización para poder ejercer sus funciones dentro de un determinado país:
   - Diseñar y establecer procesos y mecanismo que cumplan con lo requerido por la ley vigente del gobierno bajo el cual está sujeto la organización.
3. Plano Organizativo: En este plano se abarca todas la medidas organizativas de seguridad que deberán definirse para proteger los servicios de la organización, como por ejemplo:
   - Definir y establecer una política de seguridad de la información que este alineada con la estrategia del negocio
   - Diseñar e implementar mecanismo de contingencia y recuperación de los servicios de la organización.
4. Plano Técnico: Es el plano que abarca todos los recursos informáticos que mantiene la organización, sistemas de información, procesos, dispositivos de almacenamiento, equipos de cómputos y telecomunicaciones, entre otros:
   - Diseñar e implementar aplicaciones seguras que procesen la información de forma correcta.

- Realizar procesos de verificación y gestión de vulnerabilidades en la plataforma tecnológica de la organización.
- Mantener procesos de gestión de incidentes de seguridad y mejoras continuas en la organización.
- Implementar mecanismos de criptografía para asegurar las comunicaciones y datos de la organización.

4.1.4. Definición de Amenazas

En el campo de la seguridad informática el término "Amenaza" es comúnmente utilizado para referirse a cualquier suceso (accidental o intencionado) que ocurriese dentro de la organización y que cause un daño (material o inmaterial) ocasionando un mal funcionamiento de los servicios y procesos, lo cual resida en pérdidas monetarias, materiales e inclusive reputacionales.

Según el estándar internacional ISO/IEC 17799, una amenaza es una causa potencial de un incidente no deseado, el cual puede resultar un daño a un sistema u organización (ISO/IEC, 2005).

Existen diferentes tipo de clasificaciones de la amenazas, pueden ser por el origen, por el grado de intencionalidad o por el efecto causado.

1. Amenazas por el Origen: En esta clasificación se encuentran las amenazas de origen natural, internas y externas:
   - Amenazas Naturales: Son las amenazas que no pueden ser controladas por el ser humano, como las inundaciones, huracanes, incendios, terremotos, etc.
   - Amenazas Internas: Abarca las amenazas que pueden materializar el personal de la organización por diferentes motivos, como por ejemplo: mal uso de las herramientas informáticas, descuidos al momento de gestionar y/o procesar información de la organización, empleados descontentos con la organización, entre otros.
   - Amenazas Externas: En esta categoría se encierra todas las amenazas que son ejecutadas por personal externo a la organización o desde redes externas, como virus informáticos, ataques de DoS, intrusiones en las redes internas, ataques informáticos, etc.
2. Amenaza por el Grado de Intencionalidad: En esta clasificación se encuentran las amenazas de acuerdo al nivel de intencionalidad accidentales o mal intencionadas:

- Amenazas Accidentales: Son las amenazas que no son causadas de manera intencionadas como por ejemplo averías de hardware, fallos en software. Inclusive se puede considerar las amenazas naturales dentro de esta categoría.
- Amenazas por Errores: Son amenazas no intencionadas por errores en la ejecución, procesamiento, uso de herramientas tecnológicas y procesos de la organización. Usualmente este tipo de amenazas suceden por desconocimiento de parte del usuario o falta de capacitación por parte de la organización.
- Amenazas Mal Intencionadas: En esta categoría se encuentran todas las amenazas que están son ejecutadas con el objetivo de causar algún daño o comprometer la información de una organización.

3. Amenaza por el Efecto Causado: En esta categoría entran las amenazas de acuerdo al efecto que le causa a la víctima, como por ejemplo: robo de información, suplantación de identidad, destrucción de información, anulación de funcionamiento en sistemas de información, entre otros.

Para poder identificar las diferentes tipos de amenazas es común utilizar una escala definida por la organización para medir el nivel de ocurrencia de la misma, como por ejemplo: Baja, Media, Alta, etc. (Vieites, 2014).

4.1.5. Definición de Vulnerabilidades

El término vulnerabilidad es cualquier debilidad que pueda tener los recursos de una organización que permitan que una amenaza se materialice que cause daños y pérdidas a dicha organización. Tal como es expuesto en el estándar ISO/IEC 17799, la vulnerabilidad es la debilidad de un activo o grupo de activos que pueda ser explotada por una o más amenazas (ISO/IEC, 2005).

Las vulnerabilidades suelen estar ligadas más a ámbito organizativos como por ejemplo, procedimientos más definidos, políticas de seguridad obsoletas, fallo en los sistemas físicos y lógicos, falta de capacitación al personal para el uso de las herramientas, errores en configuraciones o instalaciones de recursos informáticos, entre otros.

Para poder definir las vulnerabilidades que pueden tener los activos de la organización se utiliza escalas para poder medir el nivel de la vulnerabilidad, como por ejemplo: Alta, Media o Baja (Vieites, 2014).

4.1.6. Definición de Incidentes de Seguridad

Se considera como incidente de seguridad como la materialización de una Amenaza, es decir, es cualquier evento que pueda producir una interrupción del funcionamiento normal de los servicios tecnológicos que ofrece la organización, dicho evento puede conllevar a pérdidas materiales y financieras.

De acuerdo a lo definido por el estándar internacional ISO/IEC 17799 un incidente de seguridad de la información es producido por un solo evento o una serie de eventos inesperados que poseen una probabilidad alta de comprometer las operaciones del negocio y amenazar contra la seguridad de la información (ISO/IEC, 2005).

CAPÍTULO V

5. Centro de Operaciones de Seguridad (SOC)

Hoy en día en común que en la mayoría de las organización se aplique el Principio de Defensa en Profundidad que consiste en el diseño e implementación de varios niveles o capas de seguridad que protejan toda la infraestructura tecnológica de la organización (Vieites, 2014), de esta manera en caso de que un atacante pueda quebrantar los primeros niveles de seguridad, los siguiente niveles retrasen el acceso a los sistemas internos de la organización y se pueda tomar medidas defensivas para evitar que el ataque pueda afectar la funcionalidad de los servicios del negocio.

Un ejemplo de un esquema general sobre el Principio de Defensa en Profundidad cuenta con las siguientes capas de protección:

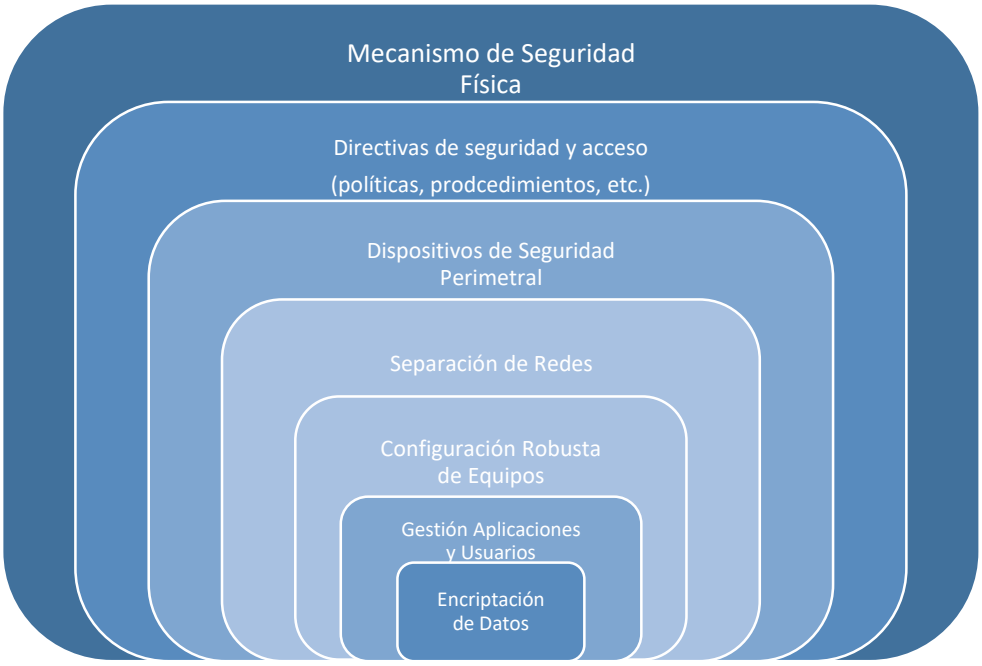


Figura 8. Esquema general del Principio de Defensa en Profundidad

Una de los puntos positivos de implementar este principio en las organizaciones es que obliga que se lleve un registro de todas las actividades que realizan en los diferentes recursos tecnológicos de la infraestructura y de los usuarios que la utiliza, adicionalmente un monitoreo constante de cada capa del esquema. Estas actividades pueden ser realizadas por el Centro de Operaciones de Seguridad (SOC).

La utilización de un Centro de Operaciones de Seguridad en una organización, es el control clave para el manejo de los riesgos cibernéticos.

A continuación se mencionará los temas principales que una organización o personal encargado de la implementación de un SOC debe considerar para el diseñe e implementación del mismo.

5.1. Definición e Importancia de un Centro de Operaciones de Seguridad

Un Centro de Operaciones de Seguridad, más conocido como SOC, es una plataforma integral que tiene el propósito de diseñar, implementar y ejecutar procesos de detección y reacción ante posibles incidentes de seguridad en las organizaciones, durante las 24 horas del día y los 7 días de la semana. Un SOC permite controlar constantemente el estado de la seguridad lógica de una organización, mediante el monitoreo en tiempo real de las actividades que se realizan en los recursos tecnológicos de la empresa, de igual manera las actividades de los usuarios que gestionan estos recursos y administrando dispositivos de seguridad perimetral para evitar que amenazas externas puedan acceder fácilmente a la red interna de la empresa.

Los SOCs proporcionan la información necesaria para que la organización pueda detectar de manera eficiente posibles brechas de seguridad y posteriormente puedan ser mitigadas mediante la implementación de controles, de esta manera se pueda reducir los tiempos de respuesta ante esta clase de eventos (Alien Vault, 2015).

Hoy en día se existen dos formas de poder utilizar los servicios de un SOC dentro de una organización:

- Diseñando e implementando un SOC dentro de la Organización como parte de la estructura jerárquica.
- Tercerizar las funciones del SOC a una empresa de seguridad para que brinde protección a la Organización.

Existen varias ventajas y desventajas de estas dos formas de utilizar los servicios de un SOC (ver Anexo I).

La solución de tercerizar las funciones de un SOC a una empresa de seguridad externa, es una forma válida de implementación utilizada, sin embargo, la organización se expone a un riesgo de seguridad al permitir que terceras personas recolecten y monitoreen los log de los recursos informáticos de la empresa. Para poder inclinarse por esta forma de implementación

hay que tener ciertos tipos de métricas definidas para controlar las actividades de la empresa externa:

- La empresa externa debe de ofrecer a la organización una interfaz virtual con información detallada sobre el servicio de seguridad que está ejecutando.
- Ofrecer varios puntos de vistas para la organización de las actividades que realiza.
- Entregar reportes periódicos de diferente tipo, como: técnicos, ejecutivos y de gestión.
- Tener un ciclo completo de "trouble ticket" y que se registre toda la información relacionada a ellos.
- SLA (acuerdos de niveles de servicios) que se encuentren bien definidos es un punto crítico.

Las organizaciones grandes en especial las que administran información sensible de sus clientes, optan por la implementación de un SOC dentro de su organigrama jerárquico para disminuir el riesgo de fuga de información, sin embargo, para poder realizar esto es necesario tener en cuenta puntos clave para hacerlo de forma exitosa:

- Personal interno entrenado
- Una buena metodología de manejo del SOC definida
- Presupuesto adecuado destinado para la implementación y crecimiento de un SOC
- Definición correcta y adecuada de los procesos del SOC.
- Un proceso integrar de respuesta a incidentes.

Es por esto que para poder comenzar a diseñar la seguridad del entorno tecnológico dentro de una organización es importante tener en cuenta ciertas preguntas básicas que permitirán conocer a fondo lo que posee la empresa y el nivel de seguridad actual:

1. ¿Qué activos debo proteger?
2. ¿Cuál de mis activos son vulnerables a ataques?
3. ¿De qué forma están siendo atacados mis activos?
4. ¿Cómo se si ha tenido lugar una brecha de seguridad?

Para poder contestar estas preguntas se puede realizar una serie actividades que nos ayudarán crear una base con la cual se podrá comenzar a diseñar la implementación del SOC y medidas de seguridad necesarias para la organización (ver Anexo II)

Las actividades mencionadas en el Anexo II pueden llegar a considerarse como las más esenciales para poder diseñar e implementar un marco de seguridad en el entorno tecnológico

de la organización, hoy en día existe un sin número de enfoques y alternativas para brindar seguridad a una empresa, sin embargo, algo en común en todos estos enfoques es que es necesario tener personal especializado en la seguridad informática que sea responsable de ejecutarlas.

Para poder realizar estas actividades de manera eficiente y adecuada es importante contar con un área dedicada a la Seguridad de la Información dentro de la organización, para poder llevar un control continuo y exhausto de las actividades que realizan los diferentes recursos, poder detectar comportamientos sospechosos que puedan incidir en una brecha de seguridad y contar con un proceso efectivo de respuesta ante los incidentes presentados.

5.2. Aspectos y Funciones de un Centro de Operaciones de Seguridad

Uno de los puntos clave para implementar un Centro de Operaciones de Seguridad es tener en claro cuáles son los aspectos con los que debe contar un SOC. Estos aspectos son los que describirán las funcionalidades del SOC, los cuales pueden ser clasificados como primarios y secundarios. Para poder diseñar correctamente desde un principio las funciones a realizarse dentro del SOC, se presentará un conjunto de aspectos considerados como la base de un Centro de Operaciones de Seguridad.

5.2.1. Aspectos Primarios de un SOC

Los aspectos primarios engloban las funciones básicas que todos los SOC de cualquier tipo de organización deben ofrecer, para poder ser considerado como un Centro de Operaciones de Seguridad (Pierre Jacobs, 2013), entre las cuales deben considerarse las siguientes:

1. Recolección de Log: Este aspecto hace referencia a la función de centralizar la recolección de los log de diferentes tipos de actividades que se realicen en los recursos informáticos como actividades administrativa, seguridad, transaccional, etc.

CAPACIDAD BAJA	CAPACIDAD ALTA
Una capacidad baja no garantizaría la recolección del log, solo realizaría el mejor esfuerzo por recolectar todos log posibles.	Una capacidad alta de recolección de log en la organización podría garantizar hasta un 99% de todos los eventos que se puedan presentar.

Tabla 4. Capacidades de Recolección de Log

2. Retención y Almacenamiento de Log: Considerado como una funcionalidad básica para los SOC, debido a que los log recolectados pueden tener información importante sobre eventos específicos para ser utilizada en el futuro.

CAPACIDAD BAJA	CAPACIDAD ALTA
Un SOC con una capacidad inferior de retención y almacenamiento de log tendrá restricciones de tiempo y espacio limitado.	Los que poseen una capacidad de mayor retención las restricciones de tiempo y espacio son mínimas.

Tabla 5. Capacidades de Retención y Almacenamiento de Log

Cabe recalcar que esta funcionalidad es exigida muchas veces por resoluciones legales y gubernamentales a varios tipos de organizaciones, por esto es necesario contar con una capacidad de retención alta para poder cumplir con los requerimientos legales de recuperación y no-repudio.

3. Análisis de Log: Este aspecto se refiere a la habilidad que el personal del SOC debe poseer para poder analizar e interpretar datos en crudo de los log y presentar los resultados del análisis de una forma entendible, utilizables y métricas adecuadas.

CAPACIDAD BAJA	CAPACIDAD ALTA
Una capacidad baja de este aspecto se basaría en presentar datos en crudo de los log con un limitado tipo de formatos y dispositivos para los resultados.	Una alta capacidad en este aspecto ofrecería como resultado del análisis, métricas y dashboard de una amplia gama de formato y tipos de dispositivos.

Tabla 6. Capacidades de Análisis de Log

4. Monitoreo de Ambientes para Eventos de Seguridad: Este aspecto hace referencia al monitoreo que se realizará para detectar posibles eventos de seguridad.

CAPACIDAD BAJA	CAPACIDAD ALTA
Una baja capacidad de este aspecto limitaría la funcionalidad del monitoreo al horario de oficina sin garantizar un tiempo reducido de respuesta	Una capacidad alta realizaría el servicio de monitoreo a modo 24x7 garantizando los tiempos de respuesta, mostrando una mejora en la seguridad de la organización.

Tabla 7. Capacidades de Monitoreo de Ambientes para Eventos de Seguridad

5. Diversidad de Dispositivos Integrados: Se refiere a los diferentes tipos de dispositivos y proveedores que pueden ser integrados y administrados por el SOC, esto también incluye como las diferentes habilidades que se mantengan en el SOC.

CAPACIDAD BAJA	CAPACIDAD ALTA
Solo podría monitorear una cantidad limitada de tipos de dispositivos o de proveedores, asimismo, carecería de habilidad para interpretar diferentes tipos de vulnerabilidades contra esos dispositivos.	Poseería una nivel de restricción casi nulo sobre los tipos de dispositivos y proveedores que se pueden integrar y monitorear, también contraría con una experiencia amplia para interpretar y entender vulnerabilidades y amenazas contra esos dispositivos

Tabla 8. Capacidades de Diversidad y Dispositivos Integrados

6. Correlación de Eventos y Flujos de Trabajo: Hace referencia a la capacidad que se tiene de correlacionar eventos de diferentes tipos de dispositivos y vendedores, como también comenzar flujos de trabajo en respuesta a la reglas de correlación que se activan.

CAPACIDAD BAJA	CAPACIDAD ALTA
Abarcará solo lo básico con reglas de correlación manuales y no contarán con la habilidad de generar flujos de trabajo.	Ofrecerá un servicio complejo y amplio de correlación de eventos con reglas automáticas integrada en sistemas de herramientas de flujo de trabajo, para dar seguimiento.

Tabla 9. Capacidades de Correlación de Eventos y Flujo de Trabajo

7. Manejo de Incidentes: Este aspecto abarca la habilidad del SOC de responder, gestionar y escalar incidentes de seguridad que se puedan presentar.

CAPACIDAD BAJA	CAPACIDAD ALTA
Una capacidad baja ofrecería la función de generar, responder y escalar a los incidentes de forma manual.	Una capacidad alta contaría con un manejo de incidentes y escalamiento automatizado e integrado a un sistema empresaria completo de gestión de incidentes

Tabla 10. Capacidades de Manejo de Incidentes

8. Respuesta ante amenazas: En este aspecto se abarca a las funciones de detectar amenazas en tiempo real y también identificar vulnerabilidades potenciales en los sistemas o dispositivos que deberán ser mitigadas de manera proactiva.

CAPACIDAD BAJA	CAPACIDAD ALTA
No tendrán la habilidad de investigación interna y de alimentación de amenazas externas.	Contará con una fuente de investigación de amenazas y vulnerabilidades automatizadas suscritas a múltiples proveedores externos.

Tabla 11. Capacidades de Respuesta ante Amenazas

9. Identificación de Amenazas: Se refiere a la capacidad del SOC para identificar amenazas y vulnerabilidades en tiempo real o también como para de una investigación.

CAPACIDAD BAJA	CAPACIDAD ALTA
Habilidad limitada para identificar amenazas y vulnerabilidades.	Contará con la habilidad de investigación y consultas en tiempo real de sistemas integrado para la gestión de amenazas

Tabla 12. Capacidades de Identificación de Amenazas

10. Reportería: Hace referencia a la capacidad de poder ofrecer distintos tipos de reportes de seguridad a los interesados.

CAPACIDAD BAJA	CAPACIDAD ALTA
Ofrecerá reportes poco personalizados, predefinidos de formatos y plataformas limitadas	Ofrecerá reportes de acuerdo a lo solicitado, con diferentes tipos de análisis de distintas plataformas y variedad de formatos

Tabla 13. Capacidades de Reportería

5.2.2. Aspectos Secundarios de un SOC

Los aspectos secundarios que un Centro de Operaciones de Seguridad puede ofrecer, engloban todas las funciones extras que se pueden realizar dentro de esta área, que no son básicas sino con un enfoque más especializado y específico, como por ejemplo:

- Análisis de malware
- Análisis y escaneo de vulnerabilidades
- Manejo de dispositivos, en especial dispositivos de seguridad
- Certificación de identidad y recertificación
- Pruebas de penetración
- Integración con controles de seguridad físico

Estos aspectos secundarios son altamente probables que cambien con el tiempo, pueden crearse más aspectos o eliminar otros, sin embargo, a diferencia de los aspectos primarios que con el tiempo mejoran pero no cambian por completo debido a que son la base de lo que representa un Centro de Operaciones de Seguridad.

5.3. Triada de las Operaciones de Seguridad

Una vez que se haya identificado lo que posee la organización, lo que se necesita en términos de seguridad y cuáles son los aspectos con los que se quiere contar dentro del SOC, es importante considerar que la implementación de un Centro de Operaciones de Seguridad requiere de una buena estrategia de colaboración y comunicación entre todas las áreas de la empresa, sus múltiples funciones, los productos de seguridad previamente utilizados y diferentes procesos y procedimientos que se mantengan en la organización.

A estos puntos se les puede dar el nombre de la Triada de las Operaciones de Seguridad, debido a que se enfoca entre aristas principales:

- Personas: Se enfoca en el personal que estará ejecutará los procesos del SOC y de las competencias que deberían poseer.
- Procesos: En esta arista se detalla todos los procesos que ejecutarán el SOC para detectar y prevenir incidentes de seguridad.
- Tecnología: Engloba las soluciones y herramientas que serán utilizadas dentro del SOC para poder realizar sus procesos diarios de monitoreo y gestión de amenazas e incidentes de seguridad.

Cada una de estas aristas encierra factores claves que deben tomarse en cuenta en el proceso de implementación de un SOC, entre los cuales se puede mencionar los siguientes:

Figura 9. Triada de las Operaciones de Seguridad

A continuación se detallará lineamientos importantes para el diseño e implementación de un Centro de Operaciones de Seguridad dentro de una organización enfocada al sector financiero.

Personal de Seguridad de un Centro de Operaciones de Seguridad

El "Personal" es la primera arista de la triada de operaciones de seguridad que es necesario definir para tener en claro los perfiles y cargos que van a integrar el personal del Centro de Operaciones de Seguridad.

Comúnmente en las organizaciones para realizar un proceso de respuesta ante incidentes de seguridad cuando no se tiene implementado un SOC, se utiliza un grupo de empleados internos que realizaran la gestión de incidentes, sin embargo, no se encuentran dedicado exclusivamente a este proceso de seguridad, de acuerdo a una encuesta de sobre Respuesta a Incidentes de seguridad realizada por SANS en el 2014 el 61.4% de los encuestado tiene un equipo imprevisto para la respuesta de incidente, mientras el 58.6% mantiene un equipo de respuesta de incidentes dedicado exclusivamente a este proceso (SANS, 2014):

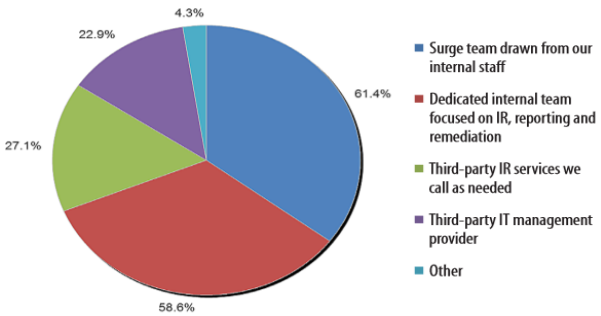


Figura 10. Encuesta sobre qué tipos de recursos utilizan las organizaciones para la respuesta de incidentes.

La carencia de un equipo dedicado y especializado para la respuesta de incidentes dentro de una organización es uno de los principales impedimentos para poder tener un proceso efectivo y adecuado, según la encuesta antes mencionada más del 50% de las industrias participantes considera la "Falta de un equipo o servicio formal de Respuesta a Incidentes" como un factor clave en un proceso deficiente para la gestión de incidentes.

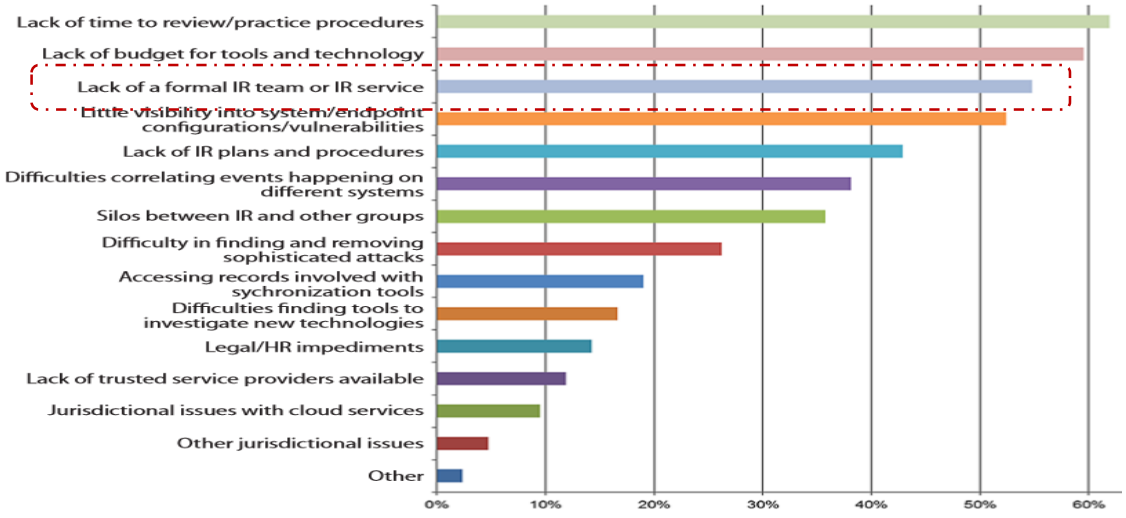


Figura 11. Encuesta sobre los principales impedimentos para un proceso efectivo de Respuesta a Incidentes.

Por esta razón, la selección de personal es paso es muy importante incluso antes de adquirir herramientas de seguridad es necesario contratar personal competente que pueda administrarlas, debido a que son ellos los que las entenderán y usarán a diario, sin olvidar de todos los procesos de seguridad que ejecutarán los cuales deberán ser realizados de manera efectiva y correcta.

Entre las varias interrogantes que se forman al momento de definir este punto, existen ciertos temas que es importante tener siempre presente:

- Los roles o cargos que se utilizarán dentro del SOC
- Las responsabilidades de cada rol que tendrán que definirse
- Cantidad de personas que integraran el equipo de trabajo del SOC
- El conjunto de habilidades que se busca

Dependiendo del tamaño y necesidades de la organización la cantidad de roles dentro de un SOC puede variar, sin embargo, es necesario tener un equipo de seguridad efectivo y bien balanceado en el que cada rol complemente y sirva de apoyo a los otros (Komand, 2016). En el presente trabajo se presentará roles que podrían utilizarse en empresa de tamaño medio a grande como por ejemplo en las Instituciones Financieras, entre los roles más utilizados en la actualidad dentro de un SOC, se puede observar los siguientes:

Figura 12. Roles de Seguridad dentro de un SOC

5.3.1.1. Rol de Analistas de Seguridad

Los Analistas de Seguridad son los roles base dentro de un SOC, son los encargado de detectar, investigar y responder ante los incidentes de seguridad que se presenten, también del monitoreo y administración de las herramientas relacionadas con estas actividades, por lo general estos cargos tienen horarios rotativos para poder ofrecer el servicio de monitoreo 24x7.

En empresas grandes es usual ver este tipo de cargo dividido en dos, como Analista de Seguridad Jr. y Analista de Seguridad Sr., debido al volumen de información a monitorear, revisar y procesar, se utiliza este esquema para distribuir las tareas y responsabilidades de manera más balanceada.

5.3.1.1.1. Rol de Analistas de Seguridad Jr.

Entre las responsabilidades y conjunto de habilidades, se nombra las siguientes:

1. Responsabilidades:
    - Monitoreo y priorización de alertas
    - Creación de alertas de monitoreo
    - Crear tickets de atención para incidentes de seguridad

- Manejo y configuración de herramientas de seguridad y monitoreo
- Investigación y respuesta ante incidentes de seguridad

2. Conjunto de Habilidades:
   - Administrador de sistemas operativos como Linux, Windows, MAC, etc.
   - Conocimientos en lenguajes de programación, como Python, Ruby, PHP, C#, Java, entre otros.
   - Conocimientos o certificaciones de seguridad, como por ejemplo CISSP, entre otros.

5.3.1.1.2. Rol de Analistas de Seguridad Sr.

Entre las responsabilidades y conjunto de habilidades, se nombra las siguientes:

1. Responsabilidades:
   - Revisar y analizar tickets de atención para incidentes de seguridad
   - Poner en práctica métodos de inteligencia en amenazas emergentes para poder detectar sistemas afectados y el alcance del ataque.
   - Planificar e implementar medidas de seguridad
   - Realizar verificaciones de riesgos de seguridad y testear procesamiento de data de los sistemas de información
   - Capacitar a personal técnico en procedimientos de seguridad de la información y redes.

2. Conjunto de Habilidades: Adicionalmente de requerir las habilidades del rol Jr. se puede requerir las siguientes habilidades adicionales:
   - Capacidad para investigar y llegar a la causa raíz de los incidentes.
   - Trabajo bajo presión.
   - Habilidades de hacker de sombrero blanco.

5.3.1.2. Rol de Ingeniero de Seguridad

Este tipo de rol se encuentra enfocado en la construcción de arquitecturas de seguridad e ingeniería en seguridad de sistemas, sin dejar de lado la documentación de requerimientos, procedimientos y protocolos de las arquitecturas y herramientas de seguridad que implementen. También puede trabajar continuamente con los grupos de desarrolladores para poder crear soluciones seguras y certificar puestas en producción.

Entre las responsabilidades y conjunto de habilidades, se nombra las siguientes:

1. Responsabilidades:
    - Crear requerimientos de seguridad para los sistemas y documentación de los mismos.
    - Definir y documentar procedimientos y protocolos de seguridad que se utilicen dentro de la organización.
    - Configuración y soporte de la infraestructura de seguridad de la empresa
    - Implementar herramientas de seguridad y dar soporte a las mismas.
    - Recomendar mejoras de herramientas de seguridad
    - Crear, probar y/o implementar planes de recuperación ante desastres de redes de telecomunicaciones
    - Automatización de procesos entre herramientas de seguridad.
    - Comunicación de incidentes de seguridad a las áreas interesadas de la organización.
    - Reportar aseguramientos y recomendaciones de mejora a otras áreas.

2. Conjunto de Habilidades: Adicionalmente de requerir las habilidades de los roles antes mencionados, se puede requerir las siguientes habilidades adicionales:
    - Conocimientos en diferentes tipos de herramientas de seguridad
    - Conocimientos en arquitectura de seguridad
    - Conocimientos en seguridad de telecomunicaciones y plataformas de TI
    - Habilidad analítica y agilidad en generación de reportes y métricas

5.3.1.3. Rol de Especialista de Análisis de Seguridad

Este rol está enfocado a una persona especializada para realizar pruebas complejas de penetración y análisis de vulnerabilidades y utilizar herramientas relacionadas con estas actividades.

Entre las responsabilidades y conjunto de habilidades, se nombra las siguientes:

1. Responsabilidades:
    - Ejecutar escaneos de vulnerabilidad en los activos informáticos de la organización de forma periódica.
    - Realizar pruebas de penetración a las redes de la organización de forma periódica y detectar puntos vulnerables.
    - Generar informes de las pruebas de seguridad que se realicen.

- Utilizando inteligencia en amenazas, identificar amenazas ocultas que no se hayan identificado en revisiones generales.
- Pruebas de penetración en sistemas de producción para validar la resiliencia e identificar puntos débiles a mitigar.
- Recomendar la optimización de herramientas de monitoreo de seguridad basadas en la identificación de amenazas.

2. Conjunto de Habilidades: Adicionalmente de requerir las habilidades de los roles antes mencionados, se puede requerir las siguientes habilidades adicionales:

- Utilizar herramientas para visualización de data como por ejemplo Maltego
- Experiencia en uso de herramientas para escaneo de vulnerabilidades y pruebas de penetración.

5.3.1.4. Rol de Jefe de SOC

Este rol es el encargado de liderar el Centro de Operaciones de Seguridad y el equipo de seguridad que trabaja dentro de él, adicionalmente, involucra la visión de crear, contratar y/o construir procesos relacionados con la seguridad. La persona que mantenga este cargo debería poseer una experiencia significativa con el manejo de equipos de seguridad y tener la habilidad de proveer tanto orientación técnica y supervisión gerencial.

Entre las responsabilidades y conjunto de habilidades, se nombra las siguientes:

1. Responsabilidades:
   - Supervisar todas las actividades del SOC
   - Proveer visión y estrategia para el equipo de trabajo, procesos y tecnología
   - Contratar personal de seguridad y supervisar crecimiento profesional.
   - Definir alertas y manejar procedimientos.
   - Desarrollo de planes de respuesta ante incidentes.
   - Desarrollo programa de manejo de vulnerabilidades
   - Analizar y optimizar flujos de trabajo incluyendo la automatización de los mismos
   - Comunicar necesidades de seguridad a las áreas interesadas de la organización
   - Manejo de presupuesto para gastos de seguridad (esto puede requerirse en caso de no haber un CISO definido).
   - Desarrollo y ejecución de planes de comunicación de crisis al CISO y otros interesados.
   - Generar reportes para ayudar a la auditoría de procesos.

- Definir métricas para medir el rendimiento de un SOC.

2. Conjunto de Habilidades: Adicionalmente de requerir las habilidades de los roles antes mencionados, se puede requerir las siguientes habilidades adicionales:

- Fuerte habilidad de liderazgo
- Habilidades de comunicación con diferentes niveles jerárquicos.

5.3.1.5. Rol de CISO

El rol de CISO dentro de una organización, es la máxima autoridad jerárquica en materia de seguridad de la información. Esta persona es la responsable de definir toda la postura de seguridad de la organización, está enfocado en planear estrategias, programas, políticas y procedimientos para proteger los activos de la organización.Dependiendo del organigrama jerárquico, el rol CISO reporta directamente al CEO o CIO de la organización, por lo cual es él quien transmite las necesidades e intereses del equipo de seguridad a la parte gerencial de la empresa.

Entre las responsabilidades y conjunto de habilidades, se nombra las siguientes:

1. Responsabilidades:
   - Supervisa el programa completo de seguridad
   - Desarrolla estrategias generales de seguridad
   - Comunica la importancia de la seguridad al equipo ejecutivo de la organización.
   - Alinea los objetivos de la organización con los de seguridad.
   - Supervisa los requerimientos de cumplimiento de diferentes entes certificadoras
   - Define el plan de continuidad de negocio
   - Desarrolla el plan para evitar la pérdida de información y prevención de fraude
   - Administración del presupuesto para gastos de seguridad
   - Maneja asuntos de privacidad.

2. Conjunto de Habilidades: Adicionalmente de requerir las habilidades de los roles antes mencionados, se puede requerir las siguientes habilidades adicionales:
   - Habilidad para manejar personal
   - Tener conocimiento técnicos
   - Comprender las implicaciones del negocio
   - Tener una extensa experiencia en seguridad y/o manejo de operaciones de TI

Un Centro de Operación de Seguridad, es un área independiente del resto de áreas dentro de la organización, debido a que monitorea y supervisa las actividades de todas las áreas de la empresa. Desde el punto de vista del organigrama jerárquico de una organización estos roles se encuentran definidos de la siguiente manera:

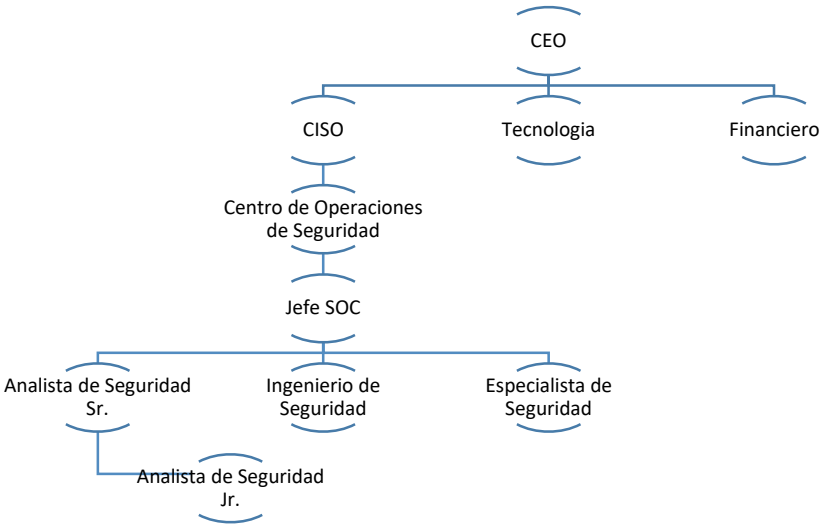


Figura 13. Situación en el organigrama jerárquica de los roles del SOC

Esta ubicación puede variar de acuerdo a la organización y su esquema jerárquico, sin embargo, es común y recomendado que el área del Centro de Operaciones de Seguridad sea un área independiente del resto de áreas para evitar colisiones o conflictos.

5.3.2. Procesos y Procedimientos de un Centro de Operaciones de Seguridad

Es importante diseñar y definir procesos para la detección y gestión de los incidentes de seguridad para poder estandarizar de esta manera todas las actividades que se realicen dentro de ellos y así evitar que tareas claves puedan ser obviadas por la falta de un trabajo estructurado y documentado.

Estos procesos pueden ser en esquemas de ciclos repetitivos que pasen por los diferentes niveles de atención que se encuentren establecidos dentro del SOC, esto más el uso de flujo de trabajo para la gestión de incidentes ayuda a que los recursos del área sean utilizados de manera eficiente.

Cada organización puede crear un esquema para la gestión de incidentes de acuerdo a sus necesidades, sin embargo, es común que la mayoría de estos esquemas usen como base el modelo de la NIST.SP.800.61r2 del departamento de comercio de los Estados Unidos (NIST

- Cichonski Paul, Millar Tom, Grance Tim, Scarfone Karen, 2012), el cual mantiene las siguientes fases generales:

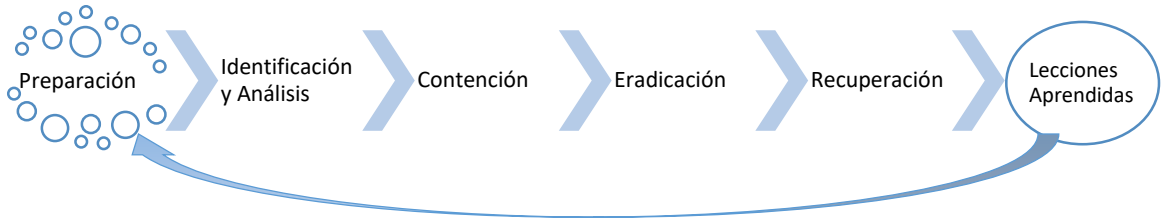


Figura 14. Fases del modelo NIST.SP.800.61r2

Estas fases pueden tomarse como un modelo general para sobre el crear su propio esquema para la gestión de los incidentes. Para el presente de trabajo utilizaremos estas fases para poder diseñar el proceso de la gestión de incidentes de la organización.

5.3.2.1. Fase de Preparación

La fase de preparación es una de las principales utilizadas diferentes metodologías relacionadas con la gestión de incidentes. En esta fase tiene como objetivo poder establecer un proceso de respuesta ante incidentes óptimo para que la Organización este lista ante la manifestación de los mismos, pero también se enfoca en la prevención de incidentes de seguridad por medio del aseguramiento de los sistemas, redes, aplicaciones, entre otros activos informáticos de la empresa.

5.3.2.1.1. Puntos Relevantes en el diseño de un Procedimiento de Gestión de Incidentes

Para poder definir un procedimiento ágil sobre la gestión y respuesta ante incidentes de seguridad es necesario establecer puntos importantes que serán utilizados durante el manejo de un incidente, como por ejemplo:

HERRAMIENTAS Y RECURSOS PARA LA GESTIÓN DE INCIDENTES	EJEMPLOS DE HERRAMIENTAS Y RECURSOS A DEFINIR
Herramientas para el manejo de comunicaciones durante la gestión del incidente: En esta sección se debe determinar cuáles serán los medios que se utilizarán para poder establecer comunicación	• Información de contacto almacenada de diferentes responsables internos o externos a la organización en caso de algún incidente • Información de escalamiento en diferentes áreas de la organización. • Mecanismos para reportar la presencia de un incidente a las personas interesadas en la organización. Esto puede ser mediante correo electrónico, sistemas gestores de incidentes, vía telefónica, etc.

HERRAMIENTAS Y RECURSOS PARA LA GESTIÓN DE INCIDENTES	EJEMPLOS DE HERRAMIENTAS Y RECURSOS A DEFINIR
durante la gestión de un incidente con los diferentes grupos de trabajo.	• Herramientas para seguimiento de tickets relacionados con el incidente para poder registrar todas las actividades realizadas, personal involucrado y tiempo de atención. • Instalaciones de almacenamiento de seguridad para poder guardar cualquier información sensible o evidencias de seguridad que hayan sido obtenidas durante la gestión del incidente
Herramientas de Hardware y Software para el análisis de los incidentes: Se refiere a todas las herramientas tecnológicas que serán necesarias utilizar para la gestión del incidente.	• Recursos de hardware necesarios para la gestión de un incidente como laptops, impresoras portables, servidores y dispositivos de red (físicos y virtualizados) para ser utilizados como equipos de pruebas o para restaurar respaldos, dispositivos de almacenamiento portátil para almacenar información, estaciones de trabajo especializadas para realizar actividades forenses y respaldos de dispositivos. • Herramientas informáticas para analizar protocolos de comunicación y sniffers para capturar el tráfico de la red. • Herramientas forenses digitales para analizar discos de equipos, entre otras actividades.
Recursos de información para análisis de incidentes: Se enfoca en la información que será necesaria revisar durante la gestión del incidente. Esta información debe estar actualizada y legible para poder identificar posibles afectados y puntos de contagio durante la presencia del incidente.	• Documentación de sistemas operativos, aplicaciones, protocolos, antivirus y detección de intrusos que son utilizados en la organización. • Lista de puertos que utiliza la organización incluyendo puertos utilizados como “caballo de troya”. • Lista de activos críticos y diagrama de red de la organización. • Líneas bases de las configuraciones actualizadas de sistemas operativos, dispositivos de red, aplicaciones, etc. • Hash criptográficos de archivos cifrados para poder realizar el análisis de los mismos de manera más rápida.

Tabla 14. Ejemplos de Herramientas y Recursos para la Gestión de Incidentes

5.3.2.1.2. Prácticas de Aseguramiento como parte de la prevención de incidentes

Debido a que durante esta fase de preparación también se enfoca en la prevención de incidentes de seguridad es necesario realizar un proceso de aseguramiento de los principales activos informáticos. Aunque el personal que conforma el Centro de Operaciones de Seguridad no es el responsable de realizar los aseguramientos de las diferentes plataformas,

si son responsables por definir, verificar, comunicar y sugerir varias prácticas de seguridad que pueden ser utilizadas en el proceso de aseguramiento.

En la fase de preparación el personal del SOC puede realizar ciertas actividades para poder identificar problemas y detectar brechas de seguridad que normalmente pasarían desapercibidas por otras áreas, existen prácticas de seguridad que son comúnmente usadas y son recomendadas por su efectividad. Para más detalle de estas prácticas ver Anexo III.

5.3.2.2. Fase de Identificación y Análisis

Esta fase se enfoca en recomendar mejores prácticas para poder manejar los incidentes de manera ágil, sin embargo, para muchas organizaciones el proceso de identificar y evaluar con precisión los posibles incidentes es difícil, debido a que es necesario determinar si el incidente ha ocurrido y de ser así identificar el tipo, la extensión y magnitud del problema.

Para poder realizar este proceso de manera precisa es necesario tomar en cuenta ciertos puntos como:

- Un incidente puede detectarse por medio de varios mecanismos, como por ejemplo mediante el uso de herramientas automatizadas como IDS (hosts o red), antivirus, monitoreo de log, entre otros, asimismo, se pueden identificar de manera manual mediantes el reporte de problemas por parte de los usuarios de la empresa.
- Se debe considerar que por lo general el volumen de posibles señales de incidentes es alto.
- Es necesario contar con personal con conocimientos especializados y experiencia para poder realizar un análisis adecuado de la información relacionada con el incidente.

5.3.2.2.1. Herramientas y Recursos para detectar señales de Incidentes

Como anteriormente se ha mencionado hoy en día es común tener varias fuentes para poder detectar señales de posibles de incidentes de seguridad, estas pueden ser de varios tipos, por esta razón a continuación mencionaremos cierto tipos de herramientas que pueden ser utilizadas durante esta fase para la identificación de posibles incidentes.

- Herramientas automatizadas de alertas: Este tipo encierra la mayoría de herramientas con funcionalidades de seguridad que generan alertas de actividades sospechosas, como por ejemplo:

HERRAMIENTA	DESCRIPCIÓN
IDPSs **Intrusion Detection and Prevention System**	Esta herramienta se enfoca en detectar actividad sospechosa y registrar su información en su base de datos como por ejemplo, tipo de ataque, direcciones IP, nombre de usuarios, entre otras cosas. También trabajan con firmas de ataques las cuales son utilizadas para monitorear actividad sospechosa y compararla con las firmas para comprobar que existen coincidencias, es necesario utilizar base de firmas actualizadas constantemente para tener una herramienta más confiable. Una de las particularidades de este tipo de herramientas es que suelen generar varias alertas de falsos positivos lo que conlleva que siempre se debe hacer un proceso manual de verificación de estas alertas por parte del personal del SOC encargado de la herramienta.
SIEMs **Security Information and Event Manager**	Este tipo de herramienta recolecta los log de varios dispositivos tecnológicos como servidores, bases de datos, sistemas operativos, dispositivos de comunicación, aplicaciones, entre otros; y genera su análisis y alertas mediante el monitoreo de los log de eventos y actividades de los diferentes recursos informáticos que posee la organización.
Software de Antivirus y Spam	El antivirus evita que estaciones de trabajo, servidores y otros dispositivos puedan contagiarse de malware, para esto la herramienta utiliza una base de virus para comparar contra los archivos de cada equipo, por esto es importante tener una base actualizada de virus para poder detectar y detener de manera efectiva el malware. La herramienta antispam ayuda a evitar que usuario considerado como spam llegue a los buzones de los empleados que usualmente contiene malware, ataques Phishing, entre otros.
Software validador de Integridad de Archivos	Esta herramienta puede detectar cambios en archivos importantes dentro de los equipos realizados durante el incidente. Utilizan algoritmos criptográficos para obtener un checksum por cada archivo importante, en caso de que el checksum haya sido alterado puede corresponder que el archivo ha sido alterado de manera maliciosa.

Tabla 15. Herramientas de Seguridad automatizadas de alertas

- Log de eventos y actividades: Se refiere a archivos de auditoría donde se registrará todas las actividades y eventos ejecutados sobre un equipo, dispositivo, sistema operativo, base de datos u otro recurso informático. Este tipo de fuente es importante debido a que puede proveer información relevante que ayudará a la solución del incidente. Entre los tipos de log se puede mencionar:

TIPO LOG	DESCRIPCIÓN
Log de Sistemas Operativos, Servicio o Aplicaciones	Este tipo de log es uno de las primeras fuentes que suele revisarse para poder identificar un posible incidente, debido a la información que almacena se puede obtener datos como por ejemplo, cuentas a la que se tuvo acceso, que tipo de acciones ejecutaron. De la misma manera, los log pueden ser utilizados por varias herramientas para correlacionar eventos durante la fase de análisis. Como buena práctica las organizaciones deberían definir una línea base sobre la configuración mínima de log a registrarse en todos recursos informáticos y en los activos considerados como críticos una línea base con una configuración que registre la mayoría de los eventos.
Log de Dispositivos de Red	Son útiles los log de dispositivos como firewalls o routers para proveer un poco de información de la naturaleza de la conexión sospechosa, asimismo, este tipo de log suelen ser usados para correlacionar eventos.

Tabla 16. Tipo de Log de Recursos Informáticos

- Información pública disponible: Este tipo de fuente es más de carácter investigativo por parte del personal del SOC. Para poder estar preparado para detectar y analizar posibles incidentes es necesarios conocer las vulnerabilidades y exploits recientes que puedan afectar a nuestra empresa, existen algunos tipos de organizaciones que pueden proveer información actualizada de manera periódica:
    - NVD (The National Vulnerability Database) la cual posee información sobre vulnerabilidades conocidas.
    - US-CERT33 y CERT®/CC puede proveer información sobre nuevas amenazas periódicamente.
- Personas: Esta fuente se basa en los reportes que puede realizar las personas sobre la funcionalidad de algún servicio de la empresa, los cueles pueden ser de personal interno como los empleados o externos como los clientes o proveedores. Es importante de verificar los reportes de problemas por parte de los usuarios y también obtener información de los mismos sobre el problema, la cual podría ayudar en el proceso de análisis de incidentes.

5.3.2.2.2. Actividades importantes dentro del proceso de Análisis de Incidentes

Es necesario contar un personal bien capacitado y con experiencia en el campo de seguridad para evitar el proceso de análisis de los incidentes se realizado de manera ineficiente y se comentan errores costosos, para esto el grupo de trabajo debe de trabajar de manera rápida

analizando cada incidente siguiendo un proceso predefinido y documentado en cada paso que den. Cuando se el personal crea que ha identificado un incidente es importante realizar un análisis inicial que ayude a determinar el alcance del mismo, quien o que lo genero, como sucedió, de esta manera contar con información suficiente para poder priorizar el incidente y definir actividades posteriores a realizarse. Para ayudar a que el proceso de análisis sea más efectivo y ágil se podría realizar las siguientes actividades:

- Perfilar sistemas y redes
- Tener conocimiento del comportamiento normal
- Crear una política de retención de información
- Realizar correlación de eventos
- Mantener el reloj de todos los Hosts sincronizado
- Utilizar motores de busque de internet
- Ejecutar Sniffers o Recolectar datos adicionales
- Filtrar Datos
- Buscar asistencia de otros.

Para un mayor detalle de estas actividades ver el Anexo IV.

5.3.2.2.3. Documentación en la gestión del Incidente

Otra actividad importante durante esta fase es la documentaciones de toda la información encontrada desde las diferentes fuentes utilizadas, todos los pasos dados desde la detección hasta la solución final debe ser documentado y registrado con hora y fecha, asimismo, cada documento relacionado debe ser registrado y firmado por el responsable del análisis. Este tipo de documentación podría ser útil en caso de ser necesario realizar un proceso legal.

Para que el personal del SOC pueda mantener información sobre el estado y actividades realizadas durante la gestión del incidente es común que se utiliza herramientas automatizadas para gestionar los tickets de incidentes, sin embargo, considerar que en estos sistemas se pueda almacenar como mínimo la siguiente información:

- El estado actual del incidente
- Un resumen de la actividades del incidente
- Señales e indicadores relacionados con el incidente
- Acciones ejecutadas por el responsables de la gestión del incidente
- Cadena de custodia de las evidencias, en caso de ser aplicable
- Evaluación de impacto del incidente

- Lista de evidencia recolectada durante la gestión
- Comentarios de los responsables de la gestión
- Próximas tareas a realizarse para la solución del incidente

Cabe mencionar que toda esta información es importante que se registrada con la hora y fecha para poder evaluar que la gestión del incidente fue realizada de manera pronta y eficaz.

5.3.2.2.4. Priorizar Incidentes

Una medida para que el proceso de gestión de incidentes sea eficaz es de poder priorizar los incidentes de manera correcta, debido a que no es recomendable gestionar los incidente de acuerdo a como se registren. Para poder realizar este proceso de priorización se puede considerar los siguientes factores:

FACTORES	DESCRIPCIÓN
Impacto funcional de Incidente	Esto se refiere al impacto que tendría el incidente en las funciones del negocio, es necesario que los responsables de la gestión evalúen este factor para poder priorizar el incidente, tomando en cuenta el impacto actual a las funciones del negocio y el impacto que conllevaría no poder solucionar el incidente rápidamente.
Impacto del incidente sobre la información	Los responsables de la gestión del incidente necesitan evaluar el impacto en la filtración de la información que puede haber causado el incidente de esta manera ver el nivel de afectación con los clientes, empleados o hasta el mismo negocio en caso de haber sido comprometida información crítica para la organización.
Recuperación del Incidente	El tamaño del incidente y los tipos de recursos afectados determinara la cantidad de tiempo y esfuerzo que se deberá emplear para recuperarse del incidente. El personal del SOC debe considerar al momento de priorizar el esfuerzo necesario que se necesitará para que la organización se recupere del incidente y compararlas cuidadosamente contra el costo la recuperación.

Tabla 17. Factores a considerar para Priorizar Incidentes

Dentro de cada factor antes mencionado las organizaciones pueden definir una tabla con diferentes niveles de categoría para poder evaluar los incidentes de acuerdo a cada factor, el estándar NIST.SP.800 propone pre establecidas para la evaluación (NIST - Cichonski Paul, Millar Tom, Grance Tim, Scarfone Karen, 2012), ver Anexo V:

5.3.2.2.5. Notificación de Incidentes

Como actividad final después del análisis y priorización del incidente, es necesario comunicarlo a todo el personal involucrado e interesado para que cada uno pueda realizar su rol durante la gestión del incidente. Dentro de las políticas de respuesta a incidentes la organización necesita definir los lineamientos para la notificación de los incidentes como por ejemplo la información mínima a notificar, a quien será necesario notificar y tiempos para notificar.

El personal a quien se notificará y el medio que se utilice para notificar la información del incidente pueden variar de acuerdo a cada organización y sus necesidades, pero generalmente se incluye los siguientes puntos:

PERSONAL A NOTIFICAR	MEDIO DE NOTIFICACIÓN
1. CEO 2. Responsables de la seguridad de la información 3. Equipos de respuesta de incidentes externos 4. Dueño del sistema o recurso afectado 5. Recursos humanos 6. Relaciones publicas 7. Departamento legal	1. Correo electrónico 2. Sitio web (interno, externo o portal) 3. Llamadas telefónicas 4. Personalmente 5. Escrito en papel

Tabla 18. Personal a notificar y medios de notificación sobre Incidentes.

5.3.2.3. Fases de Contención, Erradicación y Recuperación

Una vez que se ha identificado, analizado, priorizado y notificado el incidente, es necesario realizar actividades que ayuden a contenerlo para evitar que pueda generar un daño mayor al ya hecho y poder restablecer el funcionamiento normal de los servicios afectados.

5.3.2.3.1. Proceso de Contención de Incidentes

Un proceso importante dentro de esta fase es el proceso de contención para evitar que un incidente puede causar un daño superior, aunque algunos incidentes puede que no necesiten un proceso de contención es recomendable que las Organizaciones cuenten con una estrategia de contención de incidentes, debido a que en este proceso parte esencial es la toma de decisiones como por ejemplo dar de baja recursos, parar servicios, eliminar archivos, entre otros. La toma de decisiones se vuelve más sencilla de realizar si se cuenta con un proceso o estrategia para la contención de incidentes, es por esto que es importante definir una que esté alineada a las necesidades del negocio y los recursos que manejan.

Para poder establecer un procedimiento de contención de incidentes comúnmente es definido de acuerdo al tipo de incidente que se está gestionando, por esto es útil diseñar diferentes tipos de estrategia de contención para los tipos de incidentes más importantes que cuenten con una documentación suficiente que ayude al proceso de toma de decisiones a que sea ágil, adecuado y acertado. Dentro de cada estrategia se podría definir esta información como punto de partida, la cual podría irse aumentando de acuerdo al paso de tiempo y experiencia del personal del SOC:

- Daño potencial del incidente hacia los recursos de la organización
- Necesidad de preservación de evidencias
- Disponibilidad de los servicios
- Tiempos y recursos necesarios para poder aplicar la estrategia de contención
- Nivel de efectividad al aplicar la estrategia de contención
- Duración del proceso de solución

Cabe recalcar que no todos los incidentes pueden ser contenidos, se pueden presentar incidentes que al momento de aplicar una estrategia de contención pueden causar más daño de lo esperado, es por esto que es necesario que el personal del SOC primero analice si es factible aplicar una estrategia de contención al incidente.

5.3.2.3.2. Recolección y Manejo de Evidencia

Para poder resolver un incidente es necesario recolectar evidencia para poder descubrir la causa raíz del problema, sin embargo, otro punto importante para realizar esta actividad es que puede ser necesario por cualquier proceso legal que dicho incidente pueda disparar. Es por esta razón que es importante contar con procedimiento para la recolección, manejo y preservación de las evidencias ya sean físicas o digitales, dicho procedimiento deberá definir formularios de cadena de custodia para poder controlar que personas manejar la evidencia y los diferentes lugares donde la mantuvo.

Actualmente existen muchos procedimientos para manejo de evidencia, entre los cuales se puede recomendar los siguientes:

- Normativa ISO/IEC 27037: Esta normativa divide el proceso de adquisición de evidencia en diferentes tipos como adquisición de evidencia de dispositivos prendidos, apagados, dispositivos críticos, dispositivos de almacenamiento, entre otros (ISO/IEC, 2012).

- NIST SP 800-86, Guía para integrar técnicas forenses en la gestión de incidentes: provee información para poder establecer un proceso forense dentro de una organización, dentro de la cual se centra en técnicas forenses para equipos de cómputos y también es aplicable a otro tipo de sistemas y recursos (NIST - Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang, 2006).

De acuerdo a la normativa que la organización escoja para poder diseñar su procedimiento de manejo de evidencia, se puede crear un log detallado para todas las evidencias que se recolecten.

5.3.2.3.3. Identificación de Hosts Atacantes

Esta actividad no suele ser prioridad dentro de esta fase, debido a que consume tiempo y recursos que pueden ser utilizados para la contención, erradicación y recuperación del incidente, sin embargo, esta tarea puede ayudar a que la organización pueda reconocer al hosts atacante en posibles incidentes futuros o a bloquearlos para evitar otros incidentes.

Entre las actividades comúnmente utilizadas para identificar hosts atacantes que se pueden realizar dentro de un SOC, tenemos:

- Validar la dirección IP del Hosts atacante.
- Investigar por medio de motores de búsqueda más información sobre el Hosts atacante utilizando la dirección IP identificada.
- Utilizar base de datos de incidentes de otras organizaciones o comunidades de seguridad para poder obtener información del Hosts atacante

5.3.2.3.4. Erradicación y Recuperación del Incidente

De acuerdo al incidente o a la Organización la erradicación se puede realizar con un proceso separado de la recuperación o puede ser incluido dentro del proceso de recuperación, no obstante, es necesario realizar un proceso de erradicación para poder eliminar todos los componentes que causaron el incidente como por ejemplo eliminar archivos, bloquear usuarios comprometidos, identificación de vulnerabilidades, etc. Es de suma importancia que durante el proceso de erradicación se identifiquen todos los Hosts afectados para poder erradicarlos y evitar que componentes del incidente permanezcan y den oportunidad a un nuevo incidente.

En el proceso de recuperación está enfocado en que los administradores de los sistemas puedan restablecer sus operaciones a un funcionamiento normal y remediar vulnerabilidades

descubiertas para evitar incidentes similares en un futuro. Entre las actividades más comunes para la recuperación se puede realizar restauraciones de respaldos, restaurar equipos desde cero con configuraciones de seguridad predefinidas, instalar parches, cambiar contraseñas, etc. Es normal que se comiencen a monitorear sistemas o redes críticas afectadas después de un incidente, debido a que si un recurso fue atacado exitosamente una vez, es frecuente que sea un blanco para un próximo ataque.

Para incidentes con nivel de afectación alto, el proceso de recuperación puede tomar hasta meses de ejecución, es por esto que es necesario que el personal de responsable defina tareas a corto, mediano y largo plazo para realizarlo y de esta manera realizar la recuperación del funcionamiento normal de los servicios de la organización y prevenir incidentes futuros. Es necesario que estas tareas sean gestionadas y monitoreas para poder alcanzar una recuperación total del incidente.

5.3.2.4. Fase de Lecciones Aprendidas y Mejoras Continua

La fase final dentro del ciclo de la gestión de incidentes es por lo general omitida en algunas organizaciones, la cual se enfoca en el aprendizaje y mejoramiento de los procesos. Después de la gestión de cada incidentes es recomendable que los involucrados se tomen un tiempo para poder analizar y definir las lecciones aprendidas en el incidente, en especial los que son considerados como incidentes con un nivel de afectación alto, esto podría ser muy útil en mejorar las medidas de seguridad y el proceso de gestión de incidentes dentro de la Organización.

Para poder almacenar la información sobre las lecciones aprendidas de cada incidente se puede hacer uso de herramientas automatizadas para poder acceder a esta información de manera más ágil y organizada.

En esta última fase es recomendable utilizar la data obtenida de la gestión del incidente para poder estudiar sus características el cual podría conllevar a identificar vulnerabilidades y amenazas de seguridad sistemáticas, de igual manera esta información podría ser utilizada en las evaluaciones de riesgos para poder guiar la selección e implementación de controles de seguridad necesarios para evitar nuevos incidentes. Otra forma de utilizar esta información es para la verificación de indicadores de desempeño tanto del personal de respuesta ante incidentes y del proceso en sí. Entre las diferentes métricas que pueden utilizar la información de incidentes recolectada, se encuentran las siguientes:

- Número de incidentes gestionados en un período de tiempo, esta medida podría ayudar dar a conocer la cantidad de trabajo que el equipo de respuesta de incidentes

debe realizar en la gestión de cada uno. Es recomendable realizar este tipo de métrica de acuerdo a la categoría de cada incidente, debido a que ciertas categorías son más complejas que otras.

- Tiempo de gestión por incidente, este tipo de métrica puede variar porque existen diferentes formas de medición de tiempo, como por ejemplo:
    - Cantidad total de tiempo trabajado en el incidente
    - Tiempo transcurrido desde el inicio del incidente hasta el descubrimiento
    - Tiempo transcurrido desde la evaluación inicial de impacto hasta cada etapa del manejo del incidente
    - Tiempo que se tomó el equipo de respuesta en responder el reporte inicial del incidente
    - Tiempo que tomó en reportar el incidente a la administración o a entidades externas
- Evaluación de objetivos de cada incidente, es una métrica que determina cuan efectivas fueron las acciones tomadas, como por ejemplo:
    - Revisión de log, formularios, reportes u otra información del incidente para establecer políticas y procedimientos de respuesta del incidente
    - Identificar cuáles fueron los indicadores de los incidentes grabados para determinar el nivel efectividad de registro de identificación del mismo.
    - Determinar si el incidente causaría daño antes de ser detectado.
    - Determinar si la causa del incidente fue detectada, el vector de ataque, vulnerabilidades explotadas, etc.
    - Determinar si es un incidente recurrente
    - Calculo estimado de daño monetario potencial de cada incidente
    - Medir la diferencia entre la evaluación de impacto inicial y la evaluación de impacto final.

Como una manera adicional las organizaciones pueden también encontrar útil realizar auditorías periódicas sobre el proceso de respuesta ante incidentes para poder identificar problemas o deficiencias que puedan ser corregidas. Estas auditorías eberían evaluar los siguientes puntos:

- Políticas, procedimientos, planes, entre otros relacionados con la respuesta ante incidentes
- Herramientas y recursos que se utilizan durante la gestión del incidente
- Modelo y estructura del equipo de respuesta
- Educación y entrenamiento sobre el manejo de incidentes

- Documentación y reportes de incidentes
- Las medidas o métricas utilizadas para evaluar la efectividad del proceso.

5.3.2.5. Checklist general para acciones dentro de la Gestión de Incidentes

La guía de manejo de incidentes de NIST, sugiere el uso de un checklist de verificación donde se encuentren todos pasos generales que deben realizarse dentro de cada fase del proceso de gestión de incidentes (NIST - Cichonski Paul, Millar Tom, Grance Tim, Scarfone Karen, 2012), ver Anexo VI, el cual se enfoca en las acciones más relevantes de las últimas 3 fases del proceso.

5.3.3. Herramientas Tecnológicas de un Centro de Operaciones de Seguridad

Otro punto importante dentro de la triada de operaciones de seguridad es la Tecnología que se enfoca en las herramientas y recursos informáticos que se utilizaran dentro del Centro de Operaciones de Seguridad para poder realizar sus tareas diarias para la gestión de incidentes de seguridad.

A continuación presentaremos un listado de herramientas que serían útiles para el personal de un SOC de acuerdo a las etapas del proceso de gestión de incidentes, nos enfocaremos en las fases de Detección y Análisis; Contención, Erradicación y Recuperación de incidentes.

5.3.3.1. Herramientas útiles para la fase de Detección y Análisis de Incidentes

Como en capítulos anteriores se han mencionados tipos de herramientas que pueden ser útiles durante la ejecución de esta fase, sin embargo, en este apartado se enlistarán ejemplos de herramientas que pueden ser utilizadas de acuerdo a la actividad que se realice:

5.3.3.1.1. Herramientas de monitoreo de seguridad

Estas herramientas son útiles para identificar comportamiento anormal o sospechoso que pueda necesitar una investigación, entre ellas tenemos:

- SIEM, Administración y Análisis de Log: Debido a que los log son la fuente de información con mayor valor, es necesario contar con herramientas que ayuden a recolectarlo, centralizarlo e interpretar su contenido, de esta manera la acción de correlacionar eventos se volverán más sencilla de realizar.
  Una de las herramientas que ayuda a realizar estas actividades son las SIEM (Security Information and Event Management), sin embargo, actualmente existe diferentes herramientas de este tipo que varían según el costo y sus funcionalidad. Las

herramientas de tipo SIEM más utilizadas en la actualidad son las siguientes (Robb, TOP 10 SIEM Product, 2018):

- Splunk Enterprise Security (ES)
- LogRhythm SIEM
- AlienVault Unified Security Management (USM)
- Micro Focus ArcSight
- Micro Focus Sentinel Enterprise
- McAfee Enterprise Security Manager (ESM)
- Trustwave SIEM Enterprise and Log Management Enterprise
- IBM Security QRadar
- RSA NetWitness Suite
- SolarWinds Log & Event Manager

El website eSecurity Planet realiza un cuadro comparativo de todas estas herramientas de acuerdo a los puntos más relevantes como Bloqueo de amenazas, fuentes integradas, desempeño, valor, implementación, administración, soporte y escalabilidad (Robb, TOP 10 SIEM Product, 2018), ver Anexo VII.

- Sistemas de Detección de Intrusos (IDS) basados en Hosts y Red: Estas herramientas suelen trabajar con firmas conocidas de ataques o líneas bases para identificar comportamiento sospechoso lo cual genera una alerta que posteriormente deberá ser revisada por un analista, pueden ser basada en Hosts (monitorean servidores) o en Red (monitorean toda una red). Entre las herramientas pagadas actualmente más utilizadas podemos mencionar las siguientes (Robb, 9 TOP Intrusion Detection and Prevention Systems, 2018):
  - McAfee NSP
  - Trend Micro TippingPoint
  - Hillstone NIPS
  - Darktrace Enterprise Immune System
  - NSFocus NGIPS
  - H3C SecBlade IPS
  - Huawei NIP
  - Entrust IoTrust Identity and Data Security
  - Cisco Firepower NGIPS

  Otras opciones Open Source para este tipo de herramientas, se puede mencionar Snort, Suricata, BroIDS y OSSEC.
- Analizador de Flujo de Red: Estas herramientas pueden monitorear el tráfico actual de una red, de esta manera se podría hacer verificaciones de amenazas específicas o

protocolo utilizados en la red. Algunas opciones Open Source de este tipo de herramientas son: Ntop, NfSen y Nfdump.

- Escáneres de Vulnerabilidad: Estas herramientas ayudan a encontrar los puntos débiles de una plataforma para que puedan ser remediados y evitar que posibles amenazas se materialicen, asimismo, pueden poseer diferentes funcionalidades como aplicar parches de seguridad en ciertos recursos, proveen guías de como solventar ciertos tipos de vulnerabilidades, entre otros. Entre las herramientas de escáneres más utilizados actualmente tenemos las siguientes (Admin, 2018):
  - Comodo HackerProof
  - OpenVAS
  - Nexpose Community
  - Nikto
  - Tripwire IP360
  - Aircrack
  - Wireshark
  - Nessus Professional
  - Retina CS Community
  - Microsoft Baseline Security Analyzer (MBSA)
- Monitoreo de Disponibilidad: Estas herramientas se enfoca en monitorear la disponibilidad de un su servicio o aplicación, debido a que una de las primeras señales de un incidente es el mal funcionamiento de un recurso este tipo de herramientas ayudan a identificar más rápido un problema. Una opción Open Source de este tipo de herramienta es Nagios.
- Web Proxy: Los web proxy son útiles en la gestión de incidentes debido a que registran las conexiones que se han realizado, de esta manera se puede obtener más información sobre el ataque, entre las opciones Open Source utilizadas podemos nombre Squid Proxy y IPFire, sin embargo, también se dispone de herramientas pagadas como por ejemplo:
  - Forcepoint Web Security
  - McAfee Web Protection
  - Barracuda Web Filter
  - TitanHQ WebTitan
  - FortiCache
  - EdgeWave St. Bernard
  - M86 Web Content Filtering

5.3.3.1.2. Herramientas de Inteligencia y Orientación

Estas herramientas evalúan lo que está ocurriendo en el mundo de las amenazas cibernéticas y también nos ayudan a tener una idea más clara de la situación actual de la organización y los recursos que posee. Se puede mencionar dos tipos de herramientas:

- Inventario de Activos: Para poder priorizar eventos e incidentes es necesario que los responsables de la gestión tengan pleno conocimiento de cuáles son los activos más críticos dentro de la organización. Para poder lograr esto, la organización debe realizar un proceso de identificación y evaluación de los activos que poseen, por esta razón contar con una herramienta en la que se pueda registrar los activos de la organización, el dueño del activo, el nivel de criticidad es óptimo para poder priorizar de manera adecuada los eventos.

  Este tipo de herramientas pueden ser consideradas como software de monitoreo de inventario que está diseñada para ser manejadas por Gerentes de TI, pueden supervisar el inventario y dar el seguimiento a todo los activos de una red y servicios tecnológicos de una organización. De este tipo de herramientas se puede mencionar las siguientes soluciones (Hillsberg, 2019):
  - Freshservice
  - ManageEngine ServiceDesk
  - ServiceNow Asset Management
  - Infor EAM
  - Lansweeper
  - BelManage
  - Samanage
  - ChangeGear
  - Asset Track

  Una opción Open Source para la administración de activos de TI, es la herramienta OCS Inventory.
- Inteligencia de Amenazas: Las herramientas de inteligencia de amenazas provee una visión global sobre las amenazas actuales del mundo informático, como por ejemplo: indicadores de compromiso, direcciones IP con mala reputación, dominios, hash de archivos, entre otros. Esto ayudaría a comprender a la organización los comportamientos que pueden estar afectando a sus propias redes.

  Las plataformas de inteligencia de amenazas pueden incorporar una o varias fuentes de datos y someterlos a un análisis detallado para poder aislar patrones inusuales en los sistemas y extraer otros datos valiosos. Estas plataformas deben poseer indicadores que ayuden a identificar amenazas potenciales para la organización

(Robb, Eight Top Threat Intelligence Platforms, 2017). A continuación se detallaran sugerencias de plataformas de inteligencia de amenazas:

- IBM XForce Exchange
- Anomali ThreatStream
- Palo Alto Network AutoFocus
- RSA NetWitness Suite
- LogRhythm Threat Lifecycle Management (TLM) Platform
- FireEye iSIGHT Threat Intelligence
- LookingGlass Cyber Solutions
- AlienVault Unifed Security Management (USM)

5.3.3.2. Herramientas útiles para la fase de Contención, Erradicación y Recuperación

Las herramientas de esta fase se enfocan en remediar y recuperarse del incidente, mediante a procedimientos establecidos. Entre las herramientas se pueden mencionar:

- Herramientas forenses para captura de información, respuesta de incidentes: Este tipo de herramientas engloba todas las actividades forenses para poder identificar, preservar, recuperar, analizar y presentar evidencias, hechos y opiniones sobre la información digital. Cabe recalcar que estas herramientas están diseñadas para poder crear un log de auditoría de todas las acciones realizadas y por ende también poseen la funcionalidad de cadena de custodia para el manejo de las evidencias. Entre las mejores herramientas gratuitas para investigación forense tenemos (Tabona, 2018):
  - SANS SIFT (SANS Invetigative Forensic Toolkit)
  - CrowdStrike CrowdResponse
  - Volatility
  - The Sleuth Kit
  - FTK Imager
  - Caine
  - ExifTool
  - Free Hex Editor Neo
  - Bulk Extractor
  - PlainSight
  - LastActivity View
- Herramientas de Respaldos y Recuperación de Sistemas: Estas herramientas se enfocan en realizar actividades de restauración de respaldos, aplicación de parches, restauración de servicios y aplicaciones, para poder volver a la funcionalidad normal

después de la contención del incidente. Entre las herramientas disponibles actualmente para realizar estas tareas podemos mencionar las siguientes:

- Veeam Backup & Replication
- Rubrik
- IBM Spectrum Protect
- Acronis Backup
- Cohesity
- Zero Virtual Replication
- Veritas NetBackup
- Micro Focus Data Protector
- Reduxio
- Commvault

5.4. KPI (Indicadores) para evaluar la Gestión de Incidentes de Seguridad

Existen varias maneras de evaluar el desempeño de la gestión de los incidentes de seguridad, una de ellas es a través de la implementación de indicadores que deberán ser calculados periódicamente con información de un rango de tiempo específico, de esta manera se podría observar el desempeño del área responsable del proceso durante el transcurso del año.

A continuación presentaremos un conjunto de indicadores que pueden ser implementados para la evaluación de la gestión de incidentes dentro de un Centro de Operaciones de Seguridad:

INDICADOR	DESCRIPCIÓN	FÓRMULA	FRECUENCIA DE EJECUCIÓN
Cantidad de Incidentes	Cantidad total de los incidentes registrados en el período evaluado, divididos según su categoría.	$\#\ Total\ de\ Incidentes$	Mensual
Incidentes Repetidos	Porcentaje de incidentes repetidos en el periodo evaluado	$\%IncidentesRepetidos = (\#IncidentesRepetidos \div \#TotalIncidentes) \times 100$	Trimestral
Incidentes Solucionados	Porcentaje de incidentes que fueron solucionados o cerrados durante el periodo evaluado	$\%IncidentesSolucionados = (\#IncidentesSolucionados \div \#TotalIncidentes) \times 100$	Mensual
Incidentes Críticos Solucionados	Porcentaje de incidentes que son considerados como críticos que fueron	$\%IncidSolucionadosCriticos = (\#IncidSolucionadosCriticos \div \#TotalIncidentes) \times 100$	Mensual

INDICADOR	DESCRIPCIÓN	FÓRMULA	FRECUENCIA DE EJECUCIÓN
	solucionados o cerrados durante el periodo evaluado		
Incidentes Pendientes	Porcentaje de incidentes pendientes de solucionar durante el periodo de tiempo evaluado. Sin importar la fecha de registro del incidente	$\%IncidentesPendientes = (\#IncidentesPendientes \div \#TotalIncidentes) \times 100$	Mensual
Incidentes Críticos Pendientes	Porcentaje de incidentes considerados como críticos pendientes de solucionar durante el periodo de tiempo evaluado. Sin importar la fecha de registro del incidente	$\%IncidPendientesCriticos = (\#IncidPendientesCriticos \div \#TotalIncidentes) \times 100$	Mensual
Tiempo promedio de resolución	Tiempo promedio de resolución de los incidentes solucionados en el periodo de tiempo evaluado.	$TiempoPromedio = \left(\sum TiempoResolución\ de\ Incidentes\ Solucionados\right) \div \#IncidentesSolucionados$	Mensual

Tabla 19. Indicadores para evaluar la gestión de incidentes

Con el uso de indicadores periódicos, se podría detectar deficiencias en el proceso y poder realizar correcciones que permitan agilizar la gestión de los incidentes. Adicionalmente, estos tipos de indicadores ayudaría a presentar una fotografía actualizada del desempeño del área en base a la gestión de los incidentes, este tipo de información es comúnmente presentada a la Alta Dirección de la organización para el control de las áreas.

CAPÍTULO VI

6. Lineamientos de Seguridad estipulados en la Resolución SB-2018-771

De acuerdo a lo mencionado en el Capítulo II, la Superintendencia de Bancos del Ecuador (SB) es el ente regulatorio gubernamental encargado de la supervisión de las funciones de las organizaciones del sector financiero del país. Este ente regulatorio mantiene formalizada mediante la resolución SB-2018-771 los lineamientos con los que debe cumplir las Instituciones Financieras para poder garantizar la seguridad de la información de sus clientes y empleados.

En el Capítulo V del presente trabajo nos enfocamos en detallar todas las principales funcionalidades de un Centro de Operaciones de Seguridad (SOC) con las que debe contar las organizaciones de cualquier tipo de sector del mercado, sin embargo, existen ciertos servicios, actividades y controles adicionales que se pueden realizar y aplicar dentro de un SOC por lo cual en este capítulo nos enfocaremos en dichas funciones que además son requeridas obligatoriamente por la Superintendencia de Bancos para que se practiquen dentro del sector financiero.

Debido a que los lineamientos de seguridad de la información estipulados en la resolución SB-2018-771 tienen como referencia el estándar internacional ISO/IEC 27000, haremos un mapeo entre los requerimientos de la resolución y el estándar para la implementación de un sistema de gestión de la seguridad de la información versión 27001:2013, en donde se podrá observar que la ISO 27000 mantiene varios controles y recomendaciones que son aplicables para ser implementados por el personal del SOC para incrementar el nivel de la seguridad de la información dentro de la empresa.

La Sección VII dentro de la resolución SB-2018-771 corresponde a la los lineamientos de la Seguridad de la Información, el cual se encuentra dividido en dos artículos, N°15 y N°16, a continuación detallaremos los puntos solicitados en cada artículo y su equivalente dentro del estándar ISO/IEC 27000.

6.1. Artículo N°15 de la resolución SB-2018-771

El artículo N°15 estipula lo siguiente "*Con el objeto de gestionar la seguridad de la información para satisfacer las necesidades de la entidad y salvaguardar la información contra el uso,*

revelación y modificación no autorizados, así como daños y pérdidas las entidades controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya y contar al menos con:" (Resolución No. SB.2018.771, 2018).

a. "*Funciones y responsables de la seguridad de la información que permitan cumplir con los criterios de confidencialidad, integridad y disponibilidad de la información, acorde al tamaño y complejidad de los procesos administrados por el negocio.*
   Las entidades controladas deben conformar un comité de seguridad de la información que se encargue de evaluar y supervisar el sistema de gestión de la seguridad de la información.
   El comité debe estar conformado como mínimo por: el miembro del directorio quien lo presidirá, el representante legal de la entidad, los funcionarios responsables de las unidades de: riesgos y seguridad de la información. Mantendrá un reglamento donde se establezcan sus funciones y responsabilidades. Las reuniones de este comité se realizarán al menos trimestralmente dejando evidencia de las decisiones adoptadas.
   El comité de seguridad sesionará con la mitad más uno de sus integrantes, cuyo quórum no deberá ser menor a tres (3) y las decisiones serán tomadas por mayoría de votos. El presidente del comité tendrá voto dirimente.
b. *Un área independiente y especializada con personal capacitado y experiencia en gestión de seguridad de la información, acorde al tamaño y complejidad de sus operaciones, que lidere el establecimiento, implementación, operación, monitoreo, mantenimiento y mejora continua del sistema de gestión de seguridad de la información de la entidad que debe mantener la independencia funcionar del: área de tecnología, riesgos, áreas de negocio y función de auditoría*."

Los puntos detallados en el artículo N°15 corresponde a la estructura organizacional que debe mantener el SOC o área de Seguridad de la Información dentro de la Institución Financiera, no enfocándose en las actividades del área, sino más bien en cómo debe ser conformado, sin embargo, existen ciertos controles que podemos sugerir para estos dos literales antes mencionados.

Adicionalmente, se realizará el mapeo de los literales expuestos en el artículo N°15 versus lo definido en el documento ISO 27001 que detalla las especificaciones para un Sistema de Gestión de la Seguridad de la Información (SGSI):

LITERAL ART.N°15	CONTROL O RECOMENDACIÓN	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
		LITERAL ISO27001	DESCRIPCIÓN DE LA ESPECIFICACIÓN DEL SGSI
a.	• Contar un documento formalizado de la descripción de funciones y actividades con los que debe cumplir el SOC dentro de la Institución Financiera, el cual deberá ser aprobado por la directiva de la Organización. • Mantener un acta formalizada donde se estipule la creación del comité de la Seguridad de la Información dentro de la Organización, donde se detalle los integrantes y su cargo dentro de la institución, de igual manera las obligaciones con las que deberá cumplir el comité. • Generar actas de las reuniones del comité de la seguridad de la información, donde se detalle el personal presente y los puntos tratados, para poder verificar el número de reuniones realizada anualmente y evidenciar decisiones adoptadas.	5.1. Liderazgo y Compromiso	El punto detalla cuales son las acciones con las que la alta dirección de la organización debe comprometerse en realizar para el apoyo del SGSI.
		5.3. Roles, responsabilidades, autoridades en la Organización	Este punto define que la alta dirección es el encargado de asegurar que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen dentro de la organización.
b.	Este punto se enfoca en la creación del Centro de Operaciones de Seguridad sobre el recurso humano con el que debe contar, es por esto que para esta sección se podría considerar todos los puntos mencionados en el capítulo V, en la sección 5.3.1. *"Personal de Seguridad de un Centro de Operaciones de Seguridad"*, donde se detalla los roles que deben considerarse en un SOC, características y funciones.	7.2. Competencia de Recursos	En esta sección el estándar detalla los puntos que la organización deberá definirse para poder seleccionar al recurso humano de los responsables de la Seguridad de la Información, de manera correcta.

Tabla 20. Tabla de Recomendaciones para articulo N°15, SB-2018-771 y mapeo con el estándar ISO27000

6.2. Artículo N°16 de la resolución SB-2018-771

El artículo N°16 estipula lo siguiente "*Las entidades controladas deben establecer, implementar, operar, monitorear, mantener y mejorar un sistema de gestión de seguridad de la información que incluya al menos lo siguiente*" (Resolución No. SB.2018.771, 2018). A continuación presentaremos un listado de todos los puntos del artículo N°16 con los controles y/o recomendaciones que se pueden aplicar e implementar dentro del Centro de Operaciones

de Seguridad (SOC), y también el mapeo de los controles de la resolución versus lo estipulado en el estándar internacional de la ISO/IEC 27000:

a. "*Alcance del sistema de gestión de seguridad de la información;*"

Para poder implementar un SGSI dentro de una Organización es necesario en primer lugar definir el alcance que cubrirá el SGSI, puede ser desde un servicio específico o toda la organización, esto depende del tamaño de la empresa y los servicios que ofrezca. Para las instituciones financieras es recomendable poder determinar cuáles de sus servicios abarcará el SGSI, dicho alcance deberá ser determinado por los responsables de la Seguridad de la Información en conjunto con la alta dirección; de esta manera el personal del SOC podrá tener en claro cuáles son los servicios que cubre el SGSI y que requerimientos de seguridad deberán cumplir.

Según lo estipulado en el estándar ISO/IEC 27000 este literal se encuentra relacionado con las especificaciones que se deben realizar para la implementación de un SGSI dentro de la Organización:

LITERAL ART.N°16	**MAPEO CON EL ESTÁNDAR ISO/IEC 27000**	
	LITERAL ISO27001	**DESCRIPCIÓN DE LA ESPECIFICACIÓN DEL SGSI**
a.	4.3. Determinación del alcance del SGSI	En la especificación estipula que la organización debe delimitar el alcance del SGSI y para que plataformas y servicios será aplicable.

Tabla 21. Tabla de mapeo con el estándar ISO27000 versus literal "a" del artículo N°16

b. "*Políticas, objetivos, procesos, procedimientos y metodologías de seguridad de la información definidos bajo estándares de general aceptación, alineados a los objetivos y actividades de la entidad, así como las consecuencias de su incumplimiento.*
Las políticas, procesos, procedimientos y metodologías de seguridad de la información deben ser revisados y aceptados por el comité de seguridad de la información; y propuestos para la posterior aprobación del directorio; así como ser difundidos y comunicados a todo el personal involucrado de tal forma que se asegure su cumplimiento."

Es importante que toda Institución Financiera cuente con una política de Seguridad de la Información donde detalle todos los lineamientos con los que debe cumplirse, asimismo, otros tipos de documentos que formen el marco normativo de la empresa, dichos documentos

deberán ser definidos por los responsable de la seguridad en conjunto con el personal del SOC para contar con lineamientos actualizados y eficaces. Se enlistará las recomendaciones de los documentos de seguridad que la organización debería definir dentro del marco normativo de seguridad:

- Política de Seguridad: La cual definirá el tipo de gestión de seguridad que se quiere establecer dentro de la organización, siempre estando alineada con los objetivos del negocio. Este documento definirá las reglas que se tienen que cumplir en la organización y las sanciones en caso de incumplimiento; la política de seguridad es considerado un documento de primer nivel jerárquico dentro del marco normativo.
- Normas de Seguridad: Estos documentos detallarán aspectos concretos de la política de seguridad; estas normas deben ser claras, concisas y no ambiguas, dichas normas pueden ser divididas en diferentes documentos de acuerdo al área de seguridad que se trate. Dentro del marco normativo las normas corresponden al segundo nivel jerárquico.
- Procedimientos de Seguridad: Los documentos de procedimientos son específicos y detallan un conjunto de pasos estructurado en relación con la ejecución de un proceso o tarea, tratando de cumplir con lo especificado en las normas. Son consideradas como guías que especifican el cómo, dónde y cuándo se puede realizar actividades específicas.
- Guías y Guías de Uso: Estos documentos determinan acciones que son necesarias realizar para poder completar una actividad o un proceso concreto, asimismo, las guías de uso son las que definen cuáles serán las pautas de comportamiento que deben cumplir los usuarios sobre el uso de una plataforma, aplicación o servicio, por lo general están destinados a los usuarios finales. Tanto los documentos de Procedimientos y Guías corresponden al tercer nivel jerárquico del marco normativo.

Para poder llevar un control de estos documentos, es recomendable que se utilice códigos de identificación en cada documento, el cual puede ser creado con el siguiente formato `<abreviatura_tipo_doc><secuencial>_<nombre_documento>_<fecha-AAAAMMDD>`;
ejemplo: POL001 Política de Seguridad de la Información 201812330. De esta manera se podría llevar un control de las diferentes versiones de los documentos utilizando el código del archivo en conjunto con su fecha de actualización.

De acuerdo a lo detallado en el código de buenas prácticas ISO 27002, el literal “b” revisado se encuentra relacionado con los siguientes controles del estándar:

LITERAL ART.N°16	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
	CONTROL ISO27002	**DESCRIPCIÓN DEL CONTROL DEL SGSI**
b.	5.1.1. Políticas para la seguridad de la información	Detalla la importancia de la definición de un conjunto de políticas de seguridad de la información el cual debe estar alineado a las necesidades del negocio, aprobado por la alta dirección de la organización, publicado y comunicado a los empleados y personal externo relevante.
	5.1.2. Revisión de las políticas para la seguridad de la información.	Estipula pautas para establecer el control de la revisión periódica de las políticas de seguridad de la organización.

Tabla 22. Tabla de mapeo con el estándar ISO27000 versus literal "b" del artículo N°16

c. *"Inventario de activos de información con su clasificación en términos de: valor, requerimientos legales, sensibilidad y criticidad para la entidad, propietario, custodio y ubicación."*

Para poder llevar un control de los activos de información que posee la institución financiera es necesario que el personal del SOC en conjunto con las demás áreas de la empresa, trabajen en una matriz en la que se registren los activos identificados dentro de cada proceso y servicio que ofrezca la organización. La matriz puede poseer información como: nombre del activo, nivel de criticidad, proceso o servicio al que está vinculado, tipo de información que gestiona, propietario, custodio, ubicación. Esta matriz informativa debe ser gestionada por el personal del SOC ya que podría ser utilizada en el proceso de la gestión de incidentes de seguridad para conocer a los dueños de los activos afectados.

De acuerdo a lo detallado en el código de buenas prácticas ISO 27002, el literal "c" revisado se encuentra relacionado con los siguientes controles del estándar:

LITERAL ART.N°16	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
	CONTROL ISO27002	**DESCRIPCIÓN DEL CONTROL DEL SGSI**
c.	8.1.1. Inventario de Activos	El control menciona que la información, activos asociados a la información y los recursos que la procesan deben estar claramente clasificados y detallarse en un inventario donde se puedan identificar fácilmente.

LITERAL ART.N°16	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
	CONTROL ISO27002	**DESCRIPCIÓN DEL CONTROL DEL SGSI**
	8.2.1. Clasificación de la Información	Este control detallara que la información debería ser clasificar de acuerdo al nivel de importancia que presenta para la institución, valor sensibilidad y criticidad ante revelaciones o modificaciones no autorizadas.

Tabla 23. Tabla de mapeo con el estándar ISO27000 versus literal "c" del artículo N°16

d. *"La designación de los propietarios de los activos de información, que deben tener como mínimo las siguientes responsabilidades:"*

SUBLITERAL	RECOMENDACIÓN	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
		CONTROL ISO27002	**DESCRIPCIÓN DEL CONTROL DEL SGSI**
i. Clasificar los activos de información y revisar periódicamente el inventario de activos de información, con la finalidad de mantenerlo actualizado.	Llevar acabo la identificación y clasificación de todos los activos es una tarea que puede demandar una cantidad de tiempo considerable, es por esto que se recomienda planificar esta actividad con todas las áreas para poder hacerlo de una manera más ágil y adecuada. Una vez terminada la matriz de activos de información se recomienda definir un proceso de revisión y actualización de la misma con una frecuencia mínima anual para poder identificar nuevos activos.	8.1.2. Propiedad de los Activos	Con este control el estándar busca asegurar que todos los activos de información mantengan designado un propietario el cual será el responsable de la gestión del mismo. En este control se debería detallar que el propietario será el responsable de: • Asegurar que los activos se encuentren correctamente inventariado. • Asegurar que se clasifican y protegen adecuadamente. • Definir y revisar las reglas de acceso a los activos más críticos, tomando en cuenta políticas de acceso aplicables. • Uso adecuado para el borrado o destrucción del activo.
ii. Definir y revisar periódicamente las restricciones y accesos a los activos de información tomando en cuenta las políticas de control de acceso aplicables.	Para poder llevar un control de los activos de información en especial de los considerados como críticos para la organización es necesario definir una política de control de acceso a estos activos, donde se detalle el proceso de autorización que se deberá solicitar al dueño y custodio del activo, indicando la fecha de acceso, motivo de acceso y adjunto respaldos del motivo de acceso. Todas las solicitudes de autorizaciones deben ser centralizadas por el SOC de la organización, siendo ellos los responsables		

SUBLITERAL	RECOMENDACIÓN	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
		CONTROL ISO27002	DESCRIPCIÓN DEL CONTROL DEL SGSI
	de la seguridad de la información. Dentro de esta política de control se deberá definir que el proceso debe ser evaluado por el área de Auditoría de manera periódica para verificar el correcto acceso a los activos.		
iii. Autorizar los cambios funcionales a las aplicaciones y modificaciones a la información a través de accesos directo a la base de datos.	De acuerdo a lo nombrado en el literal anterior, en la política de control de acceso a los activos de información deberá definirse de la misma manera el proceso de autorización para poder realizar cambios funcionales a la información de los activos mediante el acceso directo a la base de datos. Estas solicitudes deberán ser centralizadas y controladas por el SOC de la organización.	8.1.3. Uso aceptable de los Activos	El control tiene como objetivo poder definir, documentar e implementar reglas para el uso aceptable de los activos y recursos que procesan la información.

Tabla 24. Tabla de Recomendaciones del Literal d. del artículo N°16, SB-2018-771

e. *"Identificación y documentación de los requerimientos y controles mínimos de seguridad para cada activo de información, con base en una evaluación de los riesgos que enfrenta la entidad, aplicando la metodología de gestión de riesgo operativo."*

El personal del SOC como responsables de la seguridad de la información, utilizando una metodología de gestión de riesgos, durante el proceso de identificación y documentación de los activos de información con las diferentes áreas de la empresa, deberá definir y establecer cuáles serán los requerimientos y controles mínimos de seguridad con los que deberá cumplir el activo de información, en especial los que son considerados como críticos para la empresa.

Una metodología que podría ser utilizada por el personal del SOC para gestión del riesgo, en el caso de que no exista una metodología previamente definida, es la norma internacional ISO 31000 versión 2018, la cual proporciona los principios y directrices para la gestión del riesgo basándose en la mejora continua.

f. *"Plan de Seguridad de la Información que permita la implementación de los controles identificados y acciones de mejora."*

El líder del SOC de la organización, como responsable principal de la seguridad de la información deberá definir un Plan de Director de Seguridad para poder implantar una estrategia de seguridad a medio – largo plazo, dicho plan establecerá las directrices de seguridad y definir actividades en seguridad.

Es recomendable que el Plan de Seguridad se lo defina mediante un proceso el cual puede considerar las siguientes fases:

- Definición de un modelo de seguridad que mantenga los objetivos y estrategia del negocio, la gestión de riesgo, necesidades del negocio, estándares y buenas prácticas del sector, circunstancias tecnológica y operativas.
- Análisis de la situación actual por medio de la información obtenida de documentación, entrevistas, indicadores, etc.
- Realizar un análisis GAP determinando el estado actual de la organización y el estado ideal que se quiere alcanzar tomando como base un estándar internacional como seria la ISO27001.
- Definir el plan de acción de todos los proyectos de seguridad que se realizaran a mediano y largo plazo donde se detalle el conocimiento interno de la empresa, los recursos y el presupuesto y la tecnología disponible.
- Aprobación y desarrollo del Plan de Seguridad, por parte del comité y directivos de la organización. En esta fase se comienza con la ejecución de todos los proyectos definidos en el punto anterior.
- Seguimiento del Plan para comprobar modificaciones respecto a tareas ejecutadas, desviaciones en asignación de recursos y estimación de nuevos costes; y también el grado de cumplimiento versus lo definido en un principio.

Este plan de seguridad deberá ser creado siempre alineándose a las necesidades del negocio.

De acuerdo a lo revisado en el estándar internacional de la ISO/IEC 27000 los literales “e” y “f” de la resolución SB-2018-771 del artículo N°16, no están directamente relacionados con el estándar, sin embargo, está basado en las mejores practica actuales de la seguridad de la información.

g. *“Información que permita verificar el cumplimiento de las políticas, procesos, procedimientos y controles definidos para gestionar la seguridad de la información.”*

El personal del SOC deberá definir cuáles serán las medidas necesarias para controlar el cumplimiento de lo definido en políticas, procedimientos, normas, etc. Entre los controles generales que pueden implementarse se pueden nombrar:

- Habilitar log de auditoría de las plataformas y servicios que se utilicen dentro de la empresa para la verificación de actividades realizadas por parte de los usuarios.
- Procesos de autorización para las modificaciones o eliminaciones de información en las diferentes plataformas de la organización.
- Utilizar herramientas de seguridad que se encuentren protegidas del acceso no autorizado, que registren la información de log y ayuden a detectar comportamiento no autorizado por parte del personal.

Para este punto se podrían definir varios controles, dependiendo de los servicios de la organización y los lineamientos definidos en el marco normativo de seguridad.

De acuerdo a lo detallado en el código de buenas prácticas ISO 27002, el literal "g" revisado se encuentra relacionado con los siguientes controles del estándar:

LITERAL ART.N°16	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
	CONTROL ISO27002	**DESCRIPCIÓN DEL CONTROL DEL SGSI**
g.	12.4.1. Registro de Eventos	El control define que se deben registrar, proteger y verificar periódicamente todas las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información. De esta manera se podría evidenciar el cumplimiento de las políticas y reglas de seguridad definidas por el SOC.
	12.4.2. Protección de la Información de Registro	Este control busca implantar medidas de seguridad para proteger todos los dispositivos del SOC que se encarguen del registro y de la información de log de actividades y eventos para evitar manipulaciones indebidas y accesos no autorizados.
	12.4.3. Registros de administración y operación	Con la implementación de este control se registraría en un log de eventos y actividades, todas las acciones realizadas por los usuarios con un perfil de administrador u operador de los sistemas.

Tabla 25. Tabla de mapeo con el estándar ISO27000 versus literal "g" del artículo N°16

h. *"Monitoreo con una frecuencia al menos semestral, del cumplimiento y efectividad de los controles establecidos y generar informes dirigidos al comité de seguridad de la información."*

Es recomendable que el personal del SOC periódicamente, realice un proceso de monitoreo de los principales controles de seguridad que se mantienen en la organización y se pueda realizar una estadística de su cumplimiento. De la misma manera se debe realizar una revisión de los principales procesos que se realizan dentro del SOC y calcular estadísticas de la efectividad de dichos procesos. Los informes sobre la evaluación realizada deben ser gestionados por el líder del SOC para posteriormente entregarlos al comité de seguridad de la información de la institución financiera y dar a conocer el estado de la seguridad dentro de la organización en un rango determinado de tiempo; es aconsejable que este tipo de revisiones se haga de manera trimestral para poder identificar cualquier anomalía en los controles o procesos del SOC.

De acuerdo a lo detallado en el código de buenas prácticas ISO 27002, el literal “h” revisado se encuentra relacionado con los siguientes controles del estándar:

LITERAL ART.N°16	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
	CONTROL ISO27002	**DESCRIPCIÓN DEL CONTROL DEL SGSI**
h.	18.2.2. Cumplimiento de las políticas y normas de seguridad	Este control va enfocado para que los funcionarios directivos de cada área de la Organización determinen medidas para revisar que los requisitos de seguridad de la información definidos en políticas, normas, procedimientos, entre otros, se cumplan correctamente, utilizando herramientas automatizadas para poder realizar una revisión periódica con la información resultante.
	18.2.3. Comprobación del cumplimiento técnico	El control se enfoca en la implementación de herramientas automatizadas de seguridad que generen informes técnicos para que sean analizados por el responsable de la verificación de cumplimiento de los controles y posteriormente realizar un informe ejecutivo con los resultados para que sean entregados periódicamente a la Alta Dirección.

Tabla 26. Tabla de mapeo con el estándar ISO27000 versus literal “h” del artículo N°16

i. *“Evaluación al menos una vez al año, del desempeño del sistema de gestión de la seguridad de la información, considerando los resultados de: auditorías de seguridad, gestión de incidentes de seguridad, monitoreo de los controles, resultados de las evaluaciones de riesgos, sugerencias, retroalimentación orientadas a mejorarlo. El resultado estas evaluaciones así como las acciones de mejora deben ser conocida y aprobadas por comité de seguridad de la información; y,”*

De manera anual el líder del SOC deberá realizar un informe en el que recolecte la información de indicadores internos de gestión y cumplimiento, revisiones externas, entre otros, que muestren una foto del desempeño del personal del SOC y funciones y controles establecidos durante el año transcurrido, el cual deberá ser entregado y revisado por el comité de seguridad de la información. Esta actividad ayudará a identificar puntos de mejora dentro de los procesos del SOC y fortalezas que posee el área y que pueden ser aprovechadas.

De acuerdo a lo revisado en el estándar internacional de la ISO/IEC 27000, el literal "i" de la resolución SB-2018-771 del artículo N°16, no están directamente relacionados con el estándar, sin embargo, está basado en las mejores practica actuales de la seguridad de la información.

j. *"Para considerar la existencia de un apropiado ambiente de gestión de seguridad de la información la unidad responsable de la seguridad de la información deberá implementar:"*

A continuación se mostrará un cuadro con los sub literales que exigen la norma versus lo recomendado el presente trabajo a implementar en la institución financiera:

SUBLITERAL	RECOMENDACIÓN	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
		CONTROL ISO27002	DESCRIPCIÓN DEL CONTROL DEL SGSI
i. Medidas para proteger la información contenida en: documentos, medios de almacenamiento u otros dispositivos externos e intercambio electrónico, contra: robo, utilización o divulgación no autorizada, por parte de su personal o terceros.	El SOC deberá definir e implementar un política de uso para medios de almacenamiento y dispositivos externos, dicha política deberá detallar como mínimo los siguientes puntos: • Registro de dispositivos de almacenamiento y externos. • Requisitos de protección física con los que debe contar y restricciones de instalación de software. • Restricciones de conexión a servicios de información y control de acceso • Técnicas criptográficas a utilizar para	6.2.1. Política de Dispositivos Móviles	El control propone medidas de seguridad que se deberían implementar en la organización para la protegerla contra los riesgos de utilizar dispositivos externos. Estas medidas de control pueden estar detalladas en una política de dispositivos móviles considerando los riesgos de trabajar con esto medios de almacenamiento en entornos desprotegidos.
		8.3.3. Soportes físicos en tránsito	El control dispone directrices para proteger los soportes físicos que contengan información de la organización, contra el acceso no autorizado, uso indebidos o deterioro

SUBLITERAL	RECOMENDACIÓN	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
		CONTROL ISO27002	**DESCRIPCIÓN DEL CONTROL DEL SGSI**
	cifrar la información y protección contra malware. • Copias de respaldo	9.1.1. Política de control de acceso	En este control se sugiere la definición de una política de control de acceso a las diferentes plataformas y sistemas que procesan la información, basándose en los requisitos del negocio y la seguridad de la información. Esta política puede ser aplicable a diferentes tipos de dispositivos.
		13.2.1. Políticas y procedimientos de intercambio de información	Se debería definir medidas y controles formales en procedimientos o políticas para la protección en el intercambio de la información mediante todo tipo de recursos de comunicación.
		13.2.3. Mensajería electrónica	Controles para proteger la información que se transmitida por medio de mensajería electrónica.
ii. Procedimientos de eliminación de la información crítica de la entidad, de manera segura y considerando los requerimientos legales y regulatorios.	El SOC deberá definir un procedimiento formalizado para la depuración y eliminación de manera segura de soportes que no vayan a ser necesarios. Este proceso debería variar de acuerdo a nivel de confidencialidad de la información a eliminar.	8.3.2. Eliminación de Soportes	El control propone que los responsables de la seguridad de la información definan procedimientos formales para la eliminación de forma segura de soportes para minimizar el riesgo de filtraciones de información confidencial a persona no autorizadas.
iii. Procedimientos para el control de accesos a la información que considera la concesión; administración de usuarios y perfiles para el registro, eliminación y modificación de la información, que garanticen una adecuada segregación	El SOC deberá definir una política formalizada sobre el control de acceso de los usuarios a los diferentes tipos de recursos que dispone la organización, asimismo, los propietarios de los activos deberán determina las reglas para el control de acceso y restricciones a sus activos para los diferentes tipos de usuarios. Esta política como	9.1.1. Política de control de acceso	El control propone que los responsables de la seguridad de la información definan procedimientos formales para la eliminación de forma segura de soportes para minimizar el riesgo de filtraciones de información confidencial a persona no autorizadas.

SUBLITERAL	RECOMENDACIÓN	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
		CONTROL ISO27002	DESCRIPCIÓN DEL CONTROL DEL SGSI
de funciones y reduzcan el riesgo de error o fraude; así como la revocación de usuarios, tanto de aplicativos, software base, red, dispositivos de seguridad perimetral, base de datos, entre otros. También se deberá controlar el acceso de los proveedores a la información de la entidad.	mínimo debería considerar lo siguiente: • Requisitos de seguridad de las aplicaciones • Políticas para la autorización de la información • Políticas de clasificación de la información de los recursos • Segregación de funciones de acceso en un entorno distribuido e integrado, asimismo, segregar funciones en base al control de acceso en diverso roles. • Requisitos para la autorización de peticiones de acceso • Revocación de acceso a usuarios • Registro de los eventos relevantes realizados por el usuario • Roles de usuarios con acceso privilegiado	9.1.2. Acceso a las redes y a los servicios de red	Este control define que solamente se debería otorgar acceso a las redes y servicios en red a los usuarios que hayan sido específicamente autorizados por los responsables de seguridad.
		9.4.1. Restricción del acceso a la información	El control propone implementar restricciones de acceso a la información basándose en los requisitos de cada aplicación del negocio, alineada con la política de control de acceso definida por la organización.
iv. Procedimiento para el monitoreo periódico de accesos, operaciones privilegiadas e intentos de accesos no autorizados, para asegurar que los usuarios solo estén realizando actividades para la cuales han sido autorizadas.	El personal del SOC deberá ejecutar revisiones periódicas, como mínimo trimestrales, para verificar el acceso de las cuentas con roles privilegiados si muestran un comportamiento anormal. También revisar el log de acceso no autorizado de las plataformas críticas de la organización para identificar potenciales usuarios maliciosos. La información obtenida de esta revisión deberá detallarse en un informe formal y ser enviado al líder del SOC.	12.4.1. Registro de eventos	El control define que se deben registrar, proteger y verificar periódicamente todas las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información. De esta manera se podría evidenciar el cumplimiento de las políticas y reglas de seguridad definidas por el SOC.
v. Procedimiento que permitan contar con pistas de auditoría a nivel de aplicativos y base de datos que registren los cambios realizados a la información crítica de la entidad. Los	El personal del SOC en conjunto con el área de Tecnología deberá habilitar los log de eventos de las aplicaciones y plataformas informáticas para registrar las	12.4.1. Registro de eventos	El control define que se deben registrar, proteger y verificar periódicamente todas las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información. De esta manera se podría evidenciar el cumplimiento

SUBLITERAL	RECOMENDACIÓN	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
		CONTROL ISO27002	DESCRIPCIÓN DEL CONTROL DEL SGSI
administradores no deben tener permiso para borrar o desactivar las pistas de sus propias actividades.	actividades realizadas por los usuarios.		de las políticas y reglas de seguridad definidas por el SOC.
		12.4.3. Registros de administración y operación	Con la implementación de este control se registraría en un log de eventos y actividades, todas las acciones realizadas por los usuarios con un perfil de administrador u operador de los sistemas.
vi. Procedimientos para el uso, protección y tiempo de vida de las llaves criptográficas utilizadas para cifrar la información.	El SOC deberá definir un procedimiento formal en el que se detalle el tiempo de validez de las llaves criptográficas, que tipo de técnica cifrado debe utilizarse y cuál es el proceso para la eliminación de llaves criptográficas no vigentes.	10.1.1. Política de uso de los controles criptográficos	El control propone la definición de una política con todas las medidas de seguridad para el uso de controles criptográficos para proteger la información. Asimismo, el tipo de información a la cual se le aplicará este tipo de medidas y sus respectivas excepciones.
vii. Técnicas de cifrado sobre la información que lo requiera como resultado del análisis de riesgos de seguridad.	Definir lineamientos de cifrados sobre ciertos tipos de información que son considerados como sensible y confidencial, en el cual se deberá especificar el tipo de cifrado y cuáles serán los casos excepcionales.		
viii. Política y controles para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia; y, para instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software malicioso.	El SOC deberá implementar herramientas de seguridad para identificación de malware en las estaciones de trabajo de la organización. Y herramientas para verificar la instalación de software no autorizado instalado en los equipos de trabajo.	12.2.1. Controles contra el código malicioso	Este control busca implementar medidas de seguridad para detectar, prevenir y recuperarse de la infección de código malicioso (malware) y también definir procedimientos de concientización al usuario.
	Definir una norma de seguridad sobre la instalación de software en las estaciones de trabajo y el proceso de solicitud de autorización para su instalación.	12.6.2. Restricción en la instalación de software	El control propone la definición de reglas formales para restringir la instalación de software por parte de los usuarios.

SUBLITERAL	RECOMENDACIÓN	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
		CONTROL ISO27002	DESCRIPCIÓN DEL CONTROL DEL SGSI
ix. La realización de las auditorías de seguridad de la infraestructura tecnológica con base en el perfil de riesgo de la entidad, por lo menos una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan. Los procedimientos de auditoría deben ser ejecutados por personal independiente a la entidad, capacitado y con experiencia, aplicando estándares vigentes y reconocidos a nivel internacional; esta auditoría debe incluir al menos pruebas de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación. Las entidades deben definir y ejecutar planes de acción sobre las vulnerabilidades detectadas.	El líder del SOC deberá definir una empresa externa de seguridad que realice pruebas de penetración y vulnerabilidades a la infraestructura de la organización con el fin de identificar posibles puntos de compromiso y vulnerabilidades presente. Esta revisión deberá ser realizada con una frecuencia anual y debe estar detallada en uno de los procedimientos del SOC.	18.2.1. Revisión Independiente de la seguridad de la información	Este control determina que la Alta Dirección de la Organización debería encargar la revisión del enfoque para la gestión de la seguridad de la información y su implementación a una entidad independiente del área evaluada, es decir el SOC, pudiendo ser el área de Auditoría Interna de la organización o empresas externas especializadas en seguridad. Este tipo de revisiones deberían someterse a intervalos planificados anualmente o cuando se produzcan cambios significativos en la implementación de seguridad. Esta evaluación debería incluir la evaluación de oportunidades de mejora y la necesidad de cambios del enfoque establecido SGSI incluyendo la política y objetivos de control.
		18.2.3. Comprobación del cumplimiento técnico	Este control propone que periódicamente los sistemas de información deberían someterse a revisiones para verificar que cumplen con todas las políticas y normas de seguridad de la organización. Esta revisión de cumplimiento técnico se debería realizar con herramientas automatizadas que generen informes técnicos que puedan ser interpretados posteriormente por un especialista, incluyendo pruebas de intrusión y evaluación de vulnerabilidades.

SUBLITERAL	RECOMENDACIÓN	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
		CONTROL ISO27002	DESCRIPCIÓN DEL CONTROL DEL SGSI
x. Con base en un análisis de riesgos, realizar la segmentación de la red de datos y la implementación de sistemas de control y autenticación tales como: sistemas de prevención de intrusos (IPS), firewalls, firewall de aplicaciones web (WAF), entre otros; para evitar accesos no autorizados inclusive de terceros y ataques externos especialmente a la información crítica.	El SOC en conjunto con el área de Redes de la organización realizar la segmentación de la red en diferentes ambientes de trabajo (desarrollo, producción, etc.) e implementar herramientas de seguridad para detectar intrusos y prevenir incidentes.	13.1.1. Controles de red	El control propone la implementación de medidas de control para garantizar la seguridad de la información en las redes y a protección de los servicios conectados frente a los accesos no autorizados.
		13.1.2. Seguridad de los servicios de Red	Este control está enfocado en controlar y supervisar la capacidad del proveedor del servicio de red de la organización para gestionar los servicios contratados de manera segura y protegiendo la información. En este control se debería determinar que la organización tiene el derecho de auditar al proveedor.
		13.1.3. Segregación en redes	El control define que para poder gestionar las redes de manera segura es necesario realizar una segregación en las redes de la organización basándose en niveles de confianza junto a unidades organizativas. El perímetro de cada dominio debería estar bien definido y acceso entre ellos debería ser permitido pero ser controlado en el perímetro usando pasarelas como firewalls, routers, etc.
xi. Procedimientos para la definición de requerimientos de seguridad de la información para nuevos sistemas o su mantenimiento.	El SOC en conjunto con el área de Tecnología deberá definir en un procedimiento formalizado el proceso para la creación de nuevos sistemas y su mantenimiento en donde se detalle los requerimientos de seguridad mínimos con los que debe cumplir los nuevos sistemas o modificaciones.	14.1.1. Análisis de requisitos y especificaciones de seguridad de la información	Este control se enfoca en la identificación de los requisitos relacionados con la seguridad de la información durante la realización de los requisitos para nuevos sistemas de información o mejoras de sistemas existentes. La identificación de estos requisitos debería ser documentada y revisados

SUBLITERAL	RECOMENDACIÓN	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
		CONTROL ISO27002	DESCRIPCIÓN DEL CONTROL DEL SGSI
			por todas las partes interesadas.
xii. Escaneo automatizado de vulnerabilidades en código fuente para mitigar los riesgos de seguridad de las aplicaciones previo a su liberación y de aquellas que encuentra en producción;	El SOC debe mantener procedimientos y herramientas para el escaneo de vulnerabilidades en código fuente de aplicaciones, estas revisiones deberá ser antes de la puesta en producción y de manera periódica (recomendable hacerlo trimestralmente) con las aplicaciones que ya se encuentran en producción.	12.6.1. Gestión de las vulnerabilidades técnicas	El control propone utilizar herramientas para poder obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información que son utilizados por la organización y así evaluar la exposición de la misma a dichas vulnerabilidades y poder implementar medidas adecuadas para afrontar el riesgo asociado.
xiii. Procedimientos de gestión de incidentes de seguridad de la información en los que se considere al menos: reporte de eventos, su evaluación, registro de incidentes, comunicación, priorización, análisis, respuesta y recolección de evidencias; y,	De acuerdo a lo mencionado en el capítulo V, es necesario la definición de un procedimiento de respuesta ante incidentes de seguridad. Los lineamientos de seguridad para este requerimiento se pueden encontrar en el capítulo V sección 5.3.2.	16.1.1. Responsabilidades y procedimientos	El control dispone la definición de las responsabilidades y procedimientos a ejecutar dentro de la gestión de incidentes de seguridad para una respuesta rápida, efectiva y adecuada.
		16.1.2. Notificación de los eventos de seguridad de la información	El control establece los tipos de situaciones que pueden ocurrir en los cuales se debería comunicar los eventos de seguridad a todos el personal interesado, tanto interno como externo. En este control también se podría determinar la creación de un procedimiento para la comunicación de eventos de seguridad y el punto de contacto dependiendo del tipo de evento.
		16.1.4. Evaluación y decisión sobre los eventos de seguridad de la información	El control determina que para que un evento sea considerado como evento de seguridad debe ser previamente evaluado y clasificado y priorizado como incidente de acuerdo a lo definido por la organización. Esta clasificación y priorización puede ayudar a identificar el

SUBLITERAL	RECOMENDACIÓN	MAPEO CON EL ESTÁNDAR ISO/IEC 27000	
		CONTROL ISO27002	**DESCRIPCIÓN DEL CONTROL DEL SGSI**
			impacto y extensión del mismo.
		16.1.5. Respuesta a incidente de seguridad de la información	El control propone la definición de un procedimiento formalizado para el proceso de respuesta ante incidentes de seguridad. Este procedimiento debería abarcar todas las actividades de las fases de la gestión del incidente.
		16.1.6. Aprendizaje de los incidentes de seguridad de la información	El control propone la implementación de mecanismos que permitan cuantificar y supervisar los tipos, volúmenes y costes de los incidentes de seguridad. Esta información obtenida de la evaluación debería utilizarse para poder identificar incidentes recurrentes o con un elevado alcance.
		16.1.7. Recopilación de evidencias	El control dispone la creación formal de un procedimiento para la identificación, recogida, adquisición y preservación de la información que pueda servicio como evidencia, basándose en las mejores prácticas actuales y requisitos legales del país donde rige la empresa.
xiv. Procedimientos de afectación directa a las bases de datos que permitan identificar los solicitantes, autorizadores y motivo de la modificación a la información, así como el registro de pistas de auditoría que facilite la trazabilidad.	Según lo comentado en el literal “d” es necesario que el SOC defina un procedimiento formal para la solicitud de autorización de modificación de información directa en base de datos y toda la información relevante que debe ser requerida.	18.1.3. Protección de los registros de la organización.	El control se enfoca en las medidas de seguridad que deben considerarse para la protección contra perdida, destrucción, falsificación, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.

Tabla 27. Tabla de Recomendaciones del Literal j. del artículo N°16, SB-2018-771

En este capítulo podemos observar que los requerimientos de seguridad definidos por la Superintendencia de Bancos del Ecuador, abarcan la mayoría de los controles de seguridad de los dominios del estándar internacional ISO/IEC 27000, de esta manera podemos determinar que con la implementación de estos requerimientos dentro de la organización estaríamos alineándonos a la implementación parcial de un SGSI y que el SOC siendo un área independiente y especializada en seguridad sería el responsable de la gestión y control de la seguridad de la información dentro de la empresa.

CAPÍTULO VII

7. Normas y Estándares Internacionales con lineamientos aplicables a un SOC

Hoy en día tenemos disponibles varias normas, estándares, guías y buenas prácticas que pueden ser implementadas en nuestra organización para mejorar nuestros servicios, procesos, productos, tiempo de respuesta, desarrollo e inclusive la seguridad de la información.

Durante el desarrollo del presente trabajo, no se evidencio un estándar o mejores prácticas exclusivamente dedicado a normar las funciones y componentes de un Centro de Operaciones de Seguridad (SOC) independientemente del tipo de organización en el que se encuentra implementado, sin embargo, se identificaron varios estándares internacionales, normas y guías internacionales reconocidos mundialmente que mantienen apartados de seguridad que son aplicables para las funciones y actividades de un SOC.

Debido a que en el Capítulo VI se menciona varios controles y recomendaciones que son aplicables para ser realizadas por el personal del SOC, en este capítulo no se mencionará nuevamente al estándar.

A continuación presentaremos una breve descripción de las actividades que podrían ser definidas y/o ejecutadas dentro de un SOC:

7.1. ITIL (Information Technology Infraestructure Library)

ITIL es considerado una librería de mejores prácticas que se encuentra enfocada al sistema de gestión de la operación de los servicios de TI, el cual fue elaborado y respaldado por la oficina del gobierno británico. Para el presente trabajo nos concentraremos en la versión 3 de ITIL, la cual cuenta cinco libros de servicios en los cuales se describen los procesos indispensables que deben considerarse en cada etapa del servicio.

Los procesos que son aplicables directamente para ser realizados por el SOC son los siguientes:

- Gestión de la Seguridad de la Información, que corresponde al libro Diseño del Servicio
- Gestión de Incidencias, que corresponde al libro Operación del Servicio

7.1.1. Gestión de la Seguridad de la Información

El objetivo principal de este proceso es poder alinear las actividades de seguridad de TI con las de la organización garantizando la adecuada gestión de la seguridad de la información en todos los servicios de la empresa. Entre las actividades que se definen que se pueden realizar en este proceso, se pueden nombrar las siguientes actividades y tareas que pueden ejecutarse o definirse por los integrantes del SOC en colaboración con el resto de áreas de la organización para poder garantizar que todas las necesidades del negocio están siendo consideradas:

- Diseñar y definir una política de seguridad de la información que sea aplicable para todos los empleados y servicios de la organización.
- Los responsables de la seguridad de la información deberán elaborar un plan de seguridad en el que se incluya los niveles adecuados de seguridad para todos los servicios prestados tanto a los clientes como a los proveedores de a empresa.
- El SOC en conjunto con la colaboración de las demás áreas de la organización, realizar la implementación del plan de seguridad definido.
- El responsable de la seguridad debería monitorear y evaluar el cumplimiento del plan de seguridad y las políticas de seguridad.
- El personal del SOC debería implementar medidas para poder supervisar proactivamente los niveles de seguridad de la empresa.
- Realizar periódicamente procesos de auditoría de seguridad tanto técnicas como de la gestión de la seguridad.

7.1.2. Gestión de Incidentes

Este proceso tiene como objetivo principal poder resolver de manera ágil y eficaz cualquier incidente que cause la interrupción o mal funcionamiento de un servicio. Este proceso de gestión de incidente como se lo menciono dentro del Capítulo V del presente trabajo, es un proceso que puede ser ejecutado y controlado por el personal del SOC dentro de una organización. Entre sus metas principales se puede nombrar las siguientes:

- Detectar cualquier alteración en los servicios de TI
- Registrar y clasificar estas alteraciones
- Asignar a personal encargado de restaurar el servicio según se define el SLA del servicio.

El proceso de gestión de incidentes de ITIL propone un conjunto de actividades (ITIL, 2011) que deben realizarse durante la ejecución de este proceso, las cuales pueden ser ejecutadas por personal del SOC:

- Identificación del Incidente: Esta actividad se enfoca en todas las tareas que se deberían realizar para poder identificar un posible incidente antes de que ocurra, un ejemplo de esto es el monitoreo por medio de herramientas automatizadas de todos los activos y servicios críticos de la empresa.
- Registro de Incidentes: Se enfoca en el registro del incidente en una herramienta automatizada para que su gestión sea más adecuada, este registro debe recopilar toda la información posible acerca de la naturaleza del incidente para que en caso de ser escalado a otras áreas, los responsables tengan toda la información disponible para su solución.
- Categorización y Priorización de Incidentes: La categorización se centra en analizar la información que se tiene del incidente y poder asignarlo a un tipo o categoría de acuerdo a lo definido por el SOC de la empresa, esto ayudaría a agilitar la solución del incidente, al contar con procedimientos para la solución de incidentes según la categoría a la que pertenece. Mientras que la priorización del incidente se enfoca en poder asignar una calificación según la urgencia e impacto del incidente sobre el negocio, para poder realizar esto, el SOC necesita definir una tabla de niveles de prioridad en ambos aspectos. Una vez realizado estas dos actividades se agilitará la solución del incidente.
- Diagnóstico Inicial: Esta actividad se refiere al análisis inicial que el analista del SOC realiza sobre el incidente para poder identificar los síntomas y la causa raíz del mismo, puede suceder que el incidente sea solucionado tras el diagnóstico inicial, en ese caso el analista procede con el cierre del mismo.
- Escalamiento del Incidente: Esta actividad se realiza después del diagnóstico inicial que el analista realiza, en caso de no poder solucionar el incidente se lo escala a un nivel superior o a otra área involucrada. Es posible que ciertos tipos de incidentes requieran más de un escalamiento a diferentes áreas de la organización.
- Investigación y Diagnóstico: Esta actividad se centra en todos los mecanismos que se utilicen para poder realizar la investigación de la información del incidente y poder diagnosticar la casusa raíz del mismo.
- Resolución y Recuperación: Se enfoca en la identificación de una solución para el incidente y las medidas a implementar para poder realizar la recuperación del servicio afectado a su funcionamiento normal.

- Cierre del Incidente: Esta actividad es realizada por el SOC, se encarga de confirmar la solución y recuperación del incidente y la información registrada. Se procede con el cierre del incidente y registro de las soluciones aplicadas y lecciones aprendidas.

7.2. NIST (National Institute of Standards and Technology)

Este instituto internacional creado por el departamento de comercio de Estados Unidos, mantiene una serie de guías para incrementar y mejorar el desempeño de los servicios de tecnología dentro de una organización. Entre las guías propuestas por el NIST, la que corresponde a la respuesta ante incidentes, es la que se puede relacionar directamente con las funciones y actividades que pueden realizarse en un SOC.

La Guía para el Manejo de Incidente (SP800-61r2), se enfoca en proveer lineamientos para una gestión efectiva de los incidentes mediante la mitigación de los riesgos de los incidentes de seguridad (Computer Security Incident Handling Guide, 2012). Esta guía mantiene dos partes importantes:

- Definir la capacidad del proceso de respuesta a los incidentes de seguridad
- Establecer un proceso para el manejo de incidentes.

Dentro de lo definido en la sección de Manejo de Incidentes, se encuentra el ciclo de vida de la respuesta ante incidentes, que mantiene las siguientes fases: Preparación, Detección y Análisis, Contención, Erradicación y Recuperación y Actividades Post-Incidente.

En cada una de estas fases se presentan actividades que son aplicables para ser realizadas por el SOC de una organización.

7.3. COBIT5 for Information Security

COBIT5 es un framework de gobierno de las tecnologías de información que provee una serie de herramientas para que los funcionarios de las organizaciones puedan relacionar los requerimientos de control con los aspectos técnicos y riesgos del negocio. COBIT5 for Information Security, es una guía profesional que provee una nueva generación de lineamientos de ISACA para la gestión empresarial y gestión de la seguridad de la información (COBIT5 for Information Security, 2012).

COBIT5 define “habilitadores” que interactúan entre sí, que son el respaldo de la organización para poder alcanzar los objetivos del negocio:

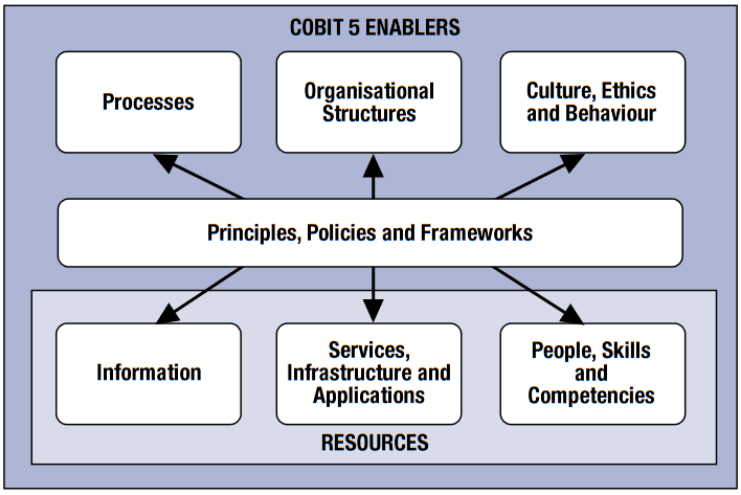


Figura 15. Habilitadores de COBIT5 (ISACA, 2012)

COBIT5 for Information Security provee una serie de lineamientos específicos que se encuentran relacionados con los habilitadores antes mostrados:

- Políticas, procedimientos y marcos de trabajo para la seguridad de la información.
- Procesos donde se incluye actividades específicas relacionadas con la seguridad de la información.
- Estructura Organizacional relacionada con la seguridad de la información.
- Factores determinantes para un gobierno y manejo de la seguridad de la información exitoso, en términos de cultura, ética y comportamiento de la organización.
- Tipos de información
- Capacidades de servicio necesarias para proveer funciones de seguridad de la información a una empresa
- Especificaciones de personas, habilidades y competencias relacionadas con la seguridad de la información.

Con la definición e implementación de estos habilitadores se podría diseñar y determinar las funciones, actividades y capacidades de un Centro de Operaciones de Seguridad dentro de la empresa, de esta manera el SOC y todo lo relacionado con la seguridad tendría un enfoque integral y orientado al negocio para la gestión de la seguridad.

CAPÍTULO VIII

8. Conclusiones

Durante el desarrollo del presente trabajo, se evidencio la importancia de tener un Centro de Operaciones de Seguridad (SOC) para controlar constantemente el estado de la seguridad lógica de una organización, mediante el monitoreo en tiempo real de las actividades que se realizan en los recursos tecnológicos de la empresa, de igual manera las actividades de los usuarios que gestionan estos recursos y administrando dispositivos de seguridad perimetral para evitar que amenazas externas puedan acceder fácilmente a la red interna de la empresa. Al no contar con un estándar o norma que se enfoque exclusivamente en las funciones o actividades dentro de un SOC, realizamos una investigación considerando las buenas prácticas actuales, en la que se identificó los aspectos primarios y secundarios que deberían considerarse en el diseño de un SOC y la triada de operaciones de seguridad en la que se pueden basar para la definición de las funciones y actividades a desempeñar dentro del SOC y que herramientas se podrían utilizar, con un especial énfasis en la gestión de respuesta ante incidentes de seguridad.

Llegando a la conclusión que un SOC es de vital importancia dentro de las organizaciones para poder garantizar la seguridad de la información y de los servicios que la tratan, en especial en las empresas con información sensible y crítica como lo son las instituciones del sector financiero.

Para poder aterrizar este trabajo dentro del sector ecuatoriano, se profundizó en los requerimientos de seguridad impuestos por parte de los entes de control (Superintendencia de Bancos) del sector financiero del Ecuador, en los cuales se observaron que se proponen diferentes actividades y controles que deberían ser gestionados por un área independiente y especializada con personal capacitado y experiencia en gestión de seguridad de la información, como lo sería un Centro de Operaciones de Seguridad. Se realizó una comparación de lo requisitos de seguridad impuestos por el ente de control del Ecuador versus el estándar internacional ISO/IEC 27000, concluyendo que se cubren la mayor parte de los dominios del estándar y se encuentra alineado con la implementación de Sistema de Gestión de la Seguridad de la Información.

Además, se analizó diferentes normas y estándares internacionales que determinan lineamientos y actividades de seguridad que son aplicables dentro de un SOC.

Finalmente, es poco probable que se pueda implementar un SOC que sea capaz de evitar el 100% de las amenazas a las que se enfrenta una empresa, sin embargo, contando con un SOC que mantenga procedimientos formales definidos basándose en guías de buenas práctica, normas y estándares internaciones; con personal especializado, capacitado y experimentado en la gestión de la seguridad; y con herramientas tecnológicas de seguridad que ayuden a prevenir, identificar, controlar y monitorear posibles amenazas de seguridad; es muy probable que se puedan prevenir varios tipos de incidentes, identificar brechas de seguridad para tomar acciones mitigantes y responder de forma ágil y efectiva ante incidentes presentados.

Bibliografía

Listado de Referencias

Admin. (16 de Marzo de 2018). *10 TOP Vulnerability Assessment Scanning Tools*. Obtenido de CWatch Comodo: https://cwatch.comodo.com/blog/website-security/top-10-vulnerability-assessment-scanning-tools/

Alien Vault. (12 de Agosto de 2015). *Guía del Técnico para establecer un Centro de Operaciones de Seguridad.* Obtenido de Alien Vault: https://learn.alienvault.com/c/5-security-controls?x=5v9G6V&utm_internal=soc-irlookbook&xs=16860

Areitio, J. (2008). *Seguridad de la Información. Redes, informática y sistemas de información.* España: Ediciones Paraninfo, S.A.

CA Technologies. (2018). *CA Tecnologies Web.* CA Technologies. Obtenido de Insider Threat 2018 Report.

ESSET. (2018). *Security Report - Latinoamérica.* ESSET.

Evans, J. D. (8 de Marzo de 2015). *Retos de la seguridad de la información para el sector financiero*. Obtenido de Notas de Prensa de TI: http://ndp.computerworld.net.ve/retos-de-la-seguridad-de-la-informacion-para-el-sector-financiero/

Hillsberg, A. (11 de Enero de 2019). *IT Asset Management Software*. Obtenido de Finances Onine: https://financesonline.com/it-asset-management/

ISACA. (2012). COBIT5 for Information Security. *COBIT5 for Information Security*. United State: ISACA.

ISO/IEC. (2005). *17799 Tecnología de la Información - Técnicas de Seguridad - Código para la práctica de la gestión de la seguridad de la Información.* ISO/IEC.

ISO/IEC. (2012). *27037 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.* ISO/IEC.

ITIL. (2011). ITIL Service Operation. *ITIL Service Operation*. United Kingdom: TSO (The Stationery Office).

Komand. (17 de Agosto de 2016). *How to Hire a strong and effective Security Team.* Obtenido de Komand: https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-komand-hire-strong-effective-security-team-whitepaper.pdf

MacMillan, L. (24 de Febrero de 2014). *Smart Protection Platform: Innovating to Beat the Bad Guys*. Obtenido de Trend Micro: https://blog.trendmicro.com/smart-protection-platform-innovating-beat-bad-guys/

NIST - Cichonski Paul, Millar Tom, Grance Tim, Scarfone Karen. (Agosto de 2012). Computer Security Incident Handling Guide. *NIST.SP.800-61r2*. Estados Unidos: NIST.

NIST - Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang. (Agosto de 2006). Guide to Integrating Forensic Techniques into Incident Response. *NIST.SP.800-86*. Estados Unidos: NIST.

Passeri, P. (22 de Febrero de 2018). *HACKMAGEDDON*. Obtenido de Information Security Timelines and Statistics: https://www.hackmageddon.com/2018/10/11/september-2018-cyber-attacks-statistics/

Pierre Jacobs, A. A. (30 de Julio de 2013). Classification of Security Operation Centers. Grahamstown, South Africa: Department of Computer Science Rhodes University.

Robb, D. (18 de Julio de 2017). *Eight Top Threat Intelligence Platforms*. Obtenido de eSecurity Planet: https://www.esecurityplanet.com/products/top-threat-intelligence-companies.html

Robb, D. (20 de Febrero de 2018). *9 TOP Intrusion Detection and Prevention Systems*. Obtenido de eSecurity Planet: https://www.esecurityplanet.com/products/top-intrusion-detection-prevention-systems.html

Robb, D. (6 de Noviembre de 2018). *TOP 10 SIEM Product*. Obtenido de eSecurity Planet: https://www.esecurityplanet.com/products/top-siem-products.html

SANS, A. T. (2014). *Incident Response: How to Fight Back.* Bethesda, MD: SANS™ Institute.

Superintendencia de Bancos del Ecuador. (30 de Julio de 2018). Resolución No. SB.2018.771. *Resolución No. SB.2018.771*. Quito, Pichincha, Ecuador: Superintendencia de Bancos del Ecuador.

Superintendencia de Bancos del Ecuador. (s.f.). *Misión y Visión*. Obtenido de Superintendencia de Bancos del Ecuador Website: https://www.superbancos.gob.ec/bancos/mision-y-vision/

Tabona, A. (10 de Julio de 2018). *Top 20 Free Digital Forensic Investigation Tools for SysAdmins*. Obtenido de TechTalk: https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/

Vieites, Á. G. (2014). *Enciclopedia de Seguridad Informática.* Madrid, España: RA-MA, S.A. .

Wueest, C. (2017). *ISTR - Financial Threats Review 2017.* Symantec.

Anexos

ANEXO I Ventajas y Desventajas de utilizar un SOC Interno o Externo en la Organización

VENTAJAS	DESVENTAJAS
Implementación de un SOC interno en la Organización.	
• Personal dedicado a las actividades de seguridad de la organización. • Mejor conocimiento de la organización que una empresa externa. • Las herramientas y soluciones son más fáciles de personalizar. • Log de actividades almacenados localmente. • Personal interno tiene mayor probabilidad de distinguir correlaciones entre personas o eventos internos.	• Mayor inversión inicial para la implementación del SOC y también un nivel de presión alto para alcanzar el ROI (Return On Investment). • Existe la probabilidad de que el personal interno llegará a colisionar con el atacante. • Puede ser difícil encontrar personal capacitado y especializado para poder realizar las funciones de un SOC.
Tercerizar un SOC a un empresa de seguridad	
• Se evade el valor capital para la implementación, por lo general se paga por el hardware o software. • Se expone a múltiples clientes dentro del sector industrial de la organización. • Frecuentemente es más económico que una solución interna. • Imparcialidad. • Pueden llegar a ser bastante flexibles y escalables • Se definen SLA entre la organización y la empresa de seguridad	• La empresa de seguridad no podrá llegar a conocer la organización al mismo nivel que el personal interno. • Carecen de personal dedicado para una organización determinada. • Riesgo de mal manejo de la información de la organización. • Probabilidad de que no todos los log de actividades se almacenen • El almacenamiento del log de actividades sería en una fuente externa a la organización.. • Pueden carecer de personalización para cada organización.

ANEXO II Interrogantes básicas para conocer los activos y nivel de seguridad de la Organización

INTERROGANTE DE SEGURIDAD	ACTIVIDADES A REALIZAR
¿Qué activos debo proteger?	• Realizar un proceso de identificación de activos críticos para que la organización siga funcionando, como por ejemplo:

INTERROGANTE DE SEGURIDAD	ACTIVIDADES A REALIZAR
	○ Sistemas críticos para actividades diarias ○ Sistemas que dependen de los sistemas críticos ○ Sistemas y dispositivos que almacenas y gestionan información sensible • Definir y Priorizar los esfuerzos de los activos considerados como críticos, para responder a los ataques y contener brechas de seguridad.
¿Cuál de mis activos son vulnerables a ataques?	• Una vez identificado los activos que son críticos para la organización, se debe realizar procesos de análisis de vulnerabilidades en estos activos para poder identificar las debilidades de cada uno. • El proceso de análisis de vulnerabilidades demanda bastante tiempo y esfuerzo, por esta razón se pueden utilizar diferentes enfoques para automatizar este proceso: ○ Escaneo activo de red para explorar los hosts de la misma, usando tráfico de red diseñado para hacer evidente posibles vulnerabilidades existentes en los hosts escaneados. ○ Análisis basados en hosts, esto se puede realizar utilizando un motor de análisis sobre los software se podría detectar de manera más precisa las vulnerabilidades, mediante la comparación de los paquetes del software verificado versus los paquetes de un software vulnerable. Para estos tipos de métodos es necesario utilizar una base de datos de vulnerabilidades actualizada, asimismo, se podría ejecutar estos métodos de verificación periódicamente para estar actualizado de las vulnerabilidades recientes.
¿De qué forma están siendo atacados mis activos?	• Para responder esta interrogante es necesario ejecutar procesos de detección de amenazas para poder detectar los ataques que se encuentran dirigidos a los activos vulnerables de la organización. • Un proceso de detección de amenazas puede realizarse por medio de diferentes enfoques: ○ Detección de Intrusiones en Red (IDS), este tipo de herramienta analizan el tráfico de red en busca de patrones o firmas de ataques que sean conocidos que indiquen actividad maliciosa. ○ Detección de Intrusiones Basadas en Host, estas herramientas se centran en el análisis del comportamiento y configuración de un sistema y detecta actividades

INTERROGANTE DE SEGURIDAD	ACTIVIDADES A REALIZAR
	sospechosas que podría conllevar a un compromiso del activo. ○ Detección de Intrusos Inalámbrica, esta herramienta evalúa las conexiones y tráfico WIFI para poder identificar redes y clientes maliciosos.
¿Cómo se si ha tenido lugar una brecha de seguridad?	• Para poder detectar si ha habido brecha de seguridad en los sistemas es necesario realizar proceso de monitoreo para buscar indicaciones de la brecha de seguridad y de esta manera poder cumplir con un tiempo de respuesta eficiente. • Para este proceso se pueden realizar emplear diferentes métodos: ○ Monitorización activa del servicio, para validar que los servicios que se están ejecutando en el host están disponibles. ○ Análisis de Flujo de Red, el cual analiza los protocolos y ancho de banda utilizado por un host de la red. ○ Captura de paquetes TCP/IP completo, para poder realizar el análisis forense del flujo en caso de ser necesario. ○ Detección de Intrusiones basadas en Host, para monitorizar los procesos y recursos que son utilizados por un sistema específico.

ANEXO III Prácticas de Seguridad para prevenir Incidentes

PRACTICA DE ASEGURAMIENTO	DESCRIPCIÓN
Evaluaciones de Riesgos	Realizar revisiones periódicas de los riesgos de por lo menos los activos más críticos de la organización es unas de las prácticas de seguridad más recomendadas. En esta práctica se hace un análisis de las vulnerabilidades y amenazas de los activos para poder determinar su prioridad y probabilidad de ocurrencia y si el riesgo puede ser mitigado, transferido o aceptado. Otro de las ventajas de realizar este tipo de evaluaciones es que se puede identificar nuevos activos críticos y por ende poder monitorear las actividades de los mismos.
Seguridad de Hosts o Servidores	Es necesario que estos equipos cuenten con un estándar de configuración basado en los lineamientos de seguridad

PRACTICA DE ASEGURAMIENTO	DESCRIPCIÓN
	previamente definidos por la organización. Asimismo, deben tener habilitada las auditorias de log de actividades y eventos de seguridad. Para poder asegurar estos equipos se debe realizar un monitoreo continuo sobre el host y su configuración.
Seguridad en Redes	La red perimetral de la empresa debe estar por defecto configurada para denegar la ejecución de cualquier actividad que no esté expresamente autorizada. Para esto hay que asegurar todos los puntos de conexión por medio del uso de VPNs, conexiones dedicadas a otras empresas, entre otros.
Prevención de Malware	Es recomendable el uso de software para detectar y detener el malware en la organización, el cual debería proteger tanto a los servidores, servidores de aplicaciones y base de datos, estaciones de trabajo, aplicaciones del cliente, entre otros.
Campañas de concienciación y entrenamiento del Usuario	Esta práctica es vital para todas las organizaciones, debido a que todos los empleados deben estar en conocimiento de las políticas y procedimientos de seguridad de la empresa para evitar crear posibles brechas de seguridad. Esta práctica debe realizarse de manera periódica para fomentar un trabajo seguro y óptimo entre los empleados Esta práctica también incluye compartir lecciones aprendidas de incidentes de seguridad pasados entre los usuarios para evitar que un incidente similar vuelva a presentarse.

ANEXO IV Actividades a realizar en el análisis de incidentes

ACTIVIDADES	DESCRIPCIÓN
Perfilar Sistemas y Redes	Perfilar se refiere a medir y registrar las características normales y esperadas de los dispositivos de sistemas y redes para que en el caso de haber sido cambiadas de manera maliciosa durante un incidente se puede identificar de manera más fácil. Las herramientas de validación de

ACTIVIDADES	DESCRIPCIÓN
	integridad de archivos realizan este proceso y crean checksums de seguridad para poder identificar cambios que puedan ser realizados.
Tener conocimiento del comportamiento normal	El personal del SOC debe poseer conocimiento sobre el comportamiento normal de la red de la empresa y sobre eventos y actividades que se ejecutan, de esta manera es más sencillo para el personal poder detectar actividad fuera de la rutina normal. Aunque es imposible llegar a conocer al 100% el comportamiento de los recursos informáticos mediante la revisión y análisis de log de los recursos se puede llegar a poseer un fotografía bastante amplia del comportamiento normal en las actividades de la organización.
Crear un política de retención de información de Log	Información relacionada con un incidente puede estar registrada en varias partes como IDPS, routers, servidores, etc. Para lo cual es importante contar con una política de retención de información donde se especifique el tiempo que deberá mantenerse los log de información, lo cual serviría para detectar actividades anteriores al incidente que se encuentren relacionada. Otra razón importante para retener información es que los incidentes comúnmente no se identifican después de cierta cantidad de tiempo, por lo cual es importante poder hacer revisiones previas a la fecha de detección del incidente.
Realizar correlación de Eventos	Este proceso es importante durante el análisis del incidente debido a que puede haber información relevante en varias fuentes es necesario hacer una correlación de eventos de diferentes fuentes para poder tener una imagen completa de lo ocurrido.
Mantener el reloj de todos los Hosts Sincronizados	Esto ayudará que el proceso de correlación de eventos sea más fácil de realizar, por eso es preferible contar con un timestamp consistente en todos los log. El protocolo NTP es el encargado de mantener sincronizado los relojes de los recursos de las organizaciones.
Mantener y Utilizar una Base de Conocimiento	La base de conocimiento debe poseer información que los responsables pueden acceder rápidamente durante el proceso de análisis. Dentro de la base es necesario tener varios tipos de información de los incidentes previamente gestionados, como características, actividades de solución, personal involucrado, log de IDPS, código de errores, entre otros.

ACTIVIDADES	DESCRIPCIÓN
Utilizar motores de búsqueda de Internet	Utilizar este tipo de herramienta podría ayudar a los analistas a encontrar información relacionada con incidentes similares que permitiría identificar más datos característicos sobre el incidente y maneras de cómo solucionarlo.
Ejecutar Sniffers o Recolectar datos adicionales	El uso de herramientas de sniffers puede llegar a ser útil para obtener información del tráfico de red durante el análisis del incidente. Para esto será necesario la configuración de un criterio específico de recolección para poder obtener un volumen de información posible de analizar. De acuerdo a la política de seguridad y privacidad de la organización podría ser necesario contar con autorización de un nivel superior para realizar esta actividad.
Filtrar Datos	Debido a que no se cuenta con tiempo y recursos ilimitados para revisar toda la información de todas las fuentes es importante contar con una estrategia para la filtración de datos y poder mostrar los más relevantes, sin embargo, esta estrategia es arriesgada debido a que puede existir cierta información de nuevos ataques o vulnerabilidades que pasen por alto los filtros y puedan ser ignorada.
Buscar asistencia de otros	Es posible que el personal del SOC no llegue a identificar toda la información necesaria para solventar el incidente, por eso es necesario consultar con otras fuentes internas de la organización como especialistas o en fuentes de información externas relacionadas con la seguridad.

ANEXO V Categoría para evaluar el impacto de un Incidente

CATEGORÍA	DEFINICIÓN
Categorías de Impacto Funcional	
Ninguno	No afecta a la habilidad de la organización de proveer sus servicios
Bajo	Afectación mínima, la organización puede todavía proveer sus servicios críticos pero ha perdido eficiencia

CATEGORÍA	DEFINICIÓN
Medio	La Organización no podrá proveer servicios críticos a un conjunto de usuarios del sistema
Alto	La Organización no puede proveer los servicios críticos a los usuarios del sistema
Categorías de Impacto sobre la Información	
Ninguno	Ninguna información fue expuesta, alterada, eliminada o comprometida.
Brecha en Privacidad	Información sensible personal e identificable de empleados, clientes, etc., ha sido expuesta.
Brecha en la Propiedad de la Información	Se accedió o filtro información de propiedad no clasificada, com por ejemplo información de estructura crítica protegida
Perdida de Integridad	Información sensitiva o crítica ha sido alterada o eliminada.
Categoría de Esfuerzo de Recuperación	
Regular	Tiempo de recuperación es predecible con los recursos existentes.
Suplementado	Tiempo de recuperación es predecible con los recursos adicionales.
Extendido	Tiempo de recuperación no predecible, recursos adicionales y ayuda externa es necesaria.
No Recuperable	Recuperación del incidente no es posible como por ejemplo información sensible es accedida y expuesta públicamente. Se realiza un proceso de investigación.

ANEXO VI Tabla Checklist para verificación de acciones generales para la Gestión de Incidentes

#	ACCIÓN	COMPLETADO
	Fase de Detección y Análisis	
1.	Determinar si un incidente ha ocurrido	
1.1	Analizar los indicadores del incidente	
1.2	Realizar correlación de información	
1.3	Realizar un proceso de investigación de información	
1.4	En cuanto se crea que un incidente ha ocurrido el analista debe comenzar a documentar y recolectar evidencia	
2.	Priorizar los incidentes gestionados basándose en los factores más importantes (impacto funcional, impacto en la información, esfuerzo de recuperación, etc.)	
3.	Notificar el incidente al personal interesado y relacionado tanto interno como externo	
	Fase de Contención, Erradicación y Recuperación	
4.	Adquirir, preservar, asegurar y documentar evidencia	
5.	Contener el incidente	
6.	Erradicar el incidente	
6.1	Identificar y mitigar todas las vulnerabilidades que fueron explotadas	
6.2	Remover malware, materiales inapropiados y otros componentes	
6.3	Si se descubre otros hosts infectados, repetir el pasos 1.1 y 1.2 para identificar todos los hosts afectados y luego realizar el paso 5 y 6	
7.	Recuperase del incidente	
7.1	Restaurar sistemas afectados a un estado operativo	
7.2	Confirmar que los sistemas afectados están funcionando de manera normal	
7.3	Si es necesario, implementar medidas de monitoreo para buscar actividad relacionada con el incidente gestionado	
	Fase de Lecciones Aprendidas y Mejora Continua	
8.	Crear un reporte de seguimiento del incidente	
9.	Realizar un levantamiento de las lecciones aprendidas del incidente con el personal involucrado	

ANEXO VII Cuadro comparativo de Herramientas SIEM

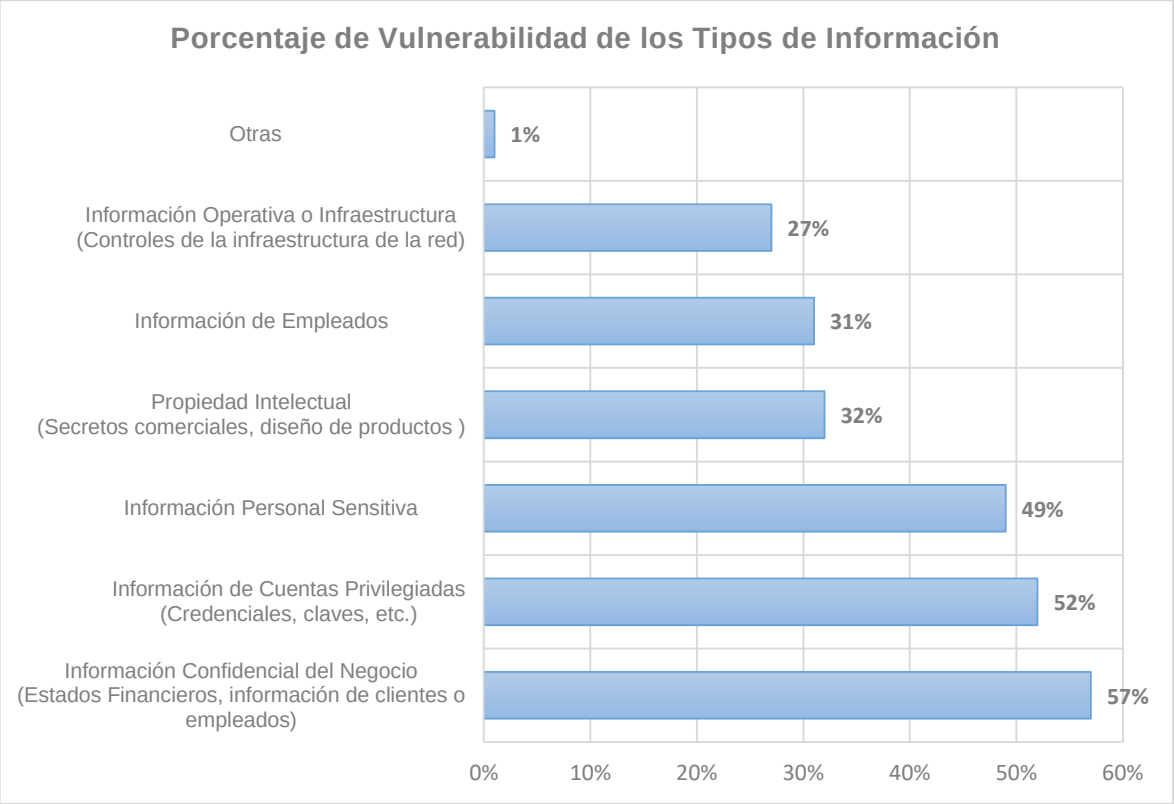
Top SIEM Vendors

●●●● BEST ●●● VERY GOOD ●● GOOD ● FAIR

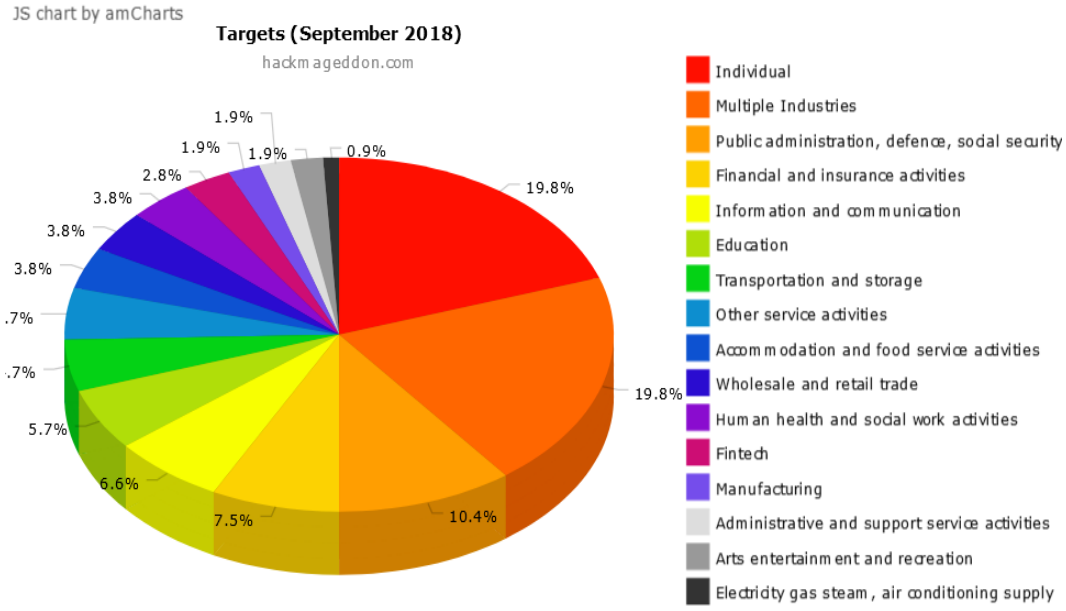
SIEM VENDOR	THREATS BLOCKED	SOURCES INGESTED	PERFORMANCE	VALUE	IMPLEMENTATION	MANAGEMENT	SUPPORT	SCALABILITY
splunk> ES	●●●●	●●●	●●●	●●●	●●	●●●	●●	●●●
LogRhythm ENTERPRISE	●●●	●●●●	●●●	●●	●●●	●●●	●●●	●●
USM	●●●	●●●	●●●	●●●●	●●●	●●	●●	●●●
MICRO FOCUS ArcSight	●●	●●●	●●●	●●	●●●	●●●●	●●	●●●
MICRO FOCUS Sentinel	●●	●●	●●	●●●	●●●	●●●	●●	●●●
McAfee ESM	●●●	●●●	●●●	●●●	●●	●●	●●●	●●●
Trustwave SIEM	●●●	●●●	●●●	●●●	●●	●●●	●●	●●●●
IBM QRadar	●●●	●●●	●●●●	●●●	●●	●●●	●●●	●●●
RSA NetWitness	●●	●●	●●●	●●	●●	●●	●●●	●●●
solarwinds LEM	●●	●●●	●●	●●	●●●●	●●	●●●	●●

SOURCE: eSecurityPlanet.com

ANEXO VIII Porcentaje de Vulnerabilidad de los tipos de Información



ANEXO IX Cuadro Estadístico "Objetivos de Ataque (Septiembre 2018)" (Passeri, 2018)



ANEXO X Mapa regional de Índices de infección por Malware en los Países de Latinoamérica

ANEXO XI Ciclo de Vida para la Defensa contra las Amenazas