ESTUDIO EXPLORATORIO SOBRE EL DESARROLLO DE UN MODELO DE GESTIÓN DE INCIDENTES DE SEGURIDAD PARA POSITIVA COMPAÑÍA DE SEGUROS S.A EN LA CIUDAD DE BOGOTÁ

JORGE ALONSO FLOREZ ROJANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS E INGENIERIA

MAESTRÍA EN GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN

BOGOTÁ

2022

ESTUDIO EXPLORATORIO SOBRE EL DESARROLLO DE UN MODELO DE GESTIÓN DE INCIDENTES DE SEGURIDAD PARA POSITIVA COMPAÑÍA DE SEGUROS S.A EN LA CIUDAD DE BOGOTÁ

JORGE ALONSO FLOREZ ROJANO

PROYECTO DE GRADO

Director
CESAR ANTONIO VILLAMIZAR NUÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
MAESTRÍA EN GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN
BOGOTÁ
2022

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá D.C. 09/06/2022

DEDICATORIA

Este trabajo de investigación lo dedico a mi esposa e hijos, quienes me acompañan con su amor y comprensión en todas las experiencias que adelanto. Sin ellos todo este esfuerzo habría sido inútil.

AGRADECIMIENTOS

A Dios por darme esta oportunidad y por permitirme alcanzar la meta luego de superar momentos difíciles, a mi familia, en especial mis hermanos por sus voces de aliento y paciencia cuando me sentí desfallecer, a compañeros como David Ramírez quien siempre brindó el acompañamiento en la “última milla” y al Ing. Cesar Antonio Villamizar Núñez por su guía y continua retroalimentación.

Tabla de contenido

Resumen

El presente trabajo propone la implementación de un Modelo de Gestión de Incidentes de Seguridad de la información para Positiva S.A. en Bogotá, que le permita contar con los recursos necesarios para reconocer y sobreponerse de las situaciones de riesgo que puedan afectar su infraestructura o información.

No obstante, que la norma ISO 27000 se refiere a la gestión de incidentes de seguridad de la información, muchas empresas no lo tienen en cuenta siendo este un aspecto muy relevante en lo concerniente a la disponibilidad, integridad y confidencialidad de la información. La norma ISO 27000 da recomendaciones para el manejo de las situaciones en las que se encuentra en riesgo la seguridad de la información y además plantea mecanismos para proceder y gestionar estos incidentes, incluyendo las responsabilidades con los usuarios encargados de su salvaguarda.

Positiva S.A. podrá contar con una herramienta (Modelo) para atender las situaciones en las que se encuentre comprometida su información

Abstract

This paper proposes the implementation of an Information Security Incident Management Model for Positiva S.A. in Bogotá, which allows you to have the necessary resources to recognize and overcome risk situations that may affect your infrastructure or information

However, that the ISO 27000 standard refers to the management of information security incidents, many companies do not take it into account, this being a very relevant aspect regarding the availability, integrity and confidentiality of information. The ISO 27000 standard gives recommendations for the management of situations in which information security is at risk and also proposes mechanisms to proceed and manage these incidents, including the responsibilities with the users in charge of safeguarding them.

Positive S.A. can have a tool (Model) to deal with situations in which your information is compromised

Contenido

En el proyecto de investigación que se pretende desarrollar se establecen las fases para la gestión de incidentes de seguridad de la información para Positiva S.A. en la ciudad de Bogotá, teniendo en cuenta que al final se entrega a la empresa un documento con la lista detallada de las Fases o acciones macro que deben aplicarse para la gestión de los incidentes de seguridad de la información, junto con una lista de actividades a ser aplicadas por un grupo multidisciplinario encargado de manejar los riesgos cibernéticos que puedan afectar el negocio.

Durante la ejecución de la metodología propuesta se plantea la entrega de los siguientes criterios:

- Acciones macro (Fases) que deben aplicarse para la gestión de los incidentes de seguridad de la información de la empresa
- Clasificación de los Incidentes de Seguridad de la Información acorde con las tendencias tecnológicas
- Grupo de respuesta a incidentes (CSIRT) para el manejo de los incidentes de Seguridad de la Información.
- Sistema de referencia (Base de datos de conocimiento) que le permita a la empresa contar con un histórico de lecciones aprendidas acorde con la tendencia del cibercrimen.

El proceso de incidentes de seguridad de la información contempla establecer una guía para el manejo de estos sucesos inesperados, por lo tanto, su compromiso será el tener un marco de referencia para la identificación y el registro de las acciones acometidas en la solución del incidente

Lista de Tablas

Lista de Figuras

Introducción

El sector productivo es cambiante incorporando procesos continuos de actualización tecnológica, lo que ha originado cambios en la manera de gestionar el negocio; se hace necesario adaptarse a los niveles de seguridad en crecimiento requeridos por los diferentes agentes de la economía,

Las organizaciones utilizan herramientas para el manejo de la información y así ofertar sus servicios en cualquier lugar del mundo, lo que conlleva a que aparezcan riesgos informáticos como la pérdida de información en un PC o amenazas por Internet que pueden llegar a generar indisponibilidad o desprestigio de una empresa.

La seguridad de la información busca preservar la confidencialidad, integridad y disponibilidad de los activos de información, entendiéndose los activos de información como los recursos que tienen valor y que le permiten a la Empresa operar correctamente para lograr los objetivos propuestos.

Un Modelo de Seguridad de la Información está basado en políticas (directriz de la organización en general), procedimientos (serie de pasos que regulan la ejecución y control de las normas) y estándares (reglas específicas de configuración que cumplen cada uno de los recursos tecnológicos de la organización).

Las tecnologías basadas en la WEB han aportado muchas ventajas a las organizaciones y sus clientes, pero las brechas de la seguridad de la información siguen siendo motivo de controversias

Propuesta investigativa

Problema de investigación

Los incidentes de seguridad de la información comienzan a identificarse con un diagnóstico al estado actual de la seguridad de la información en la organización. La metodología para la Seguridad de la Información la conforman procedimientos que involucran roles y responsabilidades asignados a la privacidad de la información, partiendo de un inventario de activos de información.

En el portal web diagnosticsnews.com (2020) se menciona que:

"(…) El crimen en línea ya supone la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo."

De acuerdo con la Norma ISO/IEC27035, un evento de seguridad se entiende como "presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad" (GTC-ISO/IEC 27035, 2012); y entiende que un incidente es:

"Un evento o una serie de eventos inesperados e indeseados, que van contra la seguridad de la información con una probabilidad significativa de comprometer las operaciones del negocio y amenazar la confidencialidad, integridad y disponibilidad la información" (Ibid. 2)

En un modelo de gestión de incidentes de seguridad de la información se contempla registrar cómo fueron tratados los incidentes para tener en cuenta lecciones aprendidas frente a las actividades realizadas antes, durante y después de los incidentes.

Un modelo de gestión de incidentes de seguridad de la información requiere además de llevar a cabo todas sus fases que haya conciencia en la empresa de la importancia de la seguridad de la información.

Para dar cumplimiento al ciclo de vida de la gestión de incidente de seguridad se contemplan las siguientes etapas:

A) Establecer las acciones macro (categorías) que deben aplicarse para la gestión de los incidentes de seguridad de la información.
B) Realizar la clasificación de los Incidentes de Seguridad de la Información acorde con las tendencias tecnológicas
C) Definir y diseñar los formatos para el reporte, valoración y resultado de incidentes
D) Llevar un registro de las lecciones aprendidas que permitan establecer acciones de mejora en el proceso de gestión de incidentes

Pregunta de Investigación

¿Cómo se puede implementar mecanismos de gestión de incidentes de seguridad de la información para que Positiva S.A. Compañía de Seguros pueda recuperarse de las situaciones de riesgo que afectan su infraestructura e información?

Tipo de Investigación

- Investigación Exploratoria: Con entrevistas y observación para levantar datos que permitan el diagnóstico inicial de debilidades provocadas por la no existencia de un modelo o guía de Gestión de Incidentes de Seguridad de la Información
- Investigación Descriptiva: Para delimitar los hechos que conforman el problema de investigación, como lo son:

- Establecer características propias de Positiva S.A. como unidad de investigación a partir de la matriz de activos de información allí existente.
- Definir las fases (etapas) en la gestión de incidentes de seguridad de la información
- Comprobar la posible asociación de las variables de investigación

La metodología de desarrollo está basada en los planteamientos definidos en materia de Seguridad de la Información y lineamientos de la Norma la ISO NTC 27000 – 2013 para la gestión de incidentes.

Para desarrollar la presente propuesta se ha contemplado las siguientes fases, basados en esa norma:

Fase 1: Recopilar información en Positiva S.A.

Realizar una consulta de la documentación existente en Positiva S.A. en materia de Gestión de Incidentes de Seguridad de la Información (políticas, procedimientos, manuales entre otros)

Fase 2: Definir las categorías (etapas) que deben aplicarse para la gestión de Incidentes de Seguridad de la Información como son:

- Planificación.
- Análisis del incidente
- Contención y recuperación del incidente
- Base de datos de conocimiento

Fase 3: Clasificar los Incidentes de Seguridad de la Información dependiendo de la infraestructura, riesgos (teniendo en cuenta que en términos de seguridad de la información aplican variables como impacto y probabilidad y que el impacto del incidente está representado

por el grado de afectación causado por el incidente) y criticidad de los activos en Positiva S.A., acorde con las tendencias tecnológicas

Fase 4: Definir el modelo de gestión de incidentes de seguridad de la información para Positiva S.A. que le permita asegurar una respuesta rápida y ordenada a los incidentes de seguridad de la información

Sistema de objetivos

El presente estudio exploratorio contempla el desarrollo de un Modelo de Gestión de Incidentes de Seguridad en el área de Gestión de TI para Positiva S.A. en la ciudad de Bogotá, que le permita contar con los recursos necesarios para recuperarse de las situaciones de riesgo que puedan afectar su infraestructura e información

- Realizar un análisis diagnóstico del estado actual de la empresa en el tratamiento de riesgos involucrados en un incidente cibernético. (Casares, 2013)
- Diseñar el método de planeación, ejecución y socialización para la implementación del estudio exploratorio.
- Mantener un registro adecuado de lecciones aprendidas para el establecimiento de acciones de mejora en las medidas de seguridad y el proceso de gestión de incidentes apoyado en la técnica de minería de datos

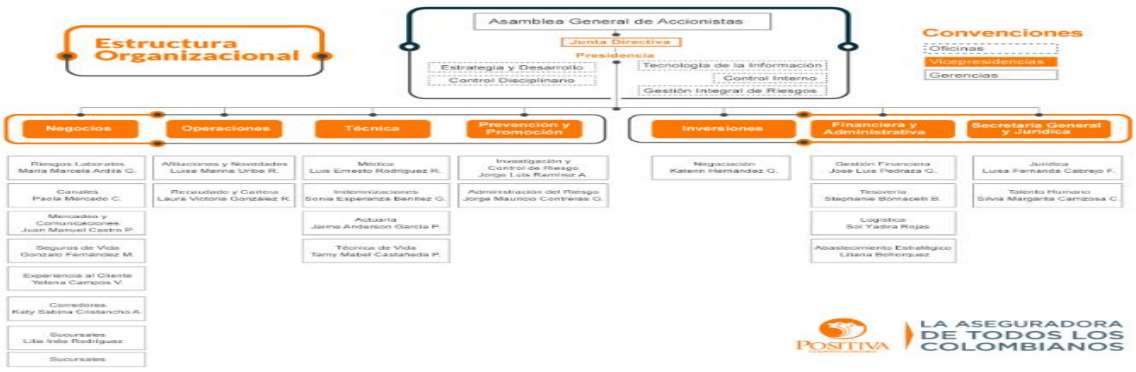
CAPITULO 1. Análisis diagnóstico para la Gestión de Incidentes de Seguridad de la Información

1.1. Estrategia organizativa de la Gestión de Incidentes de Seguridad de la Información

La historia de Positiva Compañía de Seguros S.A. inicia hace más de 60 años, cuando se constituyó Seguros Tequendama de Vida, luego adquirida por La Previsora S.A., quien recibió el 1 de septiembre 2008 la cesión de activos, pasivos y contratos de ARP Seguro Social; este mismo año, se iniciaron operaciones bajo el nombre Positiva Compañía de Seguros S.A.

Es una Sociedad Anónima con Régimen de Empresa Industrial y Comercial del Estado, su organización es la definida para las Empresas Industriales y Comerciales del Estado Colombiano: ofrece servicios en los ramos de administración de riesgos laborales - ARL y ramos de Seguros como accidentes personales, Vida Grupo y Vida Individual entre otros.

Ilustración 1. Organigrama



Fuente Quienes somos - estructura organizacional tomado de: www.positiva.gov.co

Positiva Compañía de Seguros S.A., dentro del documento "EST_2_2__MA03 Manual de Políticas de Seguridad de la Información", (Positiva S.A. 2020) ha adoptado un Sistema de Gestión de Seguridad de la Información (SGSI) basado en el Modelo de Seguridad y Privacidad de la Información del Ministerio de las TIC´s, la Norma Internacional ISO27001:2013, la Norma

Internacional ISO27032:2012, la Circular Básica Jurídica de la Superintendencia Financiera de Colombia; entre otros lineamientos del SGSI ha contemplado la existencia de un Modelo para detección, reporte y registro de incidentes de seguridad de la información.

Ilustración 2. Modelo de Operación

Fuente: Modelo de Operación tomado de: www.positiva.gov.co

Para el cumplimiento de las políticas de Seguridad de la Información en Positiva S.A., existen los siguientes roles y responsabilidades:

Oficina de Gestión Integral de Riesgos (OGIR) es la líder funcional de la gestión de riesgos y entre sus funciones es responsable de coordinar la identificación, análisis y evaluación de los riesgos existentes en los procesos y su impacto, atendiendo la metodología establecida y la información recolectada

Unidad de Seguimiento de Seguridad de la Información, fue creada a través de la Resolución 0853 de 2019, y está conformada por un grupo interdisciplinario de funcionarios de la alta dirección de la Compañía. Es el órgano encargado de conocer y asesorar al presidente en la

formulación de políticas, directrices y criterios a desarrollar entorno a la Seguridad de la Información.

Gestor o profesional de la seguridad de la información es la persona designada por Positiva S.A. para que cumpla las funciones de Oficial de Seguridad de la Información (CISO).

Administrador de Seguridad Informática persona designada para apoyar las actividades de seguridad y ciberseguridad en la implementación, operación, evaluación de los servicios tecnológicos a través de las herramientas de seguridad.

Profesional de Monitoreo de la Seguridad persona designada para apoyar las actividades de monitoreo en la implementación de las Políticas por parte de la Oficina de TI, así el cumplimiento de los usuarios en el uso de los servicios tecnológicos.

Oficina de Tecnología de Información (OTI) Es el área que está encargada de administrar la infraestructura tecnológica de la Compañía y debe cumplir la responsabilidad de cubrir los requerimientos de seguridad de la información y ciberseguridad, definidos para la operación, administración, comunicación de los sistemas y recursos de tecnológicos de la Compañía

La clasificación de los incidentes de seguridad en Positiva está acorde con la taxonomía definida por el COLCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) y homologada por la Superintendencia Financiera de Colombia – SFC- en la Circular Externa 033 de 2020.

En la Tabla 1-1 se expone la clasificación de incidentes de seguridad adoptada por Positiva, según la Circular Externa 033 de 2020 - Superintendencia Financiera de Colombia (Taxonomía Única de Incidentes Cibernéticos - TUIC)

Clase Ciberincidente	**Tipo**
Código Dañino (Malware)	Virus.

	Gusanos.
	Troyanos.
	Spyware.
	Rootkit.
	Ransomware.
	RAT (Control de Acceso Remoto).
Disponibilidad	Denegación (distribuida) de Servicios DDO/DDOS.
	Fallo (Hardware/Software).
	Error Humano.
	Sabotaje.
Obtención de Información	Escaneo de Vulnerabilidades de Activos.
	Snifing.
	Ingeniería Social.
	Phishing.
Intrusiones	Compromiso Cuenta de Usuario.
	Desfiguración.

	Spear Phishing.
	Pharming.
	Ataque de Fuerza Bruta.
	Inyección de Archivos de Forma Remota.
	Explotación de Vulnerabilidades Software.
	Explotación de Vulnerabilidades Hardware.
	Acceso no Autorizado a Red.
	Exploit.
	Poissoning.
Compromiso de Información	Acceso no Autorizado a Información.
	Modificación y Borrado no Autorizado de Información.
	Publicación no Autorizada de Información.
	Exfiltración de Información.
Fraude	Suplantación / Spoofing.
	Uso de Recursos no Autorizado.
	Uso Ilegítimo de Credenciales.

	Violación de Derechos de Propiedad Intelectual o Industrial.
Contenido Abusivo	Spam (Correo Basura).
	Acoso / Extorsión / Mensajes Ofensivos.
	Pederastia / Racismo /Apología de la Violencia, Etc.
Vulnerabilidades	Cross Site Scripting (XSS).
	Falsificación de Petición entre Sitios Cruzados (CSRF).
	Inyección SQL.
	Cookie reply, clonación de sesión.
	Ataques RFI / LFI.
	ataques SSL y certificados.
Otros	

Tabla 1 - Taxonomía de incidentes de seguridad de la información

Fuente: Circular Externa 033 de 2020 - Superintendencia Financiera de Colombia

1.2. Análisis del monitoreo sobre la infraestructura de Positiva

Positiva S.A. cuenta con un contrato tercerizado para la prestación de servicios que le permite alertar, gestionar y brindar recomendaciones sobre incidentes de seguridad mediante la utilización de un SIEM (correlación de eventos).

Alguna de las funciones que presta el SOC (Centro de Operación de Seguridad) son:

- Monitorear de forma continua (7x24) la infraestructura esencial del negocio y equipos de cómputo de usuarios finales
- Realizar actividades de identificación de identidades, vulnerabilidades, detección a través de la gestión de eventos e incidentes
- Detectar la respuesta en tiempo real de incidentes sobre los equipos de cómputo de usuarios y servidores, con el fin de mitigar ataques informáticos y fugas de información.

La figura 3 muestra cómo desde el SOC se ha gestionado en el período ago-21 a oct-21 eventos e incidentes de seguridad y eventos de identidades.

Ilustración 3 Eventos e incidentes de seguridad ago21- oct-21

La figura 4 muestra cómo desde el SOC se han identificado en el período nov-21 a ene-22 eventos de seguridad, y como fueron resueltas acorde a su criticidad.

Ilustración 4 Eventos e incidentes de seguridad nov21- ene-22

Las siguientes observaciones son el resultado del análisis de la información recopilada del sitio www.positiva.gov.co y de entrevistas con funcionarios de la Oficina de Gestión Integral de Riesgos y de la Oficina de Tecnologías de la Información:

- Las tareas que desempeña OTI en términos de monitoreo y respuesta con los eventos de seguridad que se presentan en la infraestructura de Positiva son acertadas por el uso de tecnologías de última generación acorde a la responsabilidad de preservar la integridad, disponibilidad, confidencialidad, así como la calidad de la información de Positiva S.A.; no obstante el esquema de activación y respuesta ante la materialización de eventos de seguridad (incidentes) no cuenta con un modelo o protocolo que le permita actuar oportunamente para restaurar la operación a la normalidad.
- El equipo de profesionales de OGIR y OTI que atienden los requerimientos de Seguridad de la Información y Ciberseguridad de la Compañía es calificado para sus funciones, sin embargo no disponen del suficiente personal para verificar a detalle todas las políticas aprobadas.

Resumen del Capítulo

La preparación, detección, reporte, evaluación, decisión y respuesta a un incidente de seguridad de la información de Positiva S.A. es obligación de todos los funcionarios y contratistas.

Con este estudio exploratorio se han identificado las áreas y roles que deben atender los eventos e incidentes que afecten la seguridad de la información asociados con los procesos del negocio, los sistemas de información y demás servicios tecnológicos dispuestos por Positiva, de tal forma que se tomen las acciones correctivas o preventivas que permitan gestionarlos de acuerdo con la normativa legal existente

Se hace necesario la adopción de un modelo para la detección, reporte y registro de incidentes de seguridad de la información, donde la Oficina de Gestión Integral de Riesgos con el apoyo de la Oficina de Tecnología de la Información, revisarán periódicamente y actualizará de ser necesario sus lineamientos acordes con las tendencias tecnológicas, de tal manera que puedan asegurar una respuesta rápida, eficaz, sistemática y cuyo proceso de atención sirva de referencia para el aprendizaje en la prevención de la ocurrencia de nuevos incidentes o la atención de los que se presenten con posterioridad.

CAPITULO 2. Desarrollo del Modelo para la Gestión de Incidentes de Seguridad de la Información

2.1. Características de un Modelo para la Gestión de Incidentes de Seguridad de la Información

Este capítulo establece la forma para poner en marcha un Sistema de Gestión de Incidentes de Seguridad de la información, a través de un modelo propuesto, integrando los incidentes de seguridad sobre los activos de información y estableciendo una adecuada capacidad para identificar, notificar, contener y recuperarse de los eventos no controlados que puedan afectar la infraestructura e información de Positiva, incluyendo como mínimo:

- Establecer roles y responsabilidades para evaluar los riesgos, que permita mantener la operación y la continuidad del servicio.
- Definir procedimientos formales de reporte y escalamiento de los incidentes de seguridad.
- Identificar o clasificar los incidentes de seguridad de la información para tratarlos con eficiencia.
- Registrar las lecciones que dejan los incidentes de seguridad de la información para prevenir la ocurrencia de futuros incidentes.

Las acciones para gestionar un incidente operacional se describen en la siguiente figura:

Ilustración 3 Fases de un Modelo de Gestión de Incidentes de seguridad de la información

Fuente Modelo de Seguridad de la Información Ministerio de TIC. Tomado de:

www.Mintic.gov.co

Cuando se determine que el incidente es de criticidad alta para la Compañía, la Oficina de Gestión Integral de Riesgos deberá activar el equipo de respuesta a incidentes de seguridad (CSIRT), con la función de inspeccionar, recolectar información, recuperar y dar respuesta al incidente de seguridad de la información.

Este CSIRT será el encargado de:

- Valorar el incidente identificando su clasificación e impacto.
- Determinar la causa raíz del incidente para establecer las acciones correctivas.
- Consolidar la evidencia recolectada y mantener la adecuada cadena de conservación y custodia para los fines legales del caso. Lo anterior, teniendo en cuenta el Manual de Procedimientos de Cadena de Custodia de la Fiscalía General de Nación.

Algunos de los perfiles que debe incluir el CSIRT son:

- Responsable de activar las tareas de contención y recuperación de los incidentes.
- Responsable de seguridad Informatica y la administración de las herramientas necesarias para la gestión de los incidentes
- Un equipo de comunicaciones con representantes de la alta dirección, los usuarios y los miembros del CSIRT.
- Equipo para la gestión de incidentes con representación de las diferentes áreas involucradas en el incidente de seguridad de la información

2.2. Definición del Modelo para la Gestión de Incidentes de Seguridad de la Información

En los incidentes de seguridad de la información las acciones macro que deben aplicarse para su gestión son:

- **Planificación:** En esta etapa se debe garantizar los recursos para la atención de incidentes y las herramientas necesarias para cubrir las demás etapas del ciclo de vida del incidente,

creando (si no existen) y validando (si existen) los procedimientos necesarios, incluyendo las mejores prácticas, para el aseguramiento de redes, sistemas, aplicativos, incluyendo la sensibilización y entrenamiento de usuarios en concordancia con los estándares de seguridad de la Compañía.

- **Detección, evaluación y análisis del incidente:** En esta esta etapa se realizan las actividades de análisis del incidente que permitan la identificación y gestión de los elementos de un incidente, como son las alarmas en los sistemas de seguridad, fallas en los servidores, reportes de usuarios sobre funcionamiento fuera de lo normal en los sistemas.

  Algunos elementos que suministran información sobre la futura ocurrencia de un incidente son los logs de servidores, de aplicaciones y de herramientas de seguridad..
  En Positiva se considera un incidente:

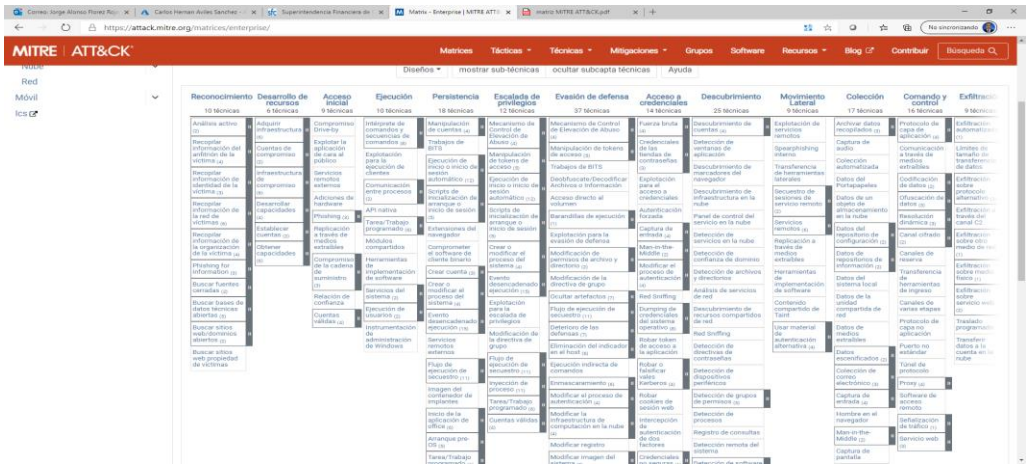
  - Incumplimiento de las políticas seguridad de la información
  - Ejecución de código malicioso
  - Ataque a través de virus (malware) contra la infraestructura tecnológica
  - Uso no autorizado de cuentas de acceso a los sistemas de información
  - Fuga de información por cualquier medio
  - Uso o acceso no autorizado de privilegios del sistema.
  - Uso inapropiado de recursos informáticos.
  - Robo o pérdida de información de carácter confidencial o reservada.
  - Alteración o modificación de un sitio de web de Positiva

  Durante la gestión del incidente es primordial la identificación de los elementos involucrados en la materialización de un incidente cibernético. La Superintendencia Financiera de Colombia (SFC), el COLCERT y la Asobancaria (Asobancaria,2019) definen

la taxonomía para el sector financiero, denominada TUIC (Taxonomía Única de Incidentes Cibernéticos), estableciendo los siguientes elementos que se deben identificar a la hora de clasificarlo:

- **Agentes de Amenaza:** Elementos causantes del incidente como por ejemplo Ciber ladrón, Empleado insatisfecho, Ciberacosador
- **Herramientas:** Elementos utilizados por los agentes de amenaza para materializar un incidente tales como herramientas físicas, scripts, agentes autónomos
- **Tácticas y Técnicas:** Se definen como el actuar de los agentes de amenaza para llegar a la materialización del incidente, haciendo uso del framework de MITRE (Mitre. 2021)

  Ilustración 4 matriz ATT



Fuente: Propia realización

- **Activos:** Identificar a qué elemento fue dirigido el ataque que concluyó con la materialización del incidente
- **Propósito:** Fin a cumplir. Este elemento brinda una clara identificación del incidente; por ejemplo asuntos políticos, pánico, daño, espionaje

- **Contención y recuperación del incidente:** En esta etapa se implementa la estrategia para evitar la transferencia del incidente y disminuir la pérdida de la integridad y disponibilidad de la información. Se toman decisiones como bloqueo de cuentas, desconectar la red, bajar sistemas.

  Una vez el incidente ha sido contenido se debe garantizar la no existencia de cualquier indicio o huella dejada por el incidente para luego proceder a restablecer la funcionalidad de los sistemas. A veces es necesario activar el Plan de Continuidad del Negocio o el Plan de Recuperación de Desastres cuando el incidente compromete de manera grave la operación de la compañía

- **Base de datos de conocimiento:** Establecer un proceso de registro de las situaciones que se presentaron en la gestión del incidente (lecciones aprendidas) es muy valioso en el establecimiento de medidas de seguridad y el proceso de atención de incidentes de seguridad de la información.

  Se debe tener en cuenta actividades que permitan obtener conocimiento frente a las actividades realizadas antes, durante y después de los incidentes de seguridad en la Compañía, tales como:

  - Análisis forense de seguridad de la información.
  - Establecer planes de mejora incluyendo controles de seguridad de la información.
  - Gestión de comunicaciones, informando a la organización los resultados en la gestión de incidentes de seguridad de la información.

La fase detección, evaluación, análisis del incidente y la fase contención y recuperación del incidente, serán tratadas a partir de las siguientes clases de Ciberincidente adoptadas por Positiva:

- Código Dañino (Malware)
- Disponibilidad
- Obtención de Información
- Intrusiones
- Compromiso de Información
- Fraude
- Contenido Abusivo
- Vulnerabilidades
- Otros

2.2.1. Código Dañino (Malware)

Código de programa diseñado para realizar una función no autorizada con un efecto negativo ya sea en la disponibilidad o la confidencialidad o la integridad de un sistema de información. Generalmente existe una interacción del usuario necesaria para activar o ejecutar el código. (Incibe-cert. 2019)

Se consideran dentro del código malicioso tipos como Virus, Gusanos, Troyanos, Spyware (tipo de malware que intenta mantenerse oculto mientras registra información en secreto y sigue sus actividades en línea), Rootkit (paquete de software malicioso diseñado para permitir el acceso no autorizado a un equipo), Ransomware (bloquea los archivos del usuario y luego reclama un pago para restaurar el acceso.

2.2.1.1 Planeación y preparación

Para la preparación en el manejo de un incidente por código dañino se debe:

- Concienciar a los usuarios acerca de los problemas que generan los códigos maliciosos, donde se les ilustre la forma que propagación y los síntomas de las infecciones.
- Mantener actualizado la base de información de virus de la herramienta contratada y tener acceso a boletines de laboratorios autorizados en el análisis de estos.
- Desplegar sistemas de detección de intrusos para detectar signos de códigos maliciosos, por ejemplo, cambios en las configuraciones o modificaciones en los ejecutables del sistema.
- Configurar los servidores de correo electrónico y clientes para bloquear los archivos adjuntos con extensiones que estén asociados con códigos malicioso.
- Limitar el uso de programas no esenciales con capacidades de transferencia de archivos, como por ejemplo mensajería instantánea no autorizados por TI.
- Concienciar a los usuarios para el manejo de los documentos adjuntos y enlaces en los correos electrónicos, es decir capacitarlos para que no abran enlaces ni archivos adjuntos de direcciones de correo desconocidas o extrañas.
- Generar boletines informativos periódicos donde se instruya a los usuarios en temas de seguridad de la información y de ciberseguridad.

2.2.1.2. Contención y recuperación del incidente

En este tipo de incidentes cuando un host ha sido infectado, lo más probable es que otros sistemas puedan ser infectados por la propagación que hace a través de la red, por lo que la contención de este incidente incluye la tarea de prevenir la propagación a otros sistemas.

La contención de un incidente por código dañino (Malware) debe contemplar:

- Bloquear comunicación entrantes y salientes: Identificar y aislar de la red los hosts infectados para evitar la propagación; Bloquear comunicación de la VLAN donde se encontró el equipo afectado

- Cerrar puertos de conexión: Realizar análisis de puertos que identifiquen los caballos de Troya en escucha de un host o puerta trasera en un puerto conocido
- Bajar servicios de aplicaciones: Analizar los registros de los servidores de correo, de seguridad y de sistemas de información a través de los cuales pudo hacer pasado el código malicioso.
- Revisar configuración de servidores de correo electrónico y cliente para bloquear correo con contenido sospechoso.

El proceso de recuperación de un incidente por código dañino (Malware) debe tener en cuenta:

- El software antivirus identifica y elimina eficazmente las infecciones de código malicioso, sin embargo, en ocasiones hay clases de código que no pueden ser eliminados o sustituidos por copias limpias, en los casos de aplicaciones, éstas pueden volver a instalarse en caso de estar infectadas.
- Restaurar el sistema desde una copia de seguridad que no se encuentre infectada.
- Desinfectar o poner en cuarentena los sistemas o servicios afectados.
- Cerrar las vulnerabilidades explotadas por el código malicioso
- Contactar al proveedor de ISP para validaciones correspondientes
- Regresar los sistemas afectados a su estado normal

2.2.2. Disponibilidad

Se considera cuando la propiedad de la disponibilidad se afecta tanto en el acceso, uso oportuno y confiable de un sistema, aplicación (servicio) o la información misma. Los incidentes que tienen que ser reportados son por denegación (distribuida) de Servicios DDO/DDOS, fallo (Hardware/Software), error Humano y sabotaje

2.2.2.1 Planeación y preparación

Para la preparación en el manejo de un incidente por denegación de servicio se debe:

- Tener claro por parte de los proveedores de servicio de internet y de los proveedores de segundo nivel su participación en el manejo de los ataques por denegación de servicios.
- Establecer claramente los procedimientos que la Oficina de Tecnología de la Información debe seguir para el escalamiento a los proveedores de servicios de internet, entre otros.
- Evaluar la posibilidad de participar e intercambiar información con otras organizaciones en una respuesta coordinada a un ataque generalizado que las afecte (ColCert, CCP y Mintic, entre otras).
- Configurar y monitorear los IDP para identificar posibles intrusiones en el tráfico de la red que deriven en ataques de Dos y DDos.
- Verificar la línea base de utilización del ancho de banda y de los recursos críticos de host con el fin de identificar alertas por desviaciones significativas.
- Mantener copias de cualquier información que permita el manejo de incidentes por denegación en caso de pérdida de internet de la organización o la conexión a la red local durante un incidente.
- Deshabilitar todos los servicios que no sean necesarios, y restringir el uso de los servicios que pueden ser explotados en un ataque DoS

2.2.2.2. Contención y recuperación del incidente

Contener un incidente generado por un ataque que afecte la disponibilidad está basado en la detención total del servicio, es decir, bajar el servicio para que los usuarios no puedan acceder a través de las IP definidas para ello. Sin embargo, el ataque puede trasladarse a otras direcciones IP.

La contención de un incidente por Disponibilidad debe contemplar:

- Bloquear dirección origen del ataque en el firewall perimetral
- Notificar IP a las demás herramientas de seguridad para realizar el bloqueo de forma manual
- Apagado del servicio afectado en servidor principal - Activar servidor alterno y dejar principal como señuelo
- Identificar las vulnerabilidades que son explotadas por el incidente
- Atacar a los atacantes

El proceso de recuperación de un incidente por disponibilidad debe tener en cuenta:

- Erradicar el incidente
- Recuperarse del incidente
- Regresar los sistemas afectados a su estado normal
- Verificar que los servicios afectados estén operativos

2.2.3. Obtención de Información

Según el portal web incibe-cert.es esta modalidad para obtener información "(…) consiste en recopilar la máxima cantidad de información de la plataforma tecnológica mediante buscadores, redes sociales, sitios web públicos con contenido filtrado, entre otros. Dicha información permite al atacante elaborar un "perfil" de su objetivo, aumentando así las probabilidades de éxito."

Algunos tipos de incidentes en esta categoría son: Escaneo de vulnerabilidades de activos, snifing (observar y grabar tráfico de red), ingeniería social, phishing (suplantación de identidad).

2.2.3.1 Planeación y preparación

Para la preparación en el manejo de un incidente por obtención de información se debe:

- Capacitar y concientizar a los empleados sobre los riesgos de ciberseguridad generados por ingeniería social
- Acentuar en los empleados lo valioso que es proteger su información personal y la forma como deben acceder a los sistemas de la empresa.
- Realizar ejercicios de prueba para conocer cómo es la respuesta de los usuarios frente a un ataque de fraude informático mediante correo (phishing).

2.2.3.2. Contención y recuperación del incidente

El incidente por obtención de información se presenta cuando un usuario o usuarios acceden a servicios que no tiene permisos, esto se logra porque se explotan vulnerabilidades en las plataformas básicas como sistemas operativos o de aplicaciones, de igual forma se presenta por la captura de nombres de usuario y contraseñas o a través de la ingeniería social.

En la contención de un incidente por obtención de información se deben tomar acciones como:

- Aislar los sistemas afectados.
- Desactivar el servicio afectado
- Eliminar de la ruta del atacante accesos en el ambiente.
- Desactivar las posibles cuentas de usuario usadas para el ataque
- Verificar las medidas de seguridad lógica y física
- Realizar la comprobación e identificación de otras alertas de intrusión

El proceso de recuperación de un incidente por obtención de información debe tener en cuenta:

- Reinstalación a través de un Backup seguro de la configuración de la máquina o del servicio afectado.
- Cambiar todas las contraseñas con la cual tenga relación.
- Desinfectar o poner en cuarentena los sistemas o servicios afectados

2.2.4. Intrusiones

Acciones tendientes para eludir los mecanismos de autenticación y acceso de un sistema. Contemplan desde un acceso a recursos sin autorización hasta múltiples intentos de inicio de sesión o mediante la ejecución de programas que aprovechen las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos o el hardware

Los tipos de incidente que deben ser analizados en esta categoría son: Compromiso cuenta de usuario, desfiguración, spear phishing (estafa de correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas específicas), pharming (el tráfico de un sitio web es manipulado para permitir el robo de información confidencial), ataque de fuerza bruta, inyección de archivos de forma remota, explotación de vulnerabilidades de software, explotación de vulnerabilidades de hardware, acceso no autorizado a red, poissoning (robar información y modificar el tráfico en las redes de datos)

2.2.4.1 Planeación y preparación

Para la preparación en el manejo de un incidente por intrusión se debe:

- Configurar software IDS de red y host para identificar y alertar los intentos de obtener acceso no autorizado.
- Contar con hardware y software IPS para prevenir intrusiones a la red.
- Capacitar a todos los administradores de los servicios tecnológicos de la Compañía para que tengan claro su papel en el proceso de gestión de estos incidentes.

- Aplicar técnicas de seguridad en red, como definir el perímetro para negar todo tráfico entrante que no esté permitido.
- Asegurar todos los métodos de acceso de remoto, módems y VPN.
- Realizar pruebas de vulnerabilidades para identificar los riegos graves en los hosts, con el fin de mitigarlos.
- Gestionar las vulnerabilidades identificadas a través de las herramientas instaladas con el fin de cerrarlas.

2.2.4.2. Contención y recuperación del incidente

El incidente por intrusión se presenta cuando un usuario o usuarios logran cambiar las configuraciones de las herramientas asignadas para la realización de las funciones, o cuando se tienen brechas de seguridad que permiten que personal ajeno del de TI pueda realizar cambios de configuraciones para beneficio propio o de terceros. Asimismo, se puede identificar un uso indebido de recursos cuando los usuarios hacen uso de la tecnología de la Compañía para temas distintos a los laborales o a los que están autorizados.

En la contención de un incidente por intrusión se deben tomar acciones como:

- Aislar los sistemas, servicios o equipos afectados.
- Identificar los cambios de configuraciones no autorizados.
- Identificar y eliminar de la ruta a través de la cual se logró cambiar la configuración.
- Desactivar las cuentas de usuario usadas para el ataque o cambio de configuración.
- Identificar cambios en los usuarios privilegiados o posibles alias no reconocidos.

El proceso de recuperación de un incidente por obtención de información debe tener en cuenta:

- Erradicar el incidente

- Restauración de los backup de configuraciones y aplicar hardening (endurecimiento o aseguramiento) a la infraestructura.
- Cerrar las vulnerabilidades explotadas que permitieron los cambios de configuración no autorizados.
- Contactar al proveedor de ISP para validaciones correspondientes de ser necesario
- Recuperarse del incidente

2.2.5. Compromiso de Información

Aquellos incidentes que puedan comprometer la información, tales como interceptaciones, acceso o alteración, directa o indirecta de información no autorizada, fuga de información sensible o no autorizada, perdida o borrado de información de forma intencionada, exfiltración de Información.

2.2.5.1 Planeación y preparación

Para la preparación en el manejo de un incidente por compromiso de información se debe:

- Disponer de servidores de registro centralizado, de igual forma, contar con la suficiente información de host de toda la organización almacenada en sitio seguro.
- Definir procedimientos para cambios de contraseñas en todos los servicios tecnológicos de la organización (aplicaciones, servidores y bases de datos).
- Verificar periódicamente las configuraciones de los permisos para acceso a los servicios tecnológicos de la compañía.
- Aplicar contraseñas que requieran complejidad para que sean difíciles de adivinar.
- Establecer procedimientos para registrar o inactivar cuentas de usuario.

2.2.5.2. Contención y recuperación del incidente

En la contención de un incidente por compromiso de información se deben tomar acciones como:

- Bloquear direcciones IP de Origen que tengan un comportamiento sospechoso de análisis de puertos en Equipos Firewall y /o Routers.
- Identificar el origen del volumen de las peticiones que superan el umbral normal de operación.
- Si se identifica que un usuario ha sido víctima de ingeniería social lo más recomendable es aislar el equipo a nivel de red mientras se confirma que este no haya sido vulnerado de alguna manera.
- Identificar el funcionario que permitió la manipulación por un tercero para realizar cambios en su equipo, bloquear usuario e inactivar en Directorio Activo

El proceso de recuperación de un incidente por compromiso de información debe tener en cuenta:

- Concienciar a los usuarios para el manejo de los documentos adjuntos y enlaces en los correos electrónicos, es decir capacitarlos para que no abran enlaces ni archivos adjuntos de direcciones de correo desconocidas o extrañas

2.2.6. Fraude

Uso de tecnologías de la información con el fin de distorsionar los datos e inducir a la víctima a hacer alguna actividad o tarea, provocando con ello afectación a la confidencialidad, integridad o disponibilidad de la información.

Se considera fraude la suplantación (Spoofing), el uso de recursos no autorizado, el uso ilegítimo de credenciales, la violación de derechos de propiedad intelectual o industrial.

2.2.6.1 Planeación y preparación

Para la preparación en el manejo de un incidente por fraude se debe:

- Los estafadores investigan y apuntan a empresas y productos con controles débiles; implementar controles de fraude sobre los procesos críticos que garanticen una protección suficiente de los activos de la Compañía.
- Fortalecer los procesos de administración de riesgos considerando en su tratamiento los aspectos éticos que enfrentan.
- Establecer herramientas de monitoreo que identifiquen el uso no autorizado de cuentas de acceso a los sistemas de información.
- Concienciar a los usuarios para el manejo de los documentos adjuntos y enlaces en los correos electrónicos, es decir capacitarlos para que no abran enlaces ni archivos adjuntos de direcciones de correo desconocidas o extrañas

2.2.6.2. Contención y recuperación del incidente

En la contención de un incidente por fraude se deben tomar acciones como:

- Cuando a un funcionario o contratista le pidan que envíe información personal, como una contraseña o un número de tarjeta de crédito, debe comunicarse con el remitente para confirmar al número de contacto indicado en el sitio web real.
- Comprobar manualmente la URL en el navegador web, para ver señales de suplantación de sitio web
- No dar clic en ningún enlace del correo electrónico sospechoso.
- Tener cuidado con los archivos adjuntos extraños, especialmente si tienen extensiones de archivo inusuales.
- Para evitar la suplantación de IP, ocultar la dirección IP al navegar por la web.

- Cambiar con regularidad las contraseñas
- No visitar sitios que no usen el cifrado HTTPS.
- Utilizar un navegador seguro especializado, priorizando la seguridad y la privacidad.
- Utilizar un software antivirus potente

El proceso de recuperación de un incidente por fraude debe tener en cuenta:

- Para el tipo de incidente uso de recursos no autorizado, validar permisos asignados sobre unidades de disco duro y carpetas de los usuarios.
- Para el tipo de incidente violación de derechos de propiedad intelectual o industrial, realizar la desinstalación de software no licenciado o no autorizado
- Para el tipo de incidente uso ilegítimo de credenciales, denegar permisos de acceso y bloquear el usuario

2.2.7. Contenido Abusivo

Los incidentes de abuso de contenido son aquellos en que se ve comprometida la imagen de la entidad o corresponden al uso de medios electrónicos de la entidad para realizar acciones que contienen aspectos prohibidos, ilícitos u ofensivos.

Dentro de esta categoría pueden encontrarse incidentes como spam (Correo basura), acoso, extorsión, mensajes ofensivos, pederastia, racismo, apología de la violencia.

2.2.7.1 Planeación y preparación

Para la preparación en el manejo de un incidente por contenido abusivo se debe:

- Establecer capacitaciones periódicas sobre procedimientos para la identificación de correos o mensajes maliciosos que permitan el abuso o mal uso de servicios informáticos internos o externos de la organización.

- Diseñar campañas de sensibilización para que los usuarios de correo identifiquen que los mensajes recibidos como parte de un grupo masivo de mensajes, todos teniendo un contenido similar, provengan de fuentes conocidas.
- Configurar los servidores de correo electrónico y clientes para bloquear los mensajes y/o archivos adjuntos con extensiones que estén asociados con pornografía infantil, glorificación de la violencia entre otros.

2.2.7.2. Contención y recuperación del incidente

En la contención y recuperación de un incidente por contenido abusivo se debe tener en cuenta:

- Para el tipo de incidente Spam (Correo Basura), marcar correo como no deseado
- Para el tipo de incidente Acoso / Extorsión / Mensajes Ofensivos, realizar la validación de mensaje y la eliminación de este
- Para el tipo de incidente Pederastia / Racismo /Apología de la Violencia, realizar la validación de mensaje y la eliminación de este.

2.2.8. Vulnerabilidades

Incidentes que son materializados por la explotación de una vulnerabilidad. Se consideran los ataques comunes como XSS (Cross Site Scripting por sus siglas en inglés), SQL injection (ataques de inyección), ataques CSRF (falsificación de petición entre sitios cruzados), ataques SSL y certificados, ataques basados en web (Cookie reply, clonación de sesión).

2.2.8.1 Planeación y preparación

Para la preparación en el manejo de un incidente por vulnerabilidades se debe:

- Gestionar las vulnerabilidades de los servicios tecnológicos y sistemas de información y aplicaciones de acuerdo con el inventario de activos de TI y su relación con los principios o criterios según sea definido por la Oficina de Tecnologías de la Información (OTI), en relación con los criterios seguridad y ciberseguridad (integridad, confidencialidad y disponibilidad), teniendo en cuenta las posibles debilidades en la infraestructura, por configuraciones por defecto, desarrollo de aplicaciones inseguras, debido a la existencia de defectos de configuración o programación, cuya activación de forma accidental o su explotación por parte de usuarios maliciosos podría afectar el correcto funcionamiento de los mismos, incrementando así el riesgo de exposición de la información que se almacena, transmite o procesa.
- Establecer el proceso de detección de vulnerabilidades tecnológicas basado en los siguientes aspectos básicos:
    - Pruebas de Intrusión (Ethical Hacking)
    - Detección automatizada de vulnerabilidades
    - Servicios de alerta temprana (Boletines de ciberseguridad)
    - Incidentes de seguridad de la información

2.2.8.2. Contención y recuperación del incidente

En la contención de un incidente por vulnerabilidades se deben tomar acciones como:

- Realizar el bloqueo - Aislar el equipo de la red.
- Restringir el acceso a la base de datos identificando plenamente el usuario que está extrayendo la información
- Identificar la dirección IP del Proxy malicioso para proceder con su respectivo bloqueo

El proceso de recuperación de un incidente por vulnerabilidades debe tener en cuenta:

- Hacer el despliegue de un backup del WAR/EAR (archivos comprimidos que contienen varias imágenes, archivos XML, archivos de propiedades y partes de código que forman una aplicación) que no tenga alguna afectación
- Proceder con el aislamiento si es posible y realizar la aplicación de algún parche de seguridad que pueda contener o controlar el incidente de seguridad.

2.3. Registro de lecciones aprendidas

Una vez han sido gestionados los incidentes de seguridad de la información comienza el registro de la forma como fueron manejados estos incidentes; se debe tener en cuenta las actividades que permiten precisar el conocimiento relacionado frente a las actividades realizadas antes, durante y después de los incidentes de seguridad en la empresa, conformando una base o repositorio de conocimiento.

2.3.1 Actividades Preliminares

- Establecer planes de mejoramiento que incluyan de controles de seguridad sobre la información
- Realizar evaluaciones sobre la operatividad de los procesos, los formatos utilizados para responder a los incidentes de seguridad de la información
- Establecer el mecanismo para compartir los resultados en la gestión de incidente de seguridad de la información.
- Definir la actividad de un análisis forense de seguridad de la información para establecer la causa raíz del incidente de seguridad de la información
- Establecer el mecanismo de participación de los terceros o proveedores cuando sean los generadores de los incidentes de seguridad de la información o a través de su infraestructura se afecte la de Positiva o su información.

2.3.2 Registro del conocimiento adquirido

Al finalizar y ser solucionado el incidente de seguridad que fue gestionado, es muy importante que se identifique y se adquiera conocimiento rápidamente de las lecciones recibidas del manejo y tratamiento del incidente y se asegure de que se actuó de acuerdo con las conclusiones.

Este registro de las lecciones aprendidas puede ser en los siguientes aspectos:

- Actualización de los controles de seguridad de la información y de los procedimientos de seguridad de la información.
- Revisión de los criterios y/o procedimientos de gestión de vulnerabilidades acorde a los resultados de la gestión en la atención del incidente
- Verificación de cambios en el esquema de gestión de incidentes de seguridad de la información, incluyendo procedimientos, reportes y base de conocimiento de seguridad de la información.
- Identificar pautas o tendencias de la forma como se presentan los incidentes de seguridad con el fin de adoptar mecanismos para actuar de forma proactiva a los riesgos que puedan generar incidentes de seguridad.

Resumen del Capítulo

Contar con un Modelo de Gestión de Incidentes de seguridad de la información le otorga a Positiva S.A. un enfoque estructurado y bien planificado para manejar adecuadamente los incidentes de seguridad de la información.

Este Modelo define responsabilidades y procedimientos para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información, incorpora una serie de actividades contempladas en el ciclo de vida de la gestión y respuesta a un incidente de seguridad, como acciones macro (Fases) que deben aplicarse para su gestión: **Planificación, Detección, evaluación y análisis del incidente, Contención y recuperación del incidente y la Base de datos de conocimiento.**

Adoptar o conformar un equipo de atención de incidentes de seguridad (CSIRT) permitirá a Positiva S.A. contar con un grupo de expertos en clasificar, estructurar y definir los procedimientos, para atender los incidentes que se presentan sobre los activos de información soportados por la infraestructura tecnológica de la entidad.

Continuar con el proceso de registrar y documentar la gestión después de un incidente es importante en la medida de reforzar el conocimiento, resaltando y acentuando los puntos de falla que permitieron se haya materializado el evento; la base de conocimiento es un punto inicial para el cambio teniendo en cuenta la dinámica cambiante de la tecnología y la rotación de personal en la empresa.

CAPITULO 3. Aplicabilidad del Modelo propuesto para la gestión de incidentes de seguridad de la información

Una vez se han establecido los elementos y criterios para la gestión de incidentes de seguridad de la información en Positiva, se describen a continuación las acciones que se deben tener en cuenta para gestionar un incidente operacional.

3.1. Notificación de incidentes

- El usuario que sospeche sobre la materialización de un incidente de seguridad informa el inconveniente o falla que se le presenta por los siguientes medios:
    - A la mesa de ayuda o a quien haga sus veces (Herramienta Aranda)
    - Telefónicamente (Extensiones 10527/28/29)
    - Correo electrónico (seguridadinformatica@positiva.gov.co)
- La mesa de ayuda analiza si el incidente reportado corresponde a un incidente de seguridad de la información o está relacionado con requerimientos propios de la infraestructura de TI; en caso que los profesionales de la mesa de ayuda puedan resolver en el instante la falla quedará atendida y se cerrará el incidente, de lo contrario, se eleva la petición a nivel funcional o técnico de segundo nivel según sea el caso, donde se procederá a identificar el activo de información afectado, alcance y pronóstico de propagación, así como los daños potenciales que el incidente pueda generar.
- En el evento que no pueda resolverse en ninguna de las instancias anteriores el caso o incidente será elevado al nivel de soporte de proveedor del servicio de la Compañía, si lo hubiere

3.2. Formatos para la gestión de incidentes

Para la gestión de incidentes se utilizarán los siguientes formatos:

- **Reporte de incidentes**: Se diligencia información relacionada con el incidente como la fecha y hora del incidente, descripción del incidente, activo de información afectado por el incidente y lugar de los hechos. De igual forma se registran datos básicos de los usuarios que reporta el evento o incidente, como, por ejemplo, Nombre, Cargo, Área, Correo electrónico, No. de teléfono o extensión, entre otros.
- **Valoración del incidente.** Se registra la información como fecha de evaluación o valoración del incidente con recomendaciones si es necesario
- **Informe de resultado del incidente.** Con la información recopilada del incidente, se procede a su análisis para determinar la causa raíz y con ellos las acciones a tomar para prevenir que el evento se repita o su impacto sea mínimo. En este formato se registran las actividades y los resultados de esta, las oportunidades de mejora y las conclusiones de la investigación del incidente.

3.3. Priorización de los incidentes y tiempos de respuesta

Con el fin de realizar una atención adecuada a los incidentes de seguridad de la información (análisis, contención y erradicación) se debe determinar el nivel de prioridad de este para atenderlo según la necesidad. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2013)

Para establecer la clasificación de los incidentes en Positiva se tendrá en cuenta la aplicación de las variables como Impacto y Criticidad, considerando la siguiente fórmula:

Impacto del incidente * Criticidad recurso afectado = Clasificación del incidente

Donde el Impacto del incidente está representado por el grado de afectación causado por el incidente, la Criticidad del recurso afectado está dado por la clasificación del recurso en el inventario de activos de información.

Después de aplicar la formula anterior, se tendría los siguientes niveles de clasificación:

Tabla 2

SEVERIDAD	DESCRIPCIÓN
Alto	Su propagación es de forma inmediata y afecta seriamente a uno o más servicios críticos. Pone en riesgo información reservada o clasificada.
Medio	Se identifica como amenaza potencial que afecta los procesos generales, pero no compromete inmediatamente un servicio crítico.
Bajo	No afecta los procesos, el evento o incidente se identifica y se controla con los recursos de primer nivel ya existentes.

El escalamiento de los incidentes se describe en la siguiente tabla:

Tabla 3

RELEVANCIA	ESCALAMIENTO
Alto	Se escala a los proveedores pertinentes y si es el caso a las autoridades externas competentes
Medio	Se escala al Equipo de Respuesta, Oficina de Gestión Integral de Riesgos, la Oficina de Tecnologías de la Información y a las áreas involucradas
Bajo	Solo se diligencia el caso en la herramienta de gestión de Mesa de ayuda, o se escala al responsable del activo de información involucrado en caso de ser necesario.

Adicionalmente se debe tener en cuenta los siguientes tiempos de respuesta para los incidentes identificados y clasificados así:

- **Alto: 0 – 6 horas:** Restablecer actividades lo más pronto posible para no presentar inconvenientes reputacionales
- **Medio: 7 - 48 horas:** Se pueden presentar inconvenientes de tipo legal.
- **Bajo: + de 48 horas:** Afecta de manera parcial la continuidad de la operación en la entidad; tratar de resolver antes de las 48 horas.

3.4. Matriz de roles y Responsabilidades

Por cada participante en la gestión de incidentes de seguridad de la información se muestra una descripción sobre sus responsabilidades y funciones.

Usuarios Positiva

- Velar porque los activos de la información no se vean afectados por malos manejos, eventos sospechosos o dejarlos desatendidos.
- Reportar a la mesa de ayuda cualquier situación extraña que ponga en riesgos los activos de información de la compañía

Profesional o gestor de seguridad de la información

- Mantener actualizada la política y los procedimientos para su implementación
- Velar por la divulgación y mantenimiento del modelo y sus procedimientos
- Diligenciar el formato de incidentes de seguridad de la Información.
- Verificar el cumplimiento del presente procedimiento al interior de la entidad.

Profesional o gestor de seguridad Informática y Tecnología

- Adelantar las gestiones y acciones operativas necesarias para dar cumplimiento al presente procedimiento.
- Escalar al líder de seguridad de la información cualquier circunstancia que se salga del presente lineamiento.

Gerencia de Talento Humano

- Incluir en el plan de capacitación anual de la entidad la aplicación del procedimiento de incidentes de seguridad de la información.
- Garantizar que todos los colaboradores y terceros vinculados con la entidad en calidad de contratistas o representantes de alguna empresa reciban la capacitación en gestión de incidentes de seguridad de la información.

Oficina de Control Disciplinario

- Adelantar las acciones disciplinarias pertinentes cuando se demuestra que un incidente de seguridad se materializó por acción u omisión al cumplimiento de las políticas de seguridad de la información adoptadas por la Compañía.

Terceros o Proveedores

- Informar de manera inmediata al funcionario supervisor del contrato de Positiva, cuando se detecte un evento o incidente de seguridad que afecta la infraestructura tecnológica asignada para ejecución de las actividades relacionadas con el contrato.
- El supervisor del contrato debe notificar a la Oficina de TI y/o a la Oficina de Gestión Integral de Riesgos una vez sea informado del evento por parte del proveedor o tercero.
- Aplicar las acciones las operativas y tecnológicas que conlleven a atender y contener el incidente en el menor tiempo posible, según el impacto del evento y la definición del equipo de respuesta CSIRT de Positiva

- El tercero debe coordinar con la Oficina de TI y la OGIR de Positiva, el plan de acciones para contener los incidentes cuando se extiendan a la infraestructura de Positiva que pueda afectar la operación CORE de negocio.

Equipo de Respuesta CSIRT

- Evaluar el incidente para identificar su clasificación e impacto.
- Recopilar la información necesaria para determinar la causa raíz del incidente con el fin de definir las acciones correctivas.
- Asegurar la información y evidencia recolectada con el fin de mantener la correcta cadena de custodia y conservación para fines legales que puedan generarse.

3.5. Recolección y Conservación de la información

Recolección de información

Tener en cuenta:

- Servicios y/o aplicaciones afectadas durante el incidente
- Lista de activos de información que se vieron involucrados
- Origen el incidente, estableciendo la causa raíz que lo genera
- Nivel de impacto identificando el Área o la operación afectada.

En los casos donde se identifique que los incidentes fueron generados por acción u omisión de un(os) usuario(s) en particular, se remitirán el informe a la Gerencia de Talento Humano para que desde allí se adelante los procedimientos o investigaciones adicionales a que haya lugar.

La recopilación de la información será realizada por el equipo de respuesta a través de su delegado con el apoyo de la Oficina TI. Así mismo partiendo del principio de prueba válida, la información recopilada puede hacer parte de una investigación legal, ésta debe recopilarse bajo medidas y acciones que aseguren la no alteración de esta.

Por lo anterior, la captura de información se debe realizar a través de herramientas que no alteren o modifiquen el entorno de la escena y la evidencia en sí, esto con el objetivo de asegurar la integridad de la información.

En la recolección de información base para la investigación, se debe considerar aspectos como la información del host, información de red e información de personas que tienen conocimiento del incidente.

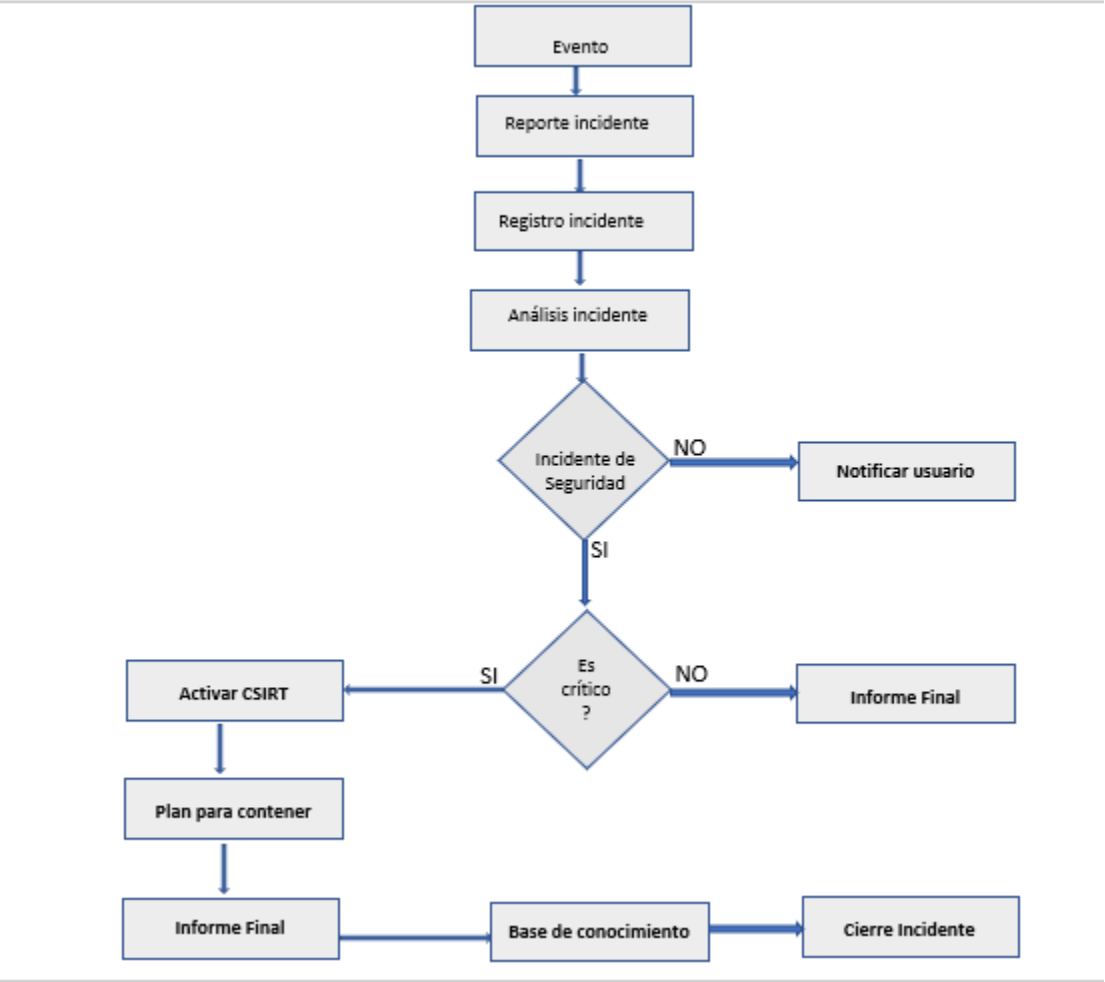
Conservación de la información

En la conservación de la información o evidencia del incidente, el equipo de respuesta de Positiva debe tener en cuenta los principios de autenticidad, para asegurar que no ha sido alterada durante su recolección; cadena de custodia, en la cual se debe llevar un registro de cada actividad realizada o proceso aplicado a la información o evidencia; y validación para probar que la información entregada a entes legales que así lo requieran es la misma que se ha recopilado.
Para la conservación de la información del evento o incidente recolectada como evidencia debe aplicar las acciones acordes con los lineamientos de cadena de custodia establecidos en el Manual del Sistema de Cadena de Cadena de Custodia de la Fiscalía General de la Nación.
Lo anterior, hace referencia a los principios de validez del sistema de cadena de custodia, entre los que se encuentra la autenticidad, la capacidad demostrada, la identidad, la integridad, preservación, la seguridad, el almacenamiento, la continuidad y el registro.

3.6. Diagrama de flujo – Modelo Gestión de incidentes

En la siguiente imagen se muestra los diferentes pasos o actividades que debe realizarse para gestionar los incidentes de seguridad de la información.

Ilustración 6. Flujograma



Fuente Elaboración propia

Resumen del Capítulo

En el evento de que algún componente de la infraestructura tecnológica (páginas Web, bases de datos, sistemas de información) de la Entidad haya sido comprometido es necesario involucrar desde el origen del evento a todo el equipo de manejo de incidentes para asegurar la debida gestión del Modelo que se pretende implementar en Positiva S.A.

Con el fin de realizar la conservación de las evidencias de naturaleza digital y soportes del incidente es necesario ejecutar todos los procedimientos técnicos y operativos para su posterior manejo judicial ante la autoridad competente.

El reporte apropiado del incidente de seguridad de la información, realizar el registro de las lecciones aprendidas, así como el establecimiento de medidas tecnológicas y disciplinarias, de ser necesarias, hacen que los activos de información en Positiva tengan una mayor protección preservando los principios de la información: Confidencialidad, Integridad y Disponibilidad.

CONCLUSIONES

El desarrollo del presente proyecto de grado permitió que las directivas de Positiva S.A. apoyaran esta iniciativa para afianzar la seguridad de la información con la implementación de un Modelo de Gestión de Incidentes de Seguridad de la Información acorde a los criterios de ciberseguridad y la normatividad legal vigente en el sector financiero al cual pertenece Positiva como entidad del Estado.

Contar en Positiva S.A. con un modelo de gestión de incidentes de seguridad de la información le permitirá controlar las vulnerabilidades o debilidades en su infraestructura y en la operación de la empresa, garantizando que su información crítica está protegida con mecanismos de reacción y respaldo debidamente estructurados.

El modelo de gestión de incidentes le reducirá a Positiva S.A. los impactos negativos de los incidentes de seguridad de la información sobre sus operaciones de negocio mediante los controles adecuados en respuesta al incidente y los procedimientos que aseguren la respuesta oportuna y eficiente.

Establecer mecanismos para hacer seguimiento de los incidentes de seguridad de la información y llevar un registro adecuado de las situaciones y acciones vividas durante la gestión del incidente, como una forma de lecciones aprendidas, le brindará a Positiva S.A. un modelo de gestión de incidentes de seguridad de la información dinámico y actualizado con las mejores prácticas en un ambiente de ciberseguridad cambiante y con mayores retos cada día.

Aunque Positiva S.A. cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI), adoptar un Modelo de Gestión de Incidentes de Seguridad de la

Información le permitirá mejorar el esquema general de la gestión de incidentes y contar con una herramienta para lograr el compromiso de los usuarios, a través de capacitaciones y concienciación en las diferentes técnicas que utilizan los atacantes para acceder a los activos de información y el uso responsable de los recursos tecnológicos en el cumplimiento de sus funciones.

BIBLIOGRAFÍA

- Asobancaria (2019). Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina. Tomado de https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf
- Casares (2013). Proceso de gestión de Riesgos y seguros en las empresas. Tomado de https://fundacioninade.org/sites/inade.org/files/primer_libro_isabel_casares.pdf
- Circular Externa 033 Superintendencia Financiera de Colombia (2020) - Guía para la clasificación de incidentes cibernéticos – proyecto TUIC. Tomado de https://www.cerlatam.com/normatividad/superfinanciera-circular-externa-033-de-2020/
- Diagnosticsnews.com (2020). tomado de https://www.diagnosticsnews.com/productos-y-tecnologias/35370-ciberseguridad-uruguay-lider-en-america-latina-y-el-caribe
- Guía Técnica Colombiana GTC-ISO/IEC 27035 (2012), Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información.
- Incibe-cert. (2019). Riesgo cibernético y ciberseguridad. Tomado de https://www.incibe-cert.es/servicios-operadores/information-gathering
- Ministerio de Tecnologías de la Información y las Comunicaciones. (2013). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Tomado de https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf
- Mitre. (2021). Enterprise Matrix . Tomado de https://attack.mitre.org/matrices/enterprise/
- Positiva S.A. (2020) EST_2_2__MA03 Manual de Políticas de Seguridad de la Información