EVALUACIÓN DE LA GESTIÓN DE INCIDENTES EN SEGURIDAD DE LA INFORMACIÓN PARA ENTIDADES FINANCIERAS

PAULA ANDREA MARTÍNEZ ROJAS
DAVID STIVENS BARONA MURCIA
SEBASTIÁN AGUDELO RAMIREZ

UNIVERSIDAD ECCI
DIRECCIÓN DE POSGRADOS
ESPECIALIZACIÓN TELECOMUNICACIONES INALÁMBRICAS
BOGOTÁ
2016

Tabla de Contenidos

Listas Especiales

Glosario

Incidente: según ITIL *"un incidente es Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo."*(S.A, OSIATIS, 2011)

Incidente de seguridad informática: Evento adverso o amenaza que ocurre en un sistema informático o telemático, que compromete cualquiera de los pilares de la seguridadinformática (disponibilidad, integridad, confidencialidad). Puede ser causado por la explotación de una o diversas vulnerabilidades de una o más fallas de un sistema informático o telemático.

Herramienta de gestión de Incidentes: Software en el cual serealiza el registro de incidentesy el cual permite realizar la trazabilidad del incidente validando los comentarios existentes sobre el incidente, la solución, los tiempos de respuesta.

Evento: Acaecimiento que no afecta la operación del servicio, se caracteriza por que puede ser observable en una red o en un sistema.

Resumen

La tecnología a través de diferentes procesos aporta todo tipo de avances, esto ha sido fundamental en el gran desarrollo tecnológico que han tenido las entidades financieras (EF), es así que como aumenta la tecnología, también aumentan los riesgos informáticos trayendo consigo controles para contrarrestar toda clase de riesgos asociados a delitos informáticos. Inicialmente y desde una perspectiva lejana pueden parecer simples, pero si no se controlan y no se mitigan con el tiempo pueden llegar a ocasionar grandes estragos en cualquier entidad. Por este motivo, la seguridad y el blindaje de la información toman un rol importante en la implementación de nuevas estrategias para la mitigación de los riesgos provenientes en el desarrollo de las actividades de una organización empresarial, llamada procesos de la cadena de valor de las organizaciones.

Actualmente las entidades financieras (EF) cuentan con herramientas y equipos de trabajo especializados en seguridad. Una de las funciones de este equipo de trabajo es detectar los incidentes de seguridad que se presentan; sin embargo, es de anotar que se deben tener procesos y procedimientos formalmente establecidos en el marco de la política de seguridad de la información, la cual sirva como soporte a la operación del área de atención de incidentes. Al interior del grupo de atención de incidentes se realiza un análisis detallado y se monitorean los incidentes que se presentan en las entidades, de esta manera se brindan soluciones óptimas para el desarrollo de la atención, monitoreo y soluciones a los incidentes.

El cómo se gestiona los incidentes de seguridad de la información, desde la detección hasta los análisis post-incidente, detallando el tratamiento de cada una de sus fases en una entidad financiera, el manejo de información, seguimiento, tiempos de respuesta y efectividad en la solución entregada. Después de analizar los puntos nombrados anteriormente, llegamos a la conclusión que los procedimientos establecidos por las EF no eran óptimos ni eficaces, por ende se tiene como objetivo siguiente diseñar e implementar un procedimiento/procesode gestión de incidentes de seguridad de la información capaz de dar respuesta oportuna a eventos y/o incidentes informáticos.

Los resultados obtenidos muestran que si se cuenta con herramientas adecuadas para su manejo y gestión, roles específicos para administrar los incidentes y responsabilidades asignadas a todo el personal que se vea involucrado en los diferentes procesos, se puede brindar una solución rápida, oportuna, segura y eficaz del tratamiento de los incidentes informáticos, causando mejoras notables, además de confiabilidad en la seguridad de la información de las EF, utilizando mejores prácticas acorde a la normativa interna.

1. INTRODUCCIÓN

Las tecnologías de la información y las telecomunicaciones, con su constante auge en el sector financiero, generan que aumente la dependencia en artefactos tecnológicos con el fin de que la operación de una compañía se mantenga estable y segura; además, la regulación colombiana se hace más estricta cada día con las entidades financieras (EF) para así ofrecer altos niveles de disponibilidad aunque se aumenten los riesgos.

Para mitigar los riesgos debemos estar preparados, y así poder responder de manera rápida y eficaz con el fin de que el golpe en el negocio se disminuya, cuanto más pronta sea la respuesta menos será el impacto en la organización.

De esta forma, nace la necesidad de generar mecanismos que puedan brindar una respuesta oportuna a los incidentes de seguridad de la información e informática cómo es la gestión de incidentes; teniendo en cuenta que cada uno de ellos tiene un proceso, el cual tendría un principio y un final y así lograr tener su control y disminuir su impacto en la compañía.

Hasta el momento la implementación en controles de seguridad son imperfectos, estos controles por distintas razones pueden fallar (fallas en la configuración, fallas en las pruebas, fallas de usuario…), o los controles pueden funcionar de manera parcial, por tal razón la organización está expuesta a que los medios preventivos fracasen. Estando así las cosas los incidentes pueden ocurrir en cualquier instante

Justificación

Al estar en contacto con un ente financiero y específicamente en el área de seguridad informática se evidencian factores que alteran el manejo de la información, a los cuales no se les está brindando un correcto trato y resolución. Situando nuestra atención en el trámite de incidentes de una EF, surge la pregunta: ¿es confiable, es óptimo, es veraz el tratamiento que se le dan a los incidentes en las entidades financieras? este interrogante nos lleva a elaborar un análisis del proceso de gestión de incidentes y llegar a la conclusión que en la mayoría de organismos financieros no se le da la importancia requerida.

Es de gran importancia contar con un procedimiento bien estructurado para el tratamiento de incidentes informáticos. Encontramos que este tipo de solución no traería solo beneficios económicos para las EF; sino también, brindaría mayor confiabilidad a sus clientes, esto puede traer consigo beneficios mutuos importantes y notorios, ya que los resultados se verán reflejados; en la rapidez con la que se trate el incidente, la

capacidad de darle prioridad según su criticidad, realizar seguimiento a todos los incidentes, mitigar la fuga de información, evitar sanciones por parte de la Superintendencia Financiera y lo más sustancial prestar un servicio confiable y eficiente a los usuarios. Teniendo un proceso definido y una estructura de manejo de incidentes tendrá como resultado la solución de conflictos de una manera rápida, confiable y segura.

Cosas que llevan a pensar sobre el manejo de incidentes informáticos no se trata con la prioridad suficiente en las compañías financieras de gran reconocimiento, son casos como el que presentaremos a continuación:

2.1 Antecedentes sobre incidentes informáticos

Antecedentes sobre incidentes informáticos según la información suministrada por BBC, las entidades financieras han tenido ataques cibernéticos de la forma más simple, y sin ninguna diferencia en su sistema, ya sea por un correo electrónico o, la mala manipulación de la plataforma o de algún servicio. La información en los bancos es totalmente confidencial y cualquier falla nos lleva a realizar procesos en los que la información no sea vulnerada o debilitada.

En el artículo(BBC, Tecnología, 2011) se hace referencia que más de 100 entidades financieras han tenido un ataque con mucho impacto debido a que lograron hurtar aproximadamente 100 millones de dólares por abrir un correo donde dice ser de una fuente confiable (ej., Gerente de la entidad).

¿Cómo funciona?

El ataque se realiza muy rápido pero de una fuente confiable como se ha mencionado anteriormente. Cualquier persona de la entidad recibe un correo del gerente, en el cual debe ejecutar, abrir o iniciar el archivo adjunto que venga en el mismo, cuando esto sucede, aparece un virus llamado "TROYANO", que tiene como objetivo desplegarse en toda la red y sistema hasta llegar a las cámaras de seguridad obteniendo así de una manera fácil, el acceso a todos los movimientos de la EF y la información necesaria de cuentas, como claves, lo que conlleva al delito.

Este incidente trajo consigo que las personas dominantes sobre la información en la EF llegaran a administrar la plataforma para que así, en unos tiempos estipulados en esta red, fuera recogido dinero de los cajeros automáticos en horarios programados.

Intervención KARSPERSKY LAB:

Todo esto hizo que KARSPEPRSKY LAB, entrara a indagar sobre el tema, líder en antivirus analiza con detenimiento las posibles causas de los hurtos mencionados anteriormente. Teniendo acceso a los servicios de seguridad del EF, donde se observa a las personas realizando grandes transacciones de dinero sin tener una tarjeta bancaria, esto hizo pensar que los bancos habían sido manipulados en cada una de las sucursales es decir, que todo se había realizado desde los mismos cajeros automáticos.

Propuestas para mitigar el problema

Según la BBC Mundo, En estados unidos, se reúnen los especialistas de seguridad informática para poder buscar una solución óptima y combatir este tipo de fraudes cibernéticos. Las entidades bancarias están buscando fortalecer esta gran falencia que se encuentra en las redes informáticas buscando mejores prácticas para el manejo de la información. Es aquí donde una plataforma de gestión de incidentes podría ser una herramienta de uso eficaz para combatir todo tipo de incidencias informáticas según la problemática del caso. Llevando consigo todo tipo de soluciones e historiales de los problemas que se hayan presentado en ocasiones anteriores, con este histórico se puede encontrar información de todo tipo de incidentes, causas y soluciones las cuales pueden ayudas a solventar cualquier tipo de problema que haya ocurrido, dando una respuesta rápida o levantando un procedimiento de los inconvenientes que ha podido causar ese incidente.

Definición del Problema

En la actualidad las EF y en general todas las empresas están expuestas a un riesgo inherente en el ámbito de las tecnologías de la información y las telecomunicaciones, por esta razón cada día se hace más necesario contar con una cantidad mayor de herramientas de seguridad, políticas de seguridad y controles perimetrales.

Las EF especialmente, todos los días están luchando contra los ataques cibernéticos los cuales generalmente se llevan a cabo por medio de malware, accesos a web no autorizados o mal intencionado, sitios web falsos o malicioso entre otros medios diseñados para robar información de una entidad. También es importante contemplar que los usuarios en ocasiones de manera ingenua pueden hacer parte de exponer la entidad al riesgo, ya sea por medio de un correo malicioso que abren sin validar antes su procedencia o ingresando a sus equipos de trabajo dispositivos de almacenamiento externo sin previa validación del antivirus, puede estar exponiendo la entidad a perdida de información

3. Objetivos

3.1. Objetivo general

Diseñar e implementar un sistema de gestión de incidentes que sea capaz de dar respuesta oportuna a eventos y/o incidentes de seguridadinformática, que afecten la disponibilidad, integridad y confidencialidad de cualquier entidad financiera, para así mitigar riesgos o fugas de información.

3.2. Objetivos específicos

- Evaluar el impacto de los posibles incidentes de seguridad informática en la entidad, que permitan analizarla problemática existente referente a la gestionó tratamiento los incidentes ocurridos dentro de una entidad financiera.
- Definir un procedimiento formal del cómo se trata un incidente de seguridad informática para minimizar su impacto al interior de la organización.
- Definir el mecanismo con el cual se cuantifica y monitorea los incidentes de seguridad informática al interior de la entidad para poder generar un orden y un estándar de la información.
- Tener una base de datos sobre incidentes de seguridad informática ocurridos en una entidad financiera y con el poder tener una respuesta rápida y efectiva a incidentes ocurridos y presentados anteriormente.
- Presentar una estructura que permita hacer una gestión adecuada de los incidentes de seguridad informática para cualquier entidad financiera

4. Gestión de incidentes

4.1.El incidente de seguridad informática.

Un incidente de seguridad informática para una entidad financiera (EF) se define como el resultado de un evento el cual afecta la integridad, disponibilidad, y/o confidencialidad de la información de la cadena de valor de la organización y cualquier acontecimiento que vaya en contra de las políticas de seguridad de EF.

Modelos de referencia

Todos los incidentes tienen unos modelos teóricos, los cuales siempre deben ser contemplados al momento de crear un sistema de gestión de incidentes, con el fin de mejorar la comunicación con los clientes y de esta forma brindarles valor, además de que desarrolla una estructura más clara y eficaz a los objetivos de la organización, los cuales veremos a continuación:

- **ITIL**

En ITIL se consolidan un conjunto de mejores prácticas en la industria. Para los incidentes ITIL indica el siguiente proceso como la mejor práctica. (S.A, OSIATIS, 2011)

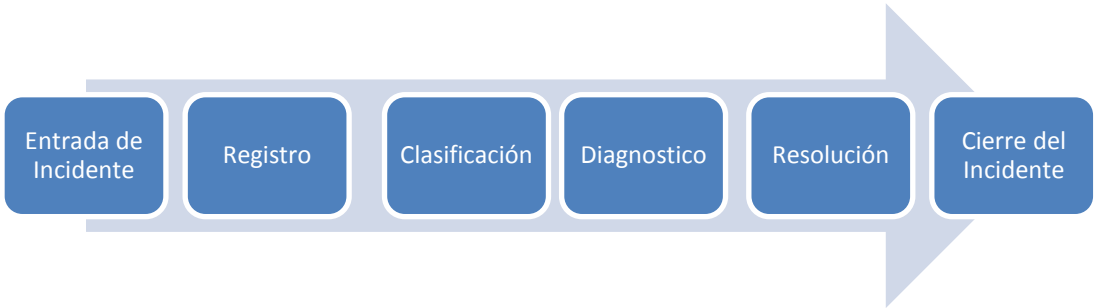

Imagen 5.Proceso de la gestión del incidente(OSIATIS S.A., 2011)

Para esto los objetivos principales de la Gestión de Incidencias en ITIL son:

- Manifestar cualquier alteración en los servicios TI.
- Inspeccionar y ordenar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio según se define en el SLA correspondiente.

Ya que se presenta en constantes ocasiones múltiples incidencias se hace necesario determinar un nivel de prioridad con el cual se atenderá este para brindar solución de la misma.

- **COBIT**

Es un marco de trabajo en el cual se establecen herramientas que soportan el Gobierno de TI. Cobit permite disminuir es sesgo que existe entre los requerimientos de negocio, la gestión de riesgos y los aspectos técnicos. (COBIT™, 1999)

Para Cobit la gestión de incidentes y la Mesa de Servicios, contempla las siguientes fases:

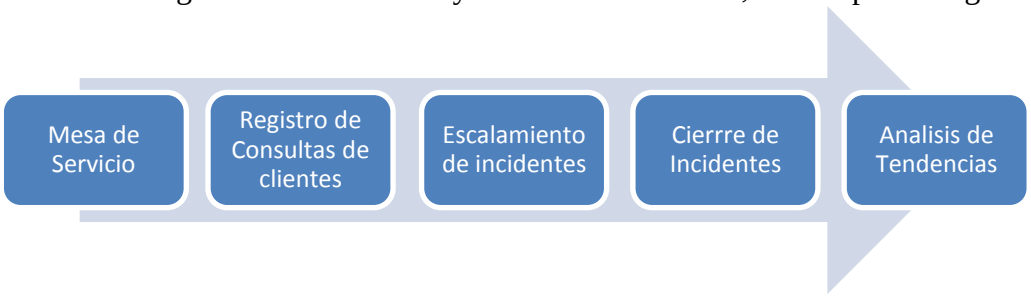

Imagen 6.Proceso de la gestión del incidente (COBIT™, 1999)

Este actúa sobre la dirigencia y ayuda a estandarizar la organización. Como podemos ver

> "COBIT define qué debemos controlar e ITIL define cómo debemos hacerlo"

- **NIST 800-61.**

El NIST es el instituto nacional de normas y tecnología.En el compendio 800 se relaciona una guía de seguridad sobre la gestión de incidentes de seguridad. En ella se evidencian aspectos relevantes para preparar un sistema de gestión de incidentes de seguridad, entre ellos tenemos. (IsecT Ltd., 2011)

Imagen 7.Proceso de la gestión del incidente(Paul Cichonski, Tom Millar, TimGrance, &

Karen Scarfone, 2012)

- **ISO 27035.**

El estándar ISO parte de la idea de que todos los sistemas son vulnerables puesto que los controles son imperfectos o no se encuentran implementados en su totalidad. Así las cosas proponen una serie de pasos.

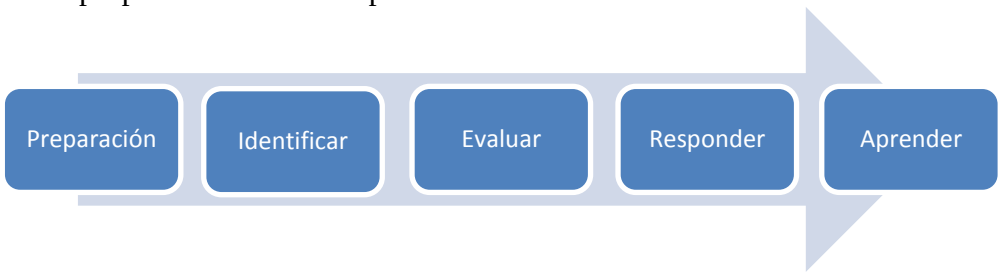

Imagen 8.Proceso de la gestión del incidente (IsecT Ltd., 2011)

4.2.Ciclo de vida Incidente

En la actualidad las entidades financieras y en general todas las empresas están expuestas a un riesgo inherente en el ámbito de las tecnologías de la información y las telecomunicaciones, por esta razón cada día se hace necesario contar con una cantidad mayor de herramientas de seguridad, políticas y controles perimetrales.

Las entidades financieras especialmente, todos los días están en constante lucha contra los ataques cibernéticos, los cuales generalmente se llevan a cabo por medio de malware, accesos webs no autorizadas o mal intencionados, sitios web falsos o maliciosos entre otros medios diseñados para robar información de una entidad. También es conveniente contemplar que los usuarios en ocasiones, de manera ingenua pueden formar parte del riesgo al cual exponen a la entidad, ya sea mediante un correo malicioso que abren sin validar antes de su procedencia o ingresando a sus equipos de trabajo dispositivos de almacenamiento externo sin previa validación del antivirus, puede estar exponiendo la entidad a la perdida de información.

Al tenerse como objetivo, resolver de la manera más pronta y eficaz posible cualquier incidente que genere una interrupción en el servicio según el modelo que se describe a continuación el cual está basado en los estándares del NIST y se alinea con los requerimientos de la norma NTC – ISO–IEC 27001 – IEC 27035.(IsecT Ltd., 2011)

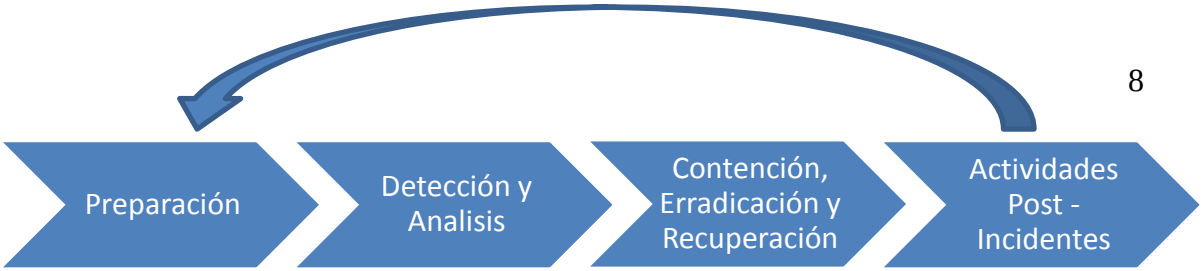

Imagen 1. Ciclo de gestión de incidentes (Mintic, 2016)

Se presentan distintas fases como se muestra en la Imagen 1. En donde iniciamos por una etapa de preparación del ciclo de vida de un incidente en donde no solo se está pesando en crear un modelo que permita a la entidad estar en capacidad de responder ante los incidentes, sino también en la forma como pueden prevenirse, asegurando que los sistemas, redes y aplicaciones sean seguras. (Mintic, 2016)

Preparación:

Dentro de las actividades dela etapa de preparación esta:
Remediación de vulnerabilidades: esta actividad se relaciona con el área de gestión de vulnerabilidades. En la cual se realiza el análisis de vulnerabilidades sobre las diferentes plataformas existentes en la entidad financiera. (Sistemas operativos, Bases de Datos, Aplicaciones, Otro software instalado). La actividad en mención ayuda a los administradores en la identificación adquisición y prueba e instalación de actualizaciones de seguridad.

Aseguramiento de la plataforma

Realizar un plan de remediación de vulnerabilidades para mitigar incidentes en la entidad.

Imagen 2. Plan remediación de vulnerabilidades

Validación de usuarios y configuraciones por defecto, es necesario validar los archivos compartidos analizar el tipo de información. Cada recurso que es accedido por externos debe mostrar la advertencia de esta forma ya comenzamos a reducir la posibilidad de que se genere una incidencia.

Se deben tener unas características mínimas de todos los servidores los cuales deben contar con los siguientes requerimientos:

- Software Legal.
- Software Antivirus Y antimalware.
- Test Vulnerabilidades.
- El servidor es de base de datos debe tener software de monitoreo.
- El servidor debe reportar los eventos al correlacionador de eventos.
- Si el servidor es web debe tener certificado digital la aplicación y debe hacer uso puertos seguros.
- No usar puertos inseguros.
- Si es base de datos y la base de datos corresponde a ambientes de pruebas y desarrollo, estas bases de datos deben estar enmascaradas.

La siguiente fase que mostraremos es la detección a través de la identificación y gestión de componentes que avisan sobre un incidente y así nos suministren información que puede alertarnos sobre la posible ocurrencia futura del mismo y generar procedimientos para minimizar el impacto. En el ente bancario debe existir una lista de fuentes generadoras de eventos que permitan la identificación de un incidente de seguridad de la información. (Mintic, 2016)

Las actividades de análisis de incidente involucran lo siguiente:

- Presentar personal con los conocimientos y capacidades idóneas para la verificación de estas
- Los administradores de TI deben tener conocimiento total sobre comportamientos de la infraestructura que se está administrando.
- Se debe mantener y usar una base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados, y experiencias con incidentes anteriores.
- Crear matrices de diagnóstico e información para los administradores menos experimentados. (Mintic, 2016)

A través de estos métodos es importante para la entidad implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los dañosa los recursos de TI y la perdida de la confidencialidad, integridad y disponibilidad de la información. (Mintic, 2016)

Por último, se debe revisar las actividades post-incidente básicamente se componen del reporte del incidente, de la generación de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias así como el registro en la base de conocimiento para alimentar los indicadores. (Mintic, 2016)

4.3Investigación Documental

Al interior de entidades

Se hace necesario conocer cómo funcionan las entidades financieras para el manejo de la información de la gestión de incidentes.

En la actualidad, las entidades financieras realiza la gestión de incidentes de seguridad por medio de una matriz que se encuentra ubicada en el servidor de la EF, dicha matriz esta implementada en una base de datos, en la cual generalmente contiene los siguientes elementos:

ITEM: identificador del incidente.

Fecha de Reporte: Fecha en la cual fue reportada el incidente.

Llamada de Servicio: Identificador el cual indica el número de servicio con el cual está registrado en la herramienta de mesa de ayuda.

Tipo de Incidente: Define la categoría del incidente.

Criticidad: Define el grado de criticidad del incidente.

Resumen: en este campo se describe el incidente.

Plan de respuesta: Describe cual es el plan de acción que se tomó en respuesta al incidente ocurrido.

Notas: Describe el estado del incidente en la herramienta mesa de ayuda. Además se escriben notas del caso.
Para un ejemplo de control de incidentes se generan estadísticas que hacen resúmenes de los distintos casos que pueden ocurrir y se pueden ver reflejados en cuadros los cuales permiten distinguir dentro de los distintos casos que se puedan presentar, como por ejemplo: se tienen registrados alrededor de 841 incidentes dentro de un sondeo en una entidad financiera. A continuación se describe las estadísticas generales de los incidentes.

Estado	Total
En espera de usuario	2
Asignada	1
Cerrada	262
Confirmada	104
Despachada	1
No Resuelta	2
Resuelta	381
En Blanco y otros	88
GRAN TOTAL	841

Imagen 2. Resumen estadístico general de incidentes

Todas las incidencias se deben manejar de una forma distinta, para esto es necesario tener un sistema de atención a incidencias, el cual veremos a continuación.

En el siguiente recuadro se evidencia los niveles de prioridad de riesgo de servicio.

NIVEL	NIVEL DE RIESGO
Alto	Son eventos que afectan la información, procesos o servicios, generando pérdidas de disponibilidad, integridad o confidencialidad de la información crítica.
Medio	Son eventos que pueden afectar la información, procesos o servicios con consecuencias que comprometen la reputación, pueden terminar en pérdidas económicas para la organización, generan un daño irreparable a datos de clientes o productos o un impacto significativo en la disponibilidad de los sistemas críticos.
Bajo	Son eventos que no comprometen la integridad, confidencialidad o disponibilidad de la información es decir, que pueden ser controladosen forma paralela a la operación.Por este motivo no requieren una acción inmediata.
Insignificante	Eventos que no representan ninguna amenaza para la organización, por lo general son los eventos que se catalogan como falsos positivos. Y son controlados fácilmente.

Imagen 3. Estándar de niveles de prioridad de riesgo

En el siguiente recuadro se evidencia las métricas o indicadores de seguridad que definen aspectos frente a cantidad de incidentes registrados, cantidad de incidentes escalados y tiempos de atención del incidente:

MÉTRICA	DESCRIPCIÓN LA METRICA	META
Incidentes repetidos	Los incidentes reportados deben tener soluciones efectivas para evitar que se presenten nuevamente. La solución de estos incidentes se encuentra documentada en la base de conocimiento.	Los incidentes repetidos deben ser menores al 0.2 de los incidentes registrados.
Cantidad de incidentes registrados	La cantidad de incidentes registrados debe mantenerse dentro de un límite constante, ya que un aumento significativo según el promedio de registros al mes debe ser analizado cuidadosamente y evitar propagación de ruido en la organización.	Se deben registrar menos de 20 incidentes durante el mes.
Incidentes escalados	Los incidentes que afectan áreas críticas de la organización deben ser escalados al nivel de investigación y deben mantenerse en un límite constante no se deben propagar este tipo de incidentes y el área de investigación debe estar siempre dispuesta a nuevas tendencias.	Se deben escalar menos del 0.1 del total de los incidentes registrados en el mes.
Tiempo medio para cerrar un incidente.	El tiempo promedio de cerrado de los incidentes debe ser controlado para evitar extender el tiempo de solución y respuesta al incidente.	Los incidentes deben ser cerrados en menos de 20 días

Imagen 4. Métricas de seguridad

Nota: De acuerdo al levantamiento de información se realiza un cuadro donde los tiempos están relacionados con las buenas prácticas que indica ITIL.

4.4Herramientas de Gestión de Incidentes.

Las entidades financieras comúnmente manejan ciertos programas o plataformas que sirven para la gestión de las incidencias, les presentaremos los más importantes que usan las entidades financieras a continuación:

- **RequesterTracker.**

  Solución de tipo open source que ofrece gestión de incidentes, está desarrollado sobre el lenguaje PERL y la base de datos puede ser MySql, PostgreSql, Oracle o SQLite.RT dispone de herramientas para reportes y cuadros de mando además posee un módulo llamado "time tracking", la cual permite realizar seguimiento de los SLA. (Best Practical Solutions, LLC, 2002)

- **OTRS (Open Ticket Request System).**

  La versión básica es gratuita. Requiere de apache una base de datos MySql, PostGreSql, DB2, Oracle o MS Sql Server. Ofrece facilidades para Time Tracking, Calendarios, Workflows, gestión de SLAs, gestión de problemas y Catálogo de Servicios y dispone de un buen sistema de reporting y un pequeño módulo para la gestión de encuestas a clientes. (OTRS, 2016)

- **GLPI (Gestionnaire Libre de Parc Informático).**

  La herramienta se desarrolló para gestionar inventarios. Además de tenermódulos de gestión de inventarios tiene un módulo de Helpdesk, que se acopla con las buenas prácticas de ITIL. (Creative Commons BY-NC-SA, 2002)
- **BMC REMEDY.**

  Herramienta para gestionar incidentes de Uso comercial. Se alinea con las prácticas de ITIL, es tan granular como se desee, todos los clientes ingresan incidentes a través de un portal WEB, que se autentica contra el directorio activo. (BMC Software, Inc., 2005)

- **Dexon Software.**

  Herramienta de uso comercial que brinda mecanismos para hacer gestión de incidentes, dentro sus módulos existe gestión de incidentes, toma de control

remoto, recolección de inventario, se acopla a ITIL, es modular y tan granular como se desee. (Dexon Software Inc., 2005)

4.5Normatividad

La necesidad de la entidad de contar con mecanismos para la gestión de incidentes de seguridad informática es alta ya que asegura la respuesta inmediata ante eventos que puedan afectar la disponibilidad integridad y confidencialidad.

A continuación se referencian algunas de las leyes que brindan una guía acerca de las responsabilidades que se adquieren en la implementación un sistema de gestión de incidentes de seguridad informática.

- LEY ESTATUTARIA 1581 DE 2012. Esta Ley es de obligado cumplimiento.
- Principio de la Responsabilidad demostrada Superintendencia de industria y comercio.
- Circular 052, 048 Superintendencia Financiera de Colombia.
- Deberes de los administradores Ley 222 de 1995 Articulo 23
- Código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares (ley 842 de 2003)
- Circular básica financiera y contable de 1995 Superintendencia Financiera

5. Resultados

5.1. Relación del sistema de Gestión de incidentes con otras áreas

Los incidentes informáticos no solo deben ser conocidos por el área encargada, sino también deben ser evaluados por distintos departamentos de la entidad, a continuación cada uno de ellos:

Imagen 8 Relación de las áreas al interior de la organización

Dirección Jurídica: Área la cual cumple el rol de representante legal ante los diferentes juzgados, en esta área se acuerda todo lo pertinente con temas legales que involucren a la compañía.

Soporte técnico: Área en la entidad bancaria que se encarga de recibir todos los requerimientos por anomalías en el servicio tecnológico de cara al cliente interno. Acorde a los SLA definidos para la prestación del servicio.

Infraestructura Tecnológica: Área de la compañía que se encarga de mantener los niveles de disponibilidad tecnológica de cara al cliente interno, acorde a la regulación y

asegurando la disponibilidad de la operación tecnológica del Banco. Ellos se encargan de remediar las vulnerabilidades tecnológicas, previo a un proceso de pruebas en un tipo de ambiente dispuesto para validar que la remediación de estas vulnerabilidades y que no afecte la operación del Banco.

Dirección De recursos Humanos: Área de la compañía la cual vela por los interés de los trabajadores, la cual se encarga del pago de nómina y de las sanciones a los trabajadores en caso de que ellos caigan en actividades que pongan en riesgo al buen nombre de la entidad bancaria.

Operación Bancaria Sección de la compañía la cual se encarga de mantener la disponibilidad de la operación del Banco de cara al cliente externo. Se encargan de operar todos los sistemas de información que soportan la operación del Banco y que brindan las ganancias para la entidad.

Continuidad del Negocio Área la cual vela por realizar el análisis de impacto de las aplicaciones tecnológicas (BIA) y realizar la planeación y pruebas de contingencias tecnológicas, según regulación de la Superintendencia financiera de Colombia.

Vulnerabilidades Área de la compañía la cual se encarga de realizar análisis de vulnerabilidades sobre la plataforma del Banco, con el fin de mantener controlado las amenazas externas que pueden poner en riesgo la operación del Banco.

Seguridad Informática Área de la compañía la cual hace parte de la Dirección de Tecnología, en esta área se encarga por velar por la disponibilidad integridad y confidencialidad de la operación bancaria con el fin de prevenir las falencias y estar en mínimos niveles de riesgos, dentro de esta área se gestiona el sistema de gestión de incidentes de seguridad.

5.2 Organigrama de la Organización

Dentro de cada entidad siempre se tiene un organigrama correspondiente a la organización, el cual nos ayuda a identificar que directrices deben participar en los procedimientos al interior de las entidades, a continuación se anexa el organigrama:

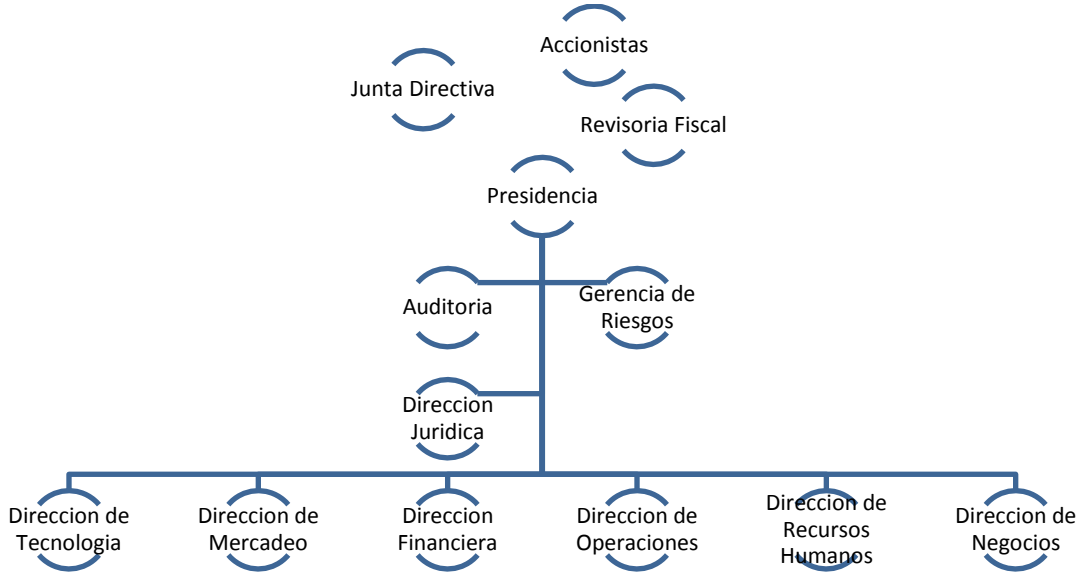

Imagen 9 Organigrama general

5.1.3Propuesta de proceso Gestión De Incidentes

Con la información recopilada anteriormente, se realiza una propuesta donde se basa un objetivo, alcance y otras condiciones que presentaremos a continuación, todo esto para poder entablar un proceso dentro de la entidad:

Objetivo

Se define la hoja de ruta cuando sucede un incidente de seguridad informática, coherente con las políticas y manuales de seguridad de la información de la entidad financiera (EF).

Alcance

Todo este procedimiento es aplicado a todos los funcionarios (Empleados, temporales, contratistas, practicantes y/o involucrados) que manejen y/o tengan la posibilidad de acceder a los sistemas de información de la EF y/o manejen información, que pueda verse implicados en incidentes de seguridad informática.

Precondiciones

Todas las acciones elaboradas para la gestión de incidentes de seguridad informática de la EF, desde su detección hasta su finalización, deben estar registradas en el sistema de información **OpenView**. Las actividades relacionadas con la gestión del incidente deben ser comunicadas al Gerente de Seguridad quien dependiendo de la criticidad del incidente reportara la novedad al Director de Seguridad y a los demás involucrados en el incidente.

Las roles y responsabilidades del personal de atención de incidentes se describen a continuación con su respectiva dedicación en horas por semana, todo esto es definido según estudios realizados dentro de la entidad.

Rol	Responsabilidad	Dedicación Semanal
Personal de Atención de Requerimiento	• Registrar el evento o incidente de seguridad reportado. • Clasificación inicial y diagnóstico del incidente • Gestión del cierre o escalamiento de ser necesario. • Validación de solución exitosa • Monitoreo de la solución	20 Horas
Centro de Atención de Incidentes de Seguridad (CAIS)	• Prioriza el incidente según el impacto de este al interior de la EF. • Identificación, análisis y orquestación de controles para la mitigación del impacto de este incidente • Propone los escenarios de recuperación según sea el caso y acompaña al personal encargado de la mencionada recuperación. • Validación de los incidentes y su	20 Horas

	cierre oportuno para que no afecte los niveles de prestación de servicio.	
Gerente de Seguridad	• Generación de informes y métricas de niveles de prestación de servicio, de niveles de atención de servicio. • Verificación de incidentes y verificación de la solución y las acciones tomadas para la contención del incidente. • Validación de aprobación en caso que se requiera de procedimientos forenses.	10 Horas
Director De Seguridad	• Colaboración en la detección de incidentes de seguridad. • Verificación y seguimiento al cierre, apertura y a las soluciones de los incidentes.	5 Horas

Roles y Etapas de Participación en el proceso

- Después de haber concretado cada uno de los roles que desempeña las áreas dentro de la entidad, se define a continuación las labores que cada uno debe desempeñar para que el proceso sea funcional y asertivo.

Quien	Que Hace	Numero de Etapa
Usuario-Herramientas de Seguridad-Recomendaciones de un Superior Correo electrónico	Reporte de Eventos de Seguridad	1
Personal de Atención de Requerimientos de Seguridad	¿Es un incidente de Seguridad de la información?	2
	Si la respuesta a la etapa 2 es afirmativa paso a la etapa 5 de lo contrario paso al punto 4	3
	Documentar el falsopositive	4
	Registro del incidente en herramienta de gestión de incidentes de Seguridad	5

	Informar al usuario que reporto los hallazgos (Líder de la herramienta de Seguridad)	6
	Análisis detallado del incidente	7
	clasificación del incidente	8
	Contención del incidente	9
	¿Es requerido Escalar al Segundo Nivel?	10
	Si la respuesta a la etapa 10 es afirmativa paso a la etapa 16 de lo contrario paso a la etapa 12	11
	Documentación del incidente	12
	Monitoreo del Incidente	13
	Cierre del incidente	14
	Comunicación a las áreas Interesadas	15
Centro de Atención de Incidentes de Seguridad (CAIS)	Contención del incidente	16
	¿Es requerido Escalar a Tercer Nivel	17
	Si la respuesta a la etapa 17 es afirmativa paso a la etapa 26 de lo contrario paso a la etapa 19	18
	Erradicar la Causa del Incidente	19
	Orquestación de la restauración del servicio y/ o sistemas y/o información afectados	20
	Toma de Evidencias	21
	¿Se requiere investigación?	22
	Si la respuesta a la etapa 22 es afirmativa paso a la etapa 26 de lo contrario paso a la etapa 23.	23
	Evaluación del Plan de Acción	24
	Presentación del plan de Acción	25
Gerente de Seguridad	Análisis del Incidente (validación con Experto Externo)	26
	Contención del incidente	27
	Cierre del incidente	28
	Aprobación de la investigación.	29
	Evaluación del Plan de Acción	24

Director de Seguridad	Validación del cierre del incidente que requirió de experto Externo	30
	¿Se requiere escalar caso con VP?	31
	Presentación de Informe en caso que sea necesario para presentárselo al VP	32

Canales de Entrada para el proceso de Incidentes

Los estudios realizados dieron como resultado que se necesitan Cinco (5) canales para dar inicio al proceso de gestión de incidentes, a continuación se mencionan cada una de las entradas.

- Usuario a través del portal de Mesa de servicio.
- Herramientas de Seguridad informática
- Recomendaciones de un superior
- Correo electrónico
- Llamadas mesa de Servicio.

Para los casos en que se presentó hurto de información o errores humanos que llevaron a perdida de información sensible dela EF, se recibirá únicamente el incidente desde la plataforma de mesa de servicio o al correo electrónico (definido por la entidad) con la descripción detallada de los hechos los cuales dieron lugar a la perdida de información, según el caso se requiere copia de la denuncia por delito informático. Estos detalles son recibidos por el personal de Gestión de incidentes y ellos continúan con el proceso anteriormente descrito.

Categorías de Incidentes de Seguridad

Los incidentes de Seguridad de la información que se presentan en la EF, están segmentados de la siguiente manera:

- ✓ Uso malversado de servicios tecnológicos.
- ✓ Hurto
- ✓ Ataques internos o externos
- ✓ Funcionamiento inapropiado de un sistema de información.
- ✓ Interrupción del servicio
- ✓ Error humano
- ✓ Efectos no contemplados de cambios.
- ✓

A continuación se detalla la categorización de todos los posibles incidentes que pueden ocurrir en una entidad financiera y la descripción junto a cada uno de los conceptos, es importante tener esta información lo más clara posible ya que la terminología no puede ir

enfocada a personal encargado del área de seguridad, sino para todas las partes de la entidad que conforman la gestión de incidentes, a continuación se presenta el esquema:

Uso malversado de servicios tecnológicos.		
Id	**Clasificación**	**Descripción**
1	Acceso No autorizado a redes y servicios	Cuando el usuario ingresa a plataformas o información la cual no debe tener ingreso.
2	Cambios de Privilegios en los sistemas de Información sin autorización	Usuario que cambia sus privilegios y se vuelve administrador de red y con esto manipular la plataforma
3	Modificación de Transacciones en las bases de datos sin autorización	Usuario que modifica o realiza cambios en la plataforma de transacciones creando molestias y problemas graves a la compañía
4	Uso inadecuado de Servicios Tecnológicos que cause interrupción del servicio o fraude.	Usuario que busca perjudicar a la compañía por medio de robos o fallas en el sistema.
5	Descarga o envió de contenido inapropiado	Descargar todo tipo de información que no del dominio de la entidad, que altere o vulnere la seguridad del mismo
6	Instalación o cambio de Software no Autorizado	Instalar todo tipo de programas no autorizados por la compañía o sin autorización previa
Hurto		
7	Piratería de Software	Instalar o suplantar un software de la compañía para perjudicar y hurtar información bancaria
8	Robo o revelación de información del Negocio	Hecho donde se ve reflejado el robo de información la cual afecta en todo tipo de ámbitos a la compañía
9	Robo de equipo de computo	Perder Activos de la empresa donde se vea involucrada información vital.
10	Robo de información de Acceso	Adquirir accesos de un usuario de la compañía para manipulación maliciosa
11	hurto de Software	Robar software de la compañía para bien propio
Ataques Internos O externos		
12	Intrusión de virus informáticos y/o de código malicioso	Ingreso de un software malicioso por diferentes tipos de canales (Correo, USB, ETC…)
13	Hacking	Persona con conocimientos suficientes para vulnerar la seguridad de la compañía
14	Craqueo de Credenciales	Por medio de software o programas ejecutables contar con la capacidad de forzar el sistema para poder ingresar a el
15	Suplantación de Pagina Web	Crear una página que cumpla exactamente con las mismas condiciones que la pagina original para hurtar información
16	Distorsión de Pagina Web	Ver en la página Web de la compañía que los colores y la letra no se encuentran legible entre otro tipo de características.

17	Manipulación o interceptación de trafico de red	Persona que tiene la capacidad de capturar paquetes de datos y el tráfico de red para hurtar todo tipo de información y credenciales
18	Afectación por ataque de denegación de servicio	Usuarios legítimos que intentan ingresar a la plataforma pero con un acceso nulo, creando molestias en los servidores de la compañía
19	Distribución de SPAM	Recibir SPAM de una manera masiva creando contradicciones en la red de la compañía
20	Aplicación de Ingeniería de Social	Método utilizado para obtener información de personas, entidades, o cualquier tipo de medio para ser manipulada
21	Suplantación de Correo	Correo que se supone, es enviado por personal de la compañía para con obtener todo tipo de información
Funcionamiento Inapropiado de Sistema de Información		
21	Funcionamiento inadecuado de las piezas y/o componentes de software desarrollados internamente	Problemas de ingreso en las plataformas de la compañía que puedan dejar a vista información confidencial
22	Funcionamiento inadecuado de las piezas y/o componentes de software desarrollados por terceros	Herramientas tercerizadas que presentan fallas en su ejecución y que pueden afectar el funcionamiento de la entidad bancaria
23	Funcionamiento inadecuado de Software de Sistemas	Problemas de software en las plataformas usadas regularmente en la compañía, que impiden su correcto funcionamiento
24	Funcionamiento inadecuado de equipos de computo	Problemas de hardware que impiden que la compañía trabaje continuamente, generando todo tipo de problemas y vulnerabilidades si llegase el caso lo equipos tuvieran que salir fuera de la entidad
Interrupción del servicio		
25	Daño o perdida de las instalaciones de computo	Problemas de hardware presentados al interior de la entidad, los cuales afectan de manera directa el proceso según el equipo afectado
26	Daño perdida de los enlaces de comunicación	Interferencias o caídas en la red, donde se pueden ver perdidos todo tipo de información y paquetes de datos de la compañía
27	Falla en la disponibilidad de la energía	Cortes de Luz imprevistos causando fallas eléctricas en los equipos
28	Daño o perdida de equipos alternos	Problemas de hardware presentados al interior de la entidad, los cuales afectan de manera directa el proceso según el equipo afectado
29	Desastres Naturales	Todo tipo de calamidad realizada por la naturaleza que pueda atacar o destruir los equipos y/o información de la entidad
30	Sobrecarga de los sistemas de información	Saturación de información, red, energía entre otros que cause un colapso en las plataformas de la entidad
Error humano		
31	Errores Operativos	Todo tipo de falla humana que afecte de manera

		directa o indirecta la información de la compañía
32	Errores de los Administradores de las plataformas	Este tipo de erros se evidencian cuando el administrador de la plataforma brinda privilegios a personas no autorizadas causando así vulnerabilidad de la información
33	Omisiones en la Operación	Personal que no realiza sus labores en la plataforma a cabalidad, trayendo consigo todo tipo de molestias en la entidad.
Efectos no contemplados de cambios.		
34	Efectos imprevistos de los cambios de software previamente planeados	Cambios en la plataforma con gran impacto en el aseguramiento de la información
35	Efectos imprevistos de los cambios en las unidades de negocio	Posibles errores en la información reflejada, dando privilegios a personas que no podían ver esta información anteriormente, trayendo consigo fugas de información.
36	Efectos de cambios en equipos de cómputo o artefactos de comunicación	Cambios físicos en las instalaciones, la cual contenga información de la compañía y que se pueda sufrir de robo o pérdida según manipulación
37	Efectos no contemplados en modificación de procesos de usuario.	Adaptar procesos que no administraba antes el usuario, brindando privilegios que antes no tenía contemplados.

Niveles de prestación de Servicio

Como un camino viable y para que la gestión de incidentes se realice de una manera efectiva, se crea un diagrama donde se podrá visualizar, categorizar y atender cualquier incidente de seguridad informática según la prioridad del mismo.

		Lunes - Viernes 8 AM - 6 PM			**Sábado - Domingos - festivo**		
		HorarioHábil			**Horario No Hábil**		
SLA	Descripción	ALTO	MEDIO	BAJO	ALTO	MEDIO	BAJO
Atención del incidente	Primer filtro para catalogar la criticidad del incidente	Inmediato	10 Minutos	15 Minutos	15 Minutos	20 Minutos	30 Minutos
Registro del Incidente	Se realiza el registro correspondiente al incidente ocurrido	40 Minutos	60 Minutos	60 Minutos	50 Minutos	60 Minutos	50 Minutos
Escalamiento a Segundo Nivel	Si el incidente no se puede resolver inmediatamente se escala a un personal con amplios conocimientos para la resolución del incidente	2 Horas	4 Horas	8 Horas	2 Horas	4 Horas	8 Horas

Escalamiento a Tercer Nivel	Si el Segundo nivel no puede resolver el incidente debe ser atendido por especialistas, en este caso tercer nivel	4 Horas	8 Horas	16 Horas	4 Horas	8 Horas	16 Horas
Validación Con Experto Externo	Según la criticidad, prioridad y problema que cause el incidente, se le consultará a un experto, el cual nos ayudará con la pronta solución del problema	8 Horas	16 Horas	36 Horas	8 Horas	16 Horas	36 Horas

5.1.4. Flujograma del Proceso

Por último se realiza un flujograma o diagrama de flujo el cual consta del procedimiento que se va a implementar de inicio a fin sobre una gestión de un incidente. Esté diagrama nos ayudara a identificar los procedimientos a grandes rasgos de que debemos hacer cuando se presenta un incidente de seguridad, guiando el proceso y dando una posible solución del incidente.

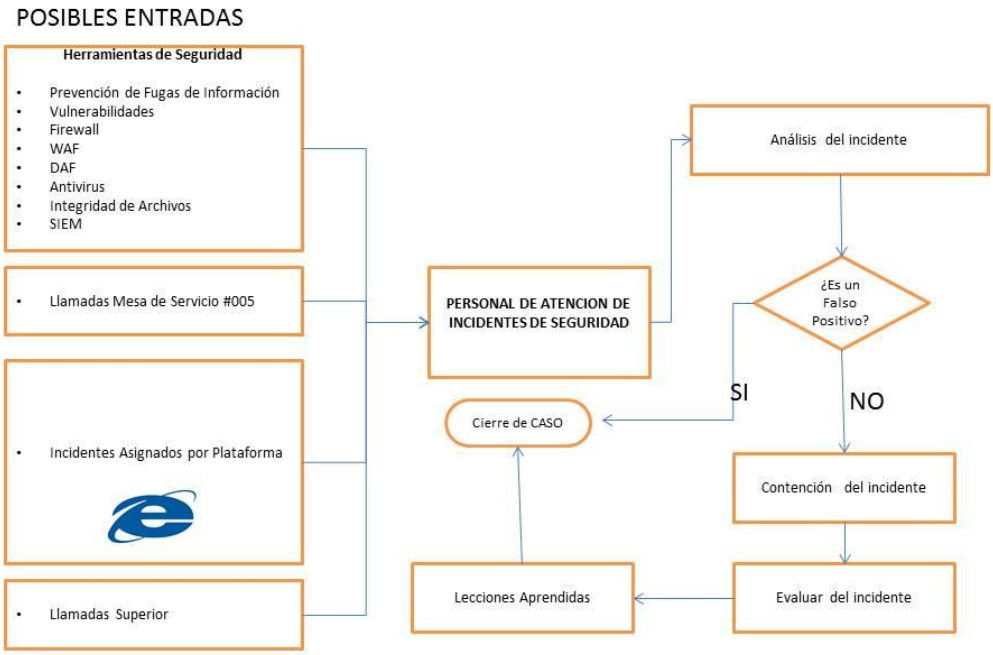

Imagen 10. Flujo grama para la gestión de un incidente

6. Conclusiones

1. Se espera que al involucrar a gran parte de la EF se sea partícipe de los incidentes de seguridad informática presentados en la compañía, se concientice a gran escala sobre todo tipo de riesgos informáticos que pueden sufrir. Creando con esto mejores prácticas y desarrollos que lleven a mantener procedimientos de seguridad más confiables.

2. La identificación de directrices, es una mejoría en caso de no saber a quién dirigirse en el momento de un incidente de seguridad informática, brindado a los involucrados un esquema, al cual pueda acudir según las necesidades del incidente.

3. Con un proceso creado acorde a las normativas de la EF se busca brindar como solución, atender de manera eficiente todo tipo de incidentes informáticos, buscando obtener como resultado una atención eficaz y correcta de los incidentes que puedan ocurrir dentro de la compañía, todo esto hilado y acorde a las normativas y procedimientos ya establecidos en la EF.

4. Ya con la información que ha sido obtenida por la EF, se tiene un listado de posibles incidentes que pueden ocurrir. Esta información se vuelve esencial para poder categorizar el incidente y saber cuál es el tratamiento, la prioridad y la veracidad con la que debe ser tratado el incidente.

7. Referencias

BBC, Tecnología. (9 de Julio de 2011). Recuperado el 2 de julio de 2016, de BBC, Tecnología: http://www.bbc.com/mundo/noticias/2011/06/110609_tecnologia_breve_historia_hackers_nc.shtml

Best Practical Solutions, LLC. (01 de 02 de 2002). *bestpractical.*Recuperado el 12 de 10 de 2016, de bestpractical: https://bestpractical.com/request-tracker

BMC Software, Inc. (2 de Enero de 2005). *Bmc.* Recuperado el 15 de Octubre de 2016, de Bmc: http://www.bmc.com/it-solutions/remedy-itsm.html

Cibertec. (1 de Febrero de 2016). *Cibertec.* Recuperado el 5 de Octubre de 2016, de Cibertec: http://www.cibertec.edu.pe/formacion-continua/certificaciones-internacionales/cursos-cobit/que-es-cobit

COBIT™. (19 de Mayo de 1999). *CONTROL and AUDIT for INFORMATION and ELATED TECHNOLOGY.* Recuperado el 11 de Octubre de 2016, de CONTROL and AUDIT for INFORMATION and ELATED TECHNOLOGY: http://alarcos.esi.uclm.es/per/fruiz/curs/mso/comple/cobit.pdf

Creative Commons BY-NC-SA. (1 de Enero de 2002). *GLPI - Gestionnaire libre de parc informatique.* Recuperado el 2 de Septiembre de 2016, de GLPI - Gestionnaire libre de parc informatique: http://glpi-project.org/spip.php?rubrique18

Dexon Software Inc. (2 de Febrero de 2005). *Dexon Software.* Recuperado el 02 de Octubre de 2016, de Dexon Software: http://dexon.us/Solutions.aspx

IsecT Ltd. (1 de Febrero de 2011). *ISO/IEC 27035:2011.* Recuperado el Septiembre de 20 de 2016, de ISO/IEC 27035:2011: http://www.iso27001security.com/html/27035.html

Mintic. (11 de Junio de 2016). *Fortalecimiento de la gestión de TI en el estado.* Recuperado el 10 de Octubre de 2016, de Fortalecimiento de la gestión de TI en el estado: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

OSIATIS S.A. (1 de Febrero de 2011). *ITIL®-Gestión de Servicios TI.* Recuperado el 7 de Septiembre de 2016, de ITIL®-Gestión de Servicios TI: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/proceso_gestion_de_incidentes/proceso_gestion_de_incidentes.php

OSSINT. (25 de Enero de 2015). *Inteligencia Estratégica y Prospectiva de Fuentes Abiertas.* Recuperado el 10 de Octubre de 2016, de Inteligencia Estratégica y Prospectiva de Fuentes Abiertas: http://www.ossint.org/dig-au-plan

OTRS. (1 de enero de 2016). *OTRS.* Recuperado el 11 de Agosto de 2016, de OTRS: https://www.otrs.com/?lang=es

Paul Cichonski, Tom Millar, TimGrance, & Karen Scarfone. (1 de Agosto de 2012). *Computer Security Incident Handling Guide.* Obtenido de Computer Security Incident Handling Guide: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

S.A, OSIATIS. (9 de Octubre de 2011). *ITIL®-Gestión de Servicios TI.* Recuperado el 10 de Octubre de 2016, de ITIL®-Gestión de Servicios TI: http://itilv3.osiatis.es/