MODELO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PARA PYMES

RAMIRO ANDRÉS DELVASTO RAMÍREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

COLOMBIA

2016

MODELO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PARA PYMES

RAMIRO ANDRÉS DELVASTO RAMÍREZ

Monografía para optar el título de Especialista en Seguridad Informática

DIRECTOR

JOHN FREDY QUINTERO

Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

COLOMBIA

2016

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

Presidente de Jurado

_____

Jurado

_____

Jurado

Bogotá, D.C., _____ de _____ de 2016

DEDICATORIA

A Dios todo poderoso que me ha dado la Fe y satisfacción de alcanzar otra meta en vida personal.

A mi familia por su apoyo incondicional para alcanzar el logro de mis metas y propósitos de superación personal y profesional.

EL AUTOR

AGRADECIMIENTOS

El autor expresa su agradecimiento a:

La Universidad Nacional Abierta y a Distancia, Sede José Acevedo y Gómez, por la oportunidad que me ha brindado para cursar estudios de especialización en el área de mi interés

Los docentes y tutores de la Universidad por compartirme sus conocimientos y experiencias tan útiles y enriquecedoras

John Fredy Quintero, asesor y tutor de trabajo por su permanente y sabia orientación en todo el proceso de desarrollo.

Todas aquellas personas que de una u otra manera colaboraron con la realización del presente documento.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ILUSTRACIONES

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: cualquier elemento tecnológico tangible o intangible que procese, almacene información y tiene valor para la organización.

ACUERDO: convenio entre dos o más partes o una resolución premeditada de una o más personas y/o entidades

APRENDIZAJE: adquisición de conocimientos, habilidades y actitudes a través del estudio, enseñanza o experiencia en una materia.

CONFIDENCIALIDAD: La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones.

DETECTAR: proceso de identificación de cualquier actividad inusual o sospechosa que pueda comprometer el normal funcionamiento de la entidad.

DISPONIBILIDAD: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

EQUIPO DE RESPUESTA: Grupo de personas que han sido designadas para atender y recolectar la información relacionada con los incidentes de seguridad de la información.

FORMATO: es el conjunto de las características técnicas y de presentación de un texto, objeto o documento en distintos ámbitos, tanto reales como virtuales.

GESTIÓN DE INCIDENTES: capacidad para gestionar de manera efectiva eventos inesperados que pueden perjudicar la operación de las organizaciones con el fin minimizar su impacto y mantener o restaurar las operaciones dentro de los tiempos establecidos.

INTEGRIDAD: que la información no sea alterada por personas no autorizadas y que refleje la realidad de la información de la entidad, por ejemplo los estados financieros.

INVESTIGACIÓN: es considerada una actividad humana, orientada a la obtención de nuevos conocimientos y su aplicación para la solución a problemas o interrogantes.

LECCIONES APRENDIDAS: documentar de forma organizada la información del conocimiento adquirido en proceso o sobre una o varias experiencias que pueden ser aprovechas para afrontarlos en eventos futuros.

MONITOREO**:** comprobar, supervisar, observar críticamente, o registrar el proceso de una actividad, acción o sistema en forma sistemática, para identificar cambios.

OPERACIÓN: coordinar y ejecutar y procesos que son necesarios para gestionar la tecnología.

PLAN DE FORMACIÓN: es un conjunto de actividades con el objetivo de obtener conocimiento para mejorar las capacidades laborales y académicas de un individuo, entre otras.

PREPARAR: proceso de definir las actividades que deben realizarse para contar con capacidad para responder a incidentes.

PROTECCIÓN: actividades que deben realizarse para asegurar los datos y la infraestructura informática crítica, así como a la comunidad de usuarios cuando se responde a un incidente.

RESPUESTA A INCIDENTES: capacidad operacional para identificar preparar y responder a los incidentes, para controlar y limitar sus daños, aplicar prácticas de investigación y normas forenses, recuperar la operación a su estado normal.

RESTRICCIONES**:** Por lo general las restricciones son establecidas o reconocidas por la dirección de la organización y están influidas por el entorno en el cual opera ésta.

SALVAGUARDAR**:** son prácticas, procedimientos o mecanismos que pueden proteger contra una amenaza, reducir una vulnerabilidad.

VULNERABILIDAD**:** muestra la fragilidad de un sistema (físico, Técnico, organizacional, cultural, etc.) que puede ser afectado adversamente, causando daños o perjuicios.

RESUMEN

TITULO MODELO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PARA PYMES

Autor: Delvasto R. Ramiro A.

El presente proyecto, tiene como objetivo general diseñar un modelo de gestión de seguridad de la información para pymes, para mejorar la atención de incidentes que atenten contra la confidencialidad, integridad y disponibilidad de la información.

En la actualidad el uso de las tecnologías de la información y las comunicaciones por parte de las empresas han llevado a que se corran o asuman ciertos riesgos que de llegar a materializase pueden afectar uno de los activos más valiosos para las mismas como lo es la información, por lo tanto se deben tomar acciones que ayuden a proteger dicho activo.

Lo anterior inclina a las empresas a implementar medidas o controles que pueden ser de tipo tecnológico, personas o procedimental para proteger la confidencialidad, integridad y disponibilidad de la información de riesgos que pueden alterar la operación normal o el logro de sus objetivos misionales u organizacionales.

La materialización de riesgos en tecnologías de la información son conocidos como incidentes de seguridad, que al no tener establecido un modelo de gestión de estos, se hace difícil para cualquier empresa poderlo identificar, contener y recuperarse de ellos.

El modelo de gestión de incidentes hace parte de las acciones que deben tomar las empresas para responder a los riesgos de seguridad de la información a los que están expuestos sus activos de información.

Palabras clave: Análisis de riesgos, identificación de activos, implementación de controles, plan de seguridad.

SUMMARY

TITLE INCIDENT MANAGEMENT MODEL OF INFORMATION SECURITY FOR MESs

Author: R. Delvasto Ramiro A.

This project's general objective is to design a management model for information security for MESs, to improve care of incidents that threaten the confidentiality, integrity and availability of information.

Currently the use of information technology and communications by companies that have been run or take CSIRTain risks that can affect materialize reach one of the most valuable assets for the same information as is therefore must take action to help protect that asset.

This inclines companies to implement measures and controls that can be technological, procedural or people to protect the confidentiality, integrity and availability of information risks that may disrupt the normal operation or the achievement of its mission or organizational objectives type.

The materialisation of risks in information technology are known as security incidents that have not established a management model of these, it becomes difficult for any company being able to identify, contain and recover from them.

The incident management model is part of the actions to be taken by companies to respond to security risks of information they are exposed to their information assets.

Keywords: Risk analysis, identification of assets, implementing controls, safety plan.

INTRODUCIÓN

Los constantes avances en el uso de las tecnologías de la información y las comunicaciones han llevado a las empresas a prepararse para afrontar los riesgos de seguridad a los que puede estar expuesta su información, toda vez que es uno de los activos que ha tomado mayor relevancia en las empresas, lo cual conlleva a implementar controles y acciones que ayuden asegurarla como una forma de anticiparse a los riesgos o eventos que la afecten.

En la mayoría de los casos el impacto de estos riesgos se ve reflejado en la confidencialidad como por ejemplo robo de información clasificada como secreto industrial, la integridad, la cual está relacionada con alteración de información de estados financieros y disponibilidad teniendo en cuenta que puede causar que los servicios tecnológicos o de información de las entidades no esté disponible, lo cual pude causar pérdidas económicas, de relaciones de confianza por los clientes que conllevarían también a la pérdida de imagen o buen nombre de las empresas ante sus grupos de interés. Riesgos que de no tomarse acciones correctivas definidas pueden llegar a repetirse.

¿Qué dejarían de perder las empresas con la implementación de un modelo de gestión de incidentes de seguridad de la información?

La gestión de incidentes de seguridad de la información es una de esas acciones (controles tecnológicos, capacitaciones, análisis de riesgos, entre otros) que se deben implementar para asegurar y proteger la información de las empresas o entidades, a través de este documento se presentará un modelo de gestión de incidentes de seguridad que pueden implementar aquellas empresas o entidades que estén en la tarea de implementar su Sistemas de Gestión de Seguridad de la Información.

Estudios previos como el realizado por Welivesecurity patrocinado por ESET y publicado en mayo de 2012 han mostrado que el 97% de los incidentes de seguridad se hubieran podido evitar si las entidades implementaran acciones, como controles, capacitaciones a sus empleados en temas de seguridad, entre otros, para proteger su información, incluyendo un modelo de gestión de seguridad de la información. Este estudio es el resultado de 8 años de seguimiento a más de 2000 brechas de seguridad que se realizaron desde el 2002, donde más de mil millones de registros fueron comprometidos.

OBJETIVOS DEL PROYECTO

Objetivo General

Definir un modelo gestión de incidentes de seguridad de la información que permita a las entidades detectar, reportar, contener y recuperarse de un evento no controlado.

Objetivos Específicos

- Identificar y clasificar eventos que pueden llegar a considerarse como incidentes de seguridad de la información.

- Definir un modelo guía para gestión de los incidentes de seguridad de la información en las organizaciones.

- Fortalecer la capacidad de las áreas de TI para gestionar incidentes de seguridad con el fin de que los eventos no se repitan o minimizar su impacto.

- Generar un indicador de medición en la socialización del modelo de gestión de incidentes de seguridad de la información.

MARCO TEORICO

Uno de los mayores activos y más significativos que tienen las empresas hoy en día después del talento humano es la información, toda vez que es a través ésta que las empresas pueden analizar cómo van dentro de la gestión que planearon o pueden tomar decisiones trascendentales para los intereses de la organizaciones.

En el libro Inseguridad de la información, una Visión Estratégica. Escrito por el Dr. Jeimy Cano (2013), se hace una descripción ejemplarizante de cada uno de los principios de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad) y como cada uno de estos puede verse afectado por acciones de los atacantes o por simple descuido de los usuarios de la información, lo cual logra desestabilizar la estrategia organizacional de las empresas.

Tomar conciencia de proteger la información, ha llevado a que las empresas implementen controles para asegurar su información, ya sea que se encuentre en medio físico o digital. Estos controles pueden estar dentro de una arquitectura tecnológica de seguridad diseñada e implementada para cumplir con este fin o pueden definir también planes de seguridad de la información donde se involucre los sistemas de información, la infraestructura tecnológica, la información misma y las también las personas, esta últimas pueden convertirse en uno de mayores medio de fuga de información por ocasión u omisión.

Pero a pesar de todos los esfuerzos y aun cuando las empresas implementan acciones o controles para que de una u otra forma su información no sea afectada, es decir, que la información no sufra o sea víctima de un evento no controlado, se presentan situaciones que han sido muy sonadas, como por ejemplo el ataque sufrido el sitio web de la Policía Nacional según noticia publicada por el diario El Espectador el 13 de octubre de 2012, o el bloqueo o denegación de servicio que impacto a los servidores de los sitios web de Ecopetrol, Ministerio de Hacienda y el Minas y Energía perpetrado en diciembre de 2012.

Otros incidentes de seguridad se han conocido como las filtraciones y revelaciones de información por parte de Wikileaks, en el 2010, el acceso no autorizados las páginas de las redes sociales de personalidades del Estado colombiano como el expresidente Álvaro Uribe y el presidente Juan Manuel Santos, entre otros.

Dentro de la literatura encontrada y analizada con referente a este tema, se puede observar que los autores coinciden en lo importante que es la gestión de los incidentes de seguridad como una acción que debe ser implementada en el aseguramiento de la información desde el mismo momento en que se piensa en la seguridad de la información y más aún si se piensa en implementar un Sistema de Gestión de Seguridad de la Información.

Así lo describe el ingeniero electrónico César A. Correa en su artículo Estrategias para la Creación de un Modelo de Atención de Incidentes de Seguridad Informática para Empresas Pymes “el tema de seguridad de la información como una preocupación”[1] que ha despertado un gran interés, debido a los diferentes eventos que han ocurrido y que afectan la información de las organizaciones.

En la Política de gestión de incidentes de seguridad de la información, definido por la agencia de gobierno electrónico y sociedad de la información (agesic) de Uruguay en el 2010. Se define y describen los lineamientos que se deben seguir para la gestión de incidentes

Sin embargo, se puede observar casos en donde se presentan eventos o incidentes que afectan la seguridad de la información y las empresas o entidades no saben cómo afrontarlos y peor aún como gestionarlos.

Por otra parte, para ayudar a combatir regladamente el abuso sobre la información de las empresas, el Estado colombiano ha venido generando una serie de leyes y decretos que sancionan a aquellas personas o entidades que accede, interrumpen, filtran o sustraen información de las empresas y que para el concepto de la norma colombiana son delitos informáticos.

Dentro de las regulaciones que existen en el territorio nacional se conocen las que se describen a continuación.

Ley 527 de 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 599 DE 2000, por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de “violación ilícita de comunicaciones”, se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el “Acceso abusivo a un sistema informático”.

Ley 1273 de 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Conocida como la Ley de Delitos Informáticos.

[1] Reyes Muñoz, Juan Carlos, Modelos para la Creación de un Grupo de Respuesta a Incidentes de Seguridad Informática Gubernamental Central en América Latina, 2006. p.

Ley Estatutaria 1581 de 2012 por la cual se dictan disposiciones generales para la Protección de Datos Personales. Ley de protección de datos personales clasificados como públicos, no públicos y sensibles.

Decreto 1377 de 2013 que reglamenta la Ley Estatutaria1581 de 2012. En el cual se definen como registrar las bases de datos que contienen información de tipo personal ante la SIC.

Decreto 886 de 2014 por el cual se reglamenta la Ley Estatutaria 1581 de 2012 para el registro de base de datos.

Ley Estatutaria 1712 de 2014, por la cual se crea la Ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

Decreto 103 de 2015, por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

METODOLOGÍA

La metodología empleada para el desarrollo de este documento es la de monografía de compilación y análisis de experiencia, es decir, "se recopiló información relacionada con el tema abordado con el fin de hacer un análisis crítico de la documentación recopilada y a su vez se pone en práctica el conocimiento y experiencia del autor sobre el tema y sobre seguridad de la información"[2].

De igual forma el proyecto se ha desarrollado teniendo en cuenta las siguientes fases:

Fase 1. Recopilación de información

En esta fase se realizó el proceso de recopilación y consulta de literatura relacionada con el tema tratado en esta monografía, entre ellos, se tuvieron en cuenta información encontrada en internet, libros de seguridad de la información, normas técnicas internacionales, indagaciones con colegas y expertos en seguridad de la información.

Fase 2. Análisis de información

En esta fase se hizo la lectura y analizaron acuciosamente toda la información recopilada para determinar los beneficios, ventajas, y porque no desventajas que ofrece la definición de modelo de gestión de incidentes de seguridad de la información dentro de un plan de seguridad y un SGSI.

Fase 3. Elaboración documento final

En esta fase y gracias al análisis de la información recopilada, se procede con la elaboración del documento final, donde se plasman las características, etapas que se deben surtir, así como otros aspectos a tener en cuenta para la definición de un modelo de gestión de incidentes de seguridad de la información.

[2] CICTAR, Estructura para la Realización de una Monografía. p. 01.

1. GESTIÓN DE INCIDENTES

En el campo de la tecnología y la informática todos los eventos que atenten contra la normal operación de la infraestructura o la información, debe entenderse como un incidente y como tal debe gestionarse para encontrar su origen, posibles consecuencias y las soluciones que estos pueden acarrear para las empresas.

Sin embargo, es preciso aclarar que en los incidentes de infraestructura y los de información deben tratarse por separado, sin llegar al punto que no se puedan relacionar entre sí. Es decir, que un incidente de infraestructura (operacional) no pueda conllevar a generar un incidente de seguridad de la información porque algunos incidentes de seguridad de la información han sido y pueden ser producto de una falla operacional.

Un ejemplo de un incidente operacional o de infraestructura podría ser el que una persona no pueda ingresar a su estación de trabajo porque olvido la clave o porque su equipo esta desconectado de la red y otra cosa es que un persona vaya a acceder a una información de la empresa y no pueda hacerlo porque la misma ha sido borrada o tiene cambios.

Para claridad de la relación entre las dos clases de incidentes, se puede mencionar que los usuarios no pueden acceder a la información almacenada en el servidor porque el mismo ha llegado a la capacidad límite de procesamiento de peticiones.

Si se parte del ejemplo citado algunos párrafos atrás, por eso es imprescindible que las Empresas definan políticas de seguridad y entre ellas políticas de backup, que deben especificar qué información es la que debe ser salvaguarda y en que sitio, la periodicidad, el tipo de backup si incremental, total o parcial.

De igual formas, la empresas deben pensar en el diseño de su centro de cómputo y si requiere o no un Centro de Cómputo Alterno (CCA), que respalde la infraestructura identificada como crítica.

Así las cosas, las acciones que se deben tener en cuenta para atender un incidente operacional son las que se mencionan a continuación:

- El usuario afectado informe a la mesa de ayuda o a quien haga sus veces el inconveniente o falla que se le presenta.

- La mesa de ayuda valora el incidente y en caso de que los técnicos de la mesa de ayuda puedan resolver en el instante la falla, ésta quedará resuelta y se cerrara el caso, de lo contrario, se elevará la petición a nivel funcional o técnico de segundo nivel.

- En el evento que no pueda resolverse en ninguna de las instancias anteriores, el caso sería elevado al nivel de soporte de proveedor del servicio para la compañía en caso de que lo hubiere.

Para el caso de los incidentes de seguridad de la información las etapas macro que deben tenerse en cuenta para su gestión son las que se enuncian a continuación.

- Etapa 1. planeación y preparación.
- Etapa 2. detección y reporte del incidente
- Etapa 3. evaluación y decisión
- Etapa 4. respuesta
- Etapa 5. Lecciones aprendidas.

Los Sistemas de Gestión de Seguridad de la Información y las mejores prácticas que sobre esta materia se pueden consultar, evocan que las acciones para salvaguardar la información de cualquier entidad, primero debe tener un proceso previo de identificación y análisis de riesgos, esto conlleva a la necesidad de revisar otros conceptos que en se seguridad de la información deben ser aclarados.

En este sentido, el primero de los conceptos que deben quedar claro es el de Amenaza, que se define como la posibilidad de que suceda un evento de tipo natural o humano, ya sea provocado por acción u omisión que puede causar daño a cualquiera de los sistemas o infraestructura tecnológica.

Dentro de las amenazas se de tipo humano se pueden encontrar (fraude por computador, piratas informáticos, phishing, funcionarios insatisfechos, terroristas, competidores de la industria, crimen organizado, entre otros). En las amenazas de tipo natural se encuentran (tormentas eléctricas, terremotos, inundaciones, incendios no provocados).

El siguiente concepto a revisar es vulnerabilidad, que se refiere a las características que condicionan la ocurrencia de las amenazas, es decir, capacidades de los sistemas, infraestructura tecnológica o de las personas que pueden ser aprovechadas por las amenazas.

Las vulnerabilidades pueden ser catalogadas de tipo físico, social o económico entre otras.

El impacto es la medición del daño causado por la presencia de una amenaza a un sistema, infraestructura tecnológica o la información misma de la Empresa, por ejemplo se mencionan las pérdidas financiera, sanciones legales o daño en la imagen corporativa.

Finalmente el riesgo se define como la probabilidad que ocurra un hecho no controlado, que afecte la normal operación de la Empresa o el logro de los objetivos y metas de la organización.

Por lo expresado con anterioridad, se analizarán y modelaran las actividades para la gestión de los incidentes de seguridad de la información, las cuales serán desarrollas a los largo de este documento.

2. ETAPA 1. PLANEACIÓN Y PREPARACIÓN

En el proceso de planeación y preparación para implementar el modelo de gestión de seguridad de la información se deben considerar los siguientes aspectos:

2.1. REVISIÓN, ACTUALIZACIÓN O DEFINICIÓN DE LAS POLÍTICAS DE SEGURIDAD

En el proceso de definición de un plan de seguridad de la información se debe iniciar con unas generalidades, un alcance, unos objetivos, unos responsables, la identificación de los activos, las áreas a cubrir o proteger con el plan, los riesgos a los que puede estar expuesta la información y los controles que deberán ser implementado y cuáles no lo serán, todo lo anterior recibe el nombre de Política de Seguridad de la Información, dentro de la cual se encuentra la política de gestión de incidentes de seguridad de la información, "Esta Política de Gestión de Incidentes de Seguridad de la Información se integrará a la normativa básica del Organismo, incluyendo su difusión previa, y la instrumentación de las sanciones correspondientes por incumplimiento de la presente política"[3]

Es primordial que si no se ha definido una política, ésta se establezca como argumento fundamental para la gestión de incidentes, porque la política se convierte en el punto de partida de toda la gestión de seguridad que se haga sobre la información de las empresas.

En el caso de existir una política, se debe hacer un análisis profundo de la misma para evaluar si es necesario hacer una actualización teniendo en cuenta puntos como por ejemplo, número desbordado de eventos no controlados, evaluación de controles que no sean operativos y sostenibles en el tiempo, desconocimiento de los funcionarios por falta de divulgación sobre las políticas de seguridad definidas.

2.2. DETERMINACIÓN DE LA ESCALA DE CLASIFICACIÓN DE LOS INCIDENTES

Antes de hablar de la escala de clasificación de los incidentes es importante tener claro la diferencia entre un evento y un incidente de seguridad, de acuerdo con la Norma ISO/IEC27035, expresa un evento de seguridad 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"[4]. Y un incidente, es "Un evento o una serie de eventos inesperados e indeseados,

[3] AGESIC, Política de Gestión de Incidentes de Seguridad de la Información, Uruguay, 2010. P. 05.

[4] GTC-ISO/IEC 27035 Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información, 2012. p. 10.

que van contra la seguridad de la información. Tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la confidencialidad, integridad y disponibilidad la información"[5].

Teniendo claro lo anterior, y conociendo que en términos de seguridad se manejan los conceptos de probabilidad e impacto es válido considerar la siguiente fórmula para ayudar a definir la clasificación de los incidentes de seguridad de la información.

Impacto negativo producido por el incidente	+	Criticidad de los recursos informáticos afectados	=	Criticidad incidente

Donde el "impacto negativo producido por el incidente" está dado por el grado de afectación que el incidente pueda producir para la organización en caso de presentarse; la "criticada de los recursos informáticos afectados" basada en los activos de información e infraestructura tecnológica que es vital importancia para la operación de la empresa y que entre otras cosas debe permitir o definir una valoración cuantitativa de pérdidas para la organización.

De lo anterior, y acorde con la formula plateada, se puede definir una tabla de clasificación según su criticidad.

Tabla 1. Ejemplo de clasificación de la criticidad de los incidentes

SEVERIDAD	DESCRIPCIÓN
ALTA	Amenaza la integridad y la vida de las personas. Afectar el buen nombre de la empresa. Afectar las relaciones o negociaciones con los grupos de interés. Afectar la estabilidad financiera de la empresa Afecta información de índole personal. Pérdida o robo de información catalogado como secreto comercial o industrial. Afecta infraestructura crítica para los procesos de la empresa Generar incumplimiento de normas legales.

[5] Ibid 2.

SEVERIDAD	DESCRIPCIÓN
MEDIA	Compromete medianamente el buen nombre de la empresa. Afecta medianamente a las personas Impacta un número moderado de sistemas o personas.
BAJA	No afecta la integridad o la vida de las personas. Impacta un número mínimo de equipos no críticos.

2.3. ESTABLECIMIENTO DE LA MATRIZ RACI

Una RACI es una matriz de vital importancia para las organizaciones que implementan esquemas de seguridad de la información toda vez que allí se definen o mapean los roles y las responsabilidades de quienes deben participar en estos esquemas, así como su intervención en cada una de las actividades con motivo de conocer quién toma parte en cada actividad y con qué nivel de participación. En este mapeo la RACI cada letra que forma su nombre es una responsabilidad específica en la actividad por parte de los involucrados.

A continuación se muestra la nomenclatura a utilizar dentro de la tabla RACI definida para el Modelo de Gestión de Incidentes de Seguridad de la Información

Tabla 2. Descripción Matriz RACI

	RESPONSABILIDAD	DESCRIPCIÓN
R	Responsible	Responsable de ejecutar la actividad.
A	Accountable	Encargado del cumplimiento y la calidad en la ejecución de la actividad.
C	Consulted	Aporta conocimiento y/o información para que el responsable ejecute la actividad.
I	Informed	Rol que debe ser informado una vez que la actividad ha finalizado.

Fuente: Elaboración Propia

De acuerdo con lo anterior, la Matriz RACI estaría representada de las siguiente Manera:

- Actividad: Nombre de la actividad

- Roles: Nombre de los roles participantes en el lineamiento de Administración de Incidentes, y de Administración de Servicios, implementados en el Área de Información y Sistemas.

Tabla 3. Definición de la RACI

Actividad / Funciones/Áreas	Junta Directiva (si existiece)	Gerente	Sub Gerente Operaciones	Dueño Procesos de Negocio	Área de Buen Gobierno, Riesgos y Auditoría (si existiece)	Coordinador de Seguridad de la Información	CSIERT	Área de Recursos Humanos	Área Jurídica "si existiece "	Dirección de Información y Tecnología o quien haga sus veces	Área de Infraestructura	Mesa de Servicio	Usuarios / Clientes
Prácticas Clave de Gestión													
Brecha potencial de seguridad identificada					I	A				I	C		
Reportar incidente de seguridad	R	R	R	R	I	R/I	A	R	R	R	R	R	R
Investigar incidente de seguridad			I			A	R	C	C	C	C		C
Informar resultado del incidente de seguridad					I	A	R			C	C	I	
Impacto del incidente		I	C	C	I	A		C	C	C			
Definir plan de acción de mejora					I	A/R		C	C	C	C		
Monitorear las acciones implementadas					C	A				I	R		
Lecciones Aprendidas			I	I	I	A	I	I	I	I	C		

Fuente: Elaboración Propia

2.4. DEFINICIÓN DE LOS FORMATOS

Para lograr una correcta gestión de los incidentes de seguridad de la información en las organizaciones es imperativo que se definan y oficialicen unos formatos donde se pueda realizar los siguientes registros:

1. Formato de reporte de Incidentes (Ver Anexo 1.)
2. Formato de valoración de incidentes (Ver Anexo 2.)
3. Formato de informe de resultado de incidentes (Ver Anexo 3.)

Lo anterior, con el fin de llevar un registro pormenorizado de cada uno de los incidentes de seguridad de la información que se presenten.

2.5. PROCEDIMIENTOS PARA EL USO DE LOS FORMATOS

Una vez se hayan establecidos los formatos, se debe elaborar un procedimiento donde se especifique a los funcionarios o colaboradores de la entidad el orden de uso de los mismos.

1. Formato para el Reporte de Incidentes: todo análisis de incidentes inicia con la detección y el reporte, para lo cual el formato a ser diligenciado por los funcionarios y colaboradores de las organizaciones es el de reporte de incidente para dar a

conocer al área correspondiente la existencia de un incidente de seguridad de la información.

En este formato se diligencia información relacionada con datos básicos de la personas que está reportando el hecho, como por ejemplo, Nombre, Cargo, Correo electrónico, No. de teléfono o extensión, entre otros. También se registra información como la fecha y hora del incidente, descripción del incidente, activo de información afectado por el incidente y lugar de los hechos.

2. Formato para Valoración de Incidentes: registrado el incidente, se procede con la valoración del mismo, es decir, se evalúa o determina el grado de impacto negativo producido por el incidente y la criticidad del recurso o activo de información afectado, esto con el fin de determinar la criticidad del incidente.

Para ello en el formato de valoración se registra la información relacionada con el reporte, entre los que se encuentra la fecha del reporte, no. de solicitud (para hacer el seguimiento) y una breve descripción del incidente, de igual manera se registran datos relacionados con la fecha de valoración del incidente, nombre de la persona o profesional que valora, la valoración dada al incidente y si es del caso una observaciones relacionadas con la valoración.

3. Formato Resultado de Incidentes: después de valorado y analizado el incidente es necesario realizar una investigación que permita determinar la causa raíz del mismo, este proceso es realizado por un equipo de personas definidas previamente que son las encargadas de recolectar toda la información relacionada con el incidente y la registra en este formato, además de consignar información de cuales fueron los pasos surtidos en la investigación, que oportunidades de mejora se pueden recomendar, las conclusiones de la investigación y los anexos recopilados por el equipo investigador.

2.6. PLAN DE DEFINICIÓN DEL CSIRT

Un Grupo de Respuesta a Incidentes de Seguridad en Cómputo (Computer Security Information Response Team (CSIRT)) es conformado por un equipo de personas cuya función es la de "monitorear, recolectar y dar respuesta a incidentes de seguridad de la información"[6]. Cada vez es más frecuente encontrar un CSIRT para responder a los incidentes de seguridad dentro de las organizaciones.

La implementación de un CSIRT no solo significa gestionar tecnología sino que también debe adoptar una serie de procesos que están compuestos por recursos humanos, económicos y lógicamente tecnológicos, entre otros.

[6] Ibid 2.

Para la definición del CSIRT se debe considerar el tamaño de la organización para que el comité, sea proporcional al tamaño de la organización, asimismo, definir el cuál será el grado de autoridad y autonomía que tendrá dentro de la misma.

Para la atención de los incidentes las organizaciones deben contar con un equipo de respuesta que será el encargado de:

- Evaluar el incidente para identificar su clasificación e impacto en la organización.

- Recolectar la información necesaria y requerida para determinar la causa del incidente con el fin de definir las acciones correctivas que deban ser aplicadas.

- Asegurar la información y/o videncia recolectada a fin de guardar la correcta y adecuada cadena de custodia y conservación para fines legales que puedan producirse.

De igual forma, es conveniente que el CSIRT cuente con los siguientes perfiles:

- *Un responsable del equipo:* como punto de contacto entre los usuarios y los miembros del equipo CSIRT, quien será la persona que liderará las acciones del equipo, entre otras la de activar la actividades para contener y recuperarse del incidente

  Esta persona debe ser conocedor de los temas de seguridad con experiencia en procesos de atención y gestión de crisis, al igual que la recuperación y continuidad de negocio.

- *Un perfil legal, que permita tomar las decisiones que a nivel jurídico deban llevarse a los estrados judiciales en los casos que así lo ameriten por acción u omisión de algún colaborador de la empresa.*

  Debe tener conocimientos en los temas relacionados con el derecho informático y todas las normas que regulan el acceso a la información y servicios tecnológicos.

- *Responsable de los sistemas y seguridad: persona encarga de la administración de las herramientas que sean necesarias para la gestión del CSIRT. Debe conocer los comportamientos de los sistemas durante el análisis de un evento.*

  El responsable de los sistemas debe contar con competencias técnicas o profesionales en la administración de sistemas de información o de infraestructura de seguridad informática.

Entre otras herramientas se pueden mencionar el portal del CSIRT, la plataforma de registro de incidentes (tickets) y de base de datos de conocimiento y los backoffice.

- *Un equipo de comunicaciones: encargado de establecer las comunicaciones entre los usuarios, los miembros del CSIRT y la alta gerencia.*

  La persona de comunicaciones debe tener habilidades en comunicaciones asertivas, es decir que se transmita el mensaje y la información de lo sucedido con la mayor claridad y exactitud posible. De igual forma sería la responsable de definir los medios a través de los cuales se realizará la divulgación de la información.

- *Equipo de gestión de incidentes, personas que serán las responsables de realizar las actividades de investigación de los eventos.*

Una vez conformado el CSIRT, este debe:

- Definir la Misión que tendrá dentro de la organización, donde se establezca los objetivos estratégicos, las metas y las prioridades principales del CSIRT.

  La misión del CSIRT es la de proveer información y asistencia a la empresa en hechos que pongan en riesgos las operación y los objetivos estratégicos de la organización.

  A su vez debe propender por las buenas prácticas en la prevención y control de los incidentes de seguridad de la información en la empresa.

- Identificar a quienes se les prestará los servicios de sensibilización y respuesta de incidentes de seguridad de la información.
- Cuáles serán las áreas de la empresa con las que tendrá relación estrecha y a su vez identificar los agentes o autoridades externas con las que trabajará.

  Teniendo en cuenta los tipos de incidentes que pueden ocasionar impacto en la operación de la empresa, el CSIRT debe tener una estrecha relación con áreas como la jurídica, control interno, auditoria, alta gerencia, tecnología, recursos humanos, etc.

- Determinar y clasificar los servicios que prestará y los que no prestará como CSIRT. Para este caso particular los servicios definidos son los que se encuentran en la tabla 4 de este documento.

- Tendrá que definir un presupuesto para su operación, en sentido, para que la empresa tenga una proyección aproximada de los recursos económicos a

asignar, en la siguiente tabla se muestra los valores estimados por cada uno de los recursos mencionados.

Tabla 4. Costo por mes aproximado para un CSIRT

Talento / Recurso	Cantidad	Valor	Total
Jefe de equipo	1	$4.500.000	$4.500.000
Asesor jurídico legal	1	$3.800.000	$3.800.000
Administrador sistemas del equipo	1	$2.000.000	$2.000.000
Responsable de comunicaciones	1	$1.500.000	$1.500.000
Personal investigador	2	$1.500.000	$3.000.000
Personal de soporte externo	3	$3.000.000	$9.000.000
Herramientas de apoyo (licencia)	2	$5.000.000	$10.000.00

El CSIRT puede y debe establecer relaciones con entes externos como:

- CSIRT de organizaciones externas con el fin de mantener en constante actualización y entendimiento de las actividades a ejecutar de acuerdo con las tendencias tecnológicas y los riesgos asociados.

- Personal de soporte contratado externamente, en caso que la infraestructura impactada tenga soporte por parte de proveedores, esto con el fin de activar los planes de recuperación tecnológica en caso de ser necesario.

- Autoridades de emergencia con el fin de controlar cualquier eventualidad en la que tenga que acudirse a centros de atención médica, o intervención de organismos como bomberos, policía, etc.

- Organizaciones gubernamentales para los casos en los que haya que elevar eventos que dentro de la organización y a nivel nacional se consideren delitos cometidos por los generadores del incidente.

- Autoridades legales, sean éstas públicas o privadas.

Por otra parte, es indispensable mencionar que en relación con el tamaño de la Empresa, así también será el número de recurso humano con los perfiles mencionados que harán parte del CSIRT, las herramientas que se deben implementar, la infraestructura física y tecnológica que deberá ser apropiada, entre otros aspectos para el correcto funcionamiento del equipo de respuesta.

Lo anterior, conlleva a las Empresas a que deben hacer la destinación de recursos para la adquisición e implementación de lo necesario para que el CSIRT ejecute su función con celeridad, eficiencia pero sobre todo con eficacia para contener los incidentes de seguridad que se generen en la organización.

3. ETAPA 2. DETECCIÓN Y REPORTE DEL INCIDENTE

Para la detección y reporte de incidentes es acertado definir los procedimientos que todos los colaboradores de la organización están en la responsabilidad de conocer y aplicar según sea el caso.

3.1. DETECCIÓN Y REPORTE DE INCIDENTES

3.1.1. Qué se puede considerar un incidente de seguridad

Se considera un incidente de seguridad

- Incumplimiento de alguno de los lineamientos definidos explícita o implícitamente en la política de seguridad de la información de la Empresa.
- Ejecución de código malicioso.
- Ataque de virus contra la infraestructura informática.
- 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 la Empresa,

Estos incidentes de seguridad de seguridad de la información pueden estar catalogados con su tipo, como se muestra en la siguiente tabla.

Tabla 5. Ejemplo de tipos de los incidentes

TIPOS DE INCIDENTES				
Denegación de Servicio	**Código Malicioso**	**Acceso no Autorizado**	**Uso indebido de Recursos**	**Análisis de Vulnerabilidades**
• Tiempo de respuesta fuera del conocido. • Interrupción de servicios	• Virus informáticos. • Ransomware • Malware	• Fuga de información. • Borrado de información.	• Uso de recursos para envío de spam.	• Configuraciones por defecto. • Puertas traseras. • Fallas en actualización de

TIPOS DE INCIDENTES				
tecnológicos no operacionales		• Modificado de información. • Intentos reiterativos de acceso a los recursos • Captura de información confidencial	• Promocionar contenido pornográfico. • Violación de las políticas de seguridad y las normas de internet.	software (parches). • Tráfico inusual en la red. • Penetración de sistemas

Fuente: Elaboración Propia

A continuación se presentará una descripción de cada una de las clasificaciones de los incidentes.

Denegación de servicio: La denegación de servicio (siglas en inglés: DoS) y denegación de servicio distribuida (siglas en inglés: DDoS) son una amplia categoría de incidentes con un denominador común. Estos incidentes hacen que un sistema, servicio o red dejen de operar a su capacidad prevista y con mucha frecuencia deja sin acceso a usuarios legítimos del sistema o servicio tecnológico afectado. Existen dos tipos de incidentes DoS/DDoS causados por medios técnicos: eliminación y agotamiento de recursos.

Como ejemplo de este incidente se puede mencionar el envío masivo de paquetes a través de le red para llenar el ancho de banda con tráfico de respuesta.

Los incidentes por denegación de servicio (DoS) son aquellos causados porque el número de peticiones lanzado desde un equipo cliente a un servidor excede el límite permitido y ello causa que el servidor afectado deje de estar disponible.

Entre tanto los incidentes generados por denegación de servicios distribuido (DDoS), son similares al DoS con la diferencia que las peticiones vienen de varios equipos haciendo peticiones a un mismo servidor.

Código Malicioso: identifican un programa o parte de éste insertado en otro programa con la intención de modificar su comportamiento original, usualmente para realizar actividades maliciosas como robo de información y de identidad, alteración o destrucción de la información y los recursos.

Actualmente los códigos maliciosos se usan para realizar ataques dirigidos. Esto se hace algunas veces modificando un código malicioso existente, creando una variante que muchas veces no reconocen las tecnologías para detección de códigos maliciosos.

Estos códigos maliciosos pueden estar dados por virus, ransomware o gusanos, entre otros.

Un ransoware está definido como un software que al memento de instalarse en el equipo víctima, permite que éste sea bloqueado por quien está generando el ataque, a tal punto que el usuario real de equipo perdería todo control sobre el mismo.

Acceso no autorizado: consiste en intentos reales no autorizados, para acceder o utilizar incorrectamente un sistema, servicio o red. Un ejemplo de este tipo de incidentes es acceso a la información por ataque de fuerza bruta.

3.1.2. Como reportar un incidente

En el caso que un funcionario, temporal o tercero contratista considere o identifique que se está presentando un incidente de seguridad debe proceder a su reporte a la mesa de servicio o quien la empresa o entidad delegue para este fin a través de los siguientes medios o canales:

Enviando correo electrónico a la mesa de ayuda o a quien se delegue para la recepción de estas solicitudes con la siguiente información como mínimo:

Nombre quien reporta
Cargo de quien reporta
Teléfono o E-mail
Fecha de reporte
Fecha del incidente
Equipo o sistema afectado
Descripción del incidente

Si la empresa o entidad dispone de una intranet, se debe hacer uso del formato para registro de reporte definido para web. (Ver anexo 1)

En caso de que la empresa o entidad, disponga de una línea (extensión telefónica) de atención de requerimientos, lo colaboradores de la misma deben comunicarse a través de esta línea donde un operador o agente de mesa de servicio le recibirá la comunicación y registrará información adicional de ser necesario.

3.2. RECOLECCIÓN Y CONSERVACIÓN DE INFORMACIÓN

3.2.1. Recolección de información

En esta etapa se debe recopilar información relacionada con:

- El alcance del incidente.
- Que activos de información fueron afectados.

- Qué o cómo se originó el incidente (métodos y herramientas utilizadas, posibles vulnerabilidades explotadas)

- Impacto en las actividades u en la operación de la organización.

Para el proceso de recolección y retención de información y/o evidencias que puedan ser utilizadas como parte de la investigación para hallar la causa del evento y/o incidente de seguridad se debe realizar siguiendo los lineamientos y las buenas prácticas de la custodia de evidencias digitales (Técnicas Forenses), tomando como marco general la legislación colombiana, en tal sentido se deberán desarrollar las siguientes actividades como parte de la recolección de esta información.

- La captura de la información será realizada por la coordinación de seguridad de la información o quien delegue para esta función, con la colaboración del administrador de los servicios de red y demás involucrados en el proceso.

  Esta información o evidencia podría hacer parte de una investigación judicial en caso de que se llegar a configurarse un delito informático, por lo cual las acciones ejecutadas para recolectar la información se deben hacer bajo las estrictas medidas de seguridad para evitar que la información o evidencia sufra algún tipo de alteración y pueda perder su validez legal.

  En término legales, un delito informático se define como un acto ilícito, es decir fuera de la ley, perpetrado para recopilar, destruir, alterar información o cualquier sistema de información con el ánimo de obtener usufructo o por generar daño[7].

- En la medida de lo posible al realizar la captura de la información y/o evidencia se debe hacer con el uso de herramientas que no modifiquen ni el entorno ni la prueba en sí, salvaguardando su integridad.

- En la recolección de la información y/o evidencias se deben tener en cuenta aspectos como:

a. *Información de los host*: es aquella información que se pueda recopilar como por ejemplo fecha y hora del sistema, identificación de aplicaciones en ejecución, puertos abiertos, últimas copia de respaldo realizada e historial de archivos copiados, entre otros.

b. Información de red: información relacionada con los logs de monitoreo, servidores de autenticación, y logs de firewalls, entre otros.

[7] CASABONA Romeo, Carlos María, Poder informático y Seguridad jurídica, Editorial Fundesco 1987

c. *Información de personas:* obedece a la información que se pueda recopilar de las personas que conocieron o identificaron de primera instancia el evento o incidente.

d. *Información adicional:* es cualquier información que pueda estar directa o indirectamente relacionada con el incidente y que pueda ayudar a establecer con más exactitud los móviles del mismo.

En el caso que hechos resultantes de seguimiento del incidente impliquen acciones de acuerdo con lo establecido por la Ley, o las disposiciones definidas por la empresa o entidad, estas serán determinadas por el área de la entidad que tenga esta competencia.

3.2.2. Conservación de Información

Una vez se ha hecho la recopilación de la información y/o evidencias del incidente se deben aplicar los conceptos de:

a. *Autenticidad:* es el proceso de demostrar que la información y/o evidencia recopilada no ha sufrido ningún tipo de cambio el proceso de recolección, es decir, que la información es original u autentica.

b. *Cadena de custodia:* se debe llevar un registro detallado del tratamiento que ha sufrido la información y/o evidencia recolectada (forma de transporte, almacenamiento, historial de las personas que han tenido relación con la evidencia).

   Este tema vale la pena precisar, que se debe tener en cuenta lo dispuesto en el Manual de Procedimientos para Cadena de Custodia, definido por la Fiscalía General de la Nación de la República de Colombia, toda vez que desde los términos jurídicos y para que la evidencia recopilada sea válida para adelantar un proceso judicial en contra de algún colaborador o contratista se debe comprobar que la información no ha sufrido ningún tipo de cambio desde su captura hasta el momento de entregarlo al ente jurídico correspondiente.

c. *Validación:* en caso de requerirse se debe demostrar que la información que se deba entregar a entes legales sea la misma que la recolectada

4. ETAPA 3. EVALUACIÓN Y DECISIÓN

4.1. EVALUACIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El área de Tecnología de la Información (TI) o de Seguridad de la Información o quien se designe para el registro de los eventos o incidentes de seguridad que sean reportados por los por lo colaboradores o empleados de la empresa, debe:

- Informar a la persona que reporta que la solicitud ha sido recibida y se le dará el trámite correspondiente.

- Registrar el incidente en el sistema o base de datos destinado para este fin y generar un número para identificar el reporte.

- Buscar una aclaración o ampliación del incidente por parte de la persona que lo reporta o registrar información adicional de otras personas que hayan podido conocer del incidente.

- Evaluar si se cataloga como incidente de seguridad, o si es un incidente de tipo operativo y hacer el escalamiento correspondiente del mismo.

- Reportar el equipo de respuesta CSIRT si el evento fue catalogado como incidente de seguridad de la información.

Por otra parte, adicionalmente después de registrar la fecha y la hora de lo sucedido, también debe complementar el registro del evento con la siguiente información:

- Que se observó y que se realizó (mencionar si utilizó alguna herramienta).

- Ubicación exacta de posibles evidencias del evento.

- Describir como se recolecto la evidencia inicial del evento.

- Detallar si se tuvo algún tipo de custodia o almacenamiento de la evidencia inicial.

4.2. DECLARACIÓN DE INCIDENTE

La responsabilidad de si un evento se declara como incidente de seguridad de la información debe ser del equipo de respuesta una vez le sea notificada la identificación y reporte del evento por parte del punto de contacto que se haya definido por el área de TI, de Seguridad de la Información o quien se designe.

Para ello el profesional o persona del CSIRT que le sea escalado o informado el evento debe:

- Confirmar el recibo del reporte de incidente con la mayor información que haya sido recopilada por el punto de contacto.

- Validar si el evento se encuentra el sistema o base de datos de registro de eventos o incidentes de seguridad y registrarlo en caso que el punto de contacto no lo haya hecho.

- Tener aclaraciones del evento o incidente con el punto de contacto de ser necesario.

- Validar y analizar el contenido del reporte enviado por el punto de contacto.

- Revisar si es posible recolectar información adicional del evento o incidente con personas que puedan estar relacionada o que hayan conocido de la situación.

Si se determina que el evento es un incidente de seguridad de la información, los miembros del equipo de respuesta CSIRT deben llevar a cabo una evaluación posterior donde se defina:

- En que consiste el incidente.

- Cómo, qué o quién lo originó.

- Que puede afectar.

- Determinar el impacto real de negocio para la empresa o entidad.

- Si el impacto es severo, se debe declarar la alerta de crisis.

- Identificar el activo o sistema o información que haya sido vulnerado o modificado.

- Efectos secundarios que pueda dejar el incidente, por acceso físicos no asegurados, brechas en el sistema de información.

- Validar y monitorear las actividades que hasta ese momento de hayan realizado con el incidente.

5. ETAPA 4. RESPUESTA

5.1. PARTICIPACIÓN DE CSIRT

El éxito de la participación del CSIRT dentro del modelo de gestión de incidentes, depende de su campo de acción y reacción frente a cada una de las etapas o fases entre las cuales se encuentran:

Preparación: que involucra todas las actividades preventivas que se implementan para manejar un incidente de seguridad de la información cuando se presentan dentro o fuera de la entidad, incluida la preparación del equipo de respuesta.

Detección: está relacionada con la capacidad del equipo de respuesta para detectar un incidente que está en ejecución o una vez ha ocurrido y es el punto de partida para que el equipo active sus acciones reactivas

Contención: una vez se han ejecutado las acciones para recolectar y registrar la información relacionada con el incidente y se ha hecho el análisis respectivo de esta información encontrando su causa raíz, se procede de ser necesario al aislamiento del o de los sistemas afectados para evitar su propagación.

Erradicación: hace referencia a las actividades que están relacionadas con la erradicación del incidente dependiendo del o los activos que resulten afectados y aplicando las mejores prácticas reconocidas.

Seguimiento: acciones para monitorear los activos de información afectados con el fin de evitar que los incidentes se repitan por esta causa.

Acorde con las fases que se han descrito anteriormente el Grupo de Respuesta a Incidentes de Seguridad en Cómputo (Computer Security Information Response Team por sus siglas en inglés) (CSIRT) debe estar preparado para tomar las acciones antes, durante y después de un incidente a saber:

Antes del Incidente: el CSIRT debe asegurar de que la información de contacto de los miembros se encuentra al día, establecer las herramientas a utilizar al momento de presentarse un incidente, conocer las políticas de seguridad de la información.

Durante el incidente: asumir la coordinación de la atención del incidente y actuar de acuerdo a lo establecido, evaluar la situación y seleccionar las mejores estrategias para inicio de recuperación, establecer contacto con las áreas necesarias (Planeación, Tecnologías Control Internos, entre otras), evaluar la situación y determinar si es necesario escalar el incidente a un nivel superior, mantener vigilancia permanente sobre el incidente, hasta que se haya llevado a cabo las actividades necesarias para salir de la crisis, mantener o salvaguardar la información registrada.

Después de la ocurrencia del incidente: realizar y entregar toda la documentación correspondiente al incidente conservando la cadena de custodia de la misma en caso de requerirse acciones legales, participar en las acciones de investigación del incidente, generar el informe de resultado del incidente, estar a disposición de las áreas que así lo requieran, adelantar las acciones para el cierre del incidente si no fue necesario escalarlo a otros niveles jerárquicos.

Para lograr satisfactoriamente sus objetivos, el CSIRT debe definir un portafolio de servicios determinados en tres frentes como lo muestra la tabla que se ve a continuación.

Tabla 6. Portafolio de servicios de CSIRT

Servicios Reactivos	**Servicios Proactivo**	**Servicios de Gestión de la Calidad de la Seguridad**
· Alertas y advertencias	· Comunicados y anuncios	· Análisis de riesgos
· Tratamiento de incidentes	· Observatorio de tecnología	· Continuidad del negocio y recuperación ante desastres
· Análisis de incidentes	· Evaluaciones o auditorías de la seguridad	· Consultoría de seguridad
· Respuesta a incidentes (in situ)	· Configuración y mantenimiento de la seguridad	· Sensibilización
· Apoyo a la respuesta a incidentes	· Desarrollo de herramientas de seguridad	· Educación / Formación
· Coordinación de la respuesta a incidentes	· Servicios de detección de intrusos	· Evaluación o certificación de productos
- Gestión y Análisis de herramientas	· Difusión de información relacionada con la seguridad	· Identificación de lecciones aprendidas
	· Monitorización de redes	

Fuente: Manejo de Incidentes de Seguridad dentro de la Organización.[8]

5.2. DETECTAR, RESPONDER, RESOLVER Y RECUPERARSE DE UN INCIDENTE

En lo relacionado con la los incidentes de seguridad de la información generalmente son generados por personal que no ha seguido o aplicado los procedimientos de TI

[8] Ardita Julio César, CIGRAS ISACA, Manejo de Incidentes de Seguridad de la Información dentro de las Organizaciones, 2013. p. 27

definidos en una organización, sin embargo también existen situaciones donde los eventos o incidentes son provocados por agentes externos a las organizaciones.

Por esta razón es que se debe definir un procedimiento que permita a la empresa o entidad detectar, resolver, atender y recuperarse de los eventos que puedan generar una pérdida en la operación de su negocio.

5.2.1. Detectar un incidente

La primera parte en un esquema de gestión de incidentes de seguridad de la información tiene que ver con la detección u ocurrencia de evento de seguridad y toda la información relacionada con el mismo.

Como parte de las actividades que se deben tener en cuenta para detectar un incidente por parte del personal o terceros o de manera automática son las siguientes:

- Monitorización de alertas generadas por herramientas como IDS/IPS, programas de antivirus, sistemas de seguimiento de registros.
- Alertas generadas por sistemas Data Loss Prevention (DLP).
- Alarmas por bloque reiterado de cuentas de usuario.
- Alertas de seguimiento y monitoreo a sistemas de red, Firewalls, análisis de flujo de redes y filtrado de contenidos, entre otros.
- Análisis de información con el registro de dispositivos, equipos, servicios y otros sistemas.
- Reportes de usuarios
- Notificaciones hechas por terceras persona o externas como por ejemplo CSIRT, servicios de seguridad de la información, PSI, proveedores de servicios de telecomunicaciones.

Eventos que deben ser monitoreados y que llegan a ser considerados causas de incidentes de seguridad de la información

- Incumplimiento de alguno de los lineamientos definidos explícita o implícitamente en la política de seguridad de la información de la empresa o entidad.
- Ejecución de código malicioso.
- Robo de contraseñas.

- Ataque de virus contra la infraestructura informática.
- 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 la empresa o entidad

Los eventos de seguridad de la información pueden ser detectados directamente por personas que observen algo inusual y que le causa preocupación, ya sea que tenga relación con aspectos técnicos, físicos o procedimentales. La detección puede ser, por ejemplo, de detectores de fuego/humo, o alarmas para intrusos (ladrones) con alertas que notifican en lugares designados previamente para acción humana.

Estos eventos en primera instancia pueden ser detectados por:

- Usuarios.
- Gerentes de línea o de seguridad.
- Clientes.
- Departamento de TI, centro de monitoreo de redes, o de operaciones de seguridad.
- Mesa de ayuda de TI, de acuerdo con los reportes que pueda recibir.
- Proveedores de servicio.
- CSIRT
- Personas que pueden detectar anomalías durante las ejecuciones diarias de su trabajo.

5.2.2. Responder incidente

Para responder de forma eficaz a los incidentes se tiene que llevar acabo lo siguiente:

- La comunicación de puntos débiles y eventos en la seguridad de la información, con la finalidad de asegurar que se realizan correctamente las acciones correctivas oportunas para hacer frente a posibles incidentes.

- Mediante el empleo de los medios adecuados de gestión, es necesaria la comunicación de la evolución y control de sucesos de seguridad de información para contrarrestar la aparición de incidentes o amenazas en la información.

- La gestión de incidentes de seguridad de la información y mejora continua, con el objetivo de asegurar la aplicación para gestionar los posibles incidentes.

- Se debe proceder con la asignación de responsabilidades y procesos de gestión para asegurar una respuesta veloz, estructurada y eficaz para hacer frente a los incidentes de la seguridad de la información.

- Estudio y análisis de los incidentes de seguridad de la información mediante dispositivos adecuados para la inspección de tipos, volúmenes, impactos o costos.

- Es necesaria la colección o recopilación de evidencias cuando comienza una actuación contra una persona u organismo, posterior a un incidente de seguridad de la información, de acuerdo con las normas de la jurisdicción aplicables.

- Asignar recursos internos e identificar recursos externos para responder a un incidente.

- Escalamiento de eventos anómalos detectados por el área de TI a los niveles superiores.

- Escalamiento de eventos anómalos detectados por la mesa de ayuda, a un nivel superior.

- Validar técnicamente la posibilidad de interrumpir o clausurar rápidamente y en forma confiable el sistema, servicio y/o red de información atacada, con el fin de contener el incidente.

5.2.3. Resolver Incidente:

Para resolver los incidentes de seguridad se debe analizar la prioridad de los mismos, es decir, validar el impacto que puede ocasionar en la organización como por ejemplo:

- Aquellos que atenten contra el recurso más importante de toda organización como lo son las personas.

- Atender aquellos incidentes que amenacen la integridad de la información sensible de la empresa o entidad.

- Concentrarse en los incidentes que atenten contra la integridad de otro tipo de información de importancia para la empresa o entidad.

- Resolver los incidentes que pueden afectar los sistemas de información de la organización.

- Atender los incidentes que causan interrupción o caídas en los servicios dispuestos por la empresa para sus usuarios.

5.2.4. Recuperarse de Incidentes:

Una vez se haya recolectado y analizado la información, se haya identificado la causa de incidentes y se hayan tomado acciones para su contención, el equipo de respuesta a incidentes debe surtir actividades como:

- Identificar todos los archivos pertinentes en el sistema, servicio y/o red, incluidos archivos normales, archivos con contraseña o protegidos de otra manera, y archivos encriptados.

- Recuperar tanto como sea posible los archivos eliminados descubiertos, y otros datos.

- Examinar la integridad de los archivos para detectar archivos con Troyanos y archivos que no estaban originalmente en el sistema

- Determinar la actividad de los usuarios y/o aplicaciones en un sistema/servicio/red.

- Extraer el contenido de archivos ocultos, temporales e intercambiados usados tanto por las aplicaciones como por el software del sistema operativo.

- Identificar el personal que deba participar en la recuperación del sistema o dispositivo afectado, por ejemplo administradores de red, base de datos, sistema operativo, sistemas de información.

- Estimar los tiempos de recuperación, acorde con el incidente presentado y con los tiempos establecidos.

- Activar planes de recuperación y procesos de recuperación de ser necesario.

6. ETAPA 5. LECCIONES APRENDIDAS

En un esquema de gestión de incidentes de seguridad de la información cuando estos han sido atendidos, solucionados y cerrados, e involucra el aprendizaje de conocimiento o la manera de cómo fueron manejados o tratados estos incidentes, se debería tener en cuenta una serie de actividades que permiten definir lecciones aprendidas involucradas con los incidentes de seguridad en la empresa o entidad.

Estas actividades se realizan con el objetivo de crear una base conocimiento que permita a la Empresa enfrentar un evento similar con mayor diligencia y a su vez implementar un modelo de mejora continua para gestión de incidentes de seguridad de la información.

6.1. ACTIVIDADES PREVIAS

Las actividades previas a tener en cuenta en un proceso de lecciones aprendidas están enmarcada en las descripciones que se hacen a continuación.

- Actividad para ejecutar un análisis forense de seguridad de la información, si así se requiere, teniendo en cuenta que de ser necesario aplicar esta técnica, se debe revisar si los resultados permitieron identificar el origen real del suceso.

- Revisar, identificar y definir planes de mejoramiento en la implementación de controles de seguridad de la información (existentes o complementarios).

- Evaluar la eficacia de los procesos, formatos y estructura organizacional para responder a un incidente de seguridad de la información.

- Actividad para compartir y comunicar los resultados en la gestión de incidente de seguridad de la información.

La etapa de lecciones aprendidas se realizan con el fin de identificar lo bueno, lo malo y lo por mejorar en la detección, reporte, contención y recuperación de un incidentes de seguridad de la información en la Empresa.

6.2. IDENTIFICACIÓN DE LECCIONES APRENDIDAS

Una vez cerrado el incidente de seguridad de la información que fue identificado, contenido y erradicado, es de vital importancia para la empresa o entidad que identifique y 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. Por otra parte, pueden existir también lecciones por aprender de la

evaluación y resolución de vulnerabilidades de seguridad de la información reportadas.

Estas lecciones pueden ser en los siguientes aspectos:

- Actualización por requisitos nuevos o modificados de los controles de seguridad de la información, los cuales pueden ser tipo técnico, humano o de procesos, lo cual según su resultado puede conllevar a la actualización del material de concientización y porque no de las directrices o políticas de seguridad de la información dentro de la empresa o entidad.

- Actualización de la base de conocimiento de las vulnerabilidades y amenazas de seguridad de la información, conforme al resultado de la evaluación de riesgos de la empresa o entidad y de seguridad de la información existente en la misma.

- Posibles cambios en el esquema de gestión de incidentes de seguridad de la información, así como sus procesos y procedimientos, formularios de reporte y base de datos de incidentes de seguridad de la información.

Por otra parte, basado en los incidentes de seguridad de la información gestionada por la empresa o entidad, también se debería identificar tendencias o patrones de preocupación con el fin de implementar acciones que permitan anticiparse a un riesgo que derive en un incidente de seguridad.

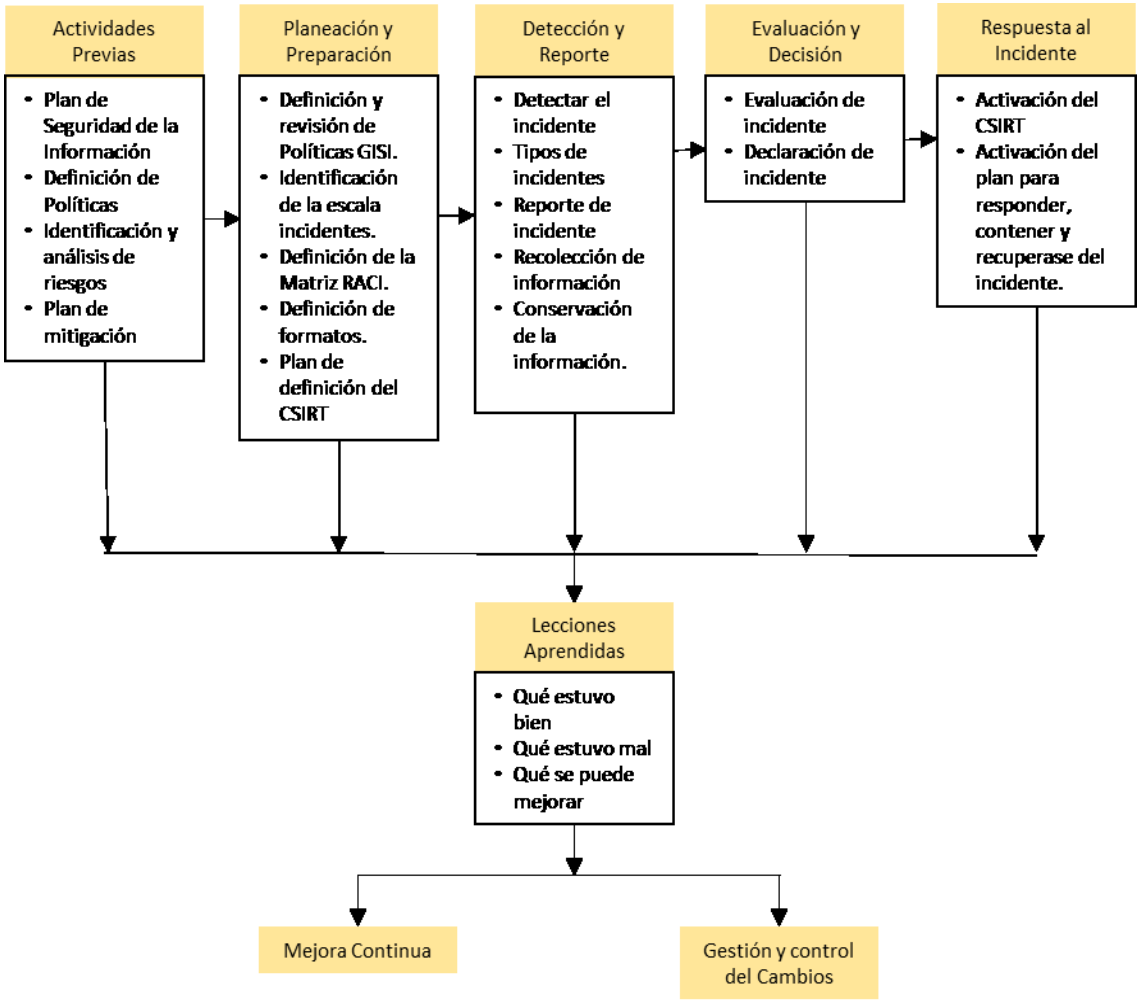
7. ESQUEMA Y FLUJOGRAMA DEL MODELO DE GESTIÓN DE INCIDENTES

7.1. ESQUEMA DEL MODELO

Como se ha venido observando a lo largo de este documento, se han desarrollado una serie de etapas que deben aplicar para definir el modelo de gestión incidentes de seguridad de la información.

La siguiente ilustración muestra el modelo con cada una de sus etapas de una manera secuencial y las actividades a realizar en cada una de ellas.

Ilustración 1. Etapas del modelo de gestión



Fuente: elaboración propia

Como se puede observar en la ilustración, el modelo de gestión de incidentes debe partir de un plan de seguridad de la información general o lo que algunos pueden llegar a llamar Sistema de Gestión de Seguridad de la Información (SGSI), y el modelo de gestión de incidentes se debe diseñar como una medida para responder a situaciones donde los controles definidos o riesgos no identificados puedan afectar la operación de la Empresa.

Por otra parte, en este modelo la etapa de lecciones aprendidas se ha dejado como una etapa transversal a todo el modelo, teniendo en cuenta y partiendo de la premisa que en seguridad de la información, lo único seguro es que nada es seguro, es decir, no existe aún el punto en el que se pueda decir que la seguridad es absoluta, solo que existe un punto de equilibrio entre los riesgos asociados a la infraestructura, procesos, procedimientos y personas con las acciones a tomar para mitigar esos riesgos, en otras palabras, no hay riesgo cero.

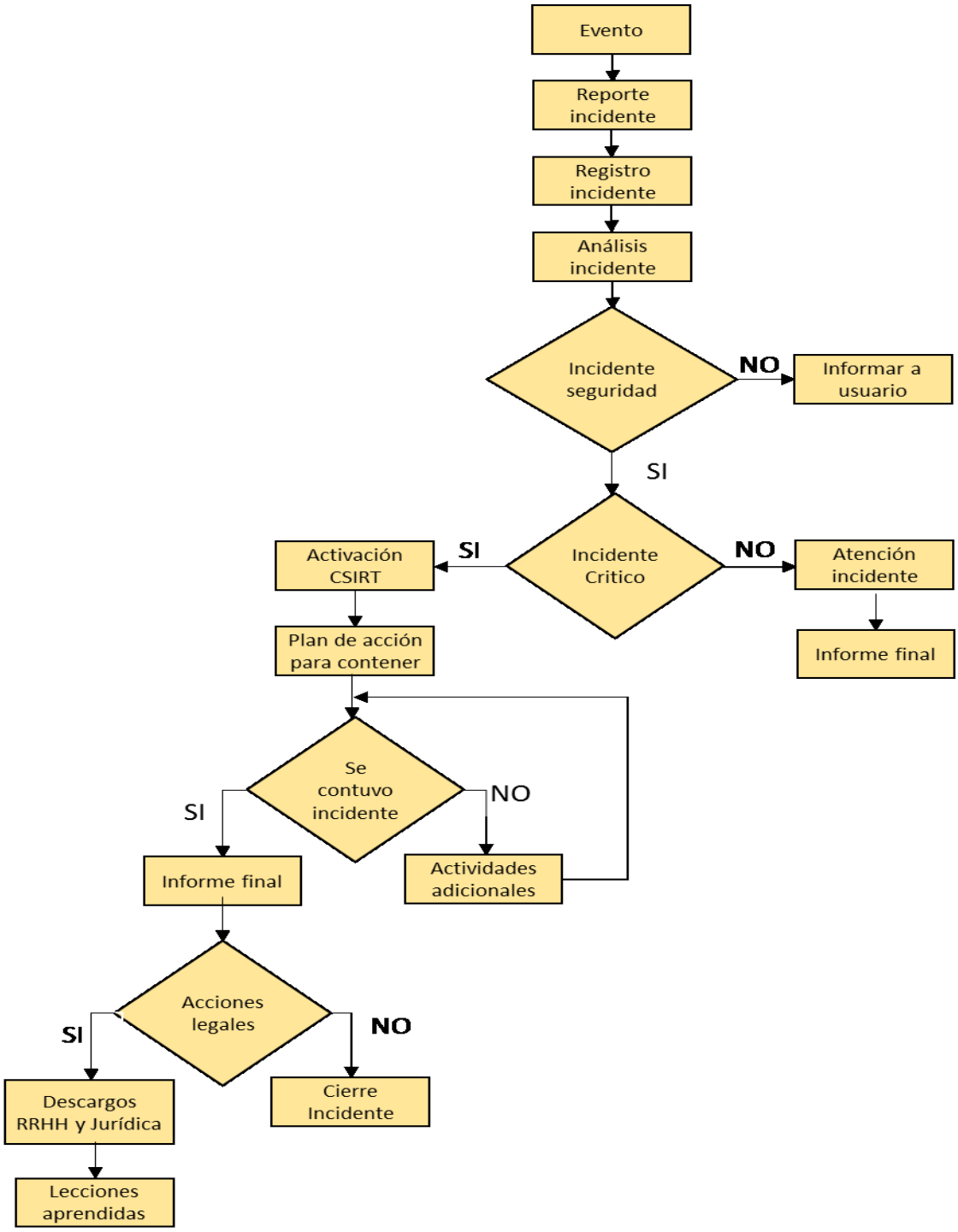
Así las cosas, cada una de la etapas que se han surtido para el esquematizar este modelo, está sujeto a acciones de mejora para fortalecer la gestión de la seguridad de la información frente a los tendientes cambios y la evolución misma de la tecnología y la seguridad, a tal punto que hoy en día ya se habla en términos de cyberataque, cyberseguridad y cyberdefensa, que hace referencia a la protección de las infraestructura critica de una nación.

7.2. FLUJOGRAMA DEL MODELO

Ya se ha analizado el esquema del modelo de gestión de incidentes de seguridad en cada una de las etapas, ahora es tiempo para analizar el flujograma del modelo cuando se presenta un incidente de seguridad.

En la siguiente ilustración que se muestra como fluye el incidente en cada uno de las etapas del modelo, desde que se presenta el evento, se detecta, se contiene, se resuelve hasta el momento que es dado por cerrado y se registran las lecciones aprendidas.

Ilustración 2.Flujograma del modelo de gestión



Fuente: elaboración propia

8. FORTALECIMIENTO DE LAS ÁREAS DE TI

Las áreas de Tecnología de la Información dentro de las organizaciones son vistas como un área operativa más, es decir, el área que atiende requerimientos y solicitudes de los usuarios relacionados con temas técnicos, como por ejemplo que el computador no enciende, o que no ingresa a la red, entre otros.

Sin embargo, de acuerdo con las buenas prácticas para la gestión de TI como ITIL, COBIT, las Normas ISO2700x, es imprescindible que la persección hacia las áreas de TI cambie, es decir, que se hagan más visibles a la organización o empresa, y para ello deben hacer parte de la estrategia de la organización, desde donde pueden definir políticas y normativas que propendan por la prestación de los servicios tecnológicos dentro del correcto funcionamiento.

ITIL es un estándar mundial que ha sido credo pensando en la gestión de los servicios informáticos y más aún cuando hoy en día la tendencia es a hacer uso de la tecnología en la gran mayoría de las Empresas.

Por su parte COBIT ha sido diseño por ISACA en colaboración con expertos en los temas de gobierno de la tecnología de la información (Gobierno TI) para una dirección eficiente de las áreas de tecnología de la información en las organizaciones, el cual ayuda a definir políticas para la transformación e innovación de las TI en las Empresas.

Una de las políticas que debe definir el área de TI es la de gestión de seguridad de la información y dentro de ella debe tener en cuenta la gestión de los incidentes de seguridad de las información.

Con la aplicación de este modelo de gestión que se ha planteado durante el desarrollo de este documento, las áreas de TI pueden fortalecer sus acuerdos y relaciones con otras áreas de la empresa que le permitan identificar y gestionar un incidente de seguridad de la información dentro de unos parámetros que le permitan recuperar de un incidente sin provocar mayores traumatismos a la operación de la organización.

8.1. ACUERDOS OPERACIONALES DE TI

La gestión de incidente de seguridad de la información dentro de la Empresa requiere de la intervención responsable de líneas que están dentro de la estructura organizacional. Por lo anterior y teniendo en cuenta la función que desempeñan dentro de la organización estas áreas son:

- *Coordinación de Seguridad de la Información*: área que propende por el monitoreo de la operación, define controles sobre los activos de información y reciben notificaciones de incidentes.

Sin embargo, es importante dejar claro que si ésta área no está definida dentro del organigrama de la Empresa si debe tener definido el profesional que dentro del área de TI tiene la responsabilidad de gestionar todo lo necesario con estos temas y velar por el cumplimiento de los lineamientos y políticas de que defina para proteger la información o su infraestructura.

- *Mesa de Servicio:* o Service Desk como se conoce en algunas organizaciones, debe ser el único punto de contacto (SPOC) entre los usuarios y las áreas de tecnología. Ayudando a los usuarios a hacer el mejor uso de la tecnología informática, suministrándoles asistencia técnica y funcional para sus consultas, requerimientos o problemas.

  En este punto las mejores prácticas como ITIL, COBIT, recomiendan que solo debe existir un único punto de contacto para todo tipo de incidentes donde los usuarios puedan reportar cualquier anomalía detectada o servicio requerido.

  De la capacitación que tenga los profesionales o encargados de la mesa ayuda depende que la identificación de los incidentes operacionales o de seguridad de la información se gestione de forma correcta. De allí la importancia que esta sea una de las áreas que este en permanente sensibilización de las definiciones todas por el responsable de la seguridad dela información.

- *Tecnología*: a través de esta área se realiza la operación de los servicios tecnológicos internos y externos prestados por la Empresa, teniendo en cuenta que en esta área se tiene el dominio y control sobre las telecomunicaciones, la administración de los datos y el soporte técnico a la infraestructura TI de la organización.

En la siguiente tabla se hace una breve descripción de cuales sería las tareas de cada una de estas áreas antes durante y después de presentado un incidente de seguridad de la información dentro de la Empresa.

Tabla 7. Tabla de Acuerdos Operacionales

Área	Etapa	Tarea	Escalamiento
Tecnología	Antes	Análisis y cierre de vulnerabilidades	Seguridad de la información
	Durante	Reportar el incidente y evaluar los daños o efectos causados por el incidente de seguridad	Mesa de Servicio y Seguridad de la información

Área	Etapa	Tarea	Escalamiento
	Después	Ejecutar los planes de acción derivados del análisis de causa raíz del incidente de seguridad y los generados por la Coordinación de Seguridad de la información	Seguridad de la información y CSIRT
Canales	Antes	Definir y preparar los canales a través de los cuales se harán los reportes de seguridad	Tecnología, Mesa de Servicio y Seguridad de la información
	Durante	Reportar el incidente y mantener canal de difusión del incidente de ser necesario	Mesa de Servicio y Seguridad de la información
	Después	Evaluar disponibilidad de canales	Tecnología
Mesa de Servicio	Antes	Evaluar solicitudes reiterativas sobre activos de información	Tecnología
	Durante	Registrar y evaluar los incidentes reportados por los usuarios o líneas de servicios. Aquellos que se identifiquen de seguridad de la información reportar a	Seguridad de la información y CSIRT
	Después	Seguimiento y cierre de los reportes abiertos por los usuarios	Usuarios y Tecnología
Seguridad de la información	Antes	Definir políticas para administración y manejo	Alta Dirección, Tecnología, Usuarios

Área	Etapa	Tarea	Escalamiento
		de incidentes de seguridad	
	Durante	Evaluar el incidente reportado por la mesa de servicio y si es el caso informar	CSIRT y Alta Dirección
	Después	Generar planes de acción y seguimiento de implementación de los mismos	Tecnología

Un indicador que permite medir el desempeño de las áreas de TI frente a la seguridad de la información, es precisamente a través del número de incidentes reportados y cerrados en un periodo de tiempo antes y después de implementado el modelo de gestión de incidentes de seguridad de la información

8.2. SOCIALIZACIÓN Y FORMACIÓN DEL RECURSO HUMANO

Cuando se habla seguridad de la información, se acostumbra a pensar o a mirar la parte de infraestructura, lo que comúnmente o popularmente se conoce como los fierros, pero es importante tener en cuenta a las personas o los usuarios como uno de los frentes que se deben trabajar y fortalecer si se quiere hablar de un sistema de gestión de seguridad de la información.

Una de las formas de fortalecer el área de TI es socializar e involucrar a los usuarios en los proyectos que se adelantan a nivel de tecnología, con el fin que los funcionarios de la empresa puedan participar en su diseño, ejecución e implementación, así mismo, deben ser capacitados en el uso y sostenibilidad de esos proyectos, es lo que en estrategia de TI se denomina Uso y Apropiación de la Tecnología.

Para el ejercicio del modelo de gestión de incidentes de seguridad de la información en las pequeñas y medianas empresas “PYMES” se realizó una primera encuesta que permite dilucidar el poco entendimiento que los usuarios y personal de empresa tenían con respecto a los temas de seguridad de la información.

En las ilustraciones 1 y 2 de este documento como resultados de la encuesta aplicada se observa que son pocos los usuarios que tiene algún grado de apropiación en los temas de seguridad e incidentes de la información

Ilustración 3. Resultados encuesta

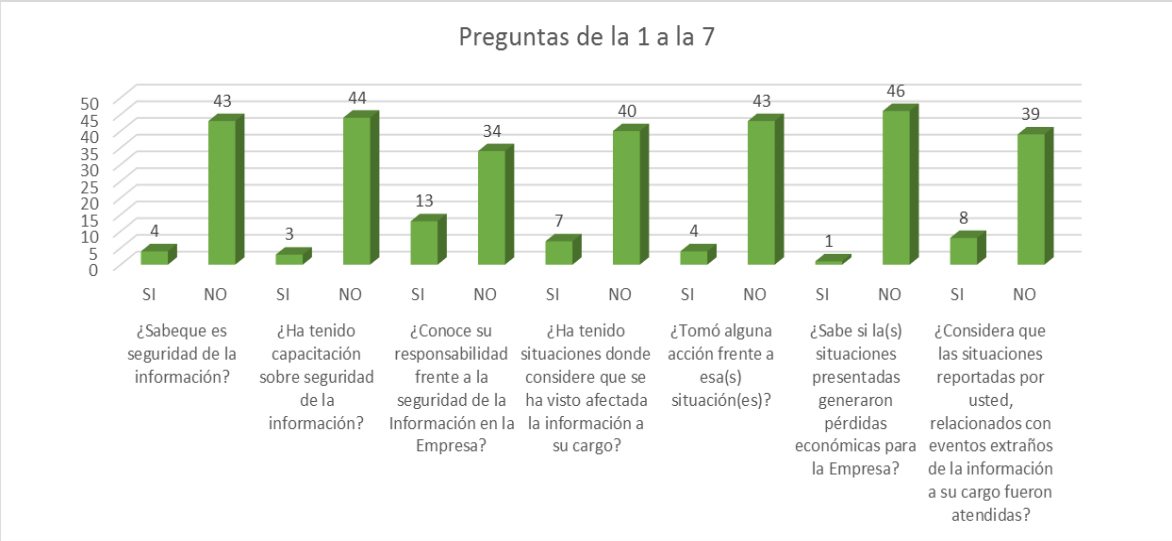
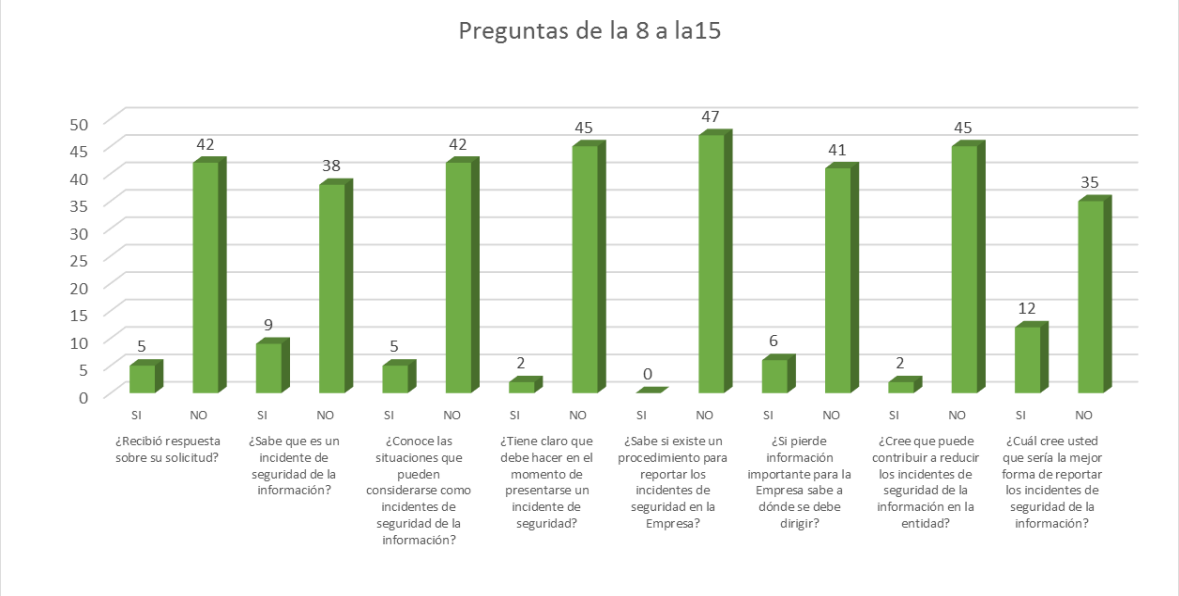
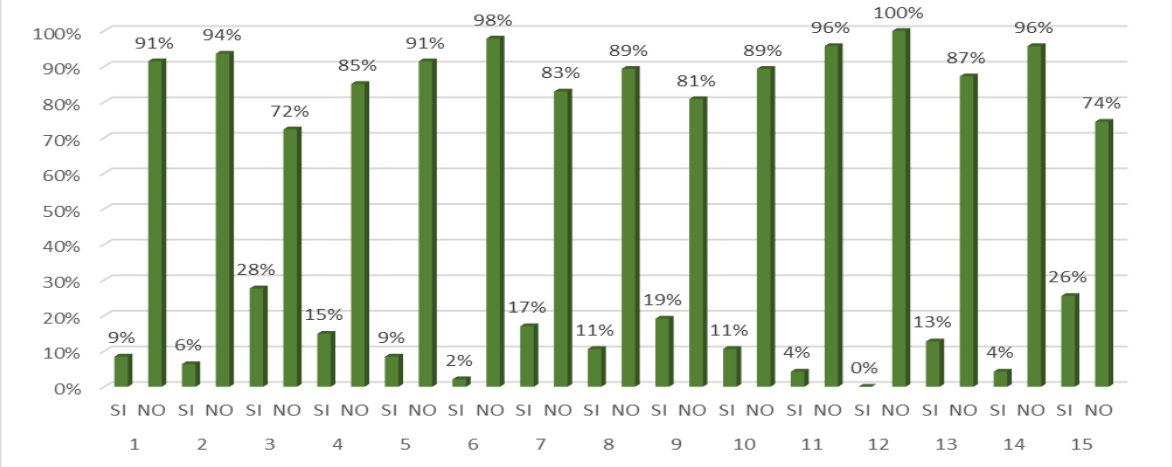


Ilustración 4. Continuación de Resultados de Encuesta.



En la siguiente ilustración se puede evidenciar el grado de desconocimiento por parte de los usuarios o colaboradores de la Empresa frente a los temas de seguridad de la información y sobre todo el desconocimiento de los pasos a seguir al momento de presentarse un hecho que afecte la normal operación de la organización.

Ilustración 5. Resultado de respuesta por porcentaje de participantes



Teniendo en cuenta los resultados que anteceden, se planteó una socialización del proyecto y plan de formación para todos los usuarios de la Empresa.

Este plan de formación está definido por los siguientes temas y la población objetivo de la Empresa que se ilustra a continuación.

Ilustración 6. Temas plan de formación

Versión 0	Gestión de Incidentes de Seguridad de la Información											
Prácticas Clave de Gestión / Funciones/Áreas	Gerente	Suberente de Operaciones	Dueño Procesos de Negocio	área de Buen Gobierno, Riesgos y Auditoría (Si esxiste)	Coordinador de Seguridad de la Información	CERT	Área de Recursos Humanos	Área Jurídica (si existiece)	Dirección de Información y Tecnología o quien haga sus veces	Área de Infraestructura	Mesa de Servicio	Usuarios / Clientes
Principios de Seguridad de la Información	x	x	x	x	x		x	x	x	x	x	x
Incidentes de seguridad y clases de incidentes	x	x	x	x	x	x	x	x	x	x	x	x
Detección y reporte de incientes	x	x	x	x	x	x	x	x	x	x	x	x
Validación de Incidente / Eventos					x	x			x	x	x	
Análisis y Reolección de información						x		x		x		

Una vez se llevó a cabo el plan de formación se realizó una nueva medición a los usuarios de la Empresa para determinar cuántos han adquirido los conceptos de seguridad de la información y primordialmente como identificar y reportar un incidente de seguridad de la información.

En este sentido los resultados, de la segunda encuesta fueron los siguientes:

Ilustración 7. Resultado segunda encuesta

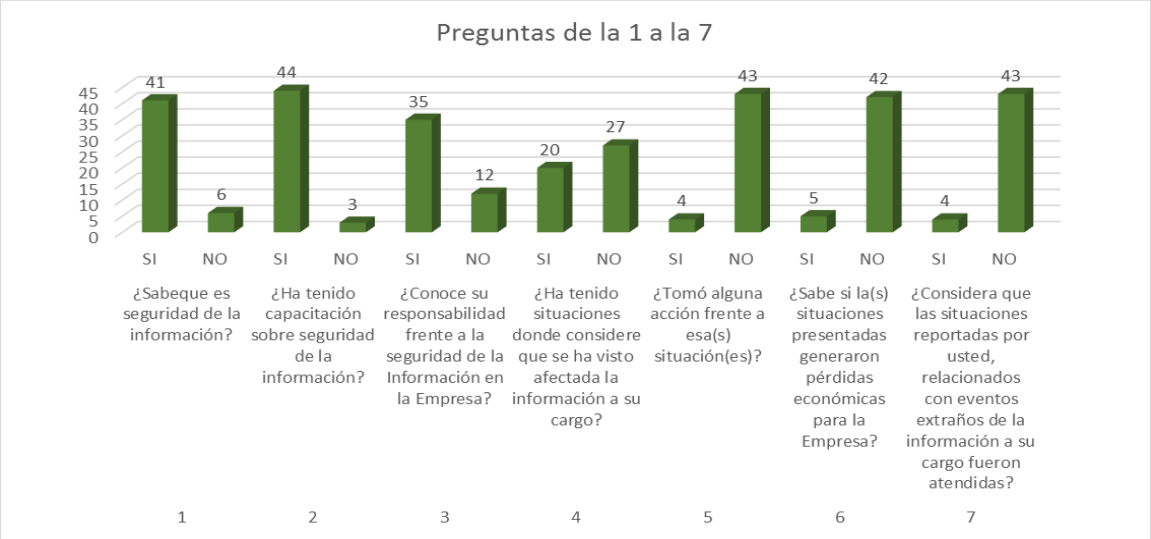
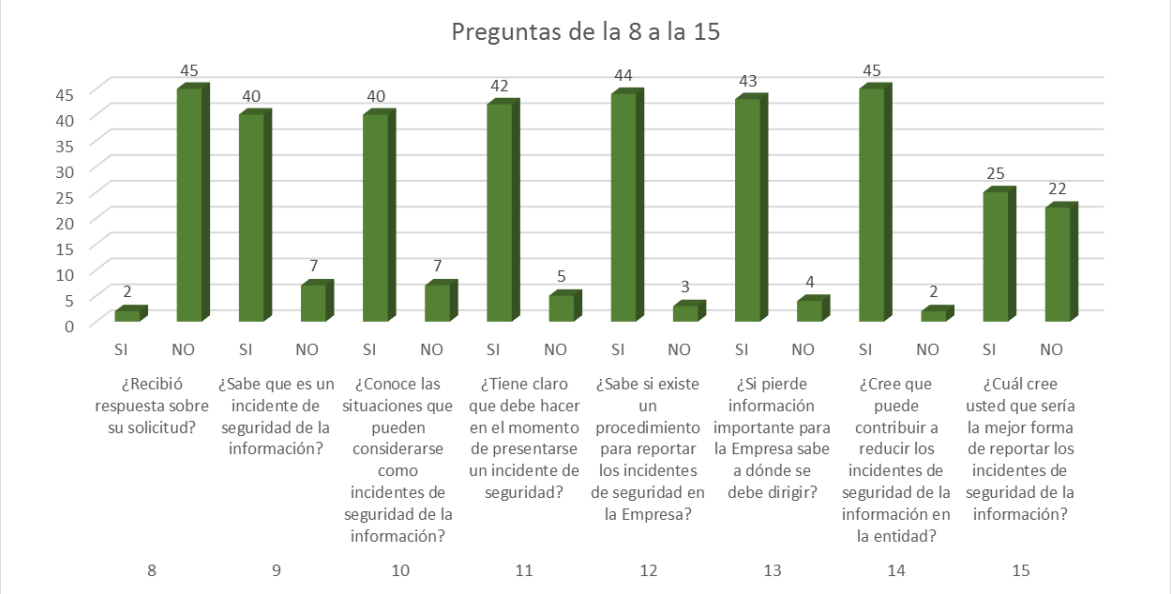
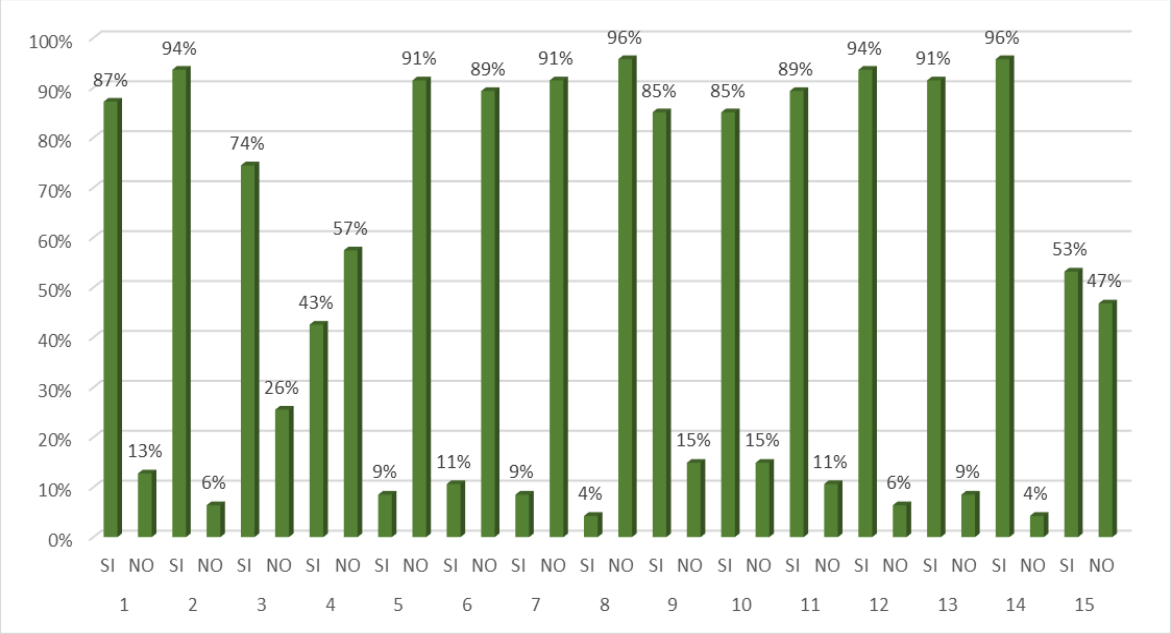


Ilustración 8. Continuación resultado encuesta



En la ilustración que se muestra a continuación, se puede observar el grado de sensibilización adoptado por el personal que ha sido capacitado durante el diseño de este modelo y el impacto positivo que trae para la empresa, si se tiene en cuenta que los usuarios ya identifican que es un incidentes de seguridad de la información y como deben actuar ante la detección de un evento no controlado.

Ilustración 9. Resultado de respuesta por porcentaje de participantes



9. CONCLUSIONES

- La seguridad de la información a nivel mundial y en Colombia es un tema que viene tomando relevancia para las empresas, sean estas pequeñas, medianas o grandes, lo importante es que se está tomando conciencia del porque se debe implementar la seguridad de la información.

- Un sistemas de gestión de seguridad de la información que no define un modelo de gestión de incidentes, es un sistemas que desde su creación tiene vacíos o debilidades que tarde o temprano tendrán su impacto para la empresa, como por ejemplo pérdida de información crítica, pérdida de confianza de los grupos de interés, oportunidades competitivas por fuga de información industrial o comercial, entre otras.

- Los modelos de gestión de incidentes de seguridad permiten a las empresas prepararse para detectar y corregir debilidades o vulnerabilidades para que éstas no se vuelvan a presentar en un futuro o si se presentan que su impacto tenga la menor afectación posible.

- Los usuarios deben ser una de las partes más importantes de la organización para evitar que se conviertan en uno de los eslabones débiles dentro del sistema de seguridad deben ser capacitados y concientizados de su responsabilidad frente al manejo de la información de la Empresa y de los recursos tecnológicos que la misma dispone para el cumplimiento de sus labores

- La literatura consultada en su mayoría está basada en las mejores prácticas de seguridad información que a nivel nacional o internacional se conoce, de allí que los términos se puedan llamar de varias formas, sin embargo, su contexto o definición es la misma en todos los documentos.

BIBLIOGRAFÍA

- Agencia de Gobierno Electrónico y Sociedad de la Información (agesic), Política de Gestión de Incidentes de Seguridad de la Información ver. 1.1. {en línea}. {Octubre de 2015} Disponible en http://www.agesic.gub.uy/innovaportal/v/1217/1/agesic/documentos.html

- Guía Técnica Colombiana GTC-ISO/IEC 27035 (2012), Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información.

- America Latina y Caribe, Proyecto Amparo, Manual: Gestión de Incidentes de Seguridad Informática versión 1.1., {en línea}. (Octubre de 2015), Disponible en http://www.proyectoamparo.net/files/manual_seguridad/manual_sp.pdf

- Ardita Julio César, CIGRAS 2013, ISACA, Manejo de Incidentes de Seguridad Dentro de la Organización, {en línea}. {Octubre de 2015}. Disponible en http://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras%202013%20-%20manejo%20de%20incidentes%20de%20seguridad%20en%20la%20organizacin%20julio%20ardita.pdf

- Reyes Muñoz, Juan Carlos (2006), Modelos para la Creación de un Grupo de Respuesta a Incidentes de Seguridad Informática Gubernamental Central en América Latina, {en línea}. {Octubre de 2015} Disponible en http://www.criptored.upm.es/guiateoria/gt_m578a.htm

- Centro de Investigaciones Científicas y Tecnológicas de Tecnar, CITAR. Estructura para la Realización de Monografía, {en línea}. {Octubre de 2015}. Disponible en http://www.tecnar.edu.co/sites/default/files/pdfs/Estructura%20Para%20Realizaci%C3%B3n%20De%20Monograf%C3%ADa.pdf

- Ramos Escobar, Carlos Eduardo. Desarrollo de la Normativa para la Gestión de Incidentes de Seguridad de la Información en el Departamento de Gestión Tecnológica de la Universidad Santiago de Cali. Santiago de Cali, 2013, Universidad Autónoma de Occidente Faculta de Ingenierías.

- Alberts, Chris. Dorofee, Audrey. Killcrece Georgia, Ruefle Robin, Zajicek Mark (2004), Defining Incident Management Processes for CSIRTs: A Work in Progress, {en línea}. {Octubre de 2015} Disponible en http://www.sei.cmu.edu/reports/04tr015.pdf

- Casanoba Romeo, Carlos María, Poder informático y Seguridad jurídica, Editorial Fundesco 1987

ANEXOS

ANEXO 1. FORMATO DE REGISTRO DE INCIDENTES

FORMATO REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			**Versión: x.x Fecha: xx/xx/xxxx Responsable:**
INFORMACIÓN GENERAL DEL REPORTE			
Fecha y hora del reporte:			
Nombre de quien reporta:			
Cargo:		**Dependencia y Extensión:**	
Sede:		**E-mail**	

INFORMACIÓN GENERAL DEL INCIDENTE	
Fecha y hora del incidente:	
Lugar o sede del incidente:	
No. de Solicitud:	
Descripción del Incidente	

RECURSO INFORMÁTICO AFECTADO
Nombre del Recurso:
Ubicación Física:
Información que contiene:
Fecha de la última copia de seguridad:

ANEXO 2. FORMATO DE VALORACIÓN DE INCIDENTES

FORMATO **VALORACIÓN DE INCIDENTES** **DE SEGURIDAD DE LA INFORMACIÓN**	**Versión: x.x.** **Fecha: xx/xx/xxxx** **Responsable:**
INFORMACIÓN GENERAL DEL INCIDENTE	
Fecha y hora del reporte:	
No. de solicitud:	
Descripción del Incidente	

INFORMACIÓN DE VALORACIÓN DE INCIDENTE	
Fecha y hora de valoración:	
Nombre de quien valora:	
Valoración del incidente:	
Observaciones de la valoración:	

ANEXO 3. FORMATO DE RESULTADO DE GESTIÓN DEL INCIDENTE

REPORTE DEL RESULTADO DE LA INVESTIGACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	**Versión: x.x** **Fecha: xx/xx/xxxx** **Responsable:**
Objetivo:	
Alcance:	El resultado reflejado en este documento solo debe ser conocido por las personas autorizadas

INFORMACIÓN GENERAL DEL INCIDENTE	
Fecha y hora del reporte:	
No. de solicitud:	
Descripción del Incidente	

INFORMACIÓN DE VALORACIÓN DE INCIDENTE	
Fecha y hora de valoración:	
Nombre de quien valora:	
Valoración del incidente:	

INFORMACIÓN EQUIPO INVESTIGADOR		
NOMBRE	**CARGO**	**E-Mail**

CAUSAS

PASOS EJECUTADOS EN LA INVESTIGACIÓN

OPORTUNIDADES DE MEJORA

No.	DESCRIPCIÓN	RESPOSABLE	FECHA DE FINALIZACIÓN

CONCLUSIONES

ANEXOS