DISEÑO DE UN MODELO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE UN SGSI BASADO EN ISO 27001 DENTRO DE UNA MESA DE SERVICIOS DE TI

TRABAJO DE GRADO

PARTICIPANTE

RICARDO FABIO COSSIO LUGO

CÓDIGO 1522010293

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

DISEÑO DE UN MODELO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE UN SGSI BASADO EN ISO 27001 DENTRO DE UNA MESA DE SERVICIOS DE TI

TRABAJO DE GRADO

PARTICIPANTE

RICARDO FABIO COSSIO LUGO

CÓDIGO 1522010293

Asesor(es)

ING. ALEJANDRO CASTILBLANCO CARO

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
2017

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

_____

_____

Firmas de los jurados

Bogotá, Septiembre 18 de 2017

CONTENIDO

1. INTRODUCCIÓN

Este documento presenta el trabajo de grado que tiene como objeto de estudio el análisis y diseño de un modelo de gestión para contrarrestar la insuficiencia o incapacidad que tienen las mesas de servicios de TI de las organizaciones para gestionar adecuadamente los eventos, vulnerabilidades e incidentes de seguridad de forma tal que logre una adecuada gestión de los mismos y garantice el cumplimiento de los requisitos de prácticas de seguridad específicas como es ISO 27001:2013.

Presenta el diseño de los procesos de gestión de eventos de seguridad y como estos a través de la automatización y de las funciones de monitoreo pueden ser integrado en el proceso de gestión de incidentes de una mesa de servicios, este diseño abordó también la integración del manejo propio de las vulnerabilidades y el tipo de solicitudes con que debe ser reportado y registrado en la mesa de servicios

La estructura del documento parte en primera instancia de la identificación de los requisitos para la gestión de incidentes de seguridad según el anexo A.16 de ISO 27001 que son de obligatorio cumplimiento para los sistemas certificados y que son los llevados al modelo diseñado para su posterior tratamiento y gestión, otro de los métodos utilizados es el del manejo de las fases de gestión de incidentes presentados en la norma especializada ISO 27035 que básicamente están orientadas a la detección, reporte, valoración, decisión, respuesta y lecciones aprendidas. Las siguientes etapas de la metodología son las del diseño de los criterios y del proceso como tal de la gestión de incidentes de seguridad embebido en una mesa de servicios de TI.

2. RESUMEN EJECUTIVO

Este proyecto de grado está orientado a crear un modelo de gestión para tratar el problema de la insuficiencia o incapacidad de las mesas de servicios de TI de las organizaciones para gestionar adecuadamente los eventos, vulnerabilidades e incidentes de seguridad de la información, de forma tal que logre una adecuada gestión de los mismos y garantice cumplimiento del total de los requisitos exigidos por el estándar ISO 27001 2013 en lo relacionado con la gestión de los incidentes.

Como motivación se tiene la necesidad de optimizar los recursos y hacer más funcional la mesa de servicios de TI logrando que sea utilizada por los sistemas de gestión de seguridad de la información para proporcionar un manejo oportuno y eficaz de los eventos, incidentes y vulnerabilidades de seguridad, cumpliendo a cabalidad con los requisitos del sistema en esta materia. Se contempla de igual forma el diseño y construcción del flujo de trabajo integrado para el registro, análisis, evaluación, respuesta y aprendizaje.

En este proyecto se trazó como objetivos, el diseño de los procesos de gestión de eventos de seguridad y como este a través de la automatización y de las funciones de monitoreo puede ser integrado en el proceso de gestión de incidentes de una mesa de servicios, este diseño abordó también la integración del manejo propio de las vulnerabilidades y el tipo de solicitudes con que debe ser reportado y registrado en la mesa de servicios.

Un segundo objetivo orientado a la creación y definición de los criterios de identificación, evaluación y criticidad de los incidentes de seguridad de la información, incluyendo la descripción de las condiciones requeridas para conocer si un evento puede convertirse en un incidente de seguridad y el tipo de acción que se debe tomar para atenderlos según su nivel de criticidad. Se incluye también una amplia lista de posibles incidentes para poder clasificarlos por categorías con base en sus características y causas que los ocasionan.

El método utilizado para desarrollar el proyecto parte en primera instancia de la identificación de los requisitos para la gestión de incidentes de seguridad según el anexo A.16 de ISO 27001 que son de obligatorio cumplimiento para los sistemas certificados y que son los que van a ser llevados al modelo a diseñar para su posterior tratamiento y gestión, otro de los métodos utilizados es el del manejo de las fases de gestión de incidentes presentados en la norma especializada ISO 27035 que básicamente están orientadas a la detección, reporte, valoración, decisión, respuesta y lecciones aprendidas. Las siguientes etapas de la metodología son las del diseño de los criterios y del proceso como tal de la gestión de incidentes de seguridad embebido en una mesa de servicios de TI.

Un punto importante que trata este trabajo y es clave para poder hacer una adecuada identificación y posterior gestión de los incidentes de seguridad es el nivel de atención o soporte de la mesa de servicios en donde se deben clasificar los incidentes como incidentes de seguridad, recordando que el propósito principal de la gestión de incidentes según ITIL V3 es el de solucionar la falla en el menor tiempo posible, aspecto que es utilizado en el modelo de gestión de incidentes de seguridad como punto clave para saber que sucedió y si la falla presentada es ocasionada por un tema pertinente a la seguridad de la información.

Unos de los aspectos claves que tiene el modelo de gestión de incidentes de seguridad de la información es la inclusión de actividades posteriores a la solución de la falla como es el análisis de la situación presentada, la necesidad de continuar con la investigación para identificar la causa raíz del problema y la determinación de lecciones aprendidas para lograr conocer a detalle que debe ser mejorado para evitar la recurrencia de los incidentes en el futuro.

El alcance del proyecto está orientado al análisis de prácticas de gestión de incidentes de TI y de seguridad de la información extrayendo los puntos más relevantes para integrarlos y posteriormente crear un modelo de gestión de incidentes de seguridad de la información

embebido dentro del proceso de gestión de eventos e incidentes de las mesas de servicios de TI. No considera la implementación del modelo ni la aplicación sobre alguna organización en particular y no pretende adoptar toda la práctica sino únicamente los aspectos relacionados directamente con el propósito del proyecto.

El modelo de gestión de incidentes de seguridad de la información está orientado principalmente para las empresas que cuentan con dos aspectos fundamentales, el primero es el de contar con una mesa de servicios (service desk) para la gestión de incidentes y requerimientos tecnológicos basado en modelos de gestión de servicios de tecnología, un segundo aspecto es el de haber adoptado e implementado un sistema de gestión de seguridad de la información y que se cuente con una certificación que exija el cabal cumplimiento de los requisitos de seguridad de la norma ISO 27001

Este modelo pretende establecer una línea base para la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información útil para cualquier tipo de empresa que tenga implementado y en funcionamiento tanto la mesa de servicios como el sistema de gestión de seguridad de la información certificado en ISO 27001, sin embargo antes de ser aplicado se debe revisar y personalizar de acuerdo a, el apetito o tolerancia al riesgo que tenga la compañía, la criticidad de las operaciones y de los servicios prestados, los acuerdos de niveles de servicios establecidos con los procesos internos y con los clientes, el tipo de sector al que pertenece la empresa, el cumplimiento de requisitos legales, contractuales y regulatorios, el tipo y proporción de la población que puede verse afectada ante cualquier indisponibilidad de las operaciones y los servicios prestados por la compañía.

3. JUSTIFICACIÓN

El diseño de un proceso de gestión de incidentes de seguridad de la información basado en buenas prácticas de gestión de seguridad y embebido dentro de los servicios de gestión de eventos e incidentes de una mesa de servicios de TI es importante para atender adecuadamente las siguientes necesidades y beneficios comunes en las organizaciones:

- Identificación de la mayoría de eventos e incidentes concernientes a la seguridad de la información.
- Disminución de incidentes de seguridad de la información presentados sobre los sistemas informáticos por la corrección oportuna de fallas evitando su reincidencia.
- Mayor oportunidad en la identificación, atención y respuesta de los incidentes de seguridad de la información.
- Centralización y optimización de recursos para la gestión de todos los eventos e incidentes que se presentan en la organización.
- Cumplimiento de los requisitos de seguridad de estándares ISO 27001 para aquellas entidades certificadas en lo relacionado con la gestión de incidentes de seguridad de la información.
- Mejor relación colaborativa entre los equipos de soporte tecnológico y las áreas de seguridad informática y de la información
- Registro centralizado para la documentación de las investigaciones de seguridad y las lecciones aprendidas para evitar la recurrencia de los incidentes
- Disposición y uso de una de las fuentes de información más importante para la identificación y el análisis de los riesgos de seguridad de la información como lo es la gestión de incidentes de seguridad

- Servir como un recurso confiable para analizar la efectividad de los controles de seguridad de un sistema de gestión de seguridad de la información basado en ISO 27001.

Los indicadores que son afectados positivamente después de implementar el modelo propuesto de gestión de incidentes de seguridad de la información son:

- Porcentaje de reducción de la reincidencia de incidentes que afecten la confidencialidad, integridad y disponibilidad de la información.
- Reducción del número de incidentes de seguridad reportados, después de seis meses de implementación del modelo

Este modelo es necesario y útil para mejorar la capacidad de las mesas de servicios ya existentes en las organizaciones en lo pertinente a la atención adecuada de los eventos e incidentes de seguridad de la información y que a su vez cumpla con la totalidad de los requisitos exigidos por el estándar ISO 27001 2013 en materia de gestión de incidentes. Este modelo permite también la optimización de los recursos de gestión ya existentes e implementados para centralizar y concentrar en un único recurso la gestión de todos los eventos e incidentes ocurrido en las organizaciones.

4. MARCO TEÓRICO Y REFERENTES

4.1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Uno de los aspectos más importantes de un Sistema de Gestión de Seguridad de la Información basado en ISO 27001 es la gestión de los incidentes de seguridad, el cual busca que se le dé un manejo adecuado, oportuno y efectivo a los eventos, incidentes y vulnerabilidades que puedan llegan a comprometer la información de las organizaciones.

Cuando las amenazas explotan vulnerabilidades y por consiguiente afectan a los activos de información se presentan incidentes en la organización que pueden incluso comprometer sus operaciones, de allí la importancia de gestionar adecuada y oportunamente los eventos, incidentes y vulnerabilidad de la seguridad de la información.

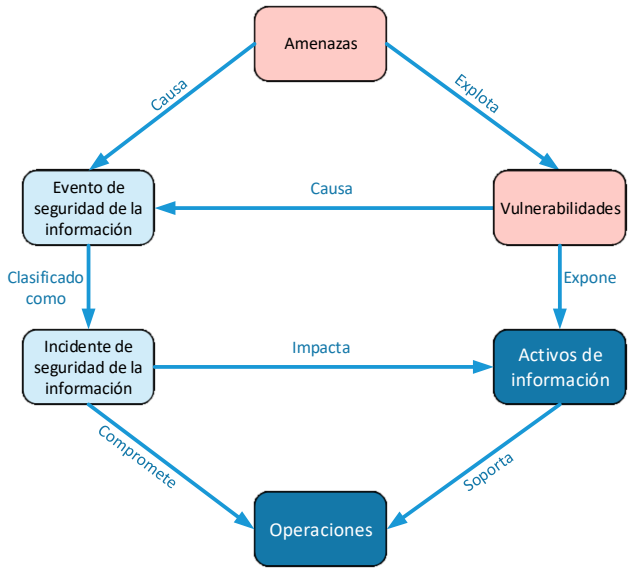


Figura 1. Relación de objetos en la gestión de incidentes de seguridad. Adaptado de International Organization for Standardization ISO, Information technology Security techniques, Information security incident management, Part 1: Principles of incident management, 32, p. 11. Geneva, Switzerland, 2016

Para entender y poder diferenciar cada uno de estos términos se presentan las definiciones de la norma de generalidades y vocabulario ISO/IEC 27000:2016 que es la versión más actualiza que existe hasta la fecha

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias, puede ocurrir una o varias veces y puede tener varias causas, puede ser algo que no ha sucedido, y algunas veces se puede referir a "incidente" o "accidente". ISO 27000:2016 2.25

Evento de seguridad de la información: Es una ocurrencia identificada de un estado en un sistema, servicio o red que indica una posible brecha de seguridad de la información, de las políticas, una falla de los controles o una situación previa desconocida que puede ser relevante a la seguridad ISO 27000:2016 2.35

Incidente de seguridad de la información: Uno o varios eventos de seguridad de la información no deseados o inesperados que tiene una probabilidad significativa de comprometer las operaciones del negocio y por ende amenazar la seguridad de la información ISO 27000:2016 2.36

Gestión de los incidentes de seguridad de la información: Proceso para detectar, reportar, valorar, responder a, tratar con, y aprender de los incidentes de seguridad de la información ISO 27000:2016 2.37

Amenaza: Causa potencial de un incidente no deseado que puede resultar en daño en los sistemas o en las organizaciones ISO 27000:2016 2.57

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas ISO 27000:2016 2.89

Equipo de respuesta a incidentes "IRT": Equipo de personas de las organizaciones confiables y con habilidades apropiadas para manejar los incidentes durante su ciclo de vida. CERT (Equipo de respuesta a emergencias en computadores) y CSIRT (Equipo de respuesta a incidentes de seguridad en computadores) son términos comunes usados para IRT. ISO 27035-1:2016 3.2

Punto de Contacto PoC: Función o role organizacional definido que sirve como coordinación o punto focal de información en todo lo concerniente a las actividades de gestión de incidentes. ISO 27035-1:2016 3.8

La gestión de incidentes de seguridad dentro de la familia de estándares ISO 27000 es encontrado en las normas ISO 27002:2013 Código de prácticas para controles de seguridad de la información, ISO 27001:2013 Anexo A.16 Gestión de incidentes de seguridad de la información, ISO/IEC 27035:2016 Gestión de incidentes de seguridad de la información - Parte 1, Principio de la gestión de incidentes y Parte 2, Guía para planear y preparar la respuesta a incidentes

Un sistema de gestión de seguridad de la información certificado ISO 27001 debe contar con controles para la gestión de incidentes, los que son comúnmente encontrados como aplicables en las declaraciones de aplicabilidad de los sistemas de gestión

Estos controles de seguridad son los requisitos propios de seguridad que se deben considerar y adaptar en los modelos de mesas de servicios de las organizaciones cuando

estos últimos son implementados con prácticas de la gestión de servicios de tecnología como son ITIL dentro de la fase del ciclo de vida de la operación del servicio.

Dentro de estos requisitos del Anexo A 16 de ISO 27001:2013 se encuentran:

- Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta adecuada y oportuna de los incidentes de seguridad de la información
- Reportar oportunamente los eventos de seguridad de la información por los canales dispuestos para tal fin
- Reportar debilidades o vulnerabilidades de seguridad de la información observadas o sospechadas sobre los servicios o sistemas de información de la organización
- Evaluar los eventos y decidir si se van a clasificar como incidentes de seguridad de la información
- Dar respuesta a los incidentes de acuerdo con los procedimientos documentados
- Documentar el conocimiento adquirido al analizar y resolver los incidentes de seguridad para que pueda ser usado para reducir la probabilidad y el impacto de incidentes futuros, “Documentar las lecciones aprendidas”
- Recolectar la evidencia a través de la identificación, recolección, adquisición y preservación de la información que pueda servir como evidencia

En resumen los aspectos indispensables con lo que debe contar las mesas de servicios para gestionar incidentes de seguridad son: La posibilidad de registrar eventos, incidentes y vulnerabilidad de seguridad, los criterios para la atención de los mismos a partir del impacto a las operaciones o el negocio, los criterios para poder determinar cuándo un evento se convierte en incidentes de seguridad, La posibilidad de registrar y

documentar las acciones de contención y tratamiento de incidentes junto con el análisis de la gestión y el registro de las lecciones aprendidas para evitar la recurrencia de dichos incidentes

La gestión de los incidentes de seguridad de la información es un aspecto muy importante dentro de los sistemas de gestión basados en ISO 27001 ya que el comportamiento de estos permite saber que tan probable es la ocurrencia de los mismos y los posibles impactos que estos causarían a la organización, dicho en otras palabras los incidentes de seguridad suministran información confiable y real muy útil para gestionar los riesgos de seguridad de la información, recordando que este estándar precisamente está basado en un modelo de gestión de riesgos.

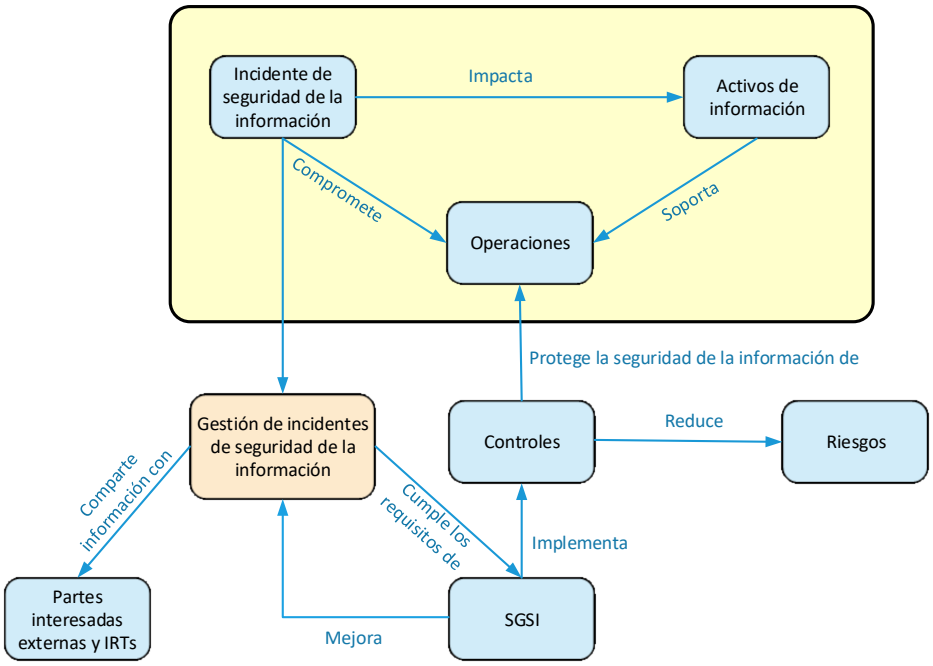


Figura 2. Gestión de incidentes de seguridad en relación con el SGSI y lo controles aplicados. Adaptado de International Organization for Standardization ISO, Information technology Security techniques, Information security incident management, Part 1: Principles of incident management, 32, p. 12. Geneva, Switzerland, 2016

4.2 FASES DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La gestión de incidentes de seguridad de la información consiste de cinco fases según ISO 27035 [1]

1. Planeación y preparación
2. Detección y reporte
3. Valoración y Decisión
4. Respuesta
5. Lecciones aprendidas

Los aspectos más importantes que considera cada fase son:

4.2.1 Planeación y preparación

- Política de gestión de incidentes de seguridad de la información y compromiso de la alta dirección
- Políticas de seguridad de la información incluyendo las de gestión de riesgos
- Plan de gestión de incidentes de seguridad de la información
- Establecimiento del IRT
- Relacionamiento y conexión con organizaciones internas y externas
- Soporte técnico, organizacional, operacional y otros requeridos
- Concienciación y entrenamiento sobre la gestión de incidentes SI
- Pruebas al plan de gestión de incidentes SI

4.2.2 Detección y reporte

- Recolección de información del conocimiento de la situación desde entornos locales, fuente de datos externas y otras entradas
- Monitoreo de los sistemas y las redes
- Detección y notificación de alertas de actividades anómalas, sospechosas o maliciosas
- Colección de los reportes de eventos de seguridad de la información desde los componentes, fabricantes, otros IRTs y los sensores automatizados
- Reportando eventos de seguridad de la información

4.2.3 Valoración y decisión

Valoración de seguridad de la información y determinación sobre los incidentes de seguridad de la información

4.2.4 Respuesta

- Determinar si los incidentes SI están bajo el control de una investigación
- Contener y erradicar los incidentes SI
- Recuperarse de los incidentes SI
- Solución y cierre de los incidentes SI

Actividad posterior

- Necesidad por continuar con la investigación en caso de ser requerido

4.2.5 Lecciones aprendidas

- Identificación de lecciones aprendidas
- Identificación y aplicación de mejoras a la seguridad de la información
- Identificación y aplicación de mejoras a la gestión de riesgos SI y de los resultados de las revisiones por la dirección
- Identificación y aplicación de mejoras al plan de gestión de incidentes SI
- Evaluación del desempeño y efectividad del IRT

Algunas actividades pueden ocurrir en múltiples fases del modelo de gestión de incidentes de seguridad de la información, como son:

- La documentación de la evidencia de los eventos e incidentes y de la información clave, acciones correctivas de respuesta dentro del proceso de gestión y de contención de la falla
- Comunicación y coordinación con partes interesadas
- La necesidad de compartir información sobre los incidentes con las partes interesadas, y equipos de respuesta, IRT externos

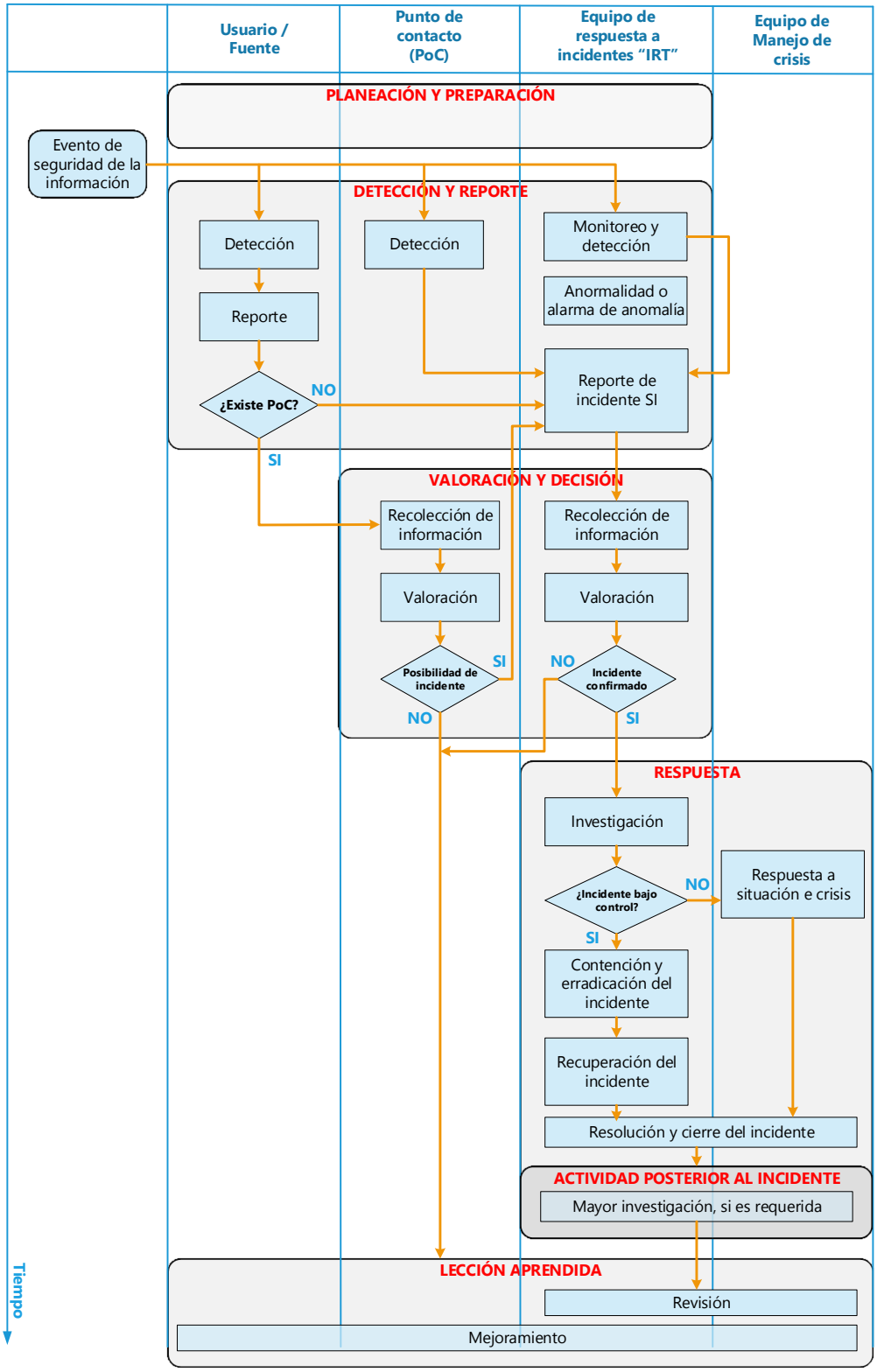
Es importante tener en cuenta que la complejidad del mecanismo utilizado para la gestión de incidentes SI es proporcional a:

- El tamaño, estructura y naturaleza del negocio, de sus activos críticos claves, sus procesos y la necesidad de proteger los datos

- Alcance definido para el SGSI y los límites para la aplicación de la gestión de los incidentes SI
- Los riesgos potenciales ocasionados por los incidentes
- Las metas y estrategias de la organización

A continuación, se presenta el diagrama de flujo de los eventos e incidentes de seguridad dentro del modelo de gestión de ISO 27035

1. International Organization for Standardization ISO, Information technology Security techniques, Information security incident management, Part 1: Principles of incident management, 32, p 17, Geneva, Switzerland, 2016



2. Figura 3. Diagrama de flujo de eventos e incidentes dentro de las fases de gestión de incidentes. Adaptado de International Organization for Standardization ISO, Information technology Security techniques, Information security incident management, Part 1: Principles of incident management, 32, p 17, Geneva, Switzerland, 2016

4.3 GESTIÓN DE EVENTOS E INCIDENTES EN LA FASE DE LA OPERACIÓN DEL SERVICIO

Según ITIL V3 la operación del servicio está a cargo de realizar todas las actividades necesarias para la gestión, prestación y el soporte de los servicios. La operación del servicio es responsable de que se ejecuten los procesos que optimizan los costos y la calidad del servicio en el ciclo de vida de la gestión del servicio, de igual forma contribuye a que el cliente (negocio) logre sus objetivos garantizando el funcionamiento eficaz de los componentes que dan soporte al servicio

4.3.1 Gestión de eventos

En ITIL V3 un evento es un suceso que afecta la gestión de la infraestructura de TI o la provisión de un servicio de TI siendo normalmente notificaciones (alertas) generadas por un servicio de TI, un elemento de la configuración o una herramienta de monitorización. Una vez conocido el estado de la infraestructura se puede identificar la desviación respecto al rendimiento habitual o esperado. Los sistemas de automatización y control son utilizados para este fin.

Un evento se puede definir como cualquier suceso detectable o discernible que tiene importancia para la gestión de infraestructura de TI o para la entrega de un servicio de TI, así como para la evaluación del impacto que podría causar una desviación sobre los servicios.

El objetivo de la gestión de eventos es detectar eventos, analizarlos y determinar la acción de gestión apropiada

La gestión de eventos supervisa todos los eventos presentados en la infraestructura de TI y lo hace a través de procesos automatizados para efectuar el seguimiento y escalamiento ante situaciones imprevistas.

Las actividades más importantes en el proceso de gestión de eventos son: Ocurrencia, Notificación, detección, filtrado, significado (clasificación), correlación, disparador, selección de respuesta, evaluación de acciones y cierre del evento. En la figura 3 se presenta un proceso general de alto nivel para la gestión de eventos de TI

El proceso de gestión de incidencias cubre todo tipo de incidencias, ya sean fallos, preguntas, consultas planteadas por usuarios o personal técnico o bien que sean detectadas automáticamente por herramientas de monitoreo de eventos.

ITIL define una incidencia como una interrupción no planificada o una reducción de calidad de un servicio de TI. El fallo de un elemento de configuración que no haya afectado todavía al servicio también se considera una incidencia.

4.3.2 Gestión de incidentes

Está a cargo de restaurar el fallo del servicio lo antes posible para los clientes, de manera que su impacto sea mínimo, incluye cualquier evento que interrumpa o pueda interrumpir un servicio.

El proceso de gestión consta de: Identificación, registro, categorización, priorización, Diagnóstico inicial, Escalado, Investigación y diagnóstico, resolución, restauración y cierre.

El principal objetivo del proceso de gestión de incidentes es volver a la situación normal lo antes posible y minimizar el impacto sobre los procesos de negocio

El valor de la gestión de incidentes reside en la posibilidad de poder controlar oportunamente los incidentes, significando menor afectación al negocio y una mayor disponibilidad del servicio y la posibilidad de poder identificar mejoras potenciales en los servicios

En la gestión de incidentes se deben considerar los siguientes elementos, los límites de tiempo a través del establecimiento de objetivos en acuerdos de nivel de servicio (OLA) y contratos de soporte; Los modelos de incidencias que indica los pasos necesarios para ejecutar correctamente un proceso, lo que significa que los incidentes estándar se gestionarán de forma correcta y dentro de los tiempos esperados; Incidentes graves que requieren un procedimiento diferente, con plazos más cortos y mayor urgencia.

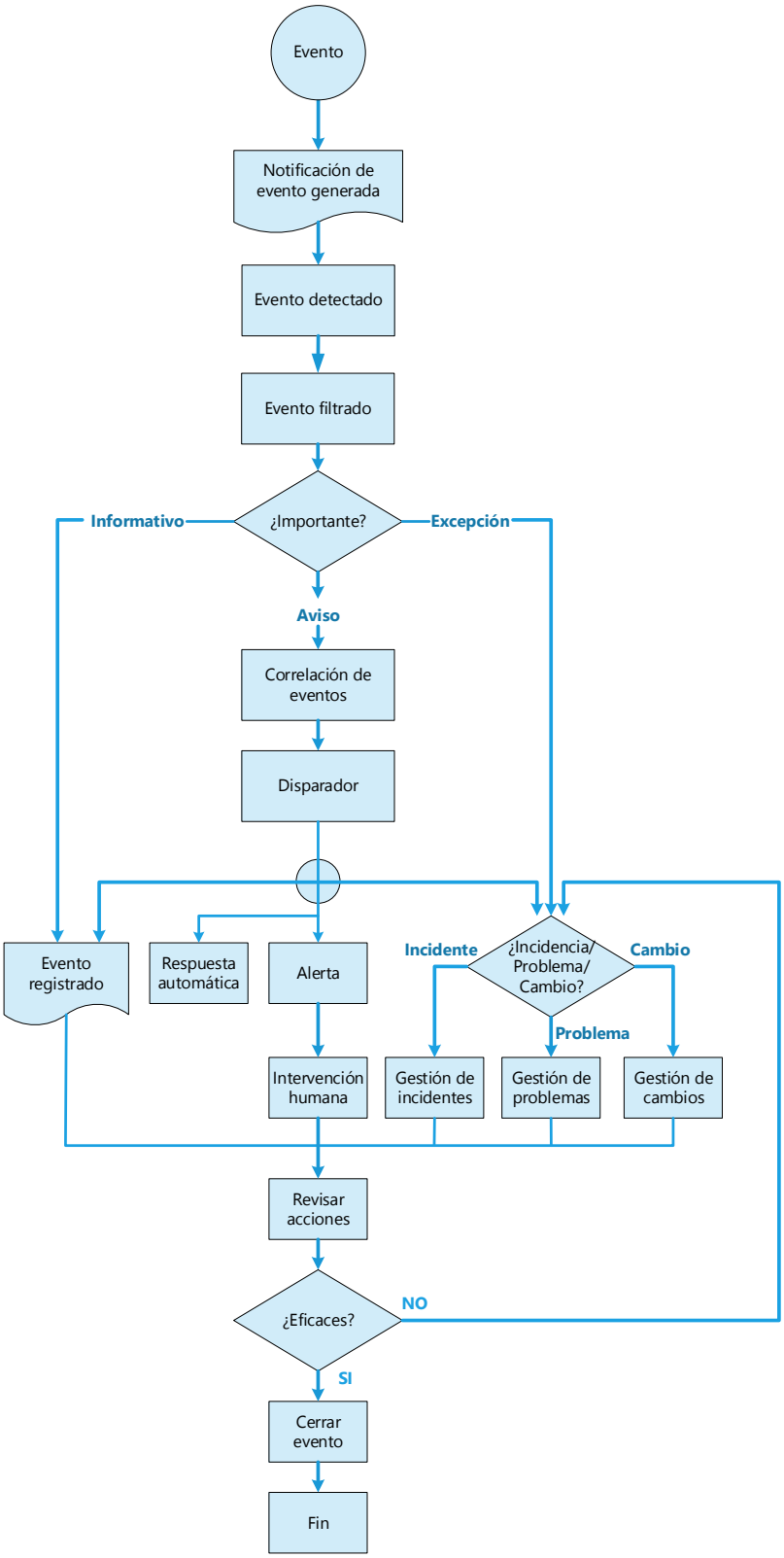


Figura 3. Proceso de gestión de eventos. Adaptado de Van J., Jong A., Kolthof., Pieper M., Tjassing R., Veen A., Verheijen T. (2008), Fundamentos de la gestión de servicios de TI Basada en ITIL V3, 383, p 283. Van Haren Publishing, Zaltbommel: itSMF International

Todos los incidentes deben quedar registrados con sus datos, incluyendo fecha y hora. Para disponer de un registro histórico completo hay que registrar toda la información sobre la naturaleza del incidente. Se debería registrar como mínimo Un número de referencia exclusivo “ticket”, la urgencia, la prioridad, el nombre/identificador de quien registra, la descripción del sistema, las actividades de mitigación

Cuando se gestiona una incidencia, cada grupo de soporte investiga qué es lo que ha fallado y diagnostica. Todas estas actividades deben quedar documentadas en el registro del incidente. En casos en donde la incidencia es solamente de solicitud de información, se debe resolver, documentar y cerrar rápidamente por el grupo de primer nivel del centro de servicios al usuario.

Cuando el agente del centro o mesa de servicio no puede resolver el incidente debe escalarlo a un nivel de soporte superior que puede ser de dos maneras

A través de **escalamiento funcional** al grupo de segunda línea de soporte a criterio de la mesa de servicio, si este grupo dado el caso no lo puede resolver lo debe escalar a un grupo superior de tercer nivel en el cual se encuentran los grupos de soporte del proveedor o fabricante del producto en caso de que se haya contratado ese servicio

El otro tipo de escalamiento es el **jerárquico** en el que los gestores de TI correspondientes deben ser avisados en caso de un incidente de prioridad alta, se usa también si no se cuenta con los recursos suficientes para resolver el incidente. Este tipo de escalamiento consiste en ir subiendo de nivel en la cadena de mando de la organización para que los directivos responsables conozcan sobre el incidente y puedan adoptar las medidas oportunas, como es la asignación de más recursos o el acudir a proveedores, entre otros.

En la figura 4 se presenta un diagrama general de la gestión de incidentes

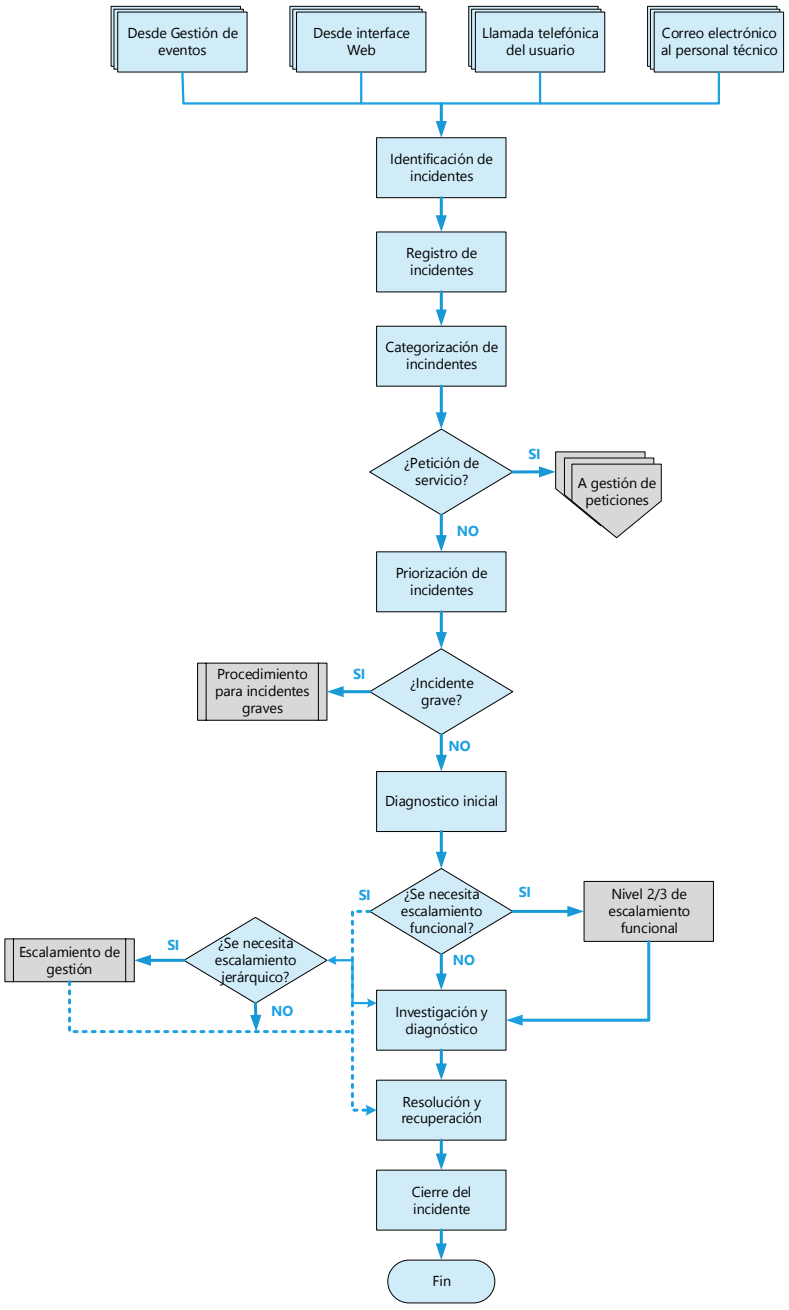


Figura 4. Proceso de gestión de incidentes. Adaptado de Van J., Jong A., Kolthof., Pieper M., Tjassing R., Veen A., Verheijen T. (2008), Fundamentos de la gestión de servicios de TI Basada en ITIL V3, 383, p 288. Van Haren Publishing, Zaltbommel: itSMF International

5. METODOLOGÍA

El método utilizado para la solución del problema de integrar los requisitos de la gestión de incidentes de seguridad de la información de ISO 27001 dentro de la gestión de eventos e incidentes de las mesas de servicios tecnológicas consta de cinco etapas debidamente desarrolladas durante el desarrollo del diseño del modelo

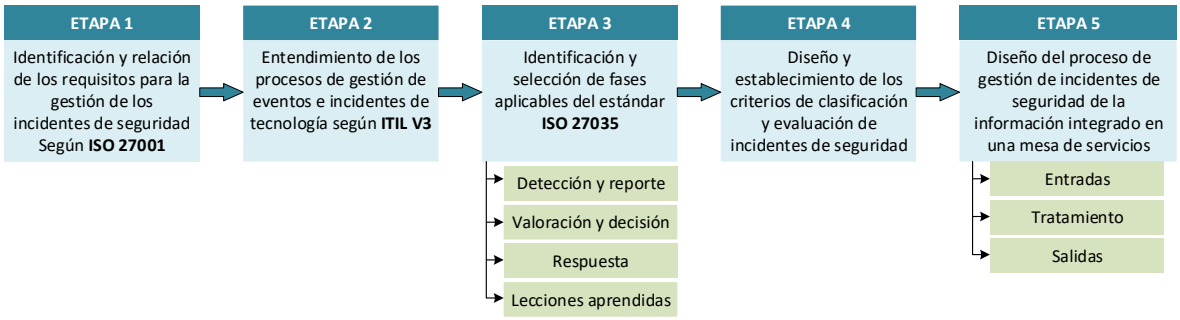


Figura 5. Etapas del marco de trabajo utilizado para el desarrollo del proyecto

Las tres primeras etapas hacen parte del proceso de estudio y análisis de normas y guías de buenas práctica ampliamente utilizadas a nivel internacional y que están relacionadas con la gestión de eventos e incidentes, estas primeras etapas son desarrolladas en su mayoría dentro del marco teórico y referencias utilizadas para el diseño del modelo.

La etapa 4 hace parte de un componente muy importante del modelo y es de los criterios a utilizar dentro de la identificación de eventos e incidentes de seguridad de la información

Los criterios que necesitan ser definidos son:

- Criterios para clasificar los incidentes por categorías o grupos comunes

- Criterios para determinar cuándo un evento SI se convierte en un incidente de seguridad
- Criterios para establecer su criticidad y urgencia

La última etapa es la construcción del modelo de gestión de incidentes embebido dentro de una mesa de servicios tomando como insumos los resultados del desarrollo de las etapas anteriores.

Este diseño es construido como un proceso que empieza con las entradas (eventos, incidentes y vulnerabilidades), su tratamiento y el resultado o la salida de ese tratamiento dentro de la gestión de los eventos e incidentes de seguridad

6. RESULTADOS Y DISCUSIÓN

MODELO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN INTEGRADO EN UNA MESA DE SERVICIOS DE TECNOLOGÍA

Este modelo de gestión está orientado a tratar dos puntos relevantes, por un lado, está el cumplimiento de los requisitos exigidos en el estándar internacional ISO 27001 2013 en lo relacionado a la gestión de incidentes de seguridad y por el otro la optimización de recursos dentro de una organización al integrar procesos de seguridad dentro de la mesa de servicios ya existente.

En lo relacionado con ISO 27001 2013, el modelo de gestión propuesto trata los siguientes aspectos de total relevancia para lograr una gestión adecuada y oportuna de los incidentes

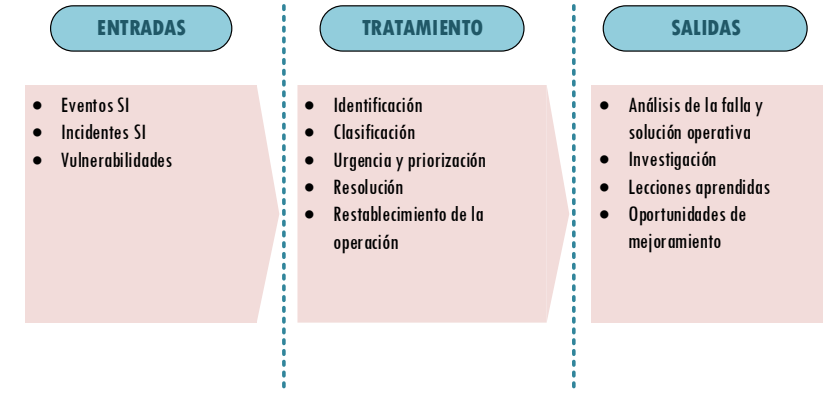
de seguridad, buscando la reducción de los efectos adversos que conlleva la materialización de dichos incidentes.

Aspectos requeridos en un SGSI para la gestión de incidentes según ISI/IEC 27001:2013 e incluidos en el modelo propuesto

- Registro y gestión de eventos de seguridad
- Registro y gestión de incidentes de seguridad (clasificación)
- Registro y gestión de vulnerabilidades
- Criterios para la identificación y priorización de incidentes
- Registro de acciones de solución operativa
- Registro para la investigación
- Documentación y registro Lecciones aprendidas
- Cierre del incidente

☛ Es importante tener en cuenta que este modelo está pensado principalmente para ajustar los flujos de gestión de incidentes de las herramientas de software ya disponibles en las organizaciones y que son usadas para registrar y gestionar eventos, requerimientos, incidentes y problemas de TI a través de un canal centralizado de mesa de servicios.

Con base en lo anterior se llevan todas las necesidades de gestión, a un esquema sencillo de proceso, que relaciona las entradas, el tratamiento y las salidas correspondientes que debe manejar el modelo de gestión de incidentes



** SI - hace refiere a Seguridad de la Información*

6.1.2 Gestión de eventos SI

Los eventos de seguridad (logs) al igual que los de TI son registrados directamente sobre los equipos o sistemas para conocer en tiempo real cualquier alerta o situación que hable sobre su estado o funcionamiento inusual y malintencionado. Esto implica tener activados los logs de auditoría en los equipos y optimizados de forma tal que no consuman en exceso los recursos de procesamiento y almacenamiento

La revisión directa sobre los logs de los equipos se vuelve muy tediosa y compleja dada la enorme cantidad de notificaciones o eventos que se generan, por lo tanto, es conveniente llevar todos estos datos (logs) a un dispositivo central que los recolecte y que puede realizar de forma oportuna y eficaz su revisión. Estas soluciones de recolección de eventos son parametrizables y están diseñadas para analizar altos volúmenes de datos y generar alertas o notificaciones según las reglas que se hayan establecido.

Desde el punto de vista de seguridad es de gran interés identificar oportunamente las acciones u operaciones inusuales o malintencionadas para luego impedir que se expanda e interrumpa las operaciones o los servicios

Figura 5. Recolección de eventos de seguridad

Tal como se presenta en la figura 5, el interés de la gestión de eventos es integrar todos los registros de logs de los sistemas incluyendo los dispositivos de seguridad en las redes, a un proceso de recolección, análisis y monitoreo para lograr esa proactividad y oportunidad en la identificación de situaciones inusuales que puedan conducir a ataques y por consiguiente a la indisponibilidad, alteración o fuga de información de las organizaciones. La gestión de eventos está fuertemente ligada a la necesidad de establecer procesos adecuados y eficaces de monitoreo de la seguridad al interior de las empresas

6.1.3 Gestión de vulnerabilidades

La identificación de vulnerabilidades viene de dos fuentes claves, por un lado, están las vulnerabilidades técnicas que son encontradas en la ejecución de actividades de revisión de controles de seguridad implementados, resultado de la ejecución de actividades de auditorías de control interno, auditoría de sistemas, y las revisiones de

seguridad a través del uso de prácticas de Ethical Hacking o el uso de soluciones de búsqueda (escaneo) de vulnerabilidades. La otra fuente, son las vulnerabilidades técnicas o no técnicas que son conocidas e identificadas por los empleados, proveedores o terceras partes y que de igual forma deben ser reportadas en los sistemas de seguridad a través de canales adecuados para su posterior gestión y tratamiento. Las medidas tomadas para gestionar vulnerabilidades no técnicas son más de tipo administrativo que recaen en la necesidad de crear o reforzar políticas de seguridad, realizar procesos disciplinarios y fortalecer el entrenamiento y la concienciación en seguridad de la información en las organizaciones.

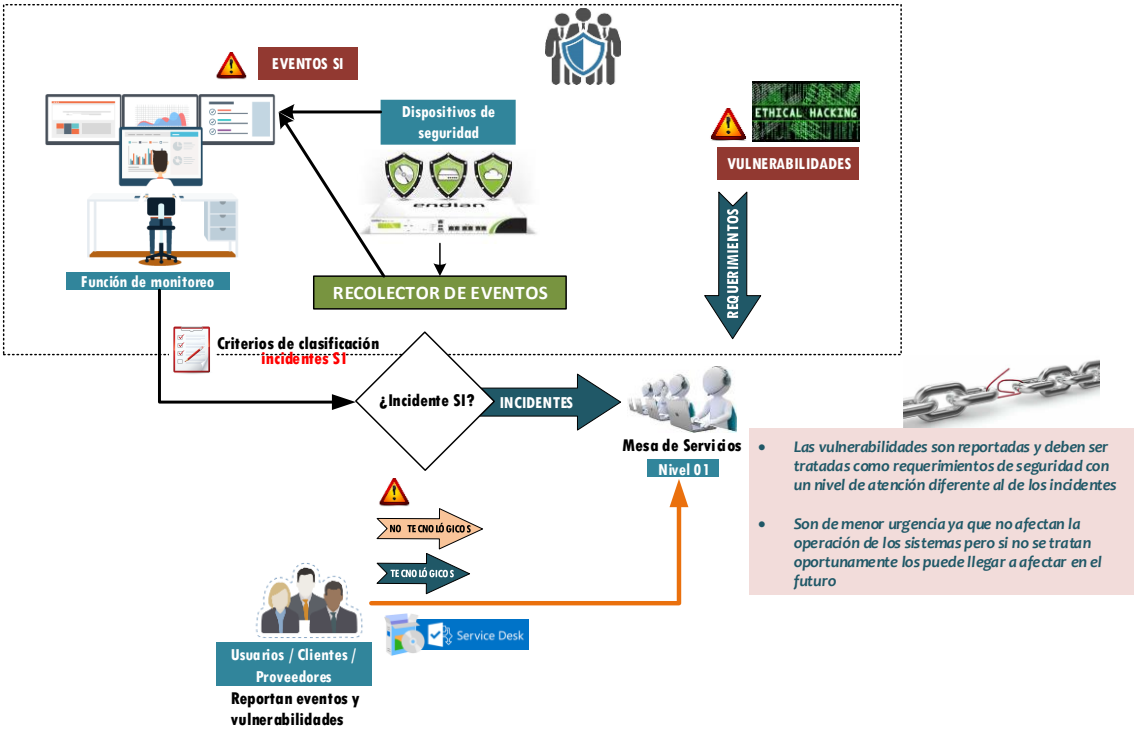


Figura 6. Entradas en la gestión de incidentes SI

Un componente importante del modelo de gestión de incidentes son los criterios a utilizar para identificarlos y evaluar su criticidad y nivel de urgencia en su tratamiento

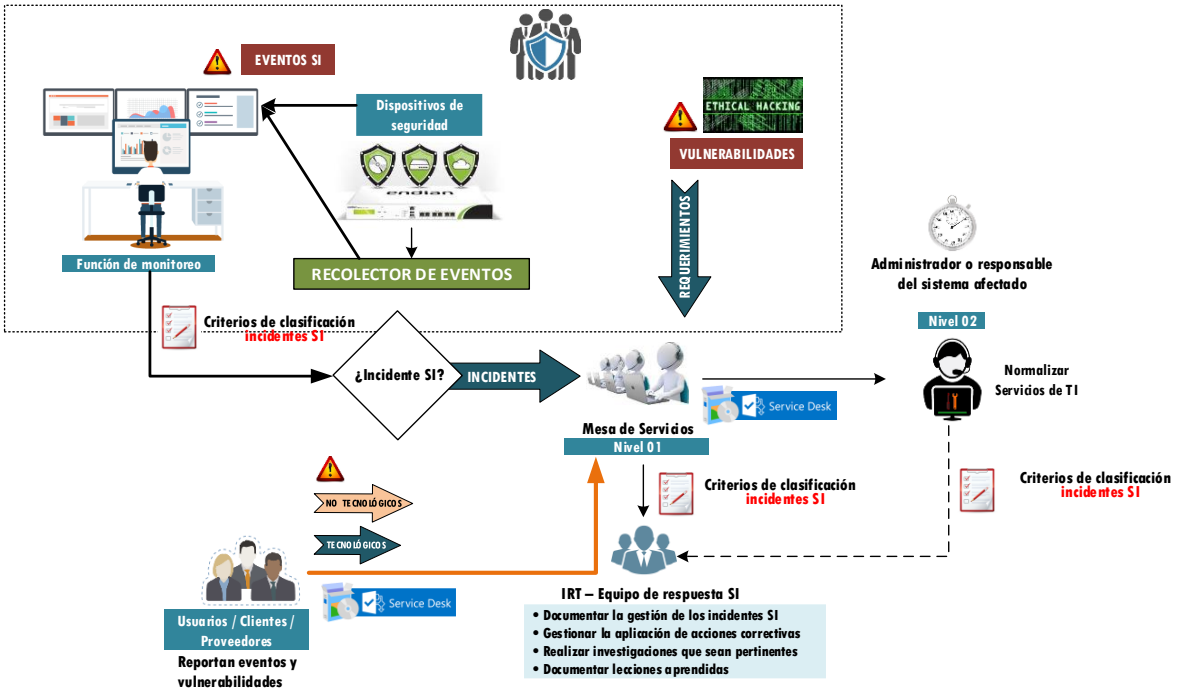
6.1.4 Atención de eventos, incidentes y vulnerabilidades desde la mesa de servicios

La atención que se le debe dar a cada uno de ellos es presentada en la siguiente relación

Situación	Acción
Evento SI	Cuando viene de la función de monitoreo, se revisa y valida la clasificación y posteriormente se direcciona al equipo de segundo nivel para su análisis y tratamiento correspondiente Si cumple con los criterios y se convierte en incidente de seguridad, se direcciona al segundo nivel más idóneo para su posterior gestión, resolución y contención de la falla presentada Si es reportado por empleados, clientes o terceras partes, se realiza el respectivo análisis para conocer su grado de afectación en la operación, se clasifica, se determina la urgencia con que debe ser gestionado y a quién debe ser direccionado para su posterior tratamiento * Es importante motivar a las personas involucradas en las operaciones de una organización a reportar aquellas situaciones de falla en los recursos tecnológicos, debilidades o ausencia de control que pongan en riesgos los activos de información o cualquier circunstancia que vayan en contra de las políticas o directrices corporativas, tratando que dichos reportes sean lo más claros y completos posibles para entender el problema y poderlo resolver de la forma más adecuada. A este punto es más importante la claridad y completitud de la información que la clasificación que le puedan dar al caso, ya es el grupo de primer

Situación	Acción
	nivel de la mesa de servicios el encargado de reclasificar de forma más idónea el evento reportado.
Incidente SI	El incidente como tal representa una mayor urgencia ya que en la mayoría de los casos está afectando los servicio o las operaciones de las organizaciones Estos incidentes se deben clasificar de acuerdo al impacto en las operaciones del negocio o en los servicios prestados por las áreas de apoyo. Normalmente sobre estos se aplican acuerdos de niveles de servicios en tiempos de solución que son más cortos según sea la criticidad de las operaciones para la organización.
Vulnerabilidad	Como ya se comentó anteriormente, este tipo de situaciones no demanda una urgencia inmediata en su resolución y dentro del modelo de gestión son designados como requerimientos con un tratamiento diferente al de los incidentes SI. La idea de integrar la gestión de vulnerabilidades dentro del modelo es la centralización de la gestión y en un solo sitio poder conocer que se ha identificado y que acciones se han realizado o se van a realizar para remediar las vulnerabilidades encontradas. Este aspecto es esencial para los sistemas de gestión y hace parte de los requisitos de seguridad comunes de obligatorio cumplimiento dentro de los sistemas de seguridad de la información en particular los ya certificados en ISO 27001

6.1.5 Modelo propuesto para la gestión de eventos, incidentes y vulnerabilidades (flujo)



La gestión del evento, incidente o vulnerabilidad tiene tres partes claves dentro del modelo propuesto

Parte o grupo dentro del modelo	Funciones realizadas
Mesa de servicios (Nivel 1)	• Recibe y analiza todas las solicitudes (eventos, incidentes y vulnerabilidades) • Gestionar con la fuente de información que el caso sea claro y que todos datos requeridos sean obtenidos • Clasifica bajo unos criterios prestablecidos los casos que deben ser direccionados directamente al equipo IRT de Seguridad

Parte o grupo dentro del modelo	Funciones realizadas
	• Cumplir con los ANS establecidos para la gestión realizada por esta área • Documentar la gestión realizada • Direcciona los casos hacia los equipos de soporte de segundo nivel para la contención de la falla y la recuperación de los servicios afectados
Grupos de soporte (Nivel 2)	• Realiza las actividades de contención y recuperación de la falla • Cumplir con lo ANS establecidos para la atención y solución del incidente • Documentar la gestión y solución realizada • Bajo unos criterios prestablecidos determinar si el incidente ocurrido es de seguridad de la información • Si no es de seguridad de la información debe cerrar el caso una vez sea realizada la documentación de las acciones • Si es de seguridad se debe reclasificar y direccionar al IRT de seguridad para la realización del resto de actividades de gestión

Parte o grupo dentro del modelo	Funciones realizadas
Equipos de respuesta a incidentes “IRT”	• Realizar las investigaciones pertinentes que sean necesarias • El propósito de realizar investigaciones adicionales es el de buscar la causa principal que ocasionó el incidente, que controles de seguridad hacen falta o son ineficientes y si se cuenta con las evidencias suficientes para demostrar la culpabilidad de los empleados en el incidente, lo cual requerirá el uso de procedimiento de cadena de custodia y dependiendo del caso la intervención de autoridad nacional competente • Documentar los resultados de la investigación • Analizar la gestión y los resultados de la investigación realizada para identificar controles de seguridad de la información que no están siendo efectivos para el propósito que fueron implementados • Identificar, establecer y documentar las lecciones aprendidas • Encontrar y gestionar la implementación de las oportunidades de mejoramiento del sistema de gestión de seguridad de la información

Parte o grupo dentro del modelo	Funciones realizadas
	• ** Las lecciones aprendidas ayudan a evitar la recurrencia de los incidentes de seguridad de la información* • Las lecciones aprendidas buscan conocer si los siguientes aspectos fueron o no adecuados El tratamiento y respuesta que se le dio al incidente Los tiempos de respuestas y solución cumplieron con los ANS pactados La efectividad y calidad de la contención o acción correctiva de la falla La efectividad de los controles y si es necesario realizar cambios en la definición e implementación de los mismos La calidad de la investigación y la competencia del equipo de soporte de segundo nivel e IRT de seguridad para resolver y gestionar el incidente • Cerrar el incidente una vez se haya realizado la documentación de investigación y lecciones aprendidas

6.2 CRITERIOS PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El establecimiento de criterios es fundamental para el desarrollo del proceso de gestión de incidentes, encontrándose la necesidad de establecer los siguientes

1. Criterios para clasificar los incidentes por categorías o grupos comunes
2. Criterios para determinar cuándo un evento SI se convierte en un incidente de seguridad
3. Criterios para establecer su criticidad y urgencia

A continuación, se describen las características más importantes de cada uno de ellos

6.2.1 Clasificación por categorías y grupos comunes

Este criterio permite la asociación de incidentes por categoría y subcategorías comunes a partir de sus características y posibles causas, para este modelo de gestión se trae una relación bastante amplia (más de 60 subcategorías) de los posibles incidentes de seguridad de la información que pueden ser encontrados en las organizaciones o en los sistemas de gestión de seguridad de la información. Esta relación fue construida con la integración de información encontrada en múltiples referencias como es ISO 27035, ISF y los recogidos por el conocimiento de diferentes sistemas de gestión de varias organizaciones.

Estos criterios son presentados en el **Anexo A**, en la parte final de este documento

6.2.2 Criterios para determinar cuándo un evento es un incidente

Partiendo de las definiciones mostradas previamente en el marco teórico se observa que la diferentes entre estos dos conceptos es básicamente el tipo de impacto que tiene en las operaciones o los servicios prestados en las organizaciones, los eventos se pueden ver más como alertas mientras que los incidentes si tienen una alta probabilidad de afectar los servicios o en algunos casos ya se han materializado causando efectos negativos en los servicios u operaciones de negocio.

Para determinar que un evento es un incidente de seguridad se establecen las siguientes reglas

1. Que el evento identificado haya afectado los servicios u operaciones
2. Que registre un número alto de incidentes o registros de las mismas características y que se encuentre en la relación de categorías y subcategorías de incidentes de seguridad de la información (Es muy conveniente cuando se están recibiendo ataques contra los sistemas y se desea identificarlos oportunamente y realizar contraofensivas)
3. Que evidencie una violación de las políticas de seguridad y que exponga seriamente la información o los datos de los sistemas o atente contra su disponibilidad o integridad

6.2.3 Criterios para evaluar su impacto y urgencia

Los criterios se establecen en tres niveles de acuerdo al impacto en las operaciones o los servicios prestados por las organizaciones y es presentado en el **Anexo B** de este documento.

7. CONCLUSIONES

A pesar de arrancar el desarrollo del proyecto con un entorno netamente tecnológico se fue flexibilizando y ampliando a incluir otros incidentes de seguridad más de tipo administrativo de la seguridad de la información, lo que indudablemente le da un mayor alcance al modelo de cara a cumplir con los requisitos de ISO 27001 que no trata solamente temas tecnológicos. Así mismo la solución trata todo tipo de incidentes (tecnológicos y no tecnológicos) canalizándolos a través de un único punto central como es la mesa de servicios. Esto puede observarse tanto en los criterios definidos como en el flujo para la gestión de los incidentes de seguridad de la información.

A pesar de que se cumplió con el objetivo de diseñar criterios para la identificación, evaluación y criticidad de los incidentes de seguridad, estableciendo una amplia relación de posibles tipos de incidentes tanto tecnológico como no tecnológico comúnmente presentado en las organizaciones, es importante que antes de ser aplicados sean revisados y ajustados a la medida de las necesidades de la empresa para garantizar que los que se utilicen reflejen los tipos de incidentes que normalmente se pueden presentar en la organización según, el tipo de negocio, el sector al que pertenece la empresa y el tipo de riesgos de seguridad de la información a los que está expuesta. El criterio sugiere también el nivel de soporte que debe clasificar el incidente como incidente de seguridad el cual debe ser revisado antes de ser aplicado, considerando la estructura de los procesos de gestión de tecnología establecidos, la existencia de equipos de respuesta a incidentes debidamente

conformados y el grado de competencia y entrenamiento de los empleados involucrados en materia de seguridad de la información.

El modelo propuesto para la gestión de incidentes de seguridad de la información está orientado principalmente para las empresas que cuentan con dos aspectos fundamentales, el primero es el de contar con una mesa de servicios (service desk) para la gestión de incidentes y requerimientos tecnológicos basado en modelos de gestión de servicios de tecnología, un segundo aspecto es el de haber adoptado e implementado un sistema de gestión de seguridad de la información y que se cuente con una certificación que exija el cabal cumplimiento de los requisitos de seguridad de la norma ISO 27001. El modelo diseño es de mayor utilidad para las empresas que cuente con las dos condiciones mencionadas en este párrafo.

Antes de aplicar este modelo en una empresa, es importante revisarlo y personalizarlo de acuerdo a, el apetito o tolerancia al riesgo que tenga la compañía, la criticidad de las operaciones y de los servicios prestados, los acuerdos de niveles de servicios establecidos con los procesos internos y con los clientes, el tipo de sector al que pertenece la empresa, el cumplimiento de requisitos legales, contractuales y regulatorios, el tipo y proporción de la población que puede verse afectada ante cualquier indisponibilidad de las operaciones y los servicios prestados por la compañía.

8. BIBLIOGRAFÍA

Van J., Jong A., Kolthof., Pieper M., Tjassing R., Veen A., Verheijen T. (2008), Fundamentos de la gestión de servicios de TI Basada en ITIL V3, Van Haren Publishing, Zaltbommel: itSMF International

National Institute of Standards and Technology NIST, Computer Security Incident Handling Guide Special Publication 800-61 Revision 2, U.S. Department of Commerce, 2012

International Organization for Standardization ISO, Information technology Security techniques, Information security incident management, Part 1: Principles of incident management, Geneva, Switzerland, 2016

International Organization for Standardization ISO, Information technology Security techniques, Information security incident management, Part 2: Guidelines to plan and prepare for incident response, Geneva, Switzerland, 2016

Instituto Colombiano de Normas Técnicas y Certificación ICONTEC, Compendio Seguridad de la Información, Segunda edición, Bogotá Colombia, 2015

9. ANEXOS

A. CRITERIOS DE CLASIFICACIÓN POR CATEGORÍAS Y SUBCATEGORÍAS DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Este anexo presenta los criterios tanto técnicos como no técnicos para poder determinar si una situación particular presentada es un incidente de seguridad, contiene una amplia cantidad de denominaciones de categorías y subcategorías de incidentes según el efecto o la causa que lo ocasiona, pensando en cubrir la mayor cantidad de situaciones comunes que son presentadas al interior de la organizaciones, sin embargo no es exhaustiva y puede requerir la inclusión de nuevos elementos según las necesidades particulares de las organizaciones.

Presenta de igual forma una guía básica para establecer que nivel de soporte es el más competente para determinar si la situación presentada corresponde a un incidente de seguridad de la información ya que es imposible determinar en una primeria instancia si por ejemplo una falla de un equipo de cómputo está relacionada directamente con un incidente de seguridad de la información. La definición de niveles (columna 3) dependerá de la estructura de la organización, del conocimiento de los empleados que conforman dichos procesos y del nivel de madurez de sus procesos tecnológicos.

CATEGORIAS	SUBCATEGORIAS	NIVEL DE SOPORTE EN DONDE SE DEBE CLASIFICAR	REFERENCIA
ATAQUES INFORMÁTICOS (EXTERNO/ INTERNO)	Ejecución de Denegación de Servicio	Nivel 2	C01SC01
	Hacking	Nivel 2	C01SC02
	Ejecución de Pruebas Maliciosas o Escaneos	Nivel 2	C01SC03
	Cracking de Contraseñas	Nivel 2	C01SC04
	Cracking de llaves	Nivel 2	C01SC05
	Desfiguración o alteración de página Web	Nivel 2	C01SC06

CATEGORIAS	SUBCATEGORIAS	NIVEL DE SOPORTE EN DONDE SE DEBE CLASIFICAR	REFERENCIA
	Suplantación de sitios Web	Nivel 2	C01SC07
	Suplantación de identidad de usuarios	Nivel 2	C01SC08
	Alteración del tráfico en la red	Nivel 2	C01SC09
	Eavesdropping (escuchar secretamente la comunicación de los demás)	Nivel 2	C01SC10
	Distribución de virus de computador	Nivel 1 & Nivel 2	C01SC11
	Introducción de troyanos	Nivel 2	C01SC12
	Introducción de código malicioso (malware)	Nivel 2	C01SC13
	Ejecución de actividades de ingeniería social	Nivel 1	C01SC14
	Aprovechamiento de vulnerabilidades	Nivel 2	C01SC15
	Distribución de spam	Nivel 2	C01SC16
ABUSO Y USO INADECUADO AL INTERIOR DE LA ORGANIZACIÓN	Acceso no autorizado a sistemas o redes	Nivel 2	C02SC01
	Cambio de privilegios de sistema sin autorización	Nivel 2	C02SC02
	Cambio o adición de software sin autorización	Nivel 1	C02SC03
	Modificación o inserción de transacciones, archivos o bases de datos sin autorización	Nivel 2	C02SC04
	Uso inadecuado de sistemas que generan interrupción	Nivel 2	C02SC05
	Uso inadecuado de sistemas para generar fraudes	Nivel 2	C02SC06
	Descarga o envió de contenido inapropiado	Nivel 1	C02SC07
	Falsificación de documentos (Ej. Falsificación de los certificados, formularios de solicitud de crédito, etc.)	Nivel 1	C02SC08
	Instalación de software no autorizado	Nivel 1	C02SC09
	Posesión y almacenamiento de contenido ilegal en equipos corporativos (Pornografía infantil, copias de música, videos, libros o documentos que violen la propiedad intelectual, Información personal sin la	Nivel 1	C02SC10

CATEGORIAS	SUBCATEGORIAS	NIVEL DE SOPORTE EN DONDE SE DEBE CLASIFICAR	REFERENCIA
	autorización de los titulares de información, racismo, violencia)		
	Revelación de información secreta de autenticación	Nivel 2	C02SC11
	Divulgación de información sensible del negocio	Nivel 1	C02SC12
	Piratería de software	Nivel 1	C03SC01
	Robo de información de negocio	Nivel 1	C03SC02
	Robo de información personal (ej.: Phishing)	Nivel 1	C03SC03
ROBO	Robo de equipo de computo	Nivel 1	C03SC04
	Robo de información de autenticación	Nivel 1	C03SC05
	Robo o uso no autorizado de credenciales bancarias	Nivel 1	C03SC06
	Robo de software	Nivel 1	C03SC07
MALFUNCIONAMIENTO DEL SOFTWARE O DE LOS SISTEMAS	Malfuncionamiento de las aplicaciones de software de negocio desarrollados internamente	Nivel 2	C04SC01
	Malfuncionamiento de las aplicaciones de software de negocio de terceros	Nivel 2	C04SC02
	Malfuncionamiento de software de sistemas	Nivel 2	C04SC03
	Malfuncionamiento de computadores o equipos de computo	Nivel 2	C04SC04
INTERRUPCIÓN DE SERVICIOS	Daño o pérdida de las instalaciones de computo	Nivel 2	C05SC01
	Daño o pérdida de los equipos auxiliares o complementarios	Nivel 2	C05SC02
	Desastres naturales	Nivel 2	C05SC03
	Fallas en el fluido eléctrico	Nivel 2	C05SC04
	Fallas en las redes de comunicaciones	Nivel 2	C05SC05
	Fallas en los sistemas de aires acondicionados	Nivel 2	C05SC06
	Fallas en el suministro de agua	Nivel 2	C05SC07

CATEGORIAS	SUBCATEGORIAS	NIVEL DE SOPORTE EN DONDE SE DEBE CLASIFICAR	REFERENCIA
	Sobrecarga de sistema (Saturación de la capacidad de los sistemas de información)	Nivel 2	C05SC08
ERROR HUMANO	Errores de usuario	Nivel 2	C06SC01
	Error humano interno cometido por empleados	Nivel 2	C06SC02
	Error humano externo cometido por el cliente	Nivel 2	C06SC03
	Error humano por personal de TI, Telecomunicaciones o personal que administra los archivos físicos	Nivel 2	C06SC04
EFECTOS IMPREVISTOS OCASIONADOS POR CAMBIOS	Efectos imprevistos con la entrada de nuevos procesos de negocio o modificados	Nivel 2	C07SC01
	Efectos imprevistos de cambios en software	Nivel 2	C07SC02
	Efectos imprevistos en cambios de información de negocio	Nivel 2	C07SC03
	Efectos imprevistos de cambios a equipos de cómputo o comunicaciones	Nivel 2	C07SC04
	Efectos imprevistos de cambios organizacionales	Nivel 2	C07SC05
	Efectos imprevistos de cambios a procesos de usuarios o instalaciones	Nivel 2	C07SC06
SOLICITUDES ENTES DE CONTROL, SUPERVISIÓN & CLIENTES	Solicitud de información por parte de la policía Nacional	Nivel 2	C08SC01
	Solicitud de información por parte de la fiscalía	Nivel 2	C08SC02
	Solicitud de información por parte de la Super Intendencia de Industria y Comercio	Nivel 2	C08SC03
	Solicitud de información por parte de los clientes (Ej. Consultas y reclamos en materia de protección de datos personales)	Nivel 2	C08SC04
	Solicitud de información por parte de la Super Intendencia Financiera	Nivel 2	C08SC05
	Incumplimiento de las políticas seguridad de la información	Nivel 1 & Nivel 2	C09SC01

CATEGORIAS	SUBCATEGORIAS	NIVEL DE SOPORTE EN DONDE SE DEBE CLASIFICAR	REFERENCIA
INCUMPLIMIENTO DE DIRECTRICES Y POLÍTICAS	Incumplimiento de los requisitos legales (Ej. Protección de datos personales, Habeas data)	Nivel 2	C09SC02
9			64

B. CRITERIOS PARA EVALUAR SU IMPACTO Y URGENCIA

Los criterios se establecen en tres niveles de acuerdo al impacto en las operaciones o los servicios prestados por las organizaciones

Los valores a establecer para los tiempos de solución dependerán de la criticidad de los servicios y operaciones de la empresa, los acuerdos de niveles de servicios ya establecidos y el apetito o tolerancia al riesgo por parte de la organización

Nivel de criticidad	Características	Urgencia de gestión
ALTA	• Se materializó y generó la interrupción de las operaciones o los servicios críticos de la compañía • Se registra un número considerable de registros (logs) similares exitosos y se determina que la organización está siendo sometida a un ataque • Se materializó y expone a la organización a sanciones ante el incumplimiento de requisitos legales y	De inmediato Resolución operativa de las fallas tecnológicas en un tiempo no superior a 1 día Notificación inmediata al área de RRHH para inicio de proceso disciplinario

Nivel de criticidad	Características	Urgencia de gestión
	regulatorios (Ej. Fuga de datos personales) • Genera una afectación total de los sistemas de información críticos • Se fuga, pierde o altera información confidencial o privada con claras evidencias de incumplimiento de las directrices de seguridad por parte de los empleados y proveedores	Notificación inmediata al área de compras y jurídica para determinar el tipo de acción que se realizará sobre el proveedor involucrado
MEDIA	• Se materializó y generó la afectación de las operaciones o los servicios no críticos de la compañía • Genera una afectación parcial del total de equipos de cómputo de la organización, no superior del 20% • Se registra un número considerable de registros (logs) similares de rechazo y se observa que están intentando atacar la infraestructura tecnológica • Genera la indisponibilidad de sistemas de información no críticos o imprescindibles para la entrega de productos o servicios • A pesar de que se evidencia un claro incumplimiento intencional de las directrices de seguridad por parte de los empleados y proveedores, no se expone información confidencial, privada o personal y no se afecta tampoco la disponibilidad de los sistemas de información	A concertar con la organización en equivalencia con otros criterios de valoración internos Resolución operativa de las fallas tecnológicas en un tiempo no superior a 3 días Notificación inmediata al área de RRHH para llamado de atención al empleado Notificación inmediata al área de compras para realizar el llamado de atención al proveedor y la definición de acciones correctivas por parte de este

Nivel de criticidad	Características	Urgencia de gestión
BAJA	• No afecta, ni interrumpe los servicios u operaciones de la organización • Genera una afectación parcial del total de equipos de cómputo de la organización, no superior del 5% • Fallas leves de incumplimiento de las directrices de seguridad de la información ocasionadas más por desconocimiento de los empleados o proveedores	A concertar con la organización en equivalencia con otros criterios de valoración internos Resolución operativa de las fallas tecnológicas en un tiempo no superior a 5 días