Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía No. 21

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0	12/31/2014	Versión inicial del documento
1.1	27/07/2015	Actualización
1.2	6/11/2016	Actualización CCP - MINTIC

TABLA DE CONTENIDO

PÁG.

1. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad de la Información con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones.

Para el desarrollo de esta guía, se recogieron aspectos importantes de mejores prácticas y documentos de uso libre por parte del NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide), tomando como base los lineamientos recomendados en Norma la ISO IEC 27001 – 2013 Numeral 16 de la misma, para la gestión de incidentes.

2. AUDIENCIA

Entidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de TI en el marco de la Estrategia de Gobierno en Línea.

3. INTRODUCCIÓN

Este anexo entrega los lineamientos básicos para poner en marcha un Sistema de Gestión de Incidentes de Seguridad de la información, a través de un modelo propuesto, el cual está concebido para que se puedan integrar los incidentes de seguridad sobre los activos de información, independiente del medio en el que se encuentren.

4. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

4.1 OBJETIVO

El objetivo principal del Modelo de Gestión de Incidentes de seguridad de la información es tener un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información.

Los objetivos del modelo son garantizar que:

- Definir roles y responsabilidades dentro de la Organización como eje puntual para evaluar los riesgos y permita mantener la operación, la continuidad y la disponibilidad del servicio.
- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- Permitir identificar los incidentes de seguridad de la información para ser evaluados y dar respuesta de la manera más eficiente y adecuada.
- Minimizar los impactos adversos de los incidentes en la organización y sus operaciones de negocios mediante las salvaguardas adecuadas como parte de la respuesta a tal incidente.
- Consolidar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para aprender rápidamente. Esto tiene como objeto incrementar las oportunidades de prevenir la ocurrencia de futuros incidentes, mejorar la implementación y el uso de las salvaguardas y mejorar el esquema global de la gestión de incidentes de seguridad de la información.
- Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y registro de incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.
- Definir los procedimientos formales de reporte y escalada de los incidentes de seguridad.
- Establecer variables de posible riesgo, en efecto, es la posible valoración de aspectos sensibles en los sistemas de información.

Para lograr estos objetivos, la gestión de incidentes de seguridad de la información involucra los siguientes procesos de manera cíclica como lo muestra la imagen:

- Planificación y preparación para la gestión del Incidente

- Detección y análisis.
- Contención, erradicación y recuperación.
- Actividades Post-Incidente.

Esta guía le permitirá a las entidades estar preparadas para afrontar cada una de las etapas anteriores, y adicionalmente definiendo responsabilidades y procedimientos para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

4.2 CARACTERÍSTICAS DE UN MODELO DE GESTIÓN DE INCIDENTES

Esta guía de gestión de incidentes de seguridad de la información plantea una serie de actividades para dar cumplimiento con el ciclo de vida de la gestión y respuesta a un incidente de seguridad.

Para definir las actividades de esta guía se incorporaron componentes definidos por el NIST alineados con los requerimientos normativos de la NTC–ISO–IEC 27035-2013 para la estrategia de Gobierno en Línea.

Es recomendable que las entidades creen un equipo de atención de incidentes de seguridad en cómputo CSIRT o un grupo que haga sus veces, quienes se encargaran de definir los procedimientos a la atención de incidentes, realizar la atención, manejar las relaciones con entes internos y externos, definir la clasificación de incidentes, y además de esto se encargaran de:

- **Detección de Incidentes de Seguridad:** Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
- **Atención de Incidentes de Seguridad:** Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
- **Recolección y Análisis de Evidencia Digital:** Toma, preservación, documentación y análisis de evidencia cuando sea requerida.

- **Anuncios de Seguridad:** Deben mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación (Web, Intranet, Correo).
- **Auditoria y trazabilidad de Seguridad Informática:** El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.
- **Certificación de productos:** El equipo verifica la implementación de las nuevas aplicaciones en producción para que se ajusten a los requerimientos de seguridad informática definidos por el equipo.
- **Configuración y Administración de Dispositivos de Seguridad Informática:** Se encargaran de la administración adecuada de los elementos de seguridad informática.
- **Clasificación y priorización de servicios expuestos:** Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
- **Investigación y Desarrollo:** Deben realizar la búsqueda constante de nuevos productos en el mercado o desarrollo de nuevas herramientas de protección para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad de la información.

Este grupo está enfocado principalmente en atender los incidentes de seguridad de la información que se presentan sobre los activos soportados por la plataforma tecnológica de la entidad.

5. DEFINICIÓN FORMAL DE LA GUÍA PROPUESTA PARA LA GESTIÓN DE INCIDENTES

5.1 PREPARACIÓN

Esta etapa dentro del ciclo de vida de respuesta a incidentes suele hacerse pensando no sólo en crear un modelo que permita a la entidad estar en capacidad de responder ante estos, sino también en la forma como pueden ser detectados, evaluados y gestionar las vulnerabilidades para prevenirse, asegurando que los sistemas, redes, y aplicaciones son lo suficientemente seguros . Aunque el equipo de respuesta a incidentes no es normalmente responsable de la prevención de incidentes, es muy importante que se considere como un componente fundamental de los programas de respuesta. El equipo de respuesta a incidentes debe actuar como una herramienta de experiencia en el establecimiento de recomendaciones para el aseguramiento de los sistemas de información y la plataforma que los soporta.

En esta etapa el grupo de gestión de incidentes o quien se designe para esta labor debe velar por la disposición de los recursos de atención de incidentes y las herramientas necesarias para cubrir las demás etapas del ciclo de vida del mismo, creando (si no existen) y validando (si existen) los procedimientos necesarios y programas de capacitación.

La etapa de preparación debe ser apoyada por la dirección de tecnologías de la información o quien haga sus veces, incluyendo las mejores prácticas para el aseguramiento de redes, sistemas, y aplicaciones por ejemplo:

- **Gestión de Parches de Seguridad:** las entidades dependiendo de su estratificación deben contar con un programa de gestión de vulnerabilidades (Sistemas Operativos, Bases de Datos, Aplicaciones, Otro Software Instalado), este programa ayudara a los administradores en la identificación, adquisición, prueba e instalación de los parches.
- **Aseguramiento de plataforma:** las entidades dependiendo de si estratificación deben ser aseguradas correctamente. Se debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos. Se deben revisar configuraciones por default (usuarios, contraseñas y archivos compartidos). Cada recurso que pueda ser accedido por externos e incluso por usuarios internos debe desplegar alguna

advertencia. Los servidores deben tener habilitados sus sistemas de auditoría para permitir el login de eventos.

- **Seguridad en redes:** Debe existir una gestión constante sobre los elementos de seguridad. Las reglas configuradas en equipos de seguridad como firewalls deben ser revisadas continuamente. Las firmas y actualizaciones de dispositivos como IDS o IPS deben encontrarse al día. Todos los elementos de seguridad y de red deben encontrarse sincronizados y sus logs deben ser enviados a un equipo centralizado de recolección de logs para su respectivo análisis.
- **Prevención de código malicioso:** Todos los equipos de la infraestructura (servidores como equipos de usuario) deben tener activo su antivirus, antimalware con las firmas de actualización al día.
- **Sensibilización y entrenamiento de usuarios:** Usuarios en la entidad incluidos los administradores de TI deben ser sensibilizados de acuerdo a las políticas y procedimientos existentes relacionados con el uso apropiado de redes, sistemas y aplicaciones en concordancia con los estándares de seguridad de la entidad. Los encargados de los sistemas de información deben establecer las necesidades de capacitación de las personas encargadas de la protección de los datos.

Las actividades descritas anteriormente buscan prevenir la ocurrencia de incidentes de seguridad de la información que esta soportada por TI, y adicionalmente es necesario realizar una evaluación mensual.

5.2 RECURSOS DE COMUNICACIÓN

En este numeral se pretende enunciar los elementos necesarios para la comunicación del equipo de atención de incidentes dentro de la entidad.

Información de Contacto: Se debe tener una lista de información de contacto de cada una de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones.

Información de Escalamiento: Se debe contar con información de contacto para el escalamiento de incidentes según la estructura de la entidad.

- Información de los administradores de la plataforma tecnológica (Servicios, Servidores)

- Contacto con el área de recursos humanos o quien realice sus funciones (por si se realizan acciones disciplinarias).
- Contacto con áreas interesadas o grupos de interés (CCP - Policía Nacional, Fiscalía, entre otras)

Política de Comunicación: La entidad debe tener una política de comunicación de los incidentes de seguridad para definir que incidente puede ser comunicado a los medios y cual no.

5.3 HARDWARE Y SOFTWARE

Para una correcta y eficiente gestión de incidentes la entidad debería tener en cuenta los siguientes elementos:

- Portátiles Forenses:
- Analizadores de protocolos.
- Software de adquisición.
- Software para recolección de evidencia.
- Kit de respuesta a incidentes.
- Software de análisis forense.
- Medios de almacenamiento

5.3 RECURSOS PARA EL ANÁLISIS DE INCIDENTES

- Tener un listado de los puertos conocidos y de los puertos utilizados para realizar un ataque.
- Tener un diagrama de red para tener la ubicación rápida de los recursos existentes
- Una Línea – Base de Información de: Servidores (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios). Esta información siempre debe estar actualizada para poder conocer el funcionamiento normal del mismo y realizar una identificación más acertada de un incidente.
- Se debe tener un análisis del comportamiento de red estándar en este es recomendable incluir: puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP con que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones.

5.4 RECURSOS PARA LA MITIGACIÓN Y REMEDIACIÓN

En este punto se consideran los elementos básicos para la contención de un posible incidente, Backup de Información, imágenes de servidores, y cualquier información base que pueda recuperar el funcionamiento normal del sistema.

5.5 DETECCIÓN, EVALUACION Y ANÁLISIS

5.5.1 Detección Identificación y Gestión de Elementos Indicadores de un Incidente

Los indicadores son los eventos que nos señalan que posiblemente un incidente ha ocurrido generalmente algunos de estos elementos son:

- Alertas en sistemas de seguridad
- Caídas de servidores
- Reportes de usuarios
- Software antivirus dando informes
- Otros funcionamientos fuera de lo normal del sistema

La identificación y gestión de elementos que alertan sobre un incidente nos proveen información que puede alertarnos sobre la futura ocurrencia del mismo y preparar procedimientos para minimizar su impacto. Algunos de estos elementos pueden ser:

- Logs de servidores
- Logs de aplicaciones
- Logs de herramientas de seguridad
- Cualquier otra herramienta que permita la identificación de un incidente de seguridad

En la entidad debe existir un listado de fuentes generadoras de eventos que permitan la identificación de un incidente de seguridad de la información.

5.5.2 Análisis

Las actividades de análisis del incidente involucran otra serie de componentes, es recomendable tener en cuenta los siguientes:

- Tener conocimientos de las características normales a nivel de red y de los sistemas.

- Los administradores de TI deben tener conocimiento total sobre los comportamientos de la Infraestructura que están Administrando.
- Toda información que permita realizar análisis al incidente debe estar centralizada (Logs de servidores, redes, aplicaciones).
- Es importante efectuar correlación de eventos, ya que por medio de este proceso se pueden descubrir patrones de comportamiento anormal y poder identificar de manera más fácil la causa del incidente.
- Para un correcto análisis de un incidente debe existir una única fuente de tiempo (Sincronización de Relojes) ya que esto facilita la correlación de eventos y el análisis de información.
- Se debe mantener y usar una base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados, y experiencias con incidentes anteriores.
- Crear matrices de diagnóstico e información para los administradores menos experimentados.

5.5.3 Evaluación

Para realizar la evaluación de un incidente de seguridad se debe tener en cuenta los niveles de impacto con base en los insumos entregados por el análisis de riesgos y la clasificación de activos de información de la entidad.

La severidad del incidente puede ser:

- **Alto Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales del Instituto. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.
- **Medio Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.
- **Bajo Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

5.5.4 Clasificación De Incidentes De Seguridad De La Información

Algunos ejemplos de clasificación de incidentes podrían ser (esta clasificación está sujeta a cada entidad dependiendo de su infraestructura, de sus riesgos y criticidad de los activos. La clasificación dada es solo un ejemplo):

- Acceso no autorizado: Es un incidente que involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información.
- Modificación de recursos no autorizado: Un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.
- Uso inapropiado de recursos: Un incidente que involucra a una persona que viola alguna política de uso de recursos.
- No disponibilidad de los recursos: Un incidente que involucra a una persona, sistema o código malicioso que impide el uso autorizado de un activo de información.
- Multicomponente: Un incidente que involucra más de una categoría anteriormente mencionada.
- Otros: Un incidente que no puede clasificarse en alguna de las categorías anteriores. Este tipo de incidentes debe monitorearse con el fin de identificar la necesidad de crear nuevas categorías.

5.5.5 Priorización De Los Incidentes Y Tiempos De Respuesta

Con el fin de permitir una atención adecuada a los incidentes (análisis, contención y erradicación) se debe determinar el nivel de prioridad del mismo, y de esta manera atenderlos adecuadamente según la necesidad.

A manera de ejemplo se definen una serie de variables que podrán ser utilizadas para realzar la evaluación de los incidentes

- Prioridad
- Criticidad de impacto
- Impacto Actual
- Impacto Futuro

Nivel de Prioridad: Depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados.

Nivel Criticidad	Valor	Definición
Inferior	**0,10**	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	**0,25**	Sistemas que apoyan a una sola dependencia o proceso de una entidad.
Medio	**0,50**	Sistemas que apoyan más de una dependencias o proceso de la entidad.
Alto	**0,75**	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	**1,00**	Sistemas Críticos.

Tabla 1: Niveles de Criticidad de Impacto

Impacto Actual: Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

Impacto Futuro: Depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

Nivel Impacto	Valor	Definición
Inferior	**0,10**	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo.
Bajo	**0,25**	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo.
Medio	**0,50**	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo.

Alto	**0,75**	Impacto moderado en uno o más componentes de más de un sistema de información.
Superior	**1,00**	Impacto alto en uno o más componentes de más de un sistema de información.

Tabal 2: Niveles de Impacto Actual y Futuro

Luego de tener definidas las variables se obtiene la *prioridad* mediante la siguiente formula:

Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)

Y los resultados obtenidos se deben compara con la siguiente tabla para determinar la prioridad de atención:

Nivel Prioridad	Valor
Inferior	**00,00 – 02,49**
Bajo	**02,50 – 03,74**
Medio	**03,75 – 04,99**
Alto	**05,00 – 07,49**
Superior	**07,50 – 10,00**

Tabla 3: Niveles de Prioridad del Incidente

5.5.6 Tiempos de Respuesta

Para el caso de la atención de incidentes de seguridad se ha establecido unos tiempos máximos de atención de los mismos, con el fin de atender adecuadamente

los incidentes de acuerdo a su criticidad e impacto. Los tiempos expresados en la siguiente Tabla son un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso.

Nivel Prioridad	Tiempo de Respuesta
Inferior	**3 horas**
Bajo	**1 hora**
Medio	**30 min**
Alto	**15 min**
Superior	**5 min**

Tabla 4: Tiempos Máximos de Atención de Incidentes

Cabe resaltar que cada entidad está en la libertad de definir tiempos de atención a incidentes como crean conveniente y dependiendo de la criticidad de los activos impactados.

5.5.7 Declaración y Notificación de Incidentes

Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad.

La notificación de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información y la interrupción de los servicios, y el proceso de tratamiento de incidentes, y manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

A continuación se describe un proceso de notificación de incidentes de seguridad que podría ser adoptado por la entidad:

Un usuario, tercero o contratista que sospeche sobre la materialización de un incidente de seguridad deberá notificarlo al primer punto de contacto definido por la entidad (Ej: Soporte de primer nivel). El incidente puede ser notificado a través de cualquier canal de comunicación (Telefónico, Correo, Aplicativo) es importante resaltar que debe existir un formato el cual el usuario que reporta el incidente debe diligenciar con la mayor cantidad posible de información relacionada con el incidente.

El primer punto de contacto identificará el tipo de incidente (de acuerdo a la tabla de clasificación de incidentes que realiza la entidad). Analizará si el incidente reportado corresponde a un incidente de seguridad de la información o está relacionado con requerimientos propios de la infraestructura de TI. En caso de ser catalogado como un incidente de seguridad se notificarán a la persona encargada de la atención de incidentes o a quien haga sus veces para que tome las decisiones correspondientes. El primer punto de contacto será el encargado de realizar el seguimiento del Incidente hasta su cierre definitivo.

Si el incidente de seguridad es identificado por otra línea diferente a un usuario de la entidad, a través de los elementos de detección o administradores de TI, este es notificado directamente a la persona encargada de atención de incidentes quien tomará las acciones necesarias de atención. Se notificará al primer punto de contacto sobre la presentación de un incidente de seguridad para que realice la documentación respectiva y esté atento al seguimiento y desarrollo del mismo.

El punto de contacto clave dentro de la gestión de incidentes es la persona encargada de la atención de los mismos, el cual se encarga de coordinar y asignar las actividades con las partes interesadas. Estos últimos se encargan de solicitar el apoyo a las personas involucradas con el proceso con el fin de la correcta ejecución de actividades que den solución al incidente.

La persona encargada de la atención de incidentes tendrá la potestad para decidir sobre las acciones que se deban ejecutar ante la presencia de un incidente de seguridad y es la persona que notificará a las altas directivas de la entidad.

5.6 CONTENCIÓN ERRADICACIÓN Y RECUPERACIÓN

Es importante para la entidad implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

Esta fase se descompone claramente en tres componentes

Contención: esta actividad busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI, para facilitar esta tarea la entidad debe poseer una estrategia de contención previamente definida para poder tomar decisiones por ejemplo: apagar sistema, desconectar red, deshabilitar servicios.

Ejemplos de estrategias de contención a incidentes

Incidente	Ejemplo	Estrategia de contención
Acceso no autorizado	Sucesivos intentos fallidos de login	Bloqueo de cuenta
Código Malicioso	Infección con virus	Desconexión de la red del equipo afectado
Acceso no autorizado	Compromiso del Root	Apagado del sistema
Reconocimiento	**Scanning** de puertos	Incorporación de reglas de filtrado en el firewall

La estrategia de contención varía según el tipo de incidente y los criterios deben estar bien documentados para facilitar la rápida y eficaz toma de decisiones. Algunos criterios que pueden ser tomados como base son:

- Criterios Forenses
- Daño potencial y hurto de activos
- Necesidades para la preservación de evidencia
- Disponibilidad del servicio
- Tiempo y recursos para implementar la estrategia
- Efectividad de la estrategia para contener el incidente (parcial o total)
- Duración de la solución

Erradicación y Recuperación: Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el administrador de TI o quien haga sus veces deben restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro.

Ejemplos de estrategias de erradicación de incidentes

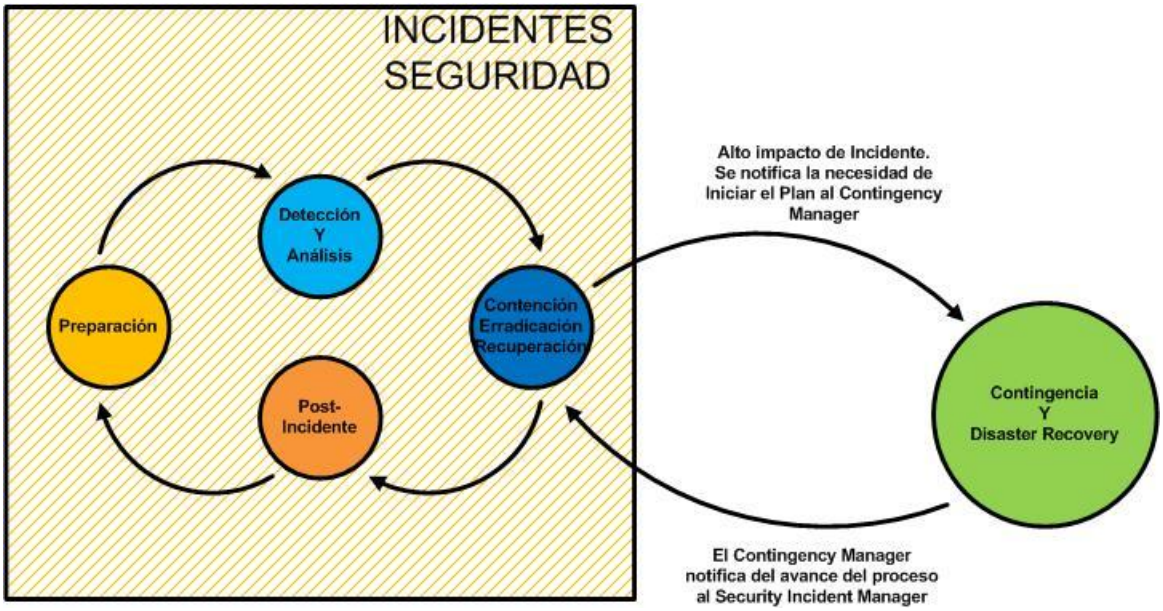
Incidente	Ejemplo	Estrategia de erradicación
DoS (denegación de servicio)	SYN Flood	Restitución del servicio caído
Virus	Gusano en la red	Corrección de efectos producidos. Restauración de backups
Vandalismo	Defacement a un sitio web	Reparar el sitio web
Intrusión	Instalación de un rootkit	Reinstalación del equipo y recuperación de datos

Ejemplos de estrategias de recuperación de incidentes

Incidente	Ejemplo	Estrategia de recuperación
DoS (denegación de servicio)	SYN Flood	Restitución del servicio caído
Virus	Gusano en la red	Corrección de efectos producidos. Restauración de Backups
Vandalismo	Defacement a un sitio web	Reparar el sitio web

Intrusión	Instalación de un Rootkit	Reinstalación del equipo y recuperación de datos

En algunas ocasiones durante el proceso de Atención de Incidentes de Seguridad Informática específicamente en la fase de "Contención, Erradicación y Recuperación" se puede hacer necesario activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres) en el caso que un incidente afecte gravemente a un determinado sistema.



Integración del Proceso de Atención de Incidentes de Seguridad con el Proceso de Contingencia y Disaster Recovery.

5.7 ACTIVIDADES POST-INCIDENTE

Las actividades Post-Incidente básicamente se componen del reporte apropiado del Incidente, de la generación de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias así como el registro en la base de conocimiento para alimentar los indicadores.

5.7.1 Lecciones Aprendidas:

Una de las partes más importantes de un plan de respuesta a incidentes de TI es la de aprender y mejorar. Cada equipo de respuesta a incidentes debe evolucionar para reflejar las nuevas amenazas, la mejora de la tecnología, y las lecciones aprendidas. Mantener un proceso de "lecciones aprendidas" después de un incidente grave, y periódicamente después de los incidentes menores, es sumamente útil en la mejora de las medidas de seguridad y el proceso de gestión de incidentes

Mantener un adecuado registro de lecciones aprendidas permite conocer:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Los procedimientos documentados.
- Si se tomaron las medidas o acciones que podrían haber impedido la recuperación.
- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
- Acciones correctivas pueden prevenir incidentes similares en el futuro.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

El proceso de lecciones aprendidas puede poner de manifiesto la falta de un paso o una inexactitud en un procedimiento y son un punto de partida para el cambio, y es precisamente debido a la naturaleza cambiante de la tecnología de la información y los cambios en el personal, que el equipo de respuesta a incidentes debe revisar toda la documentación y los procedimientos para el manejo de incidentes en determinados intervalos.

6. ROLES Y PERFILES NECESARIOS PARA LA ATENCIÓN DE INCIDENTES

A continuación presentaremos una descripción de los actores que intervienen y conforman el proceso de atención de Incidentes, para cada actor se presentará una breve descripción sobre su perfil y la función dentro del proceso de respuesta a Incidentes de Seguridad de la información.

Usuario Sensibilizado: Es un empleado, empleados de firmas contratista o terceros con acceso a la infraestructura de la entidad, quien debe estar educado y concientizado sobre las guías implementadas sobre la seguridad de la información y en particular la guía de atención de incidentes, estos usuarios serán muchas veces quienes reporten los problemas y deberán tener en cuenta lo siguiente:
Agente Primer Punto de Contacto: Es el encargado de recibir las solicitudes por parte de los usuarios sobre posibles incidentes también debe registrarlos en la base de conocimiento y debe ser el encargado de escalarlos a la persona encargada de la atención de incidentes. Este Agente debe contar adicionalmente con capacitación en Seguridad de la Información (con un componente tecnológico fuerte) y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes. Adicionalmente debe contar con una capacitación básica en técnicas forenses, específicamente en recolección y manejo de evidencia, lo cual involucra fundamentalmente dos aspectos.

- Admisibilidad de la evidencia: si la evidencia se puede utilizar o no en una corte
- Peso de la evidencia: la calidad y cabalidad de la evidencia.

Este no es un actor que realiza la centralización de los incidentes reportados por los usuarios, da un tratamiento inicial y escala el incidente para que sea tratado.

Administrador del Sistema: se define como la persona encargada para configurar y mantener un activo informático. También debe ser notificado por el agente de primer punto de contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al agente de primer punto de contacto sobre el incidente la solución del mismo. Se recomienda que los administradores cuenten con capacitación en Seguridad de la Información (con un componente tecnológico fuerte no solo en su plataforma si no en Redes y erradicación de vulnerabilidades) y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes. Adicionalmente debe contar con una capacitación en técnicas forenses, específicamente en recolección y manejo de evidencia.

Administrador de los sistemas de Seguridad: Personas encargadas de configurar y mantener un activo informático relacionado con la seguridad de la plataforma ej. Firewall, Sistemas de Prevención de Intrusos, Routers, Sistemas de Gestión y Monitoreo. También debe ser notificado por el agente de primero contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al agente de primer contacto sobre el incidente y la solución del mismo. Se recomienda que los administradores de esta tecnología sean expertos en Seguridad de la Información (con un componente tecnológico fuerte en Redes y erradicación de vulnerabilidades, Ethical Hacking y técnicas forenses) y debe conocer perfectamente la clasificación de Incidentes de la entidad.

Analista Forense: Es un experto en el tema forense, quien debe estar disponible en caso de que un incidente de impacto alto (o uno que amerite acciones disciplinarias o legales o investigación profunda) requiera una investigación completa para solucionarlo y determinar los siguientes Ítems

- Que sucedió.
- Donde sucedió.
- Cuando Sucedió.
- Quien fue el Responsable.
- Como sucedió.

Este actor debe ser un apoyo para los demás actores en caso de dudas sobre los procedimientos y debe ejercer un liderazgo técnico en el proceso de atención de Incidentes de seguridad de la información.

Líder del Grupo de Atención de Incidentes: Responde a las consultas sobre los incidentes de seguridad que impacten de forma inmediata, y es el encargado de revisar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para poder ser presentados a los directivos. El Líder Grupo de Atención de Incidentes estará en la capacidad de convocar la participación de otros funcionarios de la organización cuando el incidente lo amerita (Prensa y Comunicaciones, Gestión de Talento Humano, Gestión Jurídica, Tecnología, Representante de las Directivas para el SGSI).

También debe estar al tanto del cumplimiento de los perfiles mencionados y de revisar el cumplimiento de los procedimientos y mejores prácticas, así como también de los indicadores de gestión, y en capacidad de disparar si lo amerita planes de contingencia y/o continuidad.

Finalmente el Líder del Grupo de Atención de Incidentes será el responsable del modelo de Gestión de incidentes y debe estar en la capacidad de revisar todos los

incidentes de seguridad y los aspectos contractuales que manejan el outsourcing del servicio help desk.

7. RECOMENDACIONES FINALES Y A QUIÉN DEBO INFORMAR

1. Verificar la existencia y disponibilidad del levantamiento de información, relativa a los servicios de soporte de la infraestructura tecnológica de la entidad, incluyendo contactos de proveedores de servicios de alojamiento (hosting), gestión de contenidos en línea, disponibilidad de personal de soporte técnico, encargados de tecnología y seguridad informática, con el fin de garantizar un oportuno contacto en caso de incidentes.

2. Coordinar con los responsables de soporte técnico, que éstos hayan ejecutado o ejecuten con prontitud, todas las acciones que se requieran para asegurar y fortalecer los componentes de tecnologías de la información mencionados en la etapa de ***preparación***. Dichas acciones contemplan verificación de usuarios y claves de acceso, actualizaciones de sistemas operativos y software de plataformas de servicios de base y gestión de contenidos, entre otros. Cualquier ejercicio de auditoria o verificación del cumplimiento de este tipo de actividades será de mucha utilidad.

3. Actualizar todos los datos de contacto relativos al nombre de dominio de la entidad, de tal forma que queden reflejados en el servicio público de información de registros de nombres de dominio WHOIS.CO. Esta información es de suma importancia para contactar a la entidad, en caso de presentarse un incidente.
   Cabe aclarar que, según lo indicado en el ***artículo 5 de la Resolución 1652 del 2008***, cuando el Registrante o titular de un nombre de dominio bajo ".CO" suministre información "falsa, incorrecta o inexacta", el nombre de dominio podrá ser suspendido e incluso dado de baja.
   Si se requiere información para realizar dicha actividad de actualización, favor ingresar a la página http://www.cointernet.com.co/panel-de-control o comunicarse al siguiente número telefónico en Bogotá 6169961.

4. En el evento de que algún componente de la infraestructura tecnológica (sitios Web, aplicaciones, servicios en línea, sistemas de información, entre otros) de la Entidad, haya sido vulnerado o comprometido, reportar en primera instancia al ColCERT (***Grupo de Respuesta a Emergencias Cibernéticas de Colombia***) por medio de correo electrónico a:contacto@colcert.gov.co o al Teléfono: (+571) 2959897.

En SEGUNDA instancia, adoptar las medidas y acciones necesarias para mitigar y resolver el incidente con el apoyo del personal encargado de la gestión de incidentes de la entidad, teniendo en cuenta la relevancia de ejecutar todos los procedimientos técnicos y operativos que faciliten la conservación (preservación) de las evidencias de naturaleza digital y soportes del incidente, fundamentales para tramitar su posterior judicialización ante la autoridad competente.

5. Cuando se tenga evidencia de un incidente informático, la entidad afectada se pondrá en contacto con el Cai Virtual de la Policía Nacional www.ccp.gov.co, Centro Cibernético Policial de la Policía Nacional al teléfono 4266900 ext. 104092, para recibir asesoría del caso en particular y posterior judicialización.
   Es importante aclarar que solamente, en caso de lograrse un contacto exitoso, y tras establecerse de común acuerdo que el incidente pone en riesgo la estabilidad, seguridad y resiliencia del sistema de nombres de dominio, así como de otras entidades involucradas en el hecho, e incluso la reputación de la entidad, el responsable de la misma podrá solicitar, a través de un correo electrónico, se suspenda temporalmente el nombre de dominio mientras se gestiona internamente el incidente. Para el efecto, la comunicación deberá ser remitida desde cualquiera de las direcciones registradas en el WHOIS con destino al CCP de la Policía Nacional indicando motivo/situación detallada de afectación y solicitando de manera expresa asumiendo plena/total responsabilidad por las consecuencias técnicas/operacionales (sistema de correo, aplicaciones en línea bajo el dominio, etc.) de dicha acción solicitada. Dicho mensaje deberá incluir la información de contacto telefónico del remitente para realizar su respectiva validación y proceder de conformidad.