Control de cambios

Versión	Fecha	Descripción de la modificación
01	20 de diciembre de 2022	Versión inicial del procedimiento donde se establece la metodología, actividades, criterios y condiciones de gestión de incidentes de seguridad de la información, evidenciados en la Secretaría Distrital de Gobierno.

Método de Elaboración	Revisa	Aprueba
Se realizó la construcción del documento, por parte de la Dirección de Tecnologías e Información mediante mesas de trabajo, en las cuales participaron los profesionales del grupo y el analista del proceso de la OAP.	Orlando Benavides Santacruz **Dirección de Tecnologías e Información** Angela Patricia Cabeza Morales **Profesional OAP – Analista del proceso**	Martha Liliana Soto Iguarán **Subsecretaría de Gestión Institucional** Documento revisado y aprobado mediante caso aplicativo Hola No. **283454**

1. INFORMACIÓN GENERAL

Objetivo del Procedimiento

Establecer la metodología, las actividades, criterios y condiciones para la gestión de incidentes de seguridad de la información, necesarios para el manejo y control de situaciones o eventos relacionados con la seguridad de la información que se lleguen a presentar en la Secretaría Distrital de Gobierno, con el fin de dar una solución oportuna y eficaz por parte del personal involucrado.

Alcance

Aplica para todos los activos de información de la Secretaría Distrital de Gobierno y de los elementos de infraestructura tecnológica de la organización, que sean afectados por incidentes de seguridad de la información y debe ser de obligatorio cumplimiento por parte de todos los funcionarios, contratistas, proveedores y/o terceros vinculados a la Entidad. Contempla las diferentes etapas de un incidente de seguridad de la información: Evaluar, Analizar, Contener, Recuperar y Documentar.

Responsable

Director(a) de Tecnologías e Información

Políticas de operación

1. La Dirección de Tecnologías e Información en conjunto con la Mesa de servicios, son los encargados de coordinar las acciones conjuntas con las partes interesadas para una atención oportuna y eficaz de los incidentes de seguridad de la información reportados.

2. El manejo de incidentes de seguridad de la información, en general se atenderá de acuerdo con lo establecido en el presente procedimiento. Para un mayor detalle sobre la priorización y categorización de Incidentes de seguridad de la Información se debe revisar el Instructivo GDI-TIC-IN020.

3. Los servidores públicos, contratistas y terceros que tengan relación con la Secretaría Distrital de Gobierno deben reportar eventos e incidentes de seguridad de la información sí se llegaran a presentar, y/o las debilidades que se identifiquen en la operación de la Entidad y que puedan afectar la prestación de los servicios y/o afecten la operación diaria de la entidad, en la herramienta de gestión de servicios TI vigente.

4. Si se sospecha que ha ocurrido alguna intrusión no autorizada, se deben aislar y no utilizar los recursos afectados de tal forma que se dé aviso inmediatamente al responsable de Seguridad de la Información

o quien haga sus veces en la entidad, de esta forma se preservará la evidencia y se realizará la correcta cadena de custodia. Los incidentes de seguridad de la información descubiertos por dispositivos de monitoreo y escaneo, deberán ser comunicados directamente al propietario del Activo de Información o el administrador de recursos y registrarlo en la herramienta de gestión de servicios TI vigente en la Entidad, para que allí se evalué la falla o el incidente presentado, para así mismo determinar cuál es el proceso a seguir dentro de la Entidad así como también determinar los especialistas de TI que se requieran en cada uno de los frentes de la Secretaria Distrital de Gobierno.

5. Si existiera un incidente de seguridad de la información en un sistema o aplicación de la Entidad, este deberá ser analizado para asegurar que cualquier vulnerabilidad residual del evento presentado, se elimine. Los incidentes de seguridad de la información no deberán ser dados a conocer públicamente, sin autorización del Director de Tecnologías e Información.

6. Cuando una acción de seguimiento contra una persona u organización, después de un incidente de Seguridad de la Información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar ante las autoridades competentes, con la debida cadena de custodia. En el evento de que algún componente de seguridad en la infraestructura tecnológica (sitios web, aplicaciones, servicios en línea, sistemas de información, entre otros) de la Secretaria Distrital de Gobierno, haya sido vulnerado o comprometido en un nivel medio, alto o superior, se debe reportar en primera instancia al CSIRT Gobierno de MINTIC (Grupo de Respuesta a Incidentes Informáticos para entidades del Gobierno de Colombia) por medio de los canales de comunicación establecidos, seguido al ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) por medio del correo electrónico contacto@colcert.gov.co , adicionalmente al CSIRT Distrital por medio del email csirtdc@alcaldiabogota.gov.co y dado el caso de contar con evidencias criminales de un incidente de seguridad de la información, se reporta al Centro Cibernético Policial de la Policía Nacional, para recibir asesoría del caso en particular.

7. Cuando un incidente de seguridad de la información requiere ser denunciado a los entes de control nacional, éste debe remitirse mediante comunicación oficial a través del Sistema de Información de la entidad para poner en conocimiento la situación y la evaluación de las medidas a tomar institucionalmente.

8. 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 (GDI-TIC-M002 Plan de Continuidad TI) en el caso que un incidente afecte gravemente a un determinado servicio tecnológico que tiene gestión de la continuidad en la Secretaría Distrital de Gobierno.

2. METODOLOGÍA DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La gestión de incidentes de seguridad de la información se desarrolla a través de una serie de etapas, que tienen como fin generar información útil para la toma de decisiones basadas en hechos que ayuden a mejorar la estrategia de seguridad de la información como se indica en la Ilustración 1.

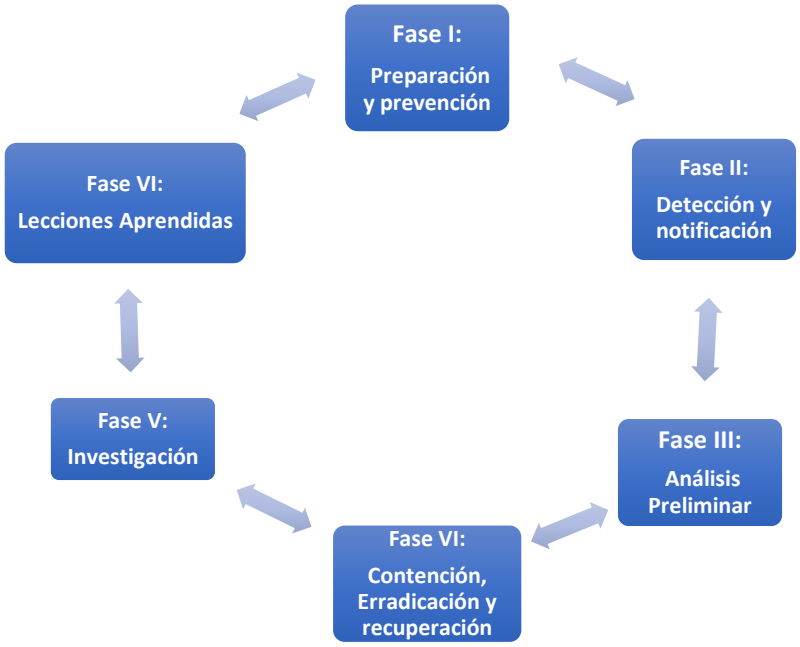


Ilustración 1. Metodología de la gestión de Incidentes de Seguridad de la información

2.1. PREPARACIÓN Y PREVENCIÓN

Prioridades de tratamiento de incidentes de seguridad de la información

En la primera fase se debe actuar para reducir los efectos reales y potenciales de un incidente de seguridad de la información, en pro de mitigar su impacto en la Entidad. Así mismo, se debe tener en cuenta que la respuesta exacta dependerá de la naturaleza del incidente al que se enfrente. No obstante, se contemplan las siguientes prioridades como punto de partida:

- ✓ Proteger la vida humana y la seguridad de las personas: esta debe ser siempre la máxima prioridad.
- ✓ Proteger los activos de información pública clasificada y publica reservada: los activos de información pública clasificada y publica reservada son los más relevantes para la Secretaría

Distrital de Gobierno, los cuales deben contar con controles robustos con el fin de preservar la confidencialidad, integridad y disponibilidad de estos.

- ✓ Proteger otra información relevante (propiedad intelectual o del ámbito directivo): dentro del entorno laboral hay otra información que también puede ser valiosa y debe ser protegida donde se dará prioridad en primer lugar a los datos más valiosos antes de pasar a otros de baja prioridad.
- ✓ Minimizar la indisponibilidad de los servicios informáticos: aunque el tiempo de producción sea muy importante en la mayoría de los entornos, el hecho de mantener los sistemas en funcionamiento durante un incidente puede tener como consecuencia problemas más graves en el futuro. Por este motivo, la minimización de la interrupción de los recursos informáticos debe ser generalmente una prioridad relativamente baja.
- ✓ Proteger el hardware y software de la Secretaría Distrital de Gobierno: esto incluye protegerlos contra pérdida y/o modificación de los archivos del sistema y contra daños físicos al hardware. Los daños en los servicios tecnológicos pueden tener como consecuencia una alta indisponibilidad o tiempo de inactividad.

Existen varias medidas que se pueden tomar para contener el daño y minimizar el riesgo en el entorno. Como mínimo, se deben llevar a cabo las siguientes acciones:

- ✓ Determinar los puntos de acceso usados por posibles atacantes e implementar las medidas adecuadas para evitar futuros accesos desautorizados.
- ✓ Evitar que los posibles atacantes conozcan las actividades que se adelanten dentro del tratamiento del incidente de seguridad de la información.
- ✓ Comparar el impacto de dejar sin conexión los sistemas en peligro y los sistemas relacionados con el riesgo de continuar funcionando.
- ✓ Considerar la opción de volver a crear un sistema con discos duros nuevos (se deben eliminar los discos duros existentes y almacenarlos, ya que se pueden usar como evidencias si se decide procesar a los posibles atacantes).
- ✓ Asegurar el cambio de las contraseñas locales, de las cuentas de aplicativos y cuentas administrativas en todo el entorno.

En esta etapa se disponen los elementos necesarios para registrar y clasificar correctamente los incidentes de seguridad de la información, de forma que, en su futuro esta información sea el insumo para desarrollas estrategias para nuevos incidentes.

También debe estar apoyada por todo el equipo de la Dirección de Tecnologías e Información, adoptando las buenas prácticas para el aseguramiento de redes, sistemas y aplicaciones. Es importante que se tengan en cuenta las siguientes disposiciones:

- ✓ Los parches de seguridad en sistemas operativos, bases de datos, aplicaciones u otro software que lo amerite, deben ser revisados y desplegados por lo menos una vez cada tres meses.
- ✓ Para el aseguramiento de plataforma se debe configurar la menor cantidad de servicios con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos.
- ✓ Se debe realizar la revisión de las configuraciones default (usuarios, contraseñas y archivos compartidos), por lo menos una vez cada cuatro meses.

- ✓ Es indispensable que para cada recurso que pueda ser accedido por externos e internos se despliegue alguna advertencia de manejo de información.
- ✓ Los servidores deben tener activo el log de eventos.
- ✓ Se debe tener una gestión constante sobre los elementos de seguridad, las reglas configuradas en los equipos de seguridad (Firewall, Waf, authenticator) deben ser revisadas continuamente.
- ✓ Las firmas y actualizaciones de los IDS o IPS deben estar al día.
- ✓ Todos los elementos de red y de seguridad deben estar sincronizados y sus logs deben ser analizados por el equipo de seguridad informática.
- ✓ Todos los equipos de infraestructura (Servidores – físicos, virtuales, equipos de cómputo) deben tener activo el antivirus con las firmas de actualización al día.
- ✓ Todos los equipos de infraestructura y de cómputo deben estar sincronizados con el reloj oficial al interior de la Entidad.

Recursos de comunicación

Se debe tener información de contacto para el escalamiento de incidentes:

- ✓ 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.
- ✓ Contacto del área de recursos humanos y oficina de asuntos disciplinarios o quien realice sus funciones (cuando amerite acciones disciplinarias).
- ✓ Contacto de áreas interesadas o grupos de interés (CCP- Policía Nacional, fiscalía, CSIRT, CSIRD Distrital, COLCERT, entre otras).

2.2. DETECCIÓN Y NOTIFICACIÓN

En la segunda fase, las siguientes son fuentes de detección de eventos:

- ✓ Todos los servidores públicos, contratistas y/o terceros de la Secretaría Distrital de Gobierno son responsables de reportar cuando observen situaciones inusuales, violaciones sobre los activos de información o se detecten vulnerabilidades de seguridad de la información, en la herramienta de gestión TI vigente en la Entidad. En el caso de los terceros, estas situaciones la reportarán al supervisor del contrato.
- ✓ Los eventos inusuales o anómalos detectados por la Mesa de servicios o por el área de infraestructura deben ser escalados y reportados en la herramienta de gestión TI, vigente en la Entidad.
- ✓ También deben ser tenidas en cuenta las alertas automáticas de eventos de seguridad de la información generadas por:
  - Alertas de Software: sistemas de detección y prevención de intrusiones IDS/ISP, antivirus y sistemas de monitoreo de servicios.

- Logs: de sistemas operativos, dispositivos de red y aplicaciones
- Información pública: nuevas vulnerabilidades y *exploits*, sitios web y listas de correo de profesionales donde se comparten experiencias de incidentes en distintas organizaciones.
- Personal: es responsabilidad de los funcionarios, contratistas y terceros informar a la Mesa de servicios de la Secretaría Distrital de Gobierno de cualquier evento de riesgo materializado o posible incidente, una vez sea detectado.

2.3. ANÁLISIS PRELIMINAR

En la tercera fase es importante que la persona que recibe la solicitud por el incidente de seguridad de la información trate de recolectar con la mayor precisión posible y determinar lo siguiente:

- ✓ ¿Es un evento de seguridad o Incidente?
- ✓ Alcance ¿Qué activos de la información afecta? (redes, sistemas, documentos, aplicaciones, personas u otros)
- ✓ ¿Qué originó el acontecimiento?
- ✓ Cómo ocurrió (o está ocurriendo) el evento, incidente; qué método, qué herramienta, qué vulnerabilidad se explotó, entre otras.
- ✓ El impacto potencial en las actividades de la Entidad.

Una vez sea registrado, se asigna el Evento o Incidente de seguridad al especialista de seguridad de la información, quien debe evaluar la información recibida o asociada al caso reportado y confirmar si se debe clasificar como un evento o se debería clasificar como un incidente de seguridad de la información, teniendo en cuenta:

- ✓ La validación de la situación reportada. Si existen dudas debe contactarse la persona que reportó el evento.
- ✓ Es necesario contestar las preguntas: ¿Cómo fue causado? ¿quién, o qué lo originó?
- ✓ Validar los activos, infraestructura tecnológica, servicios, información o procesos afectados o que se podrían afectar.
- ✓ Validar si se determina que el evento evaluado es un incidente de seguridad de la información, de ser así, el especialista de seguridad de la información debe generar la clasificación del incidente considerando los siguientes tres factores:

  - Categoría del incidente
  - Impacto del incidente.
  - Prioridad.

Responsabilidad en la atención de incidentes

Los incidentes de seguridad de la información deben ser atendidos por los administradores de los sistemas afectados (Infraestructura y sistemas de información) y de ser necesario, con el apoyo del personal de la

Mesa de Servicios. Si la atención del incidente requiere medidas adicionales a las establecidas en este manual, se deben coordinar con el responsable de Seguridad de la Información en la Entidad.

Los incidentes de alto impacto que sean causados por funcionarios de la Entidad, en primera instancia deben ser escalados a la Oficina de Asuntos Disciplinarios, en el caso que sean originados por los colaboradores, se remitirán a la respectiva área Jurídica o de contratos, para su evaluación y respectiva sanción.

En caso de que la conducta desarrollada por el servidor público o contratista esté tipificada como delito informático a la luz de la ley penal colombiana, será decisión del Representante Legal instaurar la denuncia correspondiente ante la autoridad competente. En el caso de Incidentes de Seguridad ocasionados por terceros se aplicará el mismo procedimiento descrito anteriormente ante la Autoridad competente.

2.4. CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

En la cuarta fase, la contención, erradicación y recuperación se basa en las siguientes acciones:

- ✓ Las estrategias de Contención de incidentes varían dependiendo del tipo de incidente e impacto previsible en la Entidad, puede ser necesario tomar decisiones como deshabilitar servicios, apagar sistemas o desconectar equipos de red antes de que el impacto pueda extenderse en la entidad.
- ✓ Una vez ha sido realizada la contención del incidente, se debe verificar si es necesario eliminar o limpiar componentes asociados al incidente y proceder con la recuperación de la situación de operación normal en la Entidad.
- ✓ En las actividades de erradicación se realizará la eliminación de los componentes asociados al incidente y otras actividades que se consideren adecuadas para resolver el incidente o prevenir futuras ocurrencias.
- ✓ Las actividades habituales de erradicación son la instalación de parches de seguridad, cambio de reglas en el Firewall o de listas de acceso en dispositivos de red.
- ✓ Las actividades de recuperación pueden incluir acciones como recuperar sistemas completos, restaurar backups, reemplazar componentes afectados con versiones desinfectadas, instalar versiones de software, cambiar contraseñas o reforzar el perímetro de red revisando configuraciones del firewall.

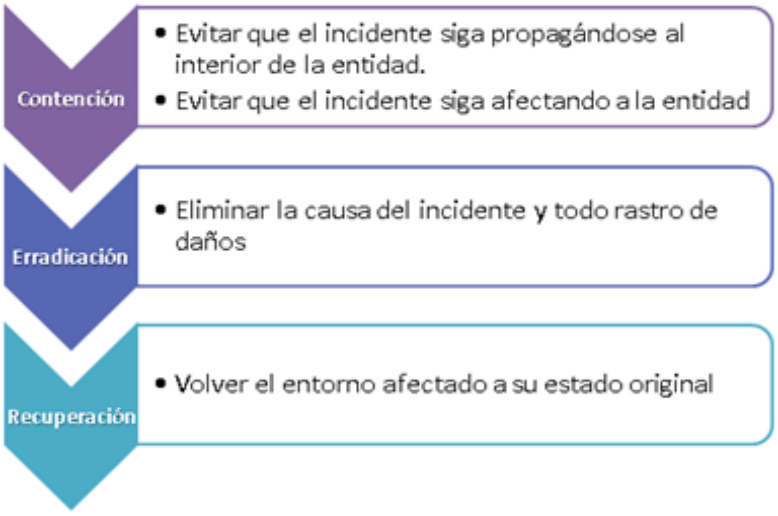


Ilustración 2. Contención, Erradicación y Recuperación

2.5. INVESTIGACIÓN

En la quinta fase, una vez el incidente de seguridad de la información haya sido tratado, el grupo de seguridad de la información y los diferentes participantes deben investigar de forma detallada y rápida de los eventos que se detecten para realizar seguimiento de las causas e implicaciones de dichos sucesos. El grupo de seguridad debe obrar de forma imparcial y responsable durante la investigación que realice para identificar las causas y registrar las consecuencias asociadas a los eventos o incidentes detectados.

Recolección de datos

Como parte del proceso de investigación se debe realizar una debida recolección de datos, teniendo en cuenta el incidente de seguridad de la información si es necesario:

- ✓ Información basada en Host
- ✓ Live Data Collection – Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la placa de red.
- ✓ Forensic duplication – Backups, archivos copiados recientemente, etc.
- ✓ Información basada en Red.
- ✓ Información recolectada mediante sniffers, logs de routers, logs de firewall, información de servidores de autenticación.
- ✓ Testimonio personal.

Recolección de evidencia

Se deben recoger evidencias de los incidentes de seguridad de la información, para su utilización con fines de análisis y como posibles pruebas en caso de ser requeridas para el inicio de acciones legales. Las evidencias

pueden ser sistemas de información (ficheros, imágenes de discos, equipos) o cualquier otra que se considere relevante para el análisis del incidente o para inicio del procedimiento legal.

Los aspectos a tener en cuenta en el momento de recolectar evidencia son los siguientes:

- ✓ Autenticidad: quien haya recolectado la evidencia debe poder probar que es autentica.
- ✓ Cadena de custodia: debe existir un registro detallado del tratamiento de la evidencia, incluyendo quiénes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometen la misma.
- ✓ Validación: garantizar que la evidencia recolectada es la misma que se presenta.

Actividades posteriores

- ✓ Organizar reuniones de autoevaluación: Se realiza un estudio de recapitulación analizando las características de los incidentes, impacto y acciones emprendidas para la detección, análisis y recuperación.
- ✓ Actualizar la documentación: será responsabilidad de todos los involucrados actualizar la documentación de procesos, instructivos de usuario, entre otros, de acuerdo con los hallazgos del incidente.
- ✓ Crear base de conocimiento: los nuevos conocimientos adquiridos a través del tratamiento del incidente se registran en la base de conocimiento de la herramienta de gestión TI o en el lugar indicado por la Dirección de Tecnologías e Información.
- ✓ Proponer mejoras y estrategias que permitan:
    - Detectar nuevas amenazas
    - Implementar controles que mitiguen los riesgos asociados
    - Implementar controles que prevengan riesgos asociados
    - Implementar controles que detengan riesgos asociados

2.6. LECCIONES APRENDIDAS

En la sexta fase se busca mejorar continuamente el esquema de gestión de incidentes de seguridad de la información a través de la identificación y el aprendizaje de las lecciones recibidas del manejo de los incidentes de seguridad. Igualmente se pretende limitar la frecuencia de incidentes recurrentes, identificar de manera temprana o evitar futuros incidentes. Una vez cerrado el incidente de seguridad de la información el responsable de seguridad de la información debe actualizar la Base de datos de eventos/incidentes de seguridad de la información o similar, documentando la categoría del incidente, el impacto, las acciones de atención ejecutadas y la evaluación del costo del incidente.

Con base en la información recopilada de los incidentes, el responsable de seguridad de la información debe:

- ✓ Analizar las tendencias o patrones que permitan identificar los incidentes recurrentes.

- ✓ Evaluar si la frecuencia con la cual se presentan cierto tipo de incidentes se debe a la deficiencia o ausencia de controles.
- ✓ A partir del análisis anterior se debe modificar o implementar nuevos controles que permitan evitar incidentes futuros o limitar la frecuencia (controles técnicos, controles físicos, refuerzos en la toma de conciencia de seguridad al interior de la organización, actualización de directrices o normas).
- ✓ Evaluar la eficacia de los procedimientos para la detección, reporte y atención de cada incidente de seguridad de la información.
- ✓ Analizar los tiempos de respuestas de los incidentes.
- ✓ Validar si el plan de recuperación de desastres y si los backups fueron efectivos.

Evaluación del costo de los incidentes de seguridad

Se debe determinar el costo aproximado del incidente teniendo en cuenta los siguientes criterios:

- ✓ Costos debidos a la pérdida de la ventaja competitiva por la divulgación de información confidencial.
- ✓ Pérdida de la reputación o de la confianza del cliente.
- ✓ Costos relacionados con el tiempo de indisponibilidad de los sistemas de información.
- ✓ Costos por reparación de acuerdo con actualización, reinstalación de software/hardware la recuperación de datos.
- ✓ Costos asociados con las remediaciones de vulnerabilidades de las plataformas tecnológicas o aplicaciones.
- ✓ Costos derivados de la pérdida o robo de equipos.
- ✓ Costos por los procesos de selección y capacitación de personal cuando la medida disciplinaria del incidente involucra despido y por consiguiente contratación de nuevo personal.
- ✓ Costos asociados a las acciones disciplinarias que conllevan suspensión temporal del personal.
- ✓ Interrupción en la prestación de los servicios.
- ✓ Multas impuestas por los clientes.

OPCIONES DE VALOR	EJEMPLO
Costo tiempo de tratamiento del incidente	Se debe tomar el promedio salarial de los profesionales dedicados al servicio y de acuerdo con el tiempo utilizado se toma dicho costo, teniendo en cuenta que la jornada laboral es de ocho (8) horas. Ejemplo: promedio salarial de $100 hora, durante el tratamiento del incidente se tomó 1 hora a tres de ellos, para un total de $300.

Costo Categoría	Se promedia el valor de los incidentes pertenecientes a la misma categoría. Ejemplo: costo incidente-2 igual a $ 100, costo incidente-3 igual a $200, por lo tanto, el promedio y valor por categoría es equivalente $150

Tabla 1. Costos de incidentes de seguridad de la información

Roles y Responsabilidades

- Soporte Nivel 1: Agente de la Mesa de Servicios, que es el contacto directo o punto de entrada de todas las solicitudes de usuario.
- Soporte Nivel 2: El especialista en temas determinados dentro de los servicios ofrecidos por la Dirección de Tecnologías e Información, para los usuarios internos y externos.
- Soporte Nivel 3: Son todos aquellos externos a la Dirección de Tecnologías e Información, que brindan elementos, servicios o soporte, para los servicios afectados por el incidente de seguridad de la información.

Glosario

- ACTIVO DE INFORMACIÓN: Es todo aquello que representa valor para la Entidad desde software, hardware, información, servicios y personas.
- AMENAZA: Posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad de la Información.
- CADENA DE CUSTODIA: Es el conjunto de procedimientos encaminados a asegurar y demostrar la autenticidad de los elementos materiales probatorios y la evidencia física.
- CÓDIGO MALICIOSO: Es un tipo de código informático o script dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.
- CONFIDENCIALIDAD: Propiedad de la información, por la que se garantiza que la misma está accesible únicamente al personal autorizado.
- CONTENCIÓN: Es la etapa en donde se impide que el incidente se extienda a otros recursos; como consecuencia, se minimizará su impacto (separando equipos de la red afectada, deshabilitando cuentas comprometidas, cambiando contraseñas, etc.).
- DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando se requiera.
- ERRADICACIÓN: Acción para el desaparecimiento o destrucción en su totalidad de la fuente que provocó el incidente de seguridad de la información.

- EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Se refiere a algo que pueda afectar los niveles de riesgo, sin afectar de forma necesaria la razón de ser de la organización o a la información.
- INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: 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.
- INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.
- RIESGO DE SEGURIDAD DE LA INFORMACION: Se define como la combinación de la probabilidad de que se produzca un incidente de seguridad de la información y sus consecuencias negativas (impacto).
- VULNERABILIDAD: Debilidad de los activos de información que puede ser utilizada o aprovechada por delincuentes informáticos, con el fin de ocasionar daño o extraer información confidencial y datos personales.

Siglas

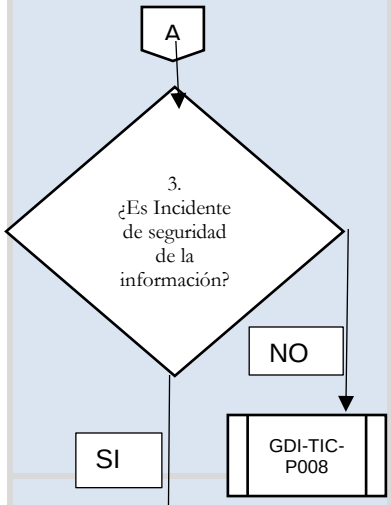
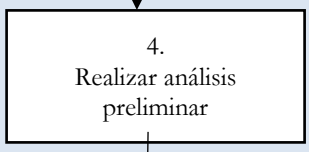
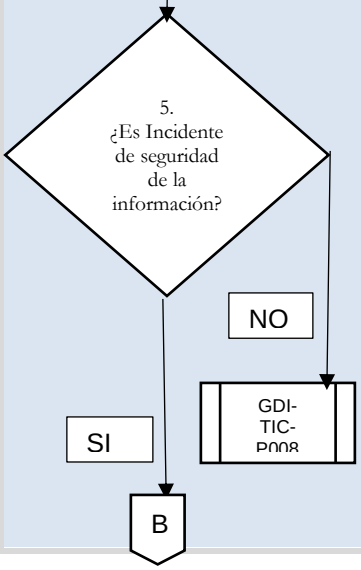
- BCP: Plan de Continuidad del Negocio
- ColCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia
- CSIRT: Organización que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad.
- DTI: Dirección de Tecnologías e Información
- MINTIC: Ministerio de las Tecnologías de la Información y Comunicaciones

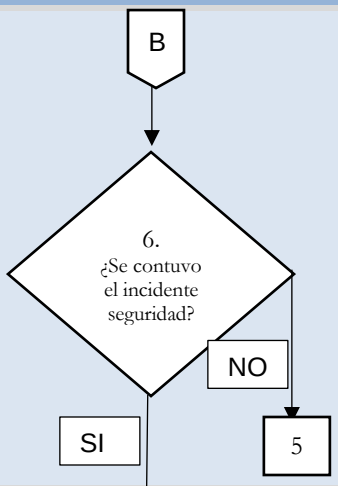
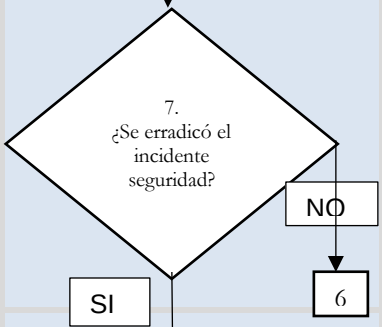
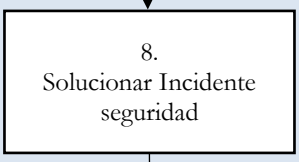
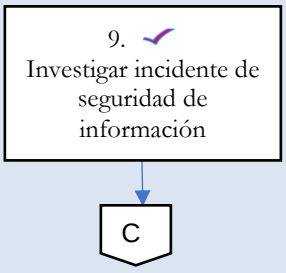
Salidas generadas del procedimiento

Salida o Resultado	Descripción de la Salida o Resultado	Destinatario
Solución a un incidente de seguridad de la información	Gestión técnica, operativa o funcional de un incidente de seguridad de la información reportado y, según sea el caso, documentación de las lecciones aprendidas del incidente, con el fin de reflejar las nuevas amenazas, la mejora de la tecnología y las mejores prácticas en caso de repetirse el incidente	Servidores públicos, contratistas de la SDG y Terceros

3. DESCRIPCIÓN ACTIVIDADES DEL PROCEDIMIENTO

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD	REGISTRO
Inicio		Inicio del procedimiento	
1. Registrar incidente	Servidores públicos/ Contratistas/ Terceros	Se ingresa con el caso reportado por el usuario en la Herramienta de Gestión vigente en la Entidad de acuerdo con el GDI-TIC-P008 Gestión de incidentes. **Nota:** En algunos casos la identificación de un Incidente se obtiene a través de herramientas de auditoria para infraestructura tecnológica, que de igual manera se debe reportar en la herramienta mesa de servicios.	Herramientas de Servicios – Ticket
2. ✓ Determinar si el caso es un incidente de seguridad de la información	Especialista Nivel 1	✓ Determinar si el caso corresponde a un incidente de seguridad de la Información, de acuerdo con la siguiente lista no exhaustiva, con el objetivo de realizar la correspondiente clasificación, teniendo en cuenta la matriz de escalamiento: 1. Violación a la política, normas y procedimientos de seguridad 2. Fuga de información 3. Uso inadecuado de los activos de información 4. Vulnerabilidades y detección de *exploits*. 5. Monitoreo, análisis de tráfico y pruebas sobre la red. 6. Infección con código malicioso. 7. Acceso no autorizado. 8. Denegación de servicio. 9. Violación de derechos a la propiedad intelectual (derechos de autor).	Herramientas de Servicios – Ticket
A			

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD	REGISTRO
	Especialista Nivel 1	¿El caso es un incidente de seguridad de información? Si: Continua con la actividad 4 No: Continuar con el procedimiento Gestión de Incidentes – GDI-TIC-P008.	
	Especialista Nivel 1	Realizar este análisis con la información suministrada por el usuario que reporta. Luego se hace el escalamiento del incidente de seguridad de la información al especialista que corresponda con el fin de apoyar con la investigación del incidente. En este análisis se debe tener en cuenta el GDI-TIC-IN020 Instrucciones para la priorización y categorización de los incidentes de seguridad de la información.	
	Especialista Nivel 1/Especialista Nivel 2/Grupo de seguridad de la información	Se realiza la recolección de información del incidente de seguridad de la información, con el fin de identificar la causa o causas que dieron origen al incidente de seguridad, dependiendo de la información afectada y la ubicación de los activos involucrados. ¿Es realmente un incidente de seguridad de la Información? **Si:** Pasa a la decisión numeral 6. **No**: Se devuelve a la mesa de servicio para su reasignación, activando el procedimiento Gestión de Incidentes – GDI-TIC-P008.	N/A

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD	REGISTRO
	Especialista Nivel 1/Especialista Nivel 2 /Grupo de seguridad de la información	Se realizan todas aquellas tareas necesarias con el fin de contener el incidente de seguridad y así minimizar su impacto ¿Se logró contener el incidente de seguridad? **Si**: Continua la decisión numeral 7. **No**: Devuelve a la decisión numeral 5	
	Especialista Nivel 1/ Especialista Nivel 2 / Grupo de seguridad de la información	Se realizan todas aquellas tareas necesarias con el fin de erradicar la causa raíz detectada ¿Se logró erradicar el incidente de seguridad? Si: Continua a la actividad 8 No: Devuelve a la decisión numeral 6	
	Especialista Nivel 1/ Especialista Nivel 2 / Grupo de seguridad de la información	Se realizará todas aquellas tareas necesarias con el fin de solucionarlo. Continuar a la actividad 9	
	Especialista Nivel 1/ Especialista Nivel 2 / Grupo de seguridad de la información/ Responsable de Seguridad de la Información	✓ Consolidar y organizar las evidencias producto de la investigación del incidente de seguridad. Una vez se consoliden las evidencias, se determinará la viabilidad de enviar el informe a los entes correspondientes. **Nota 1:** Las evidencias se deben cargar en el software de Mesa de servicios, salvo en los casos que los archivos que por su naturaleza no lo permitan (por virus, programa maligno o que puedan ser manipulados por terceros, tamaño	

ACTIVIDAD	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD	REGISTRO
C		no permitido en el software de mesa de servicios). **Nota 2:** En los casos que no se pueda cargar evidencias por tamaño, se debe reportar el enlace donde se puede consultar la evidencia. **Nota 3:** Se debe proteger las evidencias, dando cumplimiento a la cadena de custodia de las evidencias (Consultar al grupo de seguridad de la información para resolver dudas, inquietudes u observaciones).	
10. Documentar lecciones aprendidas	Especialista Nivel 1/ Especialista Nivel 2 / Grupo de seguridad de la información / Responsable de Seguridad de la Información	Se documentan las lecciones aprendidas del incidente, en el formato Informe de Incidente de Seguridad de la información GDI-TIC-F036, con el fin de reflejar las nuevas amenazas, la mejora de la tecnología y las lecciones aprendidas después de un incidente; estos informes podrán ser solicitados a demanda. **Nota:** Con base en la evidencia y documentación generada, se evalúa si la situación presentada se debe informar a entes de control o autoridades competentes.	Formato de informe de incidentes de seguridad de la información GDI-TIC-F036
11. ✓ Revisar y cargar respuesta	Especialista Nivel 2 / Grupo de seguridad de la información / Responsable de seguridad de la información	✓ El Informe de Incidente de Seguridad de la información GDI-TIC-F036, es revisado y/o ajustado por el grupo de seguridad de la información; finalmente es cargado en la herramienta de Mesa de servicios. **Nota**: Los responsables del incidente varían dependiendo del incidente presentado.	Herramientas de Servicios – Ticket
FIN		Cerrar caso y fin.	

4. DOCUMENTOS RELACIONADOS

4.1. Documentos internos

Código	Documento
GDI-TIC-M004	Manual de Gestión de seguridad de la Información
GDI-TIC-M002	Manual Plan de Continuidad TI
GDI-TIC-P008	Gestión de Incidentes
GDI-TIC-P007	Gestión de Cambios
GDI-TIC-F036	Informe de incidentes de seguridad
GDI-TIC-IN020	Instrucciones para la priorización y categorización de incidentes de seguridad de la información

4.2. Normatividad vigente

Norma	Año	Epígrafe	Artículo(s)
MODELO DE SEGURIDAD DE LA INFORMACION	http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html 2016	Guía 21	Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información

4.3. Documentos externos

Nombre	Fecha de publicación o versión	Entidad que lo emite	Medio de consulta
Ley 1581 de 2012 "Ley de protección de datos personales"	17 de octubre de 2012	Senado de la República	Virtual
Norma ISO 27001:2013 "Sistema de gestión de	2013	ICONTEC	Virtual

seguridad de la información"			
Norma ISO 27002:2013 "Information technology -- Security techniques -- Code of practice for information security controls "	2013	ICONTEC	Virtual
ISO 27032 "Marco de Ciberseguridad	2012	ISO	Virtual
COBIT "Objetivos de control para la información y tecnologías relacionadas"	12 de abril de 2012	ISACA	Virtual