1. **Objetivo**

Definir parámetros de detección, reporte y evaluación de los eventos e incidentes de Seguridad de la Información-SI, con el fin de realizar su gestión y lograr la mejora continua de la seguridad de la información de la Secretaría Distrital de Integración Social-SDIS.

1. **Glosario**

**Activo:** cualquier cosa que tiene valor para la entidad**,** bienes, derechos, información y otros recursos con los que se dispone.

**Activo de información:** hace referencia a la información que se recibe, transforma y produce en la entidad u organismo distrital en el cumplimiento de sus funciones, estos pueden ser elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.[[1]](#footnote-1)

**Cambio:** adición, modificación o eliminación de algo que podría afectar los servicios de las Tecnologías de la Información-TI. El alcance debería incluir todos los servicios de TI, elementos de configuración, procesos, documentación entre otros, los cuales pueden generar indisponibilidad por lo que deben ser evaluados por el comité de control de cambios. Entre ellos están los que solucionan fallos conocidos, mejoramiento referente a soluciones, productos nuevos (Hardware/Software), eliminación de recursos y productos, exigencias legales y obligaciones contractuales. [[2]](#footnote-2)

**Clasificación:** es la identificación y agrupamiento de características que presentan los incidentes de seguridad de la información para determinar el tratamiento del incidente.

**Comité de Control de Cambios -CCC:** grupo interno interdisciplinar encargado de revisar y aprobar los requerimientos de cambio de forma periódica.[[3]](#footnote-3)

**Comité de seguridad de la información de la SDIS:** es la instancia encargada de asegurar que exista una dirección y apoyo de la alta dirección para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos informáticos adecuados en la Secretaría Distrital de Integración Social, así como el mantenimiento de la política de privacidad y seguridad de la información a través de todo el organismo.[[4]](#footnote-4)

**Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.[[5]](#footnote-5)

**Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.[[6]](#footnote-6)

**Evento de seguridad de la información:** presencia identificada de una condición en un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.[[7]](#footnote-7)

**Herramienta de gestión:** medio por el cual los usuarios internos registran las novedades, incidentes, requerimientos y demás solicitudes relacionadas con las TI. Este es el punto de contacto de los usuarios internos con la Subdirección de Investigación e Información.

**Incidente mayor:** es todo incidente de seguridad de la información que genera afectación considerable en la confidencialidad, integridad o disponibilidad de la información.

**Incidente de seguridad de la información:** evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.[[8]](#footnote-8)

**Incidente de Tecnología:** es la interrupción no planificada de un servicio tecnológico que afecta la operación normal. Estos no afectan ni exponen la información de la entidad.

**Información:**se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia entidad o de fuentes externas) o de la fecha de elaboración.[[9]](#footnote-9)

**Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos.[[10]](#footnote-10)

**Líder del Subsistema de Gestión de Seguridad de la información[[11]](#footnote-11):** responsabilidad del Director (a) de Análisis y Diseño Estratégico.

**Seguridad de la información (SI):** preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.[[12]](#footnote-12)

**Solicitud padre:** es aquella que tiene asociada varias solicitudes sobre la misma incidencia.

**Spam:** correo basura o mensaje basura a los mensajes no solicitados, son tipo publicitario, enviados de forma masiva, que perjudican de alguna o varias maneras al receptor.

**Triada de la información:** es el conjunto de los principios básicos (confidencialidad, integridad y disponibilidad) de la seguridad de la información.

1. **Condiciones generales**

En el marco de este procedimiento, un incidente de seguridad de la información se puede identificar como todo evento o serie de eventos que tienen probabilidad significativa de comprometer la operación interna y/o los servicios sociales, amenazando la triada de la información, por ejemplo: no tener acceso a la información utilizada en el desarrollo de las actividades, pérdida o robo de carpetas físicas y magnéticas con información, ataques cibernéticos a sistemas de información y/o páginas oficiales de la Secretaría, correos de tipo SPAM con contenidos inusuales, entre otros.

Los demás eventos que se presenten a nivel tecnológico y no afectan o exponen la información de la entidad serán tratados como incidentes de tecnologías de la información, de acuerdo al *procedimiento de Gestión de incidentes de TI - PCD-MS-003*, por ejemplo: no acceso al equipo de cómputo (porque olvidó la clave, porque el equipo está desconectado de la red, por fallas técnicas etc.), desconfiguración de los sistemas de información o aplicaciones, el bloqueo de una contraseña o pérdida de la misma, etc.

* 1. **Responsabilidades**

Es responsabilidad de los funcionarios y contratistas reportar todos los posibles incidentes de seguridad de la información a la mesa de servicio, a través de:

* Mensaje de correo electrónico con la solicitud a mesadeservicio1035@sdis.gov.co.
* Llamada a la mesa de servicio a la extensión 1035.
* Reporte en la herramienta de gestión.

Todo reporte de un posible incidente de seguridad de la información debe contener como mínimo los siguientes datos:

* Nombre de funcionario o contratista que reporta el incidente.
* Teléfono y/o extensión de contacto.
* Correo electrónico.
* Descripción completa del posible incidente.

Todo reporte de un posible incidente de seguridad de la información será valorado por la mesa de servicio, teniendo en cuenta las siguientes consideraciones al momento de realizar la asignación del caso:

* Relacionar el posible incidente con una afectación en la integridad, disponibilidad y confidencialidad de la información.
* Reunir información básica (lugar, tipo de información, datos de contacto de la persona que reporta) que llevó a determinar que es un posible incidente de seguridad de la información, datos que podrán ser utilizados en la investigación y/o para empezar a contener los daños y minimizar el riesgo.

Para identificar si el incidente es real o potencial, se requiere de la información o consideraciones emitidas en el ítem anterior.

Una vez se reciba la notificación de un incidente de seguridad de información, la mesa de servicio debe realizar la primera categorización del mismo (de acuerdo con el árbol de categorías de la herramienta de gestión que utiliza la mesa de servicios) para iniciar con la atención del mismo.

El gestor de incidentes de seguridad de la información hará la tipificación de incidente mayor y solicitud padre, los cuales pueden ser asociados a los tickets según corresponda; es posible que un incidente mayor y una solicitud padre estén asociados a un mismo ticket.

El gestor de incidentes de seguridad de la información de la SDIS documentará las acciones adelantadas para tratar el incidente.

Se deben conservar las pruebas recopiladas, las cuales serán custodiadas por el líder de Seguridad de la información, con el fin de reducir la probabilidad de que las evidencias se modifiquen o se consideren no aceptables en el caso de una investigación.

El líder del Subsistema de Gestión de la Seguridad de la Información notificará a la Oficina de Asuntos Disciplinarios[[13]](#footnote-13), a la Oficina Asesora Jurídica[[14]](#footnote-14), y a la Alta Consejería Distrital de Tecnologías de Información y Comunicaciones los incidentes de seguridad de la información con consecuencias mayores o catastróficas (De acuerdo a las definiciones de la *tabla 4 Consecuencias de los incidentes de seguridad de la información*) para el trámite correspondiente, según sea el caso.

* 1. **Clasificación de los incidentes de seguridad de la información**

Los incidentes de seguridad de la información se clasifican, así:

Tabla 1 Clases de incidentes de seguridad de la información

| **Clases de incidentes de SI**  | **Descripción de la causa raíz** | **Ejemplo** |
| --- | --- | --- |
| Daño físico | Debido a acciones físicas accidentadas en las instalaciones de la SDIS. | Incendio, agua, ambiente nefasto (contaminación, polvo, corrosión, congelamiento), destrucción de equipos, destrucción de medios, robo de equipos, robo de medios, etc. |
| Malware | Causas asociadas de programas maliciosos creados y divulgados en forma intencional.  | Virus informáticos, gusanos de red, troyanos, botnet (red de robots), ataques combinados, páginas web con códigos maliciosos, sitio hosting con códigos maliciosos, etc.  |
| Ataque técnico | Resultado de ataques a sistemas de información, a través de redes u otros medios técnicos, mediante el aprovechamiento de las vulnerabilidades de los sistemas de información en cuanto a configuraciones, protocolos o programas, o por la fuerza, que genera un estado anormal de los sistemas de información. | Aprovechamiento de puertas traseras, aprovechamiento de vulnerabilidades informáticas, denegación de servicios, escaneo de redes, intentos de ingreso, interferencia, etc.  |
| Puesta en riesgo de la información | La pérdida de seguridad de la información es causada al poner en riesgo en forma accidental o intencional la confidencialidad, integridad y disponibilidad de la información. | Interceptación, espionaje, “chuzada” de teléfonos, divulgación, enmascaramiento, ingeniería social, phishing de redes (Suplantación de identidad), robo de datos, alteración de datos, errores de datos, etc. |
| Violación de reglas | Debido al uso no autorizado de recursos y violación de derechos de autor. | Uso de recursos de acceso para propósito no autorizado, por ejemplo, el uso del correo para participar en cadenas ilegales, pirámides, etc.Causada por la venta e instalación de copias de software sin licencia, u otros materiales protegidos por derechos de autor. |

 \*Basado en la Guía Técnica Colombiana 27035:2012

Un incidente de seguridad de la información que se identifique en varias de las clases citadas debe ser clasificado por la solicitud padre, de acuerdo con la tabla 1.

* 1. **Tipificación en prioridad de los incidentes de seguridad de la información**

Para la correcta gestión, todos los incidentes de seguridad de la información deberán tipificarse en prioridad de acuerdo con su impacto y urgencia por el gestor de Incidentes de Seguridad de la Información:

Tabla 2 Nivel de prioridad de los incidentes de seguridad de la información

|  |
| --- |
| **Nivel de prioridad** |
| **Impacto/Urgencia** | Alta | Media | Baja |
| Alto | Alta | Alta | Media |
| Medio | Alta | Media | Baja |
| Bajo | Media | Baja | Baja |

Tabla 3 Descripción del nivel de prioridad de los incidentes de seguridad de la información

| **Prioridad** | **Alcance** | **Descripción** |
| --- | --- | --- |
| ALTO | El incidente de seguridad puede afectar la continuidad de la prestación de los servicios sociales de la SDIS. | El incidente alto tiene un impacto considerable (afectación total a la confidencialidad, disponibilidad o integridad) en la información y se considera crítica para la misión de la SDIS, esto incluye información en diferentes medios y/o sistemas críticos.Estos incidentes implican una grave violación de seguridad o pueden dañar la confianza en la administración pública (pérdida de imagen institucional), o podrían afectar la seguridad física de las personas, causar una pérdida importante de recursos de la SDIS. |
| MEDIO | El incidente de seguridad afecta a una o más dependencias, (por ejemplo, nivel central, subdirecciones locales, etc.). | Se clasifican con este nivel aquellos eventos que puedan afectar o está afectando a los activos de información de la SDIS, con una valoración considerable en la triada de la información (confidencialidad, disponibilidad o integridad), lo cual puede resultar en la pérdida directa de información para la SDIS.  |
| BAJO | El incidente afecta a un colaborador o varios colaboradores de una dependencia. | Se clasifican con este nivel aquellos eventos que puedan ser una amenaza que afecta o está afectando a activos de información de la SDIS con una valoración de impacto limitado en la triada de la información (confidencialidad, disponibilidad o integridad). Su impacto debe ser nulo o insignificante para la SDIS. |

En caso que el incidente de seguridad de la información se considere de prioridad alta, el gestor de incidentes de seguridad de la información de la SDIS deberá proponer el equipo que participará en el tratamiento del incidente y este será aprobado por el comité de seguridad de la información de la SDIS conformado como lo indica la resolución interna 1075 del 30 de junio de 2017 Capítulo 2 artículo 39 por:

1. El (la) Director(a) de Análisis y Diseño Estratégico, quien lo presidirá coordinando las acciones del comité.
2. El (la) Subdirector(a) de Investigación e Información.
3. El (la) Jefe de la Oficina Asesora Jurídica o su delegado (a).
4. El (la) Subdirector(a) Administrativo y Financiero.

*Parágrafo 1. Serán invitados de forma permanente al comité, con voz, pero sin voto El (la) Jefe de la Oficina de Control Interno o su delegado(a) y el Gestor del Subsistema de Gestión de Seguridad de la Información.*

Los incidentes de seguridad de la información que no se consideren prioridad alta estarán liderados por el gestor de incidentes de seguridad de la información de la SDIS.

* 1. **Prioridades de tratamiento de incidentes** **de seguridad de la información**

Se debe actuar para reducir los efectos reales y potenciales de un incidente, ya que esto puede marcar la diferencia entre un impacto menor o uno de mayor importancia, ver tabla 3. La respuesta exacta dependerá de la naturaleza del incidente al que se enfrente. No obstante, se sugieren las siguientes prioridades como punto de partida:

* Proteger la vida humana y la seguridad de las personas.
* Proteger la información reservada y confidencial.
* Proteger otra información relevante (por ejemplo, propiedad intelectual o del ámbito directivo).
* Proteger el hardware y software de la SDIS.
* Minimizar la interrupción de los recursos informáticos.

Existen varias medidas que se pueden tomar para contener el daño y minimizar el riesgo en el entorno, llevadas a cabo por los integrantes del Subsistema de Gestión de Seguridad de la Información. Como mínimo debe llevar a cabo las siguientes acciones:

* Evitar que los posibles atacantes conozcan las actividades que se adelanten dentro del tratamiento.
* Evaluar el impacto al dejar sin conexión los sistemas en peligro y los sistemas relacionados con el riesgo de continuar funcionando.
* Determinar los puntos de acceso usados por los posibles atacantes e implementar las medidas adecuadas para evitar futuros accesos.
* 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 prueba si se decide procesar a los posibles atacantes).
* Asegurar el cambio de las contraseñas: locales, de las cuentas de servicio y administrativas en todo el entorno.
* Documentar cada una de las acciones realizadas.
	1. **Posibles acciones a los incidentes de seguridad de la información**
* Una solución efectiva: la gestión del incidente logró remediar los servicios o activos afectados por el incidente.
* Una solución provisional: la gestión del incidente logró remediar los servicios o activos afectados por el incidente, sin embargo, no se puede identificar la totalidad de la remediación a primera mano.
* Una solución que relaciona un cambio: la gestión del incidente logró remediar los servicios o activos afectados por el incidente, sin embargo, el incidente puede replicarse, siendo necesario ejecutar un cambio para evitar reincidencia.

Cualquier incidente que implique interrupción de algún servicio social o afectación a un proceso de manera crítica, ya sea por el número de usuarios afectados o porque se han visto involucrados sistemas o servicios sociales para la SDIS, se debe dar una respuesta inmediata, que puede incluir la generación de un control de cambios para lo cual se deberá tener en cuenta las actividades del *procedimiento de Gestión de Cambios de Tecnologías de la Información (PCD-MS-001).*

La valoración del incidente de seguridad de la información se realizará por el gestor de incidentes de seguridad de la SDIS para determinar las consecuencias, las cuales constituirán una prueba importante y necesaria si se decide emprender acciones legales. Entre ellos, se pueden contar los siguientes que deben ser debidamente documentadas:

* Consecuencias asociadas a la pérdida de información confidencial.
* Consecuencias legales.
* Consecuencias laborales por el análisis de las infracciones, la reinstalación del software y la recuperación de datos.
* Consecuencias en el tiempo de inactividad de los sistemas (por ejemplo, pérdida de productividad de los funcionarios y/o contratistas, sustitución del hardware, del software y de otras propiedades).
* Consecuencias relacionadas con la reparación y posible actualización de las medidas de seguridad físicas dañadas o ineficaces (cierres, paredes, cajas, etc.).
* Consecuencias relacionadas con la imagen del proceso afectado por un incidente.
* Otros daños derivados, como la pérdida de la reputación o de la confianza de los beneficiarios de la SDIS.

Se utilizará la siguiente tabla para valorar las consecuencias de los incidentes de seguridad de la información en la SDIS:

Tabla 4 Consecuencias de los incidentes de seguridad de la información

|  |  |  |
| --- | --- | --- |
| **Nivel** | **Descriptor** | **Descripción** |
| 1 | Insignificante | Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad. |
| 2 | Menor | Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad. |
| 3 | Moderada | Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad. |
| 4 | Mayor | Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad. |
| 5 | Catastrófica | Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad. |

Debe tenerse en cuenta que los incidentes deben clasificarse únicamente en un descriptor de consecuencia y puede tener incumplimiento legal, sanciones, costos, pérdida de imagen o afectación de la operación de la SDIS.

1. **Descripción de actividades**





1. **Disposiciones de almacenamiento y archivo**

Las disposiciones de almacenamiento y archivo de la documentación del Sistema Integrado de Gestión, se realizará de conformidad con lo dispuesto en el Subsistema Interno de Gestión Documental y Archivo (SIGA)

1. **Dependencia encargada de administrar este procedimiento**

Dirección de Análisis y Diseño Estratégico - Subdirección de Investigación e Información.

1. **Documentos asociados**

FOR-MS-017Formato informe de incidentes mayores de seguridad de la información

1. **Aprobación del documento**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Elaboró** | **Revisó** | **Aprobó** |
| **Nombre** | Diana Cantor Córdoba  | Mileni Rodríguez Gómez Álvaro Rueda Zapata | Liliana Pulido Villamil |
| **Cargo/****Rol** | Contratista Asesora Subdirección de Investigación e Información - Subdirección de Investigación e Información | Contratista Gestor proceso y dependencia Subdirector de Investigación e Información | Directora de Análisis y Diseño Estratégico |

1. Décimo primer lineamiento, inventario de activos de información-Sistema Integrado de Gestión Distrital [↑](#footnote-ref-1)
2. Fundamentos de ITIL® - Volumen3 2008 [↑](#footnote-ref-2)
3. PCD-MS-001 Procedimiento Gestión de Cambios de Tecnologías de la Información. [↑](#footnote-ref-3)
4. Resolución Interna 1075 de 30 de junio de 2017 [↑](#footnote-ref-4)
5. Norma Técnica Colombiana NTC-ISO-IEC 27001 [↑](#footnote-ref-5)
6. Ibíd. [↑](#footnote-ref-6)
7. Guía Técnica Colombiana NTC-ISO-IEC 27035. [↑](#footnote-ref-7)
8. Ibíd. [↑](#footnote-ref-8)
9. Norma Técnica Colombiana NTC-ISO-IEC 27001. [↑](#footnote-ref-9)
10. Ibíd. [↑](#footnote-ref-10)
11. Resolución SDIS 1075 de 2017, articulo 11, numeral 3 [↑](#footnote-ref-11)
12. Norma Técnica Colombiana NTC-ISO-IEC 27001. [↑](#footnote-ref-12)
13. Resolución 607 de 2007, Articulo 8, literal d [↑](#footnote-ref-13)
14. Resolución 607 de 2007, Articulo 5, literal f [↑](#footnote-ref-14)