LÍDER DE PROCESO

1. OBJETIVO

Establecer los lineamientos para la gestión de las posibles afectaciones a la seguridad delos datos logrando mitigar los riesgos y daños que se puedan causar a los activos de información del IDARTES.

2. ALCANCE

El procedimiento inicia con la fase de prevención de eventos e incidentes de seguridad de la Información, continua con la detección y análisis de los incidentes de seguridad de la información, la contención, erradicación y recuperación; y las actividades posts-incidentes y finaliza con el cierre del incidente.

3. ÁREAS RESPONSABLES

120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN - 122 ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN

4. GLOSARIO (TÉRMINOS Y DEFINICIONES ASOCIADOS)

ACTIVO DE INFORMACIÓN: Se denomina activo a aquello que tiene valor para el Instituto y por lo tanto debe protegerse.

ACTIVOS TECNOLÓGICOS: Recursos del sistema de información o relacionados con éste, necesarios para que la entidad funcione correctamente y alcance los objetivos propuestos por su Dirección. Se pueden estructurar en las siguientes categorías: Software, Hardware, Servicios, Datos, Personal, Proveedores, instalaciones físicas, Comunicaciones, Equipamiento auxiliar, etc.

ADMINISTRADOR MESA DE SERVICIOS: Recibe la información de los usuarios, registra los casos en la herramienta de mesa de servicios y es el primer contacto para la gestión de los incidentes de seguridad de la información.

ANTIVIRUS: Programa diseñado para identificar, aislar o eliminar un virus del computador.

ANS: Acuerdos de niveles de servicio.

APLICACIÓN VAULT: Herramienta que hace parte de la Suite de Google Apps para almacenamiento y consulta de copias de seguridad de cuentas de correo de licenciamiento Basic.

BACKUP: Copia de respaldo de la información realizada en medio magnético.

CATEGORÍA: Se asigna una categoría (que puede estar a su vez subdividida en más niveles) dependiendo del tipo de incidente y/o del responsable de su resolución. Se identifican los servicios afectados por el incidente.

CONFIDENCIALIDAD: Garantía que la información sea accedida únicamente por usuarios y procesos autorizados.

APLICACIÓN VAULT: Herramienta que hace parte de la Suite de Google Apps para almacenamiento y consulta de copias de seguridad de cuentas de correo de licenciamiento Basic.

BACKUP: Copia de respaldo de la información realizada en medio magnético.

CATEGORÍA: Se asigna una categoría (que puede estar a su vez subdividida en más niveles) dependiendo del tipo de incidente y/o del responsable de su resolución. Se identifican los servicios afectados por el incidente.

CONFIDENCIALIDAD: Garantía que la información sea accedida únicamente por usuarios y procesos autorizados.

CONTROL: Medida que permite garantizar la reducción del nivel de un riesgo específico o mantenerlo dentro de límites aceptables.

DISPONIBILIDAD: Garantía que los usuarios y procesos autorizados tengan acceso a los activos de información cuando los requieran.

EVENTO: Suceso que puede ocurrir en un espacio y tiempo específico, generando impactos sobre los activos tecnológicos y activos del IDARTES, un evento de seguridad de la información es la presencia identificada de un estado del sistema, del proceso, del servicio o de los recursos tecnológicos que indican un incumplimiento posible de las políticas de seguridad de la información, una falla de las medidas de seguridad tomadas o una situación previamente desconocida que genera riesgos para la entidad.

EVENTOS DE SEGURIDAD DE LA INFORMACIÓN: Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad y disponibilidad de los datos.

HARDWARE: Componentes eléctricos, dípticos, electrónicos, electromecánicos y mecánicos que conforman un instrumento o sistema de computador.

IMPACTO: Daño producido a la Entidad por la materialización de un riesgo sobre los activos tecnológicos, visto como diferencia en las estimaciones de los estados de seguridad obtenidas antes y después del evento.

INFORMACIÓN: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

INTEGRIDAD: Condición de seguridad que garantiza que la información es actualizada, en todo su ciclo de vida, sólo por el personal y procedimientos autorizados.

REGISTRO DE EVENTOS: En inglés Logs. Mecanismo mediante el cual se guarda en un archivo (generalmente de texto) toda la información correspondiente a las actividades o eventos de un determinado sistema, dispositivo o equipo.

RIESGO: Probabilidad o posibilidad de que una amenaza aprovechando la vulnerabilidad o vulnerabilidades de un sistema, equipo o cualquier otro tipo de activo, se concrete, causando daños, perjuicios o pérdidas a la Entidad propietaria del mismo.

SEGURIDAD DE LA INFORMACIÓN-SI: Actividad que regula la protección de los recursos tecnológicos de la entidad a través de políticas, normas, procedimientos y estándares.

SOFTWARE: Programas que se ejecutan en el computador para realizar una función determinada.

SISTEMA DE INFORMACIÓN: Conjunto de datos, aplicaciones y equipos que de manera conjunta proveen a la Entidad la información necesaria para la ejecución de las tareas y la toma de decisiones de los niveles estratégico, táctico y operativo.

TRAZABILIDAD: Conjunto de medidas, acciones y procedimientos que permiten registrar, identificar y realizar seguimiento a los incidentes en cada producto desde su origen hasta su respuesta final.

USUARIO: Colaborador con acceso a los recursos y servicios tecnológicos de la Entidad.

USUARIO ADMINISTRADOR: Usuarios con privilegios para instalación y configuración de software y hardware en el equipo asignado que por sus actividades requieren este perfil.

5. CONDICIONES ESPECIALES DE OPERACIÓN

- Todos los incidentes de seguridad de la información deben estar registrados en la herramienta de la mesa de servicios de TI.
- Es responsabilidad de todos los funcionarios, terceros y contratistas que tengan acceso a los activos de información del IDARTES reportar a la mesa de servicios de TI, los eventos tecnológicos o incidentes de seguridad de la información para su respectiva gestión.
- Los incidentes de seguridad de la información que se cataloguen como Muy grave y Grave deberán ser reportados ante el Computer Security Incident Response Team Centro - CSIRT, perteneciente a la Alta Consejería Distrital de TIC.
- Para el correcto análisis de un incidente debe existir una única fuente de tiempo (Sincronización de Relojes) con la finalidad de facilitar la correlación de eventos presentados.

Clasificación Incidente Seguridad de la Información

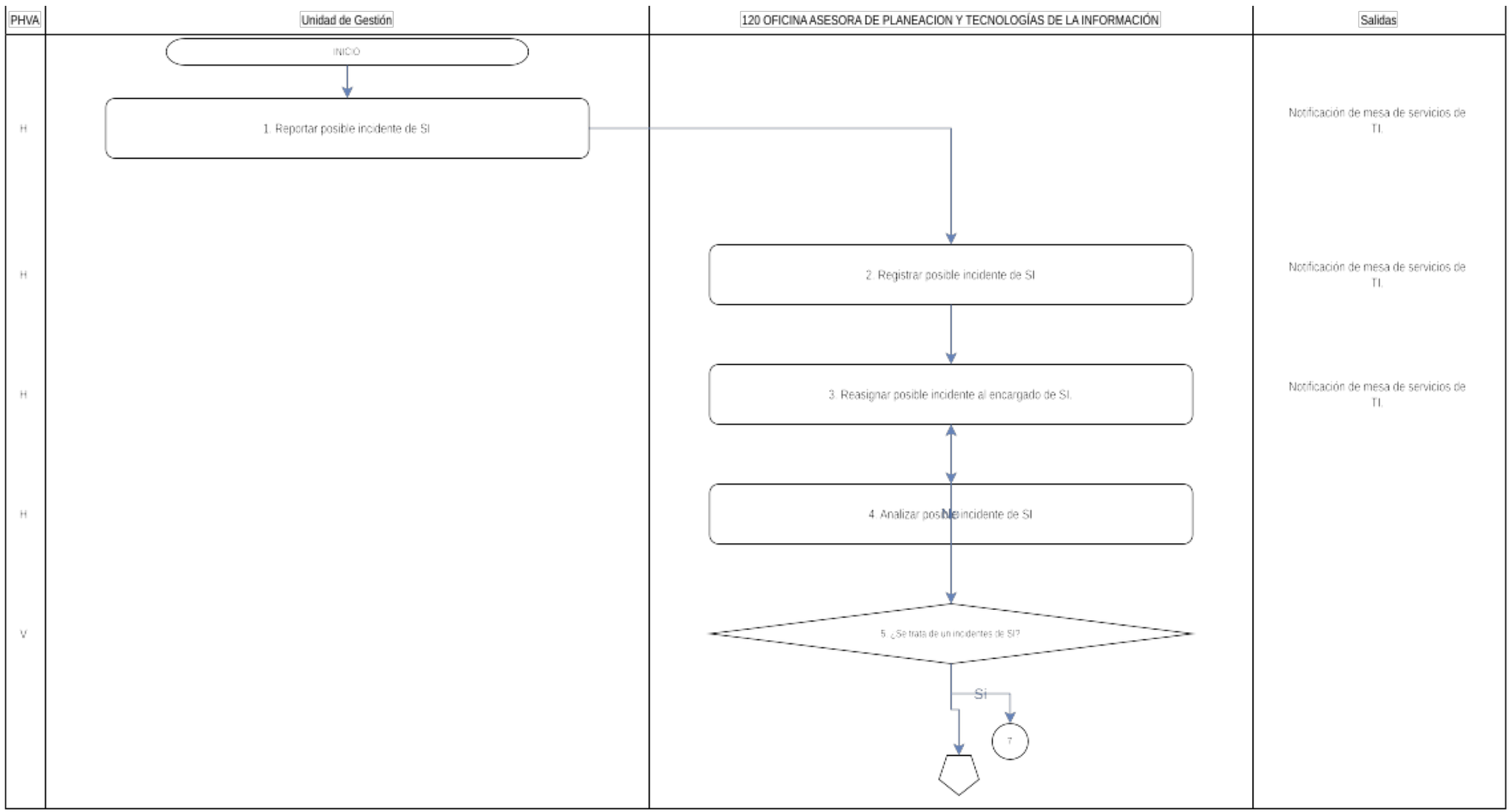
La clasificación del incidente se realiza teniendo en cuenta la taxonomía definida por la entidad.

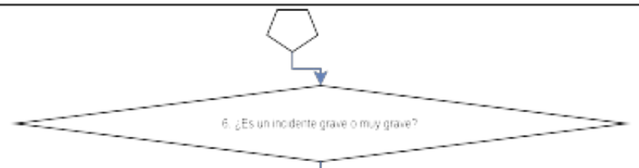
- Acceso no autorizado: Es un incidente que involucra a personas, sistemas o códigos maliciosos que obtienen acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información.
- Modificación de recursos no autorizados: Un incidente que involucra 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.

6. RELACIÓN CON OTROS PROCEDIMIENTOS Y PROCESOS

Procesos que se requieren como proveedor	Que insumos requiero del proveedor	Procedimiento	Que se obtiene del procedimiento	Para quien va dirigido el servicio o producto
• TODAS LAS ÁREAS	Reporte del incidente de seguridad en la información junto con su evidencia	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Pasos para la solución del incidente de seguridad de la información	• TODAS LAS ÁREAS Mejorar continuamente la eficiencia, eficacia y efectividad de la gestión de la entidad, a partir de los instrumentos de contingencia, seguimiento y retroalimentación que conllevan a llevar un modelo de interacción e interrelación entre los diferentes procesos, respondiendo a las dinámicas cambiantes que enfrente la entidad

7. DIAGRAMA DE FLUJO


PHVA
Unidad de Gestión
120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN
Salidas
INICIO
1. Reportar posible incidente de SI
Notificación de mesa de servicios de TI.
2. Registrar posible incidente de SI
Notificación de mesa de servicios de TI.
3. Reasignar posible incidente al encargado de SI.
Notificación de mesa de servicios de TI.
4. Analizar posible incidente de SI
5. ¿Se trata de un incidentes de SI?
Si
7
H
H
H
H
V

PHVA	Unidad de Gestión	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Salidas
V			
H			Notificación de mesa de servicios de TI.
V			Notificación de mesa de servicios de TI.
H			Notificación de mesa de servicios de TI.

8. DESCRIPCIÓN DE ACTIVIDADES

No.	Ciclo PHVA	DESCRIPCIÓN DE ACTIVIDADES Y CONTROLES	ACTORES	RESPONSABLE	TIEMPO (HORAS)	DOCUMENTO / REGISTRO
1	H	**Reportar posible incidente de SI** Identifica el posible incidente de seguridad de la información y lo reporta a través del correo electrónico soporte.ti@idartes.gov.co	Unidad de Gestión	Usuarios	1 hora	Notificación de mesa de servicios de TI.

2	H	**Registrar posible incidente de SI** Realiza la creación del Ticket en la mesa de servicios de TI, con la categorización y registro del posible incidente de seguridad.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Administrador de la mesa de servicios de TI.	1 hora	Notificación de mesa de servicios de TI.
3	H	**Reasignar posible incidente al encargado de SI.** Realiza el escalamiento del incidente de seguridad al Encargado de Seguridad de la Información.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Administrador de la mesa de servicios de TI.	2 horas	Notificación de mesa de servicios de TI.
4	H	**Analizar posible incidente de SI** Analiza y clasifica el posible incidente de seguridad reportado, de acuerdo con la categorización de la mesa de servicios de TI.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de Seguridad de la Información.	2 horas	
5	V	**¿Se trata de un incidentes de SI?** El encargado de Seguridad de la Información analiza si se trata de un incidente de SI. **Si:** Continua en la **actividad 7 No:** Se devuelve a la **actividad 3**	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de Seguridad de la Información	1 hora	
6	V	**¿Es un incidente grave o muy grave?** El encargado de Seguridad de la Información analiza si se trata de un incidente grave o muy grave. **Si:** Continua en la **actividad 7 No:** Continua en la **actividad 7**	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de Seguridad de la Información	1 hora	
7	H	**Definir el tratamiento para el incidente** El encargado de Seguridad de la Información activa el tratamiento y/o el protocolo para la atención de incidentes de seguridad de la información.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de Seguridad de la Información	1 día	Notificación de mesa de servicios de TI.
8	V	**Resolver el incidente** Resuelve el incidente, teniendo en cuenta la categoría de seguridad de la información y se informa a través de la mesa de servicios de TI la solución al incidente.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de Seguridad de la Información	5 días	Notificación de mesa de servicios de TI.
9	H	**Cerrar el caso** Se cierra el ticket en la mesa de servicios de TI.	120 OFICINA ASESORA DE PLANEACION Y TECNOLOGÍAS DE LA INFORMACIÓN	Encargado de Seguridad de la Información	1 hora	Notificación de mesa de servicios de TI.

8. POSIBLES PRODUCTOS O SERVICIOS NO CONFORME

ACTIVIDAD	PRODUCTO Y/O SERVICIO	CRITERIO DE ACEPTACIÓN	CORRECCIÓN	REGISTRO
8. Resolver el incidente: Resuelve el incidente, teniendo en cuenta la categoría de seguridad de la información y se informa a través de la mesa de servicios de TI la solución al incidente.	Notificación de mesa de servicios de TI.	Calidad: La información de la notificación de la mesa de servicios le proporciona al usuario los datos de la gestión de su solicitud. Oportunidad: De manera automática se generan las notificaciones de la mesa de servicios de TI. Confiable: Las notificaciones de la mesa de servicios de TI, proporciona la trazabilidad, la gestión y el flujo de interacción que se tiene frente al caso.	Reabrir o crear el ticket.	Notificación de mesa de servicios de TI.

9. DOCUMENTOS ASOCIADOS

Los documentos asociados del presente procedimiento se pueden acceder a través del mapa de procesos.

10. NORMATIVA ASOCIADA

Ver normograma.

11. RECURSOS

GLPI - Aplicativo mesa de servicios de TI
Encargado de Seguridad de la Información
Administradores de servicios de TI.

12. ANEXOS

No.	NOMBRE DEL ANEXO
-	Sin información.

13. CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS
1	2018-09-12	Actualización del mapa de procesos de la entidad, en LDM anterior corresponde al Código: 3AP-GTI PD-03
2	2021-07-22	Se requiere ajuste debido a cambios en la normatividad
3	2025-06-12	Incorporación de las fases de gestión del incidente de seguridad de la información, de conformidad con lo establecido por el MinTIC.

14. CONTROL DE APROBACIÓN

ESTADO	FECHA	NOMBRE	CARGO
ELABORÓ	2025-06-11	MARYURY FORERO BOHORQUEZ	ENLACE MIPG
REVISÓ	2025-06-12	MARIA CRISTINA HERRERA CALDERON	REFERENTE MIPG
APROBÓ	2025-06-12	DANIEL SANCHEZ ROJAS	LIDER DE PROCESO
AVALÓ	2025-06-12	DANIEL SANCHEZ ROJAS	JEFE DE LA OFICINA ASESORA DE PLANEACIÓN Y TECNOLOGÍAS DE LA INFORMACIÓN

15. COLABORADORES

NOMBRE
JONATHAN GONZALEZ BOLANOS
MARYURY FORERO BOHORQUEZ