

## 1. OBJETIVO:

Definir las actividades para la eficiente gestión de incidentes de seguridad que puedan impactar los activos tecnológicos de la UPME, alineados con la gestión de solicitudes de servicios TI.

## 2. ALCANCE:

El procedimiento inicia con el reporte del posible incidente de seguridad, se realiza la evaluación del mismo, se procede con la estrategia de contención, se ejecuta y se finaliza con la recuperación del incidente incluyendo la documentación del mismo para completar el ciclo de mejora continua.

## 3. RESPONSABLES

Seguridad de la información

Soporte TI

Responsables de cada área involucrada en un incidente de seguridad

Funcionarios y/o contratistas de la UPME que hagan uso de los activos de la información.

## 4. GLOSARIO:

**CAUSA:** Se entiende como la fuente o el origen que genera un evento o la razón por la cual un evento puede suceder. Algunas fuentes de riesgos son: el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.

**CONFIDENCIALIDAD:** Propiedad por la que se garantiza el grado de acceso a la información de acuerdo con su nivel de autorización.

**DISPONIBILIDAD:** Capacidad de garantizar que tanto la información como los servicios van a estar accesibles y utilizables en todo momento.

**EVENTO DE SEGURIDAD:** Es alguna ocurrencia que no compromete la confidencialidad, la integridad o la disponibilidad de la información pero que sí puede tener relevancia para la UPME.

**INCIDENTE DE SEGURIDAD:** Es una situación adversa que compromete la disponibilidad, confidencialidad o integridad de los activos de la información de la UPME y el sistema de gestión de seguridad de la información (SGSI).

**IMPACTO:** Es el daño producido sobre un activo por la materialización de una amenaza.

**INDICADOR:** es una señal de que un incidente de seguridad ocurrió o está ocurriendo en el momento.

	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL</b>	Código: P-TI-008
		Versión No. 01
		Pág. 2/9

**INTEGRIDAD:** Propiedad de los datos o la información no hayan sido modificados o alterados de forma no autorizada.

**PRECURSOR:** Es una situación de alto riesgo en la que los controles de seguridad están ausentes, son inefectivos o no se ejecutan.

## 5. LINEAMIENTOS O POLÍTICAS DE OPERACIÓN Y CONTROL

Nombre	Descripción
Incidente de seguridad.	Teniendo en cuenta que un incidente de seguridad es toda situación adversa que afecte la seguridad de los activos de la información de la UPME. Cualquier usuario de la entidad tiene la responsabilidad de comunicar todo evento o incidente de seguridad que sea detectado, esto a través de los canales dispuestos por la UPME de la mesa de servicio.
Escalamientos de incidentes.	<p>Todos los incidentes de seguridad informática se deben registrar y manejar en la herramienta que disponga la mesa de servicio.</p> <ul style="list-style-type: none"> <li>o Correo electrónico: <a href="mailto:mesadeservicio@upme.gov.co">mesadeservicio@upme.gov.co</a></li> <li>o Herramienta de Gestión: <a href="https://mesadeservicio.upme.gov.co">https://mesadeservicio.upme.gov.co</a></li> <li>o Atención telefónica: Extensión 500</li> </ul> <p>La mesa de servicio debe escalar al equipo de seguridad informática los incidentes de seguridad que se informen o identifiquen por los canales de comunicación definidos previamente.</p>
Manejo de incidentes de seguridad de la información.	<p>Todos los incidentes de seguridad deben ser clasificados, priorizados y atendidos por el oficial de seguridad de la información.</p> <p>Toda la Información relativa a los incidentes debe ser manejada con total confidencialidad y alineada con la política de seguridad y privacidad de la información.</p>
Reporte de incidentes a Colcert	En el evento de que algún componente de la infraestructura tecnológica (sitios Web, aplicaciones, servicios en línea, sistemas de información, entre otros) de la UPME, haya sido vulnerado o comprometido, se debe reportar a ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) por medio de correo electrónico a: <a href="mailto:contacto@colcert.gov.co">contacto@colcert.gov.co</a> o al Teléfono: (+571) 2959897.
Marco normativo	<p>Ley 1581 de 2012 ARTÍCULO 17 "n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares. (...)"</p> <p>El Capítulo II, Título V de la Circular Única de la Superintendencia de Industria y Comercio establece que las organizaciones que están obligadas a inscribir las Bases de Datos Personales ante el Registro Nacional de Bases de Datos (en adelante "RNBD"), deberán reportar el incidente de seguridad dentro los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o el área encargada de atenderlos.</p> <p>Todos los reportes deberán efectuarse a través del enlace previsto en la página web de la SIC.</p> <p>Ley 1273 de 2009 Por medio de esta Ley se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos", y se preservan integralmente los sistemas que utilicen las tecnologías</p>

	<b>PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL</b>	Código: P-TI-008
		Versión No. 01
		Pág. 3/9

	<p>de la información y las comunicaciones, entre otras disposiciones. Por medio de esta Ley se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.</p> <p>Ley 1712 de 2014 (Uso de las TIC) Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente.</p> <p>Resolución 1519 de 2020 Anexo 3 Condiciones Mínimas Técnicas y de Seguridad Digital</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 5.1 Tabla de identificación de incidentes.

Para el correcto tratamiento de incidentes de seguridad de la información es necesario que todos los involucrados de la UPME conozcan cómo identificarlos.

Los incidentes principales a tener en cuenta son los siguientes:

Categoría de incidente	Tipo Incidente	Descripción
Acceso no autorizado	Borrado de información	Eliminación de información contenida en archivos y/o bases de datos de la UPME
	Fuga de información	Extracción o hurto de información de archivos y/o bases de datos de la UPME
	Intento de ingreso sin éxito a los sistemas y/o tecnologías	Intento de ingreso a los sistemas y/o tecnologías que han sido bloqueados por antivirus, firewall, IPS u otros sistemas de protección
	Ingreso exitoso no autorizado a sistemas y/o tecnologías	Es el ingreso exitoso sin autorización que ha sido registrado por las soluciones de seguridad y/o evidenciado por el personal de la UPME.
	Modificación de información	Es la modificación no autorizada que se produce sobre la información contenida en archivos y/o bases de datos de la UPME
	Uso inadecuado de los sistemas y/o tecnologías	El uso inadecuado de los sistemas se da por alguna alteración en las configuraciones de los sistemas y/o tecnologías ya sea por personal autorizado o no.
Código malicioso	Gusanos informáticos	Es una variante de código malicioso que tiene la capacidad de duplicarse y copiar sus réplicas en distintos directorios de la máquina infectada y propagarse hacia otros equipos de la red.
	Troyanos	Se presenta cuando un programa que aparenta ser inofensivo ingresa a la red de datos y ante determinado evento inicia el despliegue de su arsenal contra los equipos infectados.
	Virus informáticos	Malware que se puede hospedar en una o varias máquinas y causar daño a las configuraciones e información allí contenida

Categoría de incidente	Tipo Incidente	Descripción
Denegación de servicio	Saturación de la red interna	La red de área local y/o MPLS alcanza el umbral de capacidad de uso por inundación de tráfico que no es de la operación normal y afecta el uso de los servicios.
	Saturación de Internet	La red de Internet se afecta porque supera el límite de ancho de banda debido a altos volúmenes de tráfico ajenos a la operación de la UPME.
	Servidores no responden	El almacenamiento, memoria y procesamiento de los servidores alcanza los límites de capacidad de uso y dejan de responder a peticiones propias de la operación
	Portal Web no responde	El Portal Web no responde a las solicitudes de los usuarios genuinos.
Espionaje	Escaneo de vulnerabilidades	Ejecución de escaneos por parte de sujetos no autorizados que buscan identificar vulnerabilidades en los sistemas y tecnologías.
	Escucha de tráfico	Escuchar el tráfico que viaje por los sistemas de telecomunicaciones
Mal uso de los recursos	Mal uso del correo electrónico	Usar el servicio para envío de cadenas de mensajes, contenidos maliciosos y para propósitos distintos a los encomendados por la UPME.
	Mal uso del servicio de Internet	Utilizar el servicio de Internet para descargar y/o transferir contenidos maliciosos que puedan causar daños a los activos de la UPME.
	Incumplimiento a las normas, políticas y procedimientos de seguridad	Transgresión a las normas, procedimientos y controles que la UPME tiene al servicio de la seguridad de sus funcionarios y de los grupos de interés.


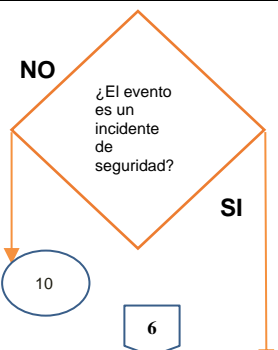
## 5.2 Tipificación de la prioridad del incidente

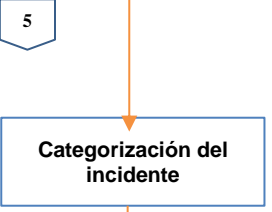
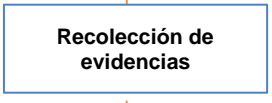
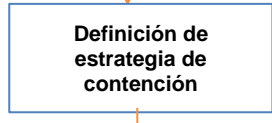
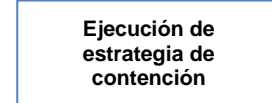
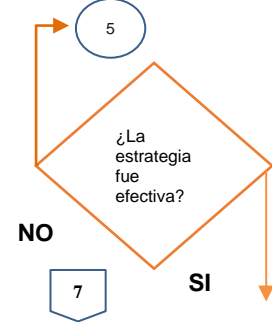
Se tipifica de acuerdo con el impacto y la urgencia que el Oficial de seguridad determine de acuerdo al siguiente cuadro:

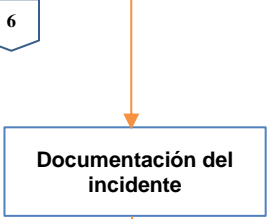
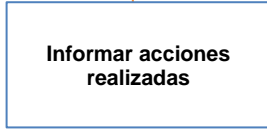
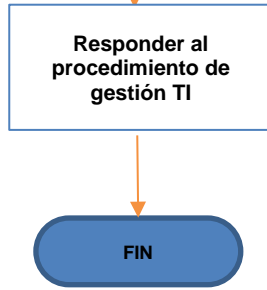
Nivel de prioridad			
Impacto/Urgencia	Alta	Media	Baja
Alto	Alta	Alta	Media
Medio	Alta	Media	Baja
Bajo	Media	Baja	Baja

Prioridad	Alcance	Descripción
<b>ALTO</b>	El incidente de seguridad puede afectar la continuidad de la prestación de los servicios de la UPME.	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 UPME, 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 y causar una pérdida importante asociada a los activos de la información de la UPME.
<b>MEDIO</b>	El incidente de seguridad afecta a una o más dependencias	Se clasifican con este nivel aquellos eventos que puedan afectar o están afectando a los activos de información de la UPME, 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 UPME.
<b>BAJO</b>	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 UPME 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 UPME.

## 6. DESARROLLO DEL PROCEDIMIENTO

No/ PC	Flujograma	Actividad	Responsable	Registro o documento
1		Recibir el posible incidente de seguridad a través del procedimiento de gestión de solicitudes de Servicio de TI donde se evalúa si el reporte es un incidente o si por el contrario solo es un evento de seguridad.	Seguridad de la información	Caso mesa de servicio.
2 PC		<p><b>Punto de Control</b></p> <p><b>Revisar evento reportado</b></p> <p>¿El evento es un incidente de seguridad?</p> <p>Si: Se pasa a la actividad 3.</p> <p>No: Pasa a la Actividad 10.</p> <p>Nota: para responder esta pregunta tenga en cuenta los lineamientos en el numeral 5 de incidentes de seguridad.</p>		

3		<p>Si hubo compromiso por parte de la infraestructura externa se debe realizar el reporte a Colcert de acuerdo al numeral 5 de este documento.</p> <p>Acto seguido se realiza la categorización del incidente de acuerdo a la tabla del numeral 5.1 y la tipificación de acuerdo al numeral 5.2 de este documento.</p> <p>Pasa a la actividad 4.</p>	Seguridad de la información	Bitácora de gestión de incidentes.
4		<p>Recolectar las evidencias pertinentes en conjunto con las áreas involucradas en el incidente, manteniendo la debida cadena de custodia.</p> <p>Pasa a la actividad 5.</p>	Soporte en Sitio Seguridad de la información Áreas involucradas	Bitácora de gestión de incidentes
5		<p>Definir la estrategia de contención del incidente teniendo en cuenta lo siguiente:</p> <ol style="list-style-type: none"> <li>1. Daño potencial a los activos, según la criticidad de estos</li> <li>2. Preservación de la evidencia</li> <li>3. Personal involucrado</li> <li>4. Tiempos de ejecución</li> <li>5. Recursos para la ejecución</li> <li>6. Efectividad de la estrategia</li> <li>7. Duración de la estrategia aplicada</li> <li>8. Características del ataque</li> <li>9. Si fue necesario la Activación del DRP</li> <li>10. Implicaciones financieras, reputacionales y de cumplimiento.</li> <li>11. Instaurar acciones legales.</li> <li>12. Responsable de la ejecución.</li> </ol> <p>Pasa a la actividad 6</p>	Seguridad de la información Áreas involucradas	Bitácora de gestión de incidentes.
6		<p>Se realiza la ejecución de la estrategia definida por los responsables asignados para esta tarea, reportando el resultado de la misma.</p> <p>Pasa a la actividad 7</p>	Responsables de la Ejecución	Correo electrónico dirigido a los involucrados notificando la ejecución de la actividad.
7 PC		<p>¿La estrategia fue efectiva?</p> <p><b>Punto de Control</b></p> <p>Si: Continuar con la actividad 8 No: Regresar a la actividad 5</p>	Seguridad de la información Áreas involucradas	Bitácora de gestión de incidentes.

8		<p>Realizar documentación del incidente presentado para:</p> <ol style="list-style-type: none"> <li>1. Definir esquemas efectivos ante los eventos que afecten la seguridad de la información</li> <li>2. Mantener actualizada la documentación de los incidentes que se han presentado.</li> <li>3. Sensibilizar a todos los interesados sobre las lecciones aprendidas en ocasión del incidente presentado.</li> </ol>	Seguridad de la información	Formato de incidentes de seguridad
9		<p>Informar a las áreas correspondientes las acciones realizadas.</p> <p>Pasa a la actividad 10</p>	Seguridad de la información	Bitácora de gestión de incidentes.
10		<p>Se responde al procedimiento de gestión de solicitudes de servicio de gestión TI, se hace reporte a la SIC en caso de ser necesario y se da fin al evento.</p> <p>FIN</p>	Seguridad de la información	Correo Electrónico a los interesados e involucrados

## 7. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Fecha	Versión	Descripción de los cambios
04/11/2022	01	Creación y definición del documento de gestión de incidentes e inclusión en el SIGUEME