1. **OBJETIVO** Estandarizar las actividades a seguir para la atención y manejo de los incidentes de seguridad de la información que se presenten en el Unidad para la Atención y Reparación Integral a las Víctimas.

2. **ALCANCE** El procedimiento de Gestión de Incidentes de Seguridad de la Información inicia con la creación del ticket en la mesa de servicios tecnológicos por parte de cualquier usuario (funcionario, contratista o colaborador) de la Entidad, basados en la afectación de la información que ocasione la perdida, divulgación o modificación no autorizada de información. Y finaliza dando respuesta al caso mediante el cierre del ticket en la mesa de servicios tecnológicos.

3. **DEFINICIONES**

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 organización o de fuentes externas) o de la fecha de elaboración.

INCIDENTE: Cualquier caso adverso en relación con la seguridad de la información que afecte la integridad, confidencialidad o disponibilidad de la Información de la Unidad.

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.

CONFIDENCIALIDAD: Propiedad de la información restringe su disposición o revelación a individuos, entidades o procesos no autorizados

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera un individuo, entidad o procesos autorizados

CATEGORÍA: Es un criterio para la clasificación de los incidentes de seguridad que se pueden llegar a materializar en la Entidad, que puedan afectar la integridad, disponibilidad y confidencialidad de la información.

DENEGACIÓN DE SERVICIO: Ataque informático a un sistema o a una red que hace que un servicio o un recurso sea inaccesible por sus usuarios legítimos. Normalmente se ejecuta sobrecargando los recursos computacionales o el canal de comunicaciones utilizado por los usuarios para acceder al servicio.[1]

CSIRT: Es un equipo de respuesta a incidentes de seguridad a cargo de la policía nacional, sus funciones se asocian a controlar y minimizar cualquier tipo de daño a la organización y su información, junto con la preservación de evidencia sobre lo ocurrido.

INFORMACIÓN COMPROMETIDA: Es aquella información, que se ve afectada en caso de presentarse alguna actividad de perdida o robo de la información sensible de la entidad.

ACTIVOS COMPROMETIDOS: son los activos de información identificados como críticos, que se ven involucrados en la materialización de un incidente.

ACTIVIDAD INUSUAL: Suceso que no se ha contemplado dentro de la actividad laboral o contractual que indique una alerta para la entidad. Con un criterio específico se estima extraño o sospechoso el evento.

HACKING INTERNO: Actividad de valoración de seguridad de los sistemas de información mediante ataques informáticos que emulan el comportamiento de un atacante al interior de la entidad.

HACKING EXTERNO: Actividad de valoración de seguridad de los sistemas de información mediante ataques informáticos que emulan el comportamiento de un atacante externo y/o de un tercero.

CORREO ELECTRÓNICO: Esta categoría hace parte del suceso en que puede verse afectado el activo correo electrónico institucional.

MALWARE: Es un virus o gusano que afecta típicamente a múltiples dispositivos de la organización, siendo activamente controlado por un atacante a través de una puerta trasera o un troyano.

[1] Fuente: http://mooc.renata.edu.co

CATEGORIAS INCIDENTES DE SEGURIDAD:[2] Las siguientes son las categorías y criterios definidos para el establecimiento de incidentes de seguridad de la información

Categoría	Criterios de clasificación
Denegación de servicio	- El sistema de información - no responde por alta cantidad de peticiones. - El sistema de información se encuentra con latencia o degradación del servicio - Ataque DOS DDOS.
CSIRT	Incidente que se materializa a nivel interno, donde se requiere comunicarse con el CSIRT.
Información comprometida	- Corrupción, destrucción intencionada o exitosa, divulgación de información corporativa sensible o de propiedad intelectual. - Se evidencia divulgación no autorizada de información de la Unidad. - Robo o perdida de información Sensible.
Activos comprometidos	Equipo comprometido, dispositivos de red, aplicaciones, cuentas de usuario. Esto incluye equipos infectados con malware donde el atacante controla activamente al equipo.
Actividad ilegal	Robo, fraude, pornografía infantil, incidentes relacionados con la informática de naturaleza criminal, que posiblemente impliquen la aplicación de la ley y/o investigaciones judiciales.
Hacking Interno	Reconocimiento de actividad sospechosa que se origina desde el interior de la red corporativa de la Unidad, excluyendo el malware.
Hacking Externo	Reconocimiento de actividad sospechosa que se origina fuera de la red corporativa de la Unidad, internet, redes de terceros, excluyendo el malware
Correo electrónico	Correos electrónicos falsos, spam y otros correos relacionados con eventos de seguridad.
Malware	- Virus o gusano que afecta típicamente a múltiples dispositivos de la Unidad, esto no incluye el equipo comprometido que está siendo controlado activamente por un atacante a través de una puerta trasera o un troyano

[2] Fuente: Infosec

Categoría	Criterios de clasificación
	- Daño (modificación o indisponibilidad de la información) que se manifiesta en memorias USB que alteran la información. - Daño (modificación o indisponibilidad de la información) que se manifiesta en un equipo y el vector de propagación fue por medio de USB contaminada o correo malicioso.
Violación de Políticas	- Uso inadecuado de los activos de información. - Compartir material de la Unidad, que se encuentre protegido por derechos de autor, además que se clasifique en confidencial o reservado. - Incumplir las políticas de seguridad de la información establecida en la Unidad. - Uso inapropiado de activos corporativos como equipo de cómputo, red o aplicación, y/u otro activo que se le sea asignado. - Ingresar de manera no autorizada aprovechando privilegios asignados para configurar controles de acceso.

4. NORMATIVIDAD APLICABLE

La Normatividad requerida para el desarrollo de las actividades citadas en el presente procedimiento se encuentra definida en el Normograma de la Unidad, disponible para consulta en la página web.

5. CRITERIOS DE OPERACIÓN

- Se debe cumplir con las políticas y lineamientos del Sistema Integrado de Gestión.
- Se debe ejecutar este procedimiento para registrar incidentes relacionados con Seguridad de la Información.
- Cualquier incidente de seguridad de la información debe registrarse en la mesa de servicios tecnológicos quien se contactará con el grupo de seguridad de la información.
- Se debe hacer seguimiento de manera periódica a la ejecución de este procedimiento por parte del personal que sea definido en el marco del Subsistema de Gestión de Seguridad de la Información.
- Dependiendo de la categoría la evidencia será almacenada por el grupo de seguridad de la OTI
- El tiempo de gestión frente al incidente varía dependiendo de su naturaleza.

- Las categorías que están incluidas para los incidentes de seguridad de la información son: Información comprometida, activos comprometidos, actividad ilegal, hacking interno, hacking externo, correo electrónico, malware, violación de políticas.
- El funcionario, contratista y/o colaborador de la Unidad, debe colaborar y/o entregar la información completa requerida por el grupo de seguridad de la OTI.
- El funcionario, contratista y/o colaborador de la Unidad es responsable de realizar el respaldo de la información crítica de la Unidad para la Atención y Reparación Integral a las Victimas existente en su estación de trabajo asignada para el desempeño de sus funciones.
- De acuerdo con el diagnóstico realizado por el grupo de seguridad de la OTI el caso podrá ser escalado al grupo de control interno disciplinario.
- Las políticas, directrices, manuales y/o cualquier documento generado en el marco del subsistema de seguridad de la información será de estricto cumplimiento por parte de funcionarios, contratistas y/o colaboradores.

6. DESCRIPCION DE ACTIVIDADES

N° PC	Descripción	Entradas Insumos	Responsable/área o grupo de trabajo	Salidas, productos, registros	CI/CE
1.	Recibir el incidente mediante correo electrónico y/o caso reportado en la Mesa de Servicios a través de los diferentes medios con que cuentan los usuarios: -Cuenta de correo: soporte.oti@unidadvictimas.gov.co - Portal web: http://mesadeservicios.unidadvictimas.gov.co/usdkv8/ - Marcando #5, Según lo establecido en el procedimiento de soporte técnico a la infraestructura tecnológica.	Correo y/o solicitud	Mesa de servicios Tecnológicos O Grupo de seguridad de la información OTI	Ticket en Mesa de Servicios	CI
2. PC	Verificar si el caso reportado corresponde a un incidente de seguridad de la información. ¿El caso corresponde a un incidente de seguridad de la información? En caso afirmativo, continuar con la actividad 4 En caso negativo continuar con la actividad 3.	Ticket en Mesa de Servicios	Mesa de servicios Tecnológicos O Grupo de seguridad de la información OTI	N.A.	CI
3.	Continua según lo establecido en el procedimiento de soporte técnico a la infraestructura tecnológica. Continua con la actividad 9.	Ticket en Mesa de Servicios	Mesa de servicios Tecnológicos	Ticket en Mesa de Servicios	CI
4.	Atender el incidente, recolectando la evidencia.	Ticket	Grupo de seguridad de la información OTI	Evidencia	CI
5.	Generar respuesta del incidente	Ticket	Grupo de seguridad de la información	- Ticket	CI

N° PC	Descripción	Entradas Insumos	Responsable/área o grupo de trabajo	Salidas, productos, registros	CI/CE
			OTI		
6. PC	Validar si el caso debe ser escalado a las Entidades compentetes. El caso debe ser escalado a entidades competentes? De ser afirmativo, continuar con la actividad 7. En caso de ser negativo, continuar con la actividad 8	Ticket	Grupo de seguridad de la información OTI	N.A.	CI
7.	Notificar a grupos de interés o entidades competentes.	Ticket	Grupo de seguridad de la información OTI	Correo electrónico	CE
8.	Cierre del ticket, según lo establecido en el procedimiento de soporte técnico a la infraestructura tecnológica.	Ticket	Grupo de seguridad de la información OTI	Registro del cierre del caso	CI
9.	Fin del procedimiento				

7. ANEXOS

No aplica

8. CONTROL DE CAMBIOS

Versión	Fecha del cambio	Descripción de la modificación
1	25/08/2017	Creación del procedimiento
2	27/12/2017	Ajuste frente a inclusión de categorías de incidentes de seguridad de la información, puntos de control