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, en base a un caso de afectación de la información almacenada en equipos de cómputo o sistemas de información, que ocasione la perdida, divulgación o modificación no autorizada de información. Y finaliza con la respuesta al incidente mediante correo electrónico y cierre de ticket de la mesa de servicios tecnológicos.

3. DEFINICIONES[1]:

- INFORMACIÓN[2]: 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 a la seguridad de La información que afecte la integridad, confidencialidad o disponibilidad de la Información de la Entidad.

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

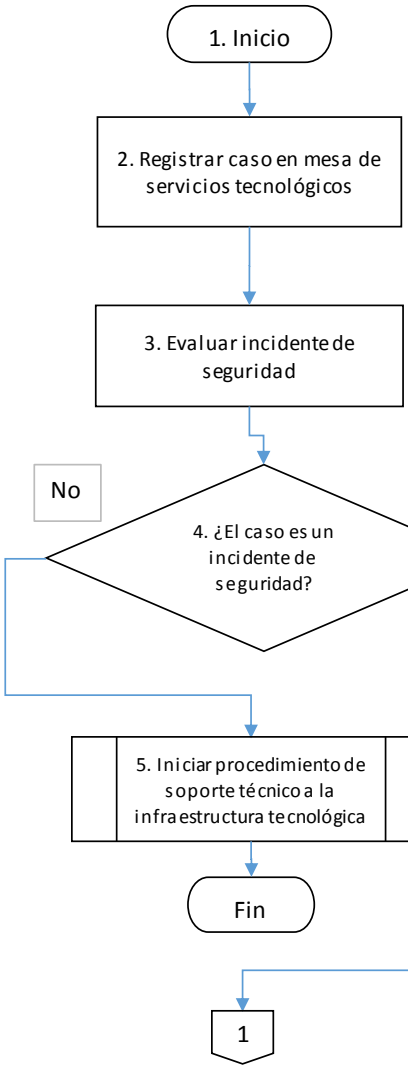
- CONFIDENCIALIDAD: Propiedad de la información restringe su disposición o revelación a individuos, entidades o procesos no autorizados

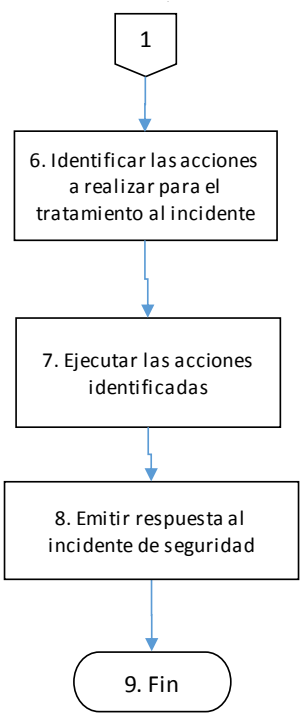
- DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera un individuo, entidad o procesos autorizados

[1] Fuente de definiciones http://www.iso27000.es/glosario.html

[2] Fuente de definición http://www.iso27000.es/sgsi.html

4. ACTIVIDADES:

N°	Actividades (Diagrama de Flujo)	Descripción	Responsable	Registro
1		Inicio del procedimiento		
2		Todo funcionario, contratista o colaborador debe reportar a la mesa de servicios tecnológicos cualquier caso de pérdida, modificación o divulgación no autorizada de la información, por medio del correo soporte.oti@unidadvictimas.gov.co	Funcionarios / Contratistas / Colaboradores	Correo electrónico Ticket
3		Evaluación interna que permite determinar si el caso corresponde a un incidente de seguridad de la Información para realizar el correspondiente escalamiento	Oficina de Tecnologías de la Información	NA
4 PC		Validar si el caso corresponde a un incidente de seguridad. Si la validación es afirmativa, continúa con la actividad 6; de lo contrario continúa con la actividad 5.	Oficina de Tecnologías de la Información	Correo electrónico
5		Si el caso reportado no corresponde a un incidente de seguridad de la información, se debe remitir al procedimiento de soporte técnico y finaliza el procedimiento	Oficina de Tecnologías de la Información	Soportes definidos en el procedimiento

N°	Actividades (Diagrama de Flujo)	Descripción	Responsable	Registro
6		En base al análisis del incidente, dependiendo de la información afectada y la ubicación de los activos involucrados, se determinan las actividades a realizar orientadas a proteger la información.	Oficina de Tecnologías de la Información	Correo electrónico
7		Se ejecutan y documentar las acciones identificadas, para la atención del incidente de seguridad incluyendo las fases de contención o aislamiento y tratamiento especial de cada caso.	Oficina de Tecnologías de la Información	Correo electrónico
8		Emitir respuesta con las conclusiones del tratamiento del incidente de seguridad de la actividad 7 y cierre de ticket en mesa de servicios	Oficina de Tecnologías de la Información	Correo electrónico
9		Fin del procedimiento		

5. DOCUMENTOS DE REFERENCIA: NA

ANEXOS:

Anexo 1 Control de cambios

Versión	Ítem del cambio	Cambio realizado	Motivo del cambio	Fecha del cambio
1	Versión inicial			29/04/2016