1. OBJETIVO:

Gestionar de manera adecuada los eventos e incidentes de seguridad de la información a través de las directrices definidas para que sean identificados, analizados, mitigados y tratados de manera oportuna.

2. ALCANCE:

Inicia con el reporte del posible incidente/ evento a través de los canales de mesa de ayuda que estén disponibles para tal fin, adjuntando la información/evidencia recolectada y finaliza cuando se realiza la evaluación de la evidencia y documentación generada para determinar si la situación presentada debe reportarse ante las instancias consideradas.

3. GENERALIDADES:

El canal a través del cual deben reportarse los incidentes/eventos es el correo electrónico de la mesa de ayuda: soportetic@agenciaatenea.gov.co

4. DESCRIPCIÓN DE ACTIVIDADES:

No	Descripción de la actividad	Responsable	Registro
	Inicio		
1	Reportar el posible incidente/ evento a través de los canales de mesa de ayuda que estén disponibles para tal fin, adjuntando la información/evidencia recolectada. El Colaborador y/o Proveedor debe reunir la información sobre la posible ocurrencia del incidente/evento de seguridad de la información (la cual será utilizada en la atención de este), como por ejemplo, capturas de pantalla, correos electrónicos, fotografías, videos entre otros.	Colaboradores institucionales y/o Proveedores	Correo electrónico institucional de la Mesa de Ayuda.
2	Comprobar la veracidad y exactitud de la información que se suministra y si es suficiente para la atención del caso, de lo contrario deberá ser completada por el profesional de la Subgerencia de Tecnologías de la Información y las Comunicaciones.	Profesional designado por la Mesa de ayuda de la Subgerencia de Tecnologías de la Información y las Comunicaciones	Correo electrónico institucional de la Mesa de Ayuda.

No	Descripción de la actividad	Responsable	Registro
3 P. C	Realizar la primera clasificación, evidenciando si este es un incidente, teniendo en cuenta los criterios establecidos en la Guía de Gestión de Incidentes de Seguridad de la Información. ¿Fue clasificado como incidente? SI: Continuar con actividad 5 NO: Continuar con actividad 4	Mesa de ayuda de la Subgerencia de Tecnologías de la Información y las Comunicaciones	No aplica
4	Evaluar la clasificación de la solicitud. Finaliza del procedimiento.	Mesa de ayuda de la Subgerencia de Tecnologías de la Información y las Comunicaciones	Correo electrónico institucional.
5 P. C	Clasificar el evento como incidente de seguridad de la información en la herramienta de mesa de ayuda. ¿El incidente es categorizado de alto impacto? SI: pasa a la actividad 6 NO: pasa a la actividad 8 **Nota 1:** Conforme a la prioridad e impacto se categorizará el incidente para iniciar la atención (se deben tener en cuenta los criterios establecidos en la Guía de Gestión de Incidentes de Seguridad de la Información) **Nota 2:** De acuerdo con la clasificación y categorización del incidente, se asigna al grupo interno del proceso, el cual debe iniciar la atención de este.	Profesional designado por la Mesa de ayuda de la Subgerencia de Tecnologías de la Información y las Comunicaciones	Correo electrónico
6	Citar a la Mesa de Incidentes, si el incidente es considerado de alto impacto(conforme a lo establecido en la Guía de Gestión de Incidentes de Seguridad de la Información)	Subgerente de Tecnologías de la Información y las Comunicaciones	Correo electrónico
7	Notificar a las partes interesadas sobre la interrupción del servicio que se generó a raíz del incidente y solicitar a la Dirección General, a través de las estrategias de comunicación, la divulgación de la información sobre incidente presentado.	Profesional designado por la Subgerencia de Tecnologías de la Información y Comunicaciones	Correo electrónico/pieza gráfica/comunicado

No	Descripción de la actividad	Responsable	Registro
9	Definir y ejecutar las acciones para contener el incidente y erradicar la causa raíz, minimizando su impacto. **Nota:** En algunos casos la solución del incidente puede ser dada desde la contención, sin embargo, en otros casos se requiere la recuperación o restauración del servicio a su estado normal de operación.	El profesional designado por la Subgerencia de Tecnologías de la Información y Comunicaciones	Correo electrónico institucional. Formato Reporte de Incidentes de seguridad de la información
10	Documentar el incidente a través del Formato Reporte de Incidentes de seguridad de la información y los casos que se consideren se debe generar un reporte técnico independiente, así como un plan de mejoramiento.	Profesional designado como Oficial de Seguridad de la Información	Correo electrónico institucional. Formato Reporte de Incidentes de seguridad de la información
11	Documentar a través de la herramienta de mesa de ayuda y cargar el Formato Reporte de Incidentes de seguridad de la información. ¿El incidente se debe reportar ante alguna autoridad competente? SI: Continuar con la actividad 12 NO: Finalizar el procedimiento	Los profesionales designados por la Subgerencia de Tecnologías de la Información y Comunicaciones	Correo electrónico institucional.
12	Evaluar la evidencia y documentación generada para determinar si la situación presentada debe reportarse ante las instancias consideradas en la Guía de Gestión de Incidentes de seguridad de la información	Profesional designado como Oficial de Seguridad de la Información de la Subgerencia de las Tecnologías de la Información y Comunicaciones	Correo electrónico Comunicado página web de autoridad competente
	Fin		

Punto de Control: P.C.

5. **RESULTADO FINAL:** Contención, erradicación y documentación de los incidentes de seguridad de la información**.**

6. **DEFINICIONES:** Describir las siglas y dar la definición de términos desconocidos y/o técnicos propios del procedimiento que son necesarios para su ejecución.

Evento de seguridad de la información: Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad y privacidad de la información, una

falla en los controles o una situación previa desconocida hasta el momento y que puede ser relevante para la seguridad.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.

Gestión de incidentes de seguridad de la información: Procesos para la detección, reporte, evaluación, respuesta, tratamiento y aprendizaje de incidentes de seguridad de la información.

Sistema de Información: Aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar información

7. **DOCUMENTOS DE REFERENCIA:** Referenciar los documentos internos o externos como procedimientos, instructivos, normas, etc., que contenga información asociada y/o conectada al procedimiento.

- Ley 1273 5-ene-2009: “Por medio de la cual se modifica el Código Penal. Título VII Bis “De la protección de la información y de los datos”. Artículos 269A a 269J.
- Ley 1581 17-oct-2012: “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Decreto 1377 de 2013: “Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015”.
- Decreto 886 13-may-2014: “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos”.
- Decreto 2573 12-dic-2014: “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones”.
- Resolución 500 de 2021: “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
- Decreto 1008 14-jun-2018: “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”.
- Política de Gobierno Digital
- Manual de Políticas de Seguridad de la Información
- Guía de Gestión de Incidentes de Seguridad

8. **RELACIÓN DE FORMATOS:**

CODIGO	NOMBRE DEL FORMATO
F1_P2_TIC	Reporte Incidentes de seguridad de la información

9. ANEXOS: No Aplica

10. CONTROL DE CAMBIOS:

Fecha	Versión	Descripción del Cambio
06/06/2023	V2 GTI-PR-02	Se modifica el procedimiento en los siguientes aspectos: Cambio de estructura de presentación de la información, ajuste en cada uno de sus ítems, lo que incluye modificación en la descripción de las actividades del procedimiento, responsabilidades, cambio en la asignación del código, entre otras. En este mismo sentido, se modifica el Formato Reporte Incidentes De Seguridad De La Información creándose la versión 3 del documento. Todo lo anterior de acuerdo con las directrices establecidas en el Procedimiento de Elaboración, Modificación o Anulación de Documentos y Control de Documentos.
16/01/2023	V1 GTI-PR-02	Modificación de pie de página según manual de identidad de Atenea y asignación cuadro control de cambios.

VALIDACIÓN	NOMBRE	CARGO	FECHA
Elaboró	**Maria Alejandra Suarez**	**Contratista – Subgerencia TIC**	**19/05/2023**
Revisó	**Lira Jazmin Pineda Moreno**	**Subgerente TIC**	**26/05/2023**
Aprobó	**Lira Jazmin Pineda Moreno**	**Subgerente TIC**	**26/05/2023**