1. OBJETO:

Definir los lineamientos para el reporte, identificación y análisis de incidentes de seguridad de la información o eventos, que permitan gestionarlos de forma oportuna y adecuada mitigando el impacto a las posibles pérdidas de la confidencialidad, integridad y disponibilidad de la información o continuidad del negocio y operaciones de la Entidad.

2. ALCANCE:

Aplica para el personal de la Oficina TIC encargado de gestionar los reportes y posibles incidentes de seguridad de la información.

Inicia con el reporte de un posible incidente de seguridad de la información que afecte la confidencialidad, integridad y disponibilidad, continua con la solución o restablecimiento del servicio y finaliza con el cierre.

3. DEFINICIONES:

Activos de información: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tenga valor para la organización y por lo tanto se debe proteger.

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

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

Disponibilidad: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

Evento: Cualquier cambio de estado que tenga importancia para la gestión de un servicio o elemento de configuración. Los eventos generalmente se reconocen a través

de notificaciones creadas por un servicio TI, elemento de configuración o herramienta de monitoreo.

Incidente: Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar, una interrupción o una reducción de la calidad de este.

Incidente de seguridad de la información: Un evento o una serie de eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la organización y amenaza la seguridad de la información. [ISO/IEC 27000:2018].

Información: Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos.

Log o Logs: Registro o Registros. Termino técnico usado para los datos en digital que se genera en los sistemas (Servidores, Aplicaciones, Programas, etc) en forma de trazas textuales en el que constan cronológicamente los acontecimientos que afectan a un sistema o el conjunto de cambios que generan.

Mesa de Servicios: Es un conjunto de recursos tecnológicos y humanos, encargado de recibir, gestionar y resolver las solicitudes y problemas de los usuarios en una organización, brindando soporte y asistencia técnica de manera eficiente y efectiva como principal y único punto de contacto con la Oficina de Tecnologías de la Información y Comunicaciones.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital.

Seguridad Digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

4. NORMATIVA:

NUMERO	DESCRIPCIÓN
Ley 1581 del 17 de octubre de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 del 6 de marzo de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 2573 del 12 de diciembre de 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.
Decreto 103 del 20 de enero de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1078 del 26 de mayo de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1081 del 26 de mayo de 2015	Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.
Decreto 415 del 7 de marzo de 2016	Lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Decreto 1008 del 14 de junio de	Por el cual se establecen los lineamientos generales

NUMERO	DESCRIPCIÓN
2018	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.
CONPES 3701 del 14 de julio de 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES 3854 del 11 de abril de 2016	Política Nacional de Seguridad Digital.
CONPES 3920 del 17 de abril de 2018	política nacional de explotación de datos (big data).
Resolución 500 del 10 de marzo 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.

5. LINEAMIENTOS DE OPERACIÓN

5.1 Todo evento o posible incidente de seguridad de la información, debe ser reportado en mesa de ayuda. El registro puede venir de un reporte de usuario final de acuerdo con el GTI-PC-05 o de cualquier indicador de eventos.

5.2 Todo incidente de seguridad digital catalogado con un nivel de impacto Grave o Muy Grave, debe ser notificado al CSIRT Gobierno, para el respectivo apoyo y coordinación en la gestión.

5.3 Todo incidente de seguridad digital catalogado con un nivel de impacto Menos Grave o Menor, debe ser notificado al CSIRT Gobierno una vez gestionados.

6. DESCRIPCIÓN DE ACTIVIDADES:

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
1	**Registrar el incidente** Registra el posible incidente de seguridad de la información e informa al oficial de seguridad de la información.	Mesa de Servicio	Administrador Mesa de Servicio	Reporte Mesa de Servicio
2	**Categorizar el incidente** Categoriza o recategoriza el tipo de incidente. Si es necesario, consulte y convoque a las personas necesarias del equipo de respuesta a incidentes.	GTI-IN-03 Tratamiento de Incidentes de Seguridad de la Información. Mesa de Servicio	Oficial de Seguridad de la información	Creación del ticket en la herramienta Mesa de Servicio
	¿Es un incidente de seguridad de la información? **Si**: Continúa con la actividad No 3. **No**: Continúa con el procedimiento GTI-PC-05 Soporte a la infraestructura tecnológica y finaliza el			

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	procedimiento.			
3	**Realizar Clasificación y priorización del Incidente** Clasifica y define nivel de prioridad de acuerdo con el Instructivo Gestión de Incidentes.	GTI-IN-03 Tratamiento de Incidentes de Seguridad de la Información	Oficial de Seguridad. Administrador Mesa de Servicio.	Registro en la herramienta Mesa de Servicio
4	**Asignar el caso en la herramienta** Asigna el caso al soporte en sitio o de primer nivel para la atención del requerimiento o Incidente.	Mesa de Servicio	Administrador Mesa de Servicio	Registro en la herramienta Mesa de Servicio
5	**Gestionar el Incidente** Gestiona el incidente de acuerdo con los planes definidos para la categoría del incidente relacionada en el GTI-IN-03. **Nota 1**: Si el incidente no puede ser solucionado o su tratamiento no es efectivo, continuar con la actividad No 6.	GTI-IN-03 Tratamiento de Incidentes de Seguridad de la Información. Lineamientos de Operación	Profesional, contratista o Técnico Oficina TIC	

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	¿Se debe reasignar? **Si**: Continúa con la actividad No 6. **No**: Continúa con la actividad No 8.			
6	**Escalar o Reasignar reporte** Escala de acuerdo con la información de contacto que tiene la Mesa de servicios. **Nota**: De ser necesario, escalar los incidentes hasta los proveedores, fabricantes o autoridades competentes.	Mesa de servicios Sistema de Gestión Documental Correo Electrónico	Responsable del caso	Actualización del reporte en Mesa de servicios Comunicación oficial
7	**Reportar a organismos de emergencia cibernética** Informa al jefe de la Oficina TIC y Reporta a CSIRT Gobierno (Equipo de Respuesta a Incidentes de Seguridad Digital). Nota 1: Si se considera pertinente, reportar al ColCERT o el Centro	Lineamientos de Operación Correo Electrónico Medio definido por el organismo de ciberseguridad	Jefe de la Oficina TIC. Oficial de seguridad de la información	Reporte comunicación Oficial

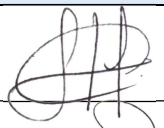
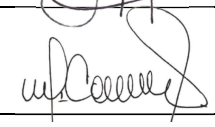
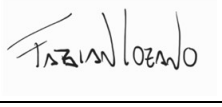
No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	Cibernético Policial CCP. Nota 2: De acuerdo con el impacto, regrese a la actividad 4 y gestione, o siga las instrucciones del CSIRT o quien haga sus veces.			
8	**Realizar el reporte Interno** Reporta a Subdirección de Asuntos Legales o a la Oficina de Control Disciplinario Interno para las acciones a que haya lugar, si el jefe de la Oficina TIC junto con el Oficial de seguridad evidencian u observan intencionalidad del funcionario, contratista o tercero.	Correo Electrónico	Jefe de la Oficina TIC. Oficial de seguridad de la información	Reporte por comunicación oficial interna
9	**Documentar las evidencias** Documenta las evidencias producto de la investigación, tratamiento y solución del incidente.	GTI-IN-03 Tratamiento de Incidentes de Seguridad de la Información	Oficial de seguridad de la información	Registro en la herramienta Mesa de Servicio. Bitácora

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	Ejemplo: Registros o logs de monitoreo, logs de routers, firewall, información de servidores, información de aplicaciones, conexiones de red, listado de puertos, testimonio de funcionarios o contratistas y demás información relevante para la investigación, solución e informe de cierre.	Mesa de Servicio		
10	**Cerrar el incidente y ticket** Da solución al incidente en la herramienta, luego de la gestión realizada por la persona responsable del caso, y cerrar el ticket.	Mesa de Servicio	Profesional, contratista o Técnico Oficina TIC	Registro en la herramienta Mesa de Servicio
11	**Registrar las lecciones Aprendidas** Registra las lecciones aprendidas y las comunica al personal técnico, usuarios u organismos que correspondan.	Mesa de Servicio	Oficial de seguridad de la información	Registro en la herramienta Mesa de Servicio. Bitácora

7. CONTROL DE CAMBIOS:

Versión	Fecha	Descripción de la modificación
1	06/08/2021	Creación del documento
2	10/07/2023	Se ajusta el nombre del documento, de "Reporte de incidentes de seguridad de la información" a "Gestión de incidentes de seguridad de la información". Se eliminan las actividades asociadas al procedimiento GTI-PC-05 y se ajustan las asociadas a gestión de incidentes

8. AUTORIZACIONES:

	NOMBRE	CARGO	FIRMA
Elaboró	Juan Sebastián Perdomo Méndez	Profesional Universitario Oficina TIC	
	Maria Consuelo Torres Pinto	Contratista – Oficina TIC	
	Fabian Andres Lozano Aguilar	Contratista – Oficina TIC	
	Eduardo Andres Rozo Revelo	Profesional Universitario – Oficina TIC	
Revisó	Cesar Mauricio Beltrán López	Jefe Oficina TIC	
	Luz Mary Palacios Castillo	Profesional Universitario Oficina Asesora de Planeación	
Aprobó	Yesly Alexandra Roa	Jefe Oficina Asesora de Planeación	Alexandra Roa Mendoza Firmado digitalmente por Alexandra Roa Mendoza Fecha: 2023.07.07 19:10:28 -05'00'