PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

CÓDIGO:D103PR03
Versión: 01
Fecha:2021-02-23

IMPORTANTE: Cómo leer este procedimiento

	Estructura del Procedimiento:	**Sección 1.** Generalidades: esta sección se compone de objetivo, alcance, disposiciones generales sobre el procedimiento, definiciones y documentos asociados. **Sección 2.** Descriptivo de las actividades del procedimiento: esta sección da una descripción detallada de cada actividad, tiempos, responsables, registros e identificación de controles para gestionar los incidentes de seguridad de la información. **Sección 3.** Registro de aprobación: esta sección registra los cambios que se efectúan en cada versión donde se registra el nombre y cargo de quien elabora, revisa y aprueba el procedimiento. **Sección 4.** Línea de tiempo: describe los tiempos máximos para ejecutar cada una de las actividades contempladas en el descriptivo, bajo condiciones normales de operación.

	Convenciones del descriptivo:	**Actividades genéricas**	*Registros en cursiva y subrayado: Controlados por el SGC y disponibles en GINA*	**Puntos de Control:** Implican verificaciones, revisiones y toma de decisiones.
	Cómo hacer lectura del descriptivo	**Procedimiento = Descripción General + Modalidad Específica**		

1. OBJETIVO

Detectar, reportar, controlar, monitorear y responder de manera oportuna y apropiada ante la ocurrencia de un evento y/o incidente de seguridad de la información presentados en el Ministerio de Ciencia Tecnología e Innovación.

2. ALCANCE

Aplica a funcionarios, contratistas, proveedores y terceros con acceso autorizado a los recursos tecnológicos y activos de información del Ministerio de Ciencia Tecnología e Innovación. La gestión de incidentes de seguridad de la información está compuesto por etapas, iniciando con la preparación ante un incidente de seguridad, seguido de las etapas de detección, contención, erradicación, recuperación del incidente de seguridad de la información, y finalizando con las lecciones aprendidas .

3. DISPOSICIONES GENERALES

De acuerdo a los lineamientos dados por el Ministerio de Tecnologías de la Información y Comunicaciones - MinTIC a través de sus decretos y normativa reglamentaria, específicamente del componente del Modelo de Seguridad y Privacidad de la Información - MSPI, se elabora el presente procedimiento en cumplimiento de estas directrices.

El Modelo de Seguridad y Privacidad de la Información - MSPI se apoya en las buenas prácticas establecidas en la norma ISO 27001 de 2013, la Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", la Ley 1712 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”, entre otras,

El MSPI se encuentra alineado con los objetivos institucionales y requisitos de seguridad, con el fin de garantizar la preservación de la integridad, confidencialidad y disponibilidad de la información, por tal razón el procedimiento fue elaborado tomando como base las buenas prácticas de la gestión de incidentes de seguridad de la información que dispone la norma ISO 27035 y en cumplimiento a las guías emitidas por MinTIC para la elaboración del mismo.

	Nivel del Incidente: Considerando la criticidad de la información y la protección de los activos que la soportan, la respuesta a incidentes de seguridad se consolida como una herramienta estratégica que permite al Ministerio, no solo estar en la capacidad de dar respuesta oportuna a incidentes de seguridad, sino también detectar, evaluar y gestionar las vulnerabilidades de la plataforma tecnológica que soporta la operación informática, de los sistemas de información misional, de gestión administrativa y de apoyo, y principalmente de los medios que alojan los activos de información del Ministerio. La severidad del incidente puede ser: * **Alto Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales del Instituto. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata. **- Medio Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado. **- Bajo Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.
	Clasificación del Incidente: Está sujeta a la infraestructura, riesgos y criticidad de los activos * **Acceso no autorizado:** Es un incidente que involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información. * **Modificación de recursos no autorizado:** Un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento. * **Uso inapropiado de recursos:** Un incidente que involucra a una persona que viola alguna política de uso de recursos. * **No disponibilidad de los recursos**: Un incidente que involucra a una persona, sistema o código malicioso que impide el uso autorizado de un activo de información. * **Multicomponente:** Un incidente que involucra más de una categoría anteriormente mencionada. * **Otros:** Un incidente que no puede clasificarse en alguna de las categorías anteriores. Este tipo de incidentes debe monitorearse con el fin de identificar la necesidad de crear nuevas categorías. En los casos que se sospechen de Fuga de Información por parte de funcionarios, contratistas, proveedores y terceros con acceso autorizado a los recursos tecnológicos y activos de información del Ministerio de Ciencia Tecnología e Innovación se debe realizar las siguientes acciones: *Detectar el Incidente de seguridad *Confirmar el Incidente de Seguridad (Realizar investigación del incidente que involucra a la persona) *El usuario es Inactivado inmediatamente, restringiendo el acceso a los servicios. *Una vez se determine si se presento el incidente de seguridad se inhabilita el usuario, de lo contrario se reactiva el Usuario
	Reportar incidentes de seguridad a los entes externos: En caso de presentarse un incidente de seguridad de la información el Representante legal o a quien este delegue, son los únicos autorizados para reportarlos de ser necesario. Se pueden reportar incidentes de seguridad de la información a través de los siguientes canales: - ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), reportar al correo electrónico: contacto@colcert.gov.co o al Teléfono: (+571) 2959897. - CSIRT Gobierno reportar al correo csirtgob@mintic.gov.co - Centro cibernético Policial reportar en la siguiente ruta: https://caivirtual.policia.gov.co/

¿Que situaciones se consideran como incidentes de Seguridad de la Información? Cualquier situación que atenta contra la confidencialidad, integridad y disponibilidad de la información, algunos casos pueden ser:

* Daño o pérdida de información.
* Modificación no autorizada de la información.
* Suplantación de identidad.
* Acceso no autorizado.
* Pérdida o alteración de registros de base de datos.
* Pérdida de un activo de información.
* Presencia de código malicioso “malware, Ransomware”
* Incumplimiento de las políticas de seguridad de la información
* Violación a Políticas de Seguridad de la Información
* Denegación al Servicio
* Fallas de Infraestructura Tecnológica que afecte los principios fundamentales de seguridad

Desde la oficina de Tecnologías y Sistemas de Información se determinan los siguientes roles para el manejo del incidente de Seguridad:
Analista Nivel 1: Analista de primera línea de soporte, es el contacto directo o punto de entrada de todas las solicitudes de usuario.
Analista Nivel 2: Analista especialista en temas determinados dentro de los servicios ofrecidos por la Oficina de Tecnologías y Sistemas de Información, para los usuarios internos y externos.
Responsables del Incidente de Seguridad: Son los responsables que intervienen en el manejo del incidente de seguridad.

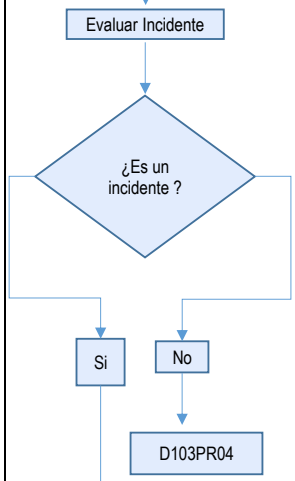
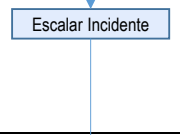
4. DEFINICIONES

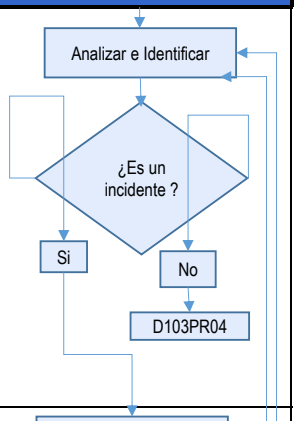
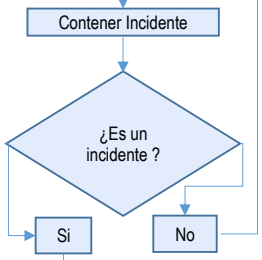
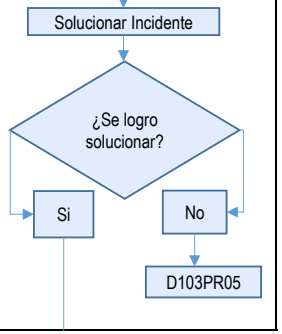
Activo de información:	Es todo aquello que representa valor para la Entidad desde software, hardware, información, servicios y personas.
Amenaza:	Posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática.
Confidencialidad	Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
Daño Antijurídico	El perjuicio que es provocado a una persona que no tiene el deber jurídico de soportarlo. La Corte considera que esta acepción del daño antijurídico como fundamento del deber de reparación del Estado armoniza plenamente con los principios y valores propios del Estado Social de Derecho, pues al propio Estado corresponde la salvaguarda de los derechos y libertades de los particulares frente a la actividad de la administración
Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera un individuo, entidad o procesos autorizados
Evento de Seguridad de la Información	Se refiere a algo que pueda afectar los niveles de riesgo, sin afectar de forma necesaria al negocio o a la información.
Incidentes Seguridad de la Información:	Es un evento adverso que atenta contra los principios fundamentales de la seguridad como son: la disponibilidad, confidencialidad e integridad, así mismo es alguna violación o inminente amenaza de violación de una política de seguridad de la información.
Integridad:	Propiedad de la información relativa a su exactitud y completitud.

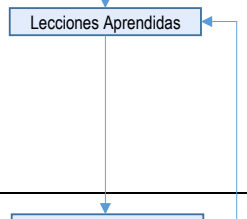
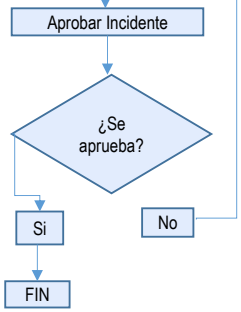
Mesa de Servicios:	Es un conjunto de servicios que ofrece la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados con las Tics (Tecnologías de Información y Comunicaciones)
Riesgo de seguridad informática:	Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o eliminar.
Vulnerabilidad:	Debilidad de los sistemas, ya sean equipos de computo, servidores, tanto hardware como software, sistema operativo, sistemas de información, aplicaciones, redes, etc. que puede ser utilizados o aprovechados por delincuentes informáticos, con el fin de ocasionar daño o extraer información confidencial y datos personales.

5. DOCUMENTOS DE REFERENCIA

Documentos internos de referencia	Gestión de Incidentes (Código: D103PR04)
Documentos externos controlados	Norma ISO 9001: 2015 (consulta en medio físico Oficina Asesora de Planeación e Innovación Institucional - Equipo Calidad).
Normatividad Legal Asociada	ISO 27001 de 2013, la Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", la Ley 1712 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”

N°	6. DESCRIPCIÓN GENERAL	RESPONSABLE	TIEMPOS	*REGISTROS*	DIAGRAMA DE BLOQUES
1	**Reportar posible incidente de seguridad.** Se debe reportar el posible incidente de seguridad de la información a la herramienta mesa de servicios ver procedimiento de Gestión de Solicitudes (Código D103PR01), cualquier situación que atenta contra la confidencialidad, integridad y disponibilidad de la información **Nota:** En algunos casos la identificación de un Incidente se obtiene a través de herramientas de auditoria para infraestructura tecnológica, que de igual manera se reportará en la herramienta mesa de servicios.	Servidores públicos/ Contratistas/ Terceros	Cuando se presente un incidente de seguridad	Herramienta Mesa de Servicios - Ticket	
2	**Evaluar incidente de seguridad** Evaluación interna que permita determinar si el caso corresponde a un incidente de seguridad de la Información de acuerdo con la siguiente lista no exhaustiva, para posteriormente realizar el correspondiente escalamiento: * Daño o pérdida de información. * Modificación no autorizada de la información. * Suplantación de identidad. * Acceso no autorizado. * Pérdida o alteración de registros de base de datos. * Pérdida de un activo de información. * Presencia de código malicioso “malware, Ransomware” * Incumplimiento de las políticas de seguridad de la información * Denegación al Servicio * Fallas de Infraestructura Tecnológica que afecte los principios fundamentales de seguridad ¿El caso es un incidente de seguridad de información? **Si:** Continua con la actividad 3 **No:** Iniciar procedimiento Gestión de Incidentes (Código: D103PR04) Nota 1: En el evento de presentarse alguna falla, circunstancia o hecho que pueda afectar la operación de los sistemas de información o infraestructura Tecnológica dispuesta para el manejo y automatización de la información de las convocatorias, se debe informar de manera inmediata de tal situación a la Oficina Asesora Jurídica del Ministerio de Ciencia, Tecnología e Innovación, para que en articulación con el área técnica que corresponda se determine las acciones a seguir. Nota 2 : En algunos casos la evaluación del incidente de seguridad lo puede realizar el analista de nivel 2	Analista Nivel 1/ Analista Nivel 2	Una vez se evalúe el incidente de seguridad	Herramienta Mesa de Servicios - Ticket	
3	**Escalar incidente para su análisis y clasificación** Realizar el escalamiento del incidente de seguridad al Profesional de la Oficina de Tecnologías y Sistemas de Información que apoya la gestión de incidentes de seguridad de la información, para su análisis y clasificación.	Analista Nivel 1	Una vez se identifique como incidente de seguridad de información	Herramienta Mesa de Servicios - Ticket	

N°	6. DESCRIPCIÓN GENERAL	RESPONSABLE	TIEMPOS	*REGISTROS*	DIAGRAMA DE BLOQUES
4	**Analizar e identificar el incidente de seguridad de la información** Se realiza el análisis y clasificación del incidente, con el fin de identificar la causa o causas que dieron origen al incidente de seguridad, dependiendo de la información afectada y la ubicación de los activos involucrados. ⓘ ¿Es realmente un incidente de seguridad de la Información? **Si**: Pasa a la actividad 5. **No:** Se devuelve a la mesa de servicio para su reasignación, activando el procedimiento Gestión de Incidentes (Código: D103PR04) y finaliza el procedimiento.	Analista Nivel 2	Una vez cuando es escalado el incidente	*Informe de Incidente de Seguridad (D103PR03F01)*	
5	**Contener incidente de seguridad** Se realizará todas aquellas tareas necesarias con el fin de contener el incidente de seguridad y así minimizar su impacto ⓘ ¿Se logró contener el incidente de seguridad? **Si**: Continua a la actividad 6 **No**: Devuelve a la actividad 4	Analista Nivel 2 /Responsables del incidente	Depende de la severidad del incidente	*Informe de Incidente de Seguridad (D103PR03F01)*	
6	**Erradicar el incidente de seguridad de la información.** Se realizarán todas aquellas tareas necesarias con el fin de erradicar la causa raíz detectada ⓘ ¿Se logró erradicar el incidente de seguridad? **Si**: Continua a la actividad 7 **No**: Devuelve a la actividad 4	Analista Nivel 2 /Responsables del incidente	Depende de la severidad del incidente	*Informe de Incidente de Seguridad (D103PR03F01)*	
7	**Solucionar el incidente de seguridad** Se realizará todas aquellas tareas necesarias con el fin de solucionarlo. ⓘ ¿Se logró solucionar el incidente de seguridad? **Si**: Continua a la actividad 8 **No**: Iniciar procedimiento de Gestión de problemas (Código:D103PR05)	Analista Nivel 2 /Responsables del incidente	Depende de la severidad del incidente	*Informe de Incidente de Seguridad (D103PR03F01)*	

N°	6. DESCRIPCIÓN GENERAL	RESPONSABLE	TIEMPOS	*REGISTROS*	DIAGRAMA DE BLOQUES
8	**Identificar las evidencias del incidente de seguridad** Recopilar y organizar las evidencias producto de la investigación del incidente de seguridad. Una vez se recolectan las evidencias, se inicia el análisis de las mismas, para determinar el origen y responsables del incidente. **Nota**: Proteger las evidencias	Analista Nivel 2 /Responsables del incidente	Una vez solucionado el incidente	*Informe de Incidente de Seguridad (D103PR03F01)*	
9	**Documentar Lecciones Aprendidas del incidente de seguridad** Se documentan las lecciones aprendidas del incidente, en el formato Informe de Incidente de Seguridad (Código: D103PR03F01), con el fin de reflejar las nuevas amenazas, la mejora de la tecnología y las lecciones aprendidas después de un incidente. **Nota**: Con base en la evidencia y documentación generada, se evalúa si la situación presentada se debe informar a entes de control o autoridades competentes.	Analista Nivel 2	Una vez solucionado el incidente	*Informe de Incidente de Seguridad (D103PR03F01)*	
10	**Revisar y aprobar respuesta a incidentes de seguridad.** El Informe de Incidente de Seguridad (Código: D103PR03F01) es revisado y aprobado por los responsables que interactuaron durante la atención del incidente. ¿Se aprueba el informe de incidente de seguridad? **Si:** Fin del procedimiento **No:** Devuelve a la actividad 9 **Nota1:** Los responsables del incidente varían dependiendo del incidente presentado **Nota2:** La aprobación del informe se realiza por parte de cada uno de los responsables que interactuaron en el incidente.	Analista Nivel 2	Una vez solucionado el incidente	*Informe de Incidente de Seguridad (D103PR03F01)* Lista de asistencia	

7. CONTROL DE CAMBIOS			
Versión	**Fecha**	**Numerales**	**Descripción de la modificación**
00	29/10/2020	Todos	Creación del documento
1	23/02/2021	2. Alcance 3. Disposiciones Generales 4.Definiciones 6.2 En descripción General	Se ajusta el alcance, donde se incluye las etapas del incidente En Disposiciones Generales se incluye que acciones se deben tomar si se sospecha de Fuga de Información y roles para el manejo del incidente de Seguridad de la Información. En Definiciones se incluye la definición de Daño antijurídico En descripción General, actividad 2 se incluyen otras situaciones de Incidentes de seguridad. Adicionalmente se incluye la nota "En el evento de presentarse alguna falla, circunstancia o hecho que pueda afectar la operación de los sistemas de información o infraestructura Tecnológica dispuesta para el manejo y automatización de la información de las convocatorias, se debe informar de manera inmediata de tal situación a la Oficina Asesora Jurídica del Ministerio de Ciencia, Tecnología e Innovación, para que en articulación con el área técnica que corresponda se determine las acciones a seguir".

V	**Elaboró**	**Revisó**	**Aprobó**
00	**Nombre:**	**Nombre:**	**Nombre:**
	Erika Viviana Chacón Gamba	Lorena Arias Puentes	Elvia Consuelo Castañeda Camargo
	Cargo:	**Cargo:**	**Cargo:**
	Contratista Oficina de Tecnologías y Sistemas de Información	Contratista Oficina Asesora de Planeación e Innovación Institucional	Jefe Oficina de Tecnologías y Sistemas de Información

V	**Elaboró**	**Revisó**	**Aprobó**
01	**Nombre:**	**Nombre:**	**Nombre:**
	Erika Viviana Chacón Gamba	Lorena Arias Puentes	Elvia Consuelo Castañeda Camargo
	Cargo:	**Cargo:**	**Cargo:**
	Contratista Oficina de Tecnologías y Sistemas de Información	Contratista Oficina Asesora de Planeación e Innovación Institucional	Jefe Oficina de Tecnologías y Sistemas de Información