Manual para la gestión de incidentes de seguridad y privacidad de la información

Proceso

Gestión de Servicios de Información y Soporte Tecnológico

Versión 2

22/05/2025

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

El Ministerio de Ambiente y Desarrollo Sostenible, en adelante Ambiente reconoce la importancia de proteger su información y sus recursos informáticos frente a las amenazas internas y externas que puedan comprometer su seguridad. De igual manera, es consciente de su responsabilidad legal y ética de dar cumplimiento a las normas y regulaciones aplicables en materia de seguridad de la información, así como de respetar los derechos y expectativas de las partes interesadas al interior del Ministerio y de todos aquellos que mantengan algún tipo de relación con la entidad.

En este sentido, se formula el presente Manual para la Gestión de Incidentes de Seguridad y Privacidad de la Información, el cual establece los lineamientos y procedimientos para la adecuada gestión, atención y respuesta ante incidentes de seguridad de la información, en conformidad con los principios y requisitos definidos en la Norma Técnica Colombiana NTC-ISO/IEC 27001.

2. OBJETIVO

Establecer las actividades, condiciones y responsabilidades necesarias para gestionar los incidentes de seguridad y privacidad de la información, de manera que se permita su oportuna detección, reporte, evaluación, respuesta, tratamiento y análisis posterior. Todo ello con el propósito de mitigar el impacto asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información, fortaleciendo así la resiliencia institucional y promoviendo la mejora continua.

3. ALCANCE

El presente manual aplica a todos los eventos o incidentes de seguridad de la información que se presenten al interior de la entidad. El proceso inicia con la revisión, análisis y clasificación del incidente de seguridad, y finaliza con el registro y cierre del mismo, con el objetivo de documentar las lecciones aprendidas a través de la mesa de asistencia, fortalecer la gestión del conocimiento institucional y promover la mejora continua, evitando así la repetición o materialización de incidentes similares en el futuro.

4. MARCO LEGAL Y NORMATIVIDAD

El presente documento se elabora con referencia en la Norma Técnica Colombiana NTC-ISO-27001 y la Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información formulada por el Ministerio de las Tecnologías de la Información - MINTIC.

- **Decreto 1008 de 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".

- **Decreto 1499 de 2017:** El Modelo Integrado de Planeación y Gestión - MIPG emitido por la función pública.

- **Decreto 1499 de 2017**: (...) ARTÍCULO 2.2.22.1.5. Articulación y complementariedad con otros sistemas de gestión. El Sistema de Gestión se complementa y articula, entre otros, con los Sistemas Nacional de Servicio al Ciudadano, de Gestión de la Seguridad y Salud en el Trabajo, de Gestión Ambiental y de Seguridad de la Información. (…).

- **Decreto 338 de 2022:** Se formaliza la Definición y el alcance de los Equipos de respuesta a Incidentes Cibernéticos".

- **Decreto 612 de 2018**: Artículo 1. (…) Las entidades del Estado, de acuerdo con el ámbito de aplicación del MIPG, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: (...) 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, 12. Plan de Seguridad y Privacidad de la Información (...).

- **Directiva Presidencial 02 de 2022:** Reiteración de la Política Publica en Materia de Seguridad Digital.

- **Directiva Presidencial 03 del 15 de marzo de 2021:** Respecto a lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

- **NTC-ISO/IEC 27001:2013:** Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI).

- **NTC-ISO/IEC 27002:2013**: Tecnología de la información. Código prácticas para la Gestión de Seguridad en la Información.

- **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. TÉRMINOS Y CONCEPTOS

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Bases de datos personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- **Consecuencia:** Resultado de un evento que afecta a los objetivos [ISO/IEC 27000: 2016].

- **Contención:** Acciones necesarias para garantizar el control del incidente mientras se realiza un análisis más detallado y se definen las acciones necesarias para remediar el incidente.

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Criterios de decisión:** Umbrales, objetivos o patrones utilizados para determinar la necesidad

de una acción o de una mayor investigación, o para describir el nivel de confianza en un resultado determinado. [ISO/IEC 27000: 2016]

- **Evento:** Aparición o cambio de un conjunto particular de circunstancias. [ISO/IEC 27000: 2016]

- **Eventos en seguridad de la información:** Ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o el fracaso de los controles, o una situación previamente desconocida que puede ser la pertinente a seguridad. [ISO/IEC 27000: 2016].

- **Gestión de Incidentes de Seguridad de la Información**: Proceso para detectar, informar, evaluar, responder, tratar, y aprender de los incidentes de seguridad de la información. [ISO/IEC 27000: 2016].

- **Incidente de seguridad digital:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable. (Decreto 338 De 2022 - Gestor Normativo, n.d.)

- **Incidente en Seguridad de la Información**: Un evento o una serie de eventos de seguridad de la información 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: 2016]

- **Log's**: Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por un determinado usuario o sistema.

- **Malware**: Software malicioso, Código malicioso. Programa informático diseñado para realizar acciones no deseadas o perjudiciales para el usuario legítimo de una computadora.

- **Incidente cibernético**: Proceso donde se detecta, reporta, evalúa, responde y aprende de los incidentes de seguridad de la información (ISO/IEC 27000).

- **Riesgo de seguridad:** Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro

de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad. (Decreto 338 De 2022 - Gestor Normativo, n.d.).

6. ROLES Y RESPONSABILIDADES

El equipo para la atención y gestión de incidentes de seguridad de la información es el responsable de ejecutar los procedimientos para responder a los eventos o incidentes que afectan a la seguridad de la información, gestionar las relaciones con entidades internas y externas, establecer la categorización de los incidentes y centrarse principalmente en resolver los incidentes de seguridad de la información que se producen sobre los activos de información respaldados por la plataforma tecnológica de la entidad. Para dar cumplimiento a lo anterior se conformará el siguiente equipo:

- **Especialista Nivel 1**: Personal de mesa de asistencia que, en una primera revisión, determina si se trata de un incidente de seguridad de la información y escala el caso al especialista de nivel 2 de acuerdo con la especialidad del incidente.

- **Especialista Nivel 2**: Profesional con experiencia en la gestión de una o más especialidades como; redes, servidores, programación, infraestructura, nube, entre otros, es quien recibe el informe del especialista nivel 1, revisa, analiza y recopila la información disponible sobre el evento o incidente de seguridad y privacidad de la información, lo anterior con el fin de identificar su causa raíz, su vector de ataque, los objetivos del ataque y sus posibles consecuencias.

- **Especialista Nivel 3:** Si el incidente aún persiste, el especialista de nivel 2 debe escalar la solicitud de acompañamiento al especialista nivel 3 (Proveedor de servicios).

- **Jefe Oficina TIC**: Adelantar las gestiones operativas necesarias para conformar el equipo de respuesta a la gestión de incidentes multidisciplinar cuando así se requiera.

- **Profesional de seguridad OTIC**: Persona encargada de mantener actualizado el proceso de gestión de incidentes, realizar divulgación cuando se realicen cambios al proceso, hacer seguimiento a la atención de los incidentes de seguridad de la información que le sean asignados.

- **Servidores públicos, terceros y/o contratistas sensibilizados**: Es responsabilidad y deber reportar cualquier situación anormal que pueda llegar a convertirse en un incidente de seguridad

de la información, a la mesa de ayuda de la Entidad.

7. CICLO DE VIDA PROCEDIMIENTO ATENCIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Gestión de Incidentes de Seguridad de la Información para Ambiente se plantea en cuatro (4) fases, estas fases permiten gestionar un incidente desde el momento anterior a su ocurrencia, hasta las actividades posteriores que consoliden los aprendizajes para los futuros eventos:

Fases Gestión de Incidentes de Seguridad de la Información

- Elaboración propia

7.1 Gestión de Eventos ó Incidentes de Seguridad de la Información

La información sobre eventos o incidentes de seguridad es un recurso valioso para Ambiente, como quiera que esta permita identificar riesgos, tomar medidas preventivas y fortalecer la protección de los activos de información. Por esta razón, es fundamental garantizar la seguridad de los medios de comunicación utilizados para reportar, recopilar, analizar, compartir, almacenar y usar dicha información.

Estos medios deben cumplir con los estándares técnicos y legales que aseguren la confidencialidad, integridad, disponibilidad y trazabilidad de la información. Adicionalmente, deben contar con mecanismos de control y supervisión que prevengan el acceso no autorizado, la manipulación indebida o la pérdida accidental de los datos.

Para atender los incidentes que puedan ocurrir por diversas causas, Ambiente estableció el **Procedimiento Gestión de la operación de servicios tecnológicos P-A-GTI-11** el cual define la ruta a seguir y las actividades que deben ejecutarse para la adecuada gestión de los eventos o incidentes de seguridad.

7.1.1 Detección

Es deber de los colaboradores del Ministerio de Ambiente y Desarrollo Sostenible y partes interesadas, reportar el o los eventos o incidentes de seguridad de la información de los que tengan conocimiento. El funcionario, tercero o contratista que sospeche sobre la materialización de un incidente de seguridad deberá notificarlo a través de la herramienta de gestión de asistencia (GEMA), este reporte se puede originar por uno o varios de los siguientes eventos:

- Análisis de riesgos de seguridad de la información o cada vez que se produzca un cambio significativo en la infraestructura de TI.
- Alertas en sistemas de seguridad
- Caída de servidores
- Caída de servicio
- Reporte de usuarios
- Auditorías de seguridad de la información
- Pruebas técnicas de seguridad
- Verificación de licencia y equipos
- Reporte de posibles incidentes por parte de un tercero o proveedores
- Ciberataques
- Reporte de Antivirus

Es preciso recordar que, en caso de que la página web de GEMA, donde se reportan los evento o incidentes se encuentre fuera de servicio o sea un tercero quien reporta, la notificación se realizará a través del siguiente canal: segurinfo@minambiente.gov.co con el asunto **NOTIFICACIÓN DE INCIDENTE DE SEGURIDAD**.

Nota: El reporte se debe realizar acudiendo al principio de debe ser lo más rápido posible para activar el procedimiento de gestión de incidentes.

7.1.2 Análisis

La gestión de incidentes implica identificar y analizar las señales que indican una posible interrupción de las operaciones, así como actuar de forma rápida y eficaz para resolverla. Sin embargo, no siempre es fácil reconocer los precursores o los indicadores de un incidente. Por eso, el equipo de gestión de incidentes debe evaluar la relevancia de las señales detectadas y seguir las mejores prácticas para afrontarlos. En general, se debe asumir que hay un incidente en curso hasta que se confirme lo contrario. El equipo de gestión de incidentes también debe ser capaz de analizar información ambigua, contradictoria o incompleta para determinar si hay o no un incidente.

Se debe analizar rápidamente cualquier incidente que detecte, para identificar su alcance (qué redes, sistemas o aplicaciones se ven afectados), su origen (quién o qué lo está causando) y su modo de operación (qué herramientas o vulnerabilidades se están aprovechando para realizar el ataque). El análisis inicial debe proporcionar información relevante para establecer las prioridades en el manejo del incidente.
El Agente Primer Punto de Contacto de la mesa de ayuda, asigna el caso o ticket a un especialista de nivel 1, quien deberá:

- Realizar la visita en sitio al usuario que radicó el caso, indagar, verificar y recopilar la información suficiente para determinar la ocurrencia de un evento o incidente de seguridad de la información.

- Si no se trata de un evento o incidente de seguridad de la información, el especialista de nivel 1 documenta de forma clara lo encontrado en sitio, mediante un informe justificando la inexistencia del evento o incidente, posteriormente se procede a dar cierre al caso en la herramienta de gestión GEMA.

Si el especialista de nivel 1 determina que puede tratarse de un incidente de seguridad de la información, realiza un informe con el registro de evidencias encontradas y escala el caso al especialista de nivel 2 de acuerdo con la especialidad.

7.1.3 Identificación y reporte de posible incidente

La identificación de un incidente de seguridad de la información es una tarea compleja que requiere la atención del responsable de seguridad de la información o quien haga sus veces.

- La detección de incidentes de seguridad informática puede realizarse mediante diversos métodos que ofrecen distintos grados de precisión y confiabilidad. Entre los métodos automáticos se encuentran los sistemas de detección/prevención de intrusos, el software antivirus y los analizadores de registros (logs), que pueden alertar sobre posibles ataques o vulnerabilidades. Los métodos manuales consisten en los informes de problemas de los usuarios, quienes pueden informar sobre anomalías o fallos en el funcionamiento de los sistemas. Algunos incidentes se detectan fácilmente por estos métodos, pero otros pueden pasar desapercibidos hasta que causan daños evidentes.

- Para analizar las señales potenciales de un incidente, es necesario filtrarlas adecuadamente, pues son abundantes y generan ruido. Un ejemplo de esto es un sistema de detección de intrusiones (IDS), que puede generar miles de falsos positivos que dificultan la identificación de

las amenazas reales. Así pues, es importante seleccionar la información relevante que provienen de las herramientas automáticas.

- El especialista de nivel 2, recibe el informe del especialista nivel 1 analiza y recopila la información disponible sobre el incidente, con el fin de identificar su causa raíz, su vector de ataque, su objetivo y sus consecuencias. El análisis debe permitir clasificar el incidente según su naturaleza, origen, severidad y urgencia.

- Si durante la etapa de investigación y análisis, se determina que está relacionado con una posible falla en un componente o servicio tecnológico y es de su competencia, le dará solución y cierre. De lo contrario el caso o ticket se recategoriza o reasigna.

- Si durante la etapa de investigación y análisis, se determina que no se trata de un incidente de seguridad de la información, se documenta y se cierra el caso.

- Si durante la etapa de investigación y análisis, se confirma la existencia de un evento o un incidente de seguridad de la información se pasa a la siguiente actividad.

Tabla 1 clasificación de incidentes de seguridad

No	Servicio	categoría	subcategorías	Nueva criticidad de impacto	ANS	Responsable
0	**Seguridad de la información**	**Acceso no Autorizado** (Alguien accede a información o sistemas sin permiso.)	Acceso, modificación, eliminación/borrado no autorizado de la información, tanto física como lógica, sistemas de información, servicios o infraestructura tecnológica.	Muy Grave	2 horas	N2-N3
			Suplantación de identidad (alguien se hace pasar por otra persona).	Grave	6 horas	N1-N2
			Compromiso de cuenta privilegiada, sin privilegios, cuenta servicio	Grave	6 horas	N1-N2
			Fuga de información	Grave	6 horas	N1
			Exposición o divulgación no autorizada de información sensible, sin el permiso o la autorización del propietario	Menos Grave	24 horas	N1-N2

No	Servicio	categoría	subcategorías	Nueva criticidad de impacto	ANS	Responsable
1		**Ataques de Correo y Programas Maliciosos (**Malware - Programas dañinos que afectan tu computadora o red.**)**	Malware: Virus, Spyware y Adware	Menos Grave	24 horas	N1
			Ingeniería Social: Spam y Phishing	Menos Grave	24 horas	N1
			Ransomware - software malicioso diseñado para cifrar archivos en el sistema de la víctima y luego exigir un rescate	Muy Grave	2 horas	N2-N3
			Las Amenazas Persistentes Avanzadas (APT) son ciberataques sofisticados y dirigidos	Muy Grave	2 horas	N2-N3
			Error de seguridad antivirus (Enpoint) y liberación de correos en cuarentena	Menos Grave	24 horas	N1
2		**Tratamiento de Datos Personales**	Pérdida o sustracción de información de datos personales	Grave	6 horas	N2
			Modificación o alteración no autorizada de información de datos personales	Grave	6 horas	N2
			Eliminación o borrado no autorizado de información de datos personales	Grave	6 horas	N2
			Tratamiento inadecuado o uso no autorizado de información de datos personales.	Grave	6 horas	N2
3		**Intentos de Intrusión**	Intentos de acceso	Grave	6 horas	N1
			Explotación de vulnerabilidades	Muy Grave	2 horas	N2-N3
			Ataque de diccionario y fuerza bruta	Muy Grave	2 horas	N2-N3
			Múltiples intentos de inicio de sesión	Menos Grave	24 horas	N1
4		**Fraude Informático**	Derechos de Autor (Licenciamiento)	Menor	48 horas	N1
			Copyright y Marca	Menor	48 horas	N1

No	Servicio	categoría	subcategorías	Nueva criticidad de impacto	ANS	Responsable
			Sabotaje - acciones deliberadas e intencionales con el objetivo de dañar, interrumpir, manipular o destruir sistemas, redes o datos (Daño Físico o Manipulación de Hardware, Daño a Software y Datos)	Menos Grave	24 horas	N1
			Suplantación de entidades o de sus funcionarios en sitios WEB o en Redes Sociales	Menor	48 horas	N2
6		**Recopilación de Información**	Scanning - se refiere al proceso de examinar un sistema, red o aplicación para identificar información específica, vulnerabilidades, o configuraciones que puedan ser utilizadas para un análisis más detallado o para la explotación.	Grave	6 horas	N2
			Sniffing - es una técnica utilizada en redes de computadoras para interceptar y analizar el tráfico de datos que circula a través de una red.	Grave	6 horas	N2
			Intercepción de información	Muy Grave	2 horas	N2-N3
			Uso no autorizado de utilitarios	Grave	6 horas	N2
7		**Ataques y Vulnerabilidades en aplicativos WEB**	Ataques ciberneticos: Ataque de Denegación de Servicio (DoS/DDoS), Defacement, Ataques de Inyección SQL, Ataques de XSS (Cross-Site Scripting), Ataques de RFI (Remote File Inclusion) y Puertas Traseras (Backdoors)	Muy Grave	2 horas	N2-N3
			Seguridad WEB: Certificados SSL/TLS (protocolos de seguridad para establecer conexiones cifradas y seguras en Internet)	Grave	6 horas	N2-N3
			Vulnerabilidades y Exposiciones: Exposición	Grave	6 horas	N2-N3

No	Servicio	categoría	subcategorías	Nueva criticidad de impacto	ANS	Responsable
			Pública (datos, sistemas o recursos accesibles sin autorización).			
8		**Ataques de Red**	Ataques de red: Ataques de Red Man-in-the-Middle (MITM), ARP Poisoning (Envenenamiento ARP), DNS Poisoning (Envenenamiento de DNS) y Sesión Hijacking - secuestro de sesiones o cuentas	Grave	6 horas	N2
			Movimiento lateral - intento de controlar recursos dentro de la misma red.	Grave	6 horas	N2
			Errores o malas configuraciones en seguridad perimetral, errores en segmentación y manipulación de Red	Menos Grave	24 horas	N2
9		**Indisponibilidad**	Fallo de red cableada o Inalámbrica	Menor	48 horas	N1
			Falla, energía, UPS o Planta Eléctrica	Menor	48 horas	N1-N2
			Fallo aire acondicionado	Menor	48 horas	N1-N2
			Fallo de dispositivos o sistemas	Menor	48 horas	N1-N2
			Indisponibilidad de Servicios de TI	Menor	48 horas	N1-N2
10		**Reporte de Robo o Pérdida de Elementos**	Dispositivos Móviles (Celulares, Tablets, Portátiles, Otros)	Menos Grave	24 horas	N1
			Medios de Almacenamiento	Menos Grave	24 horas	N1
			Equipos de Comunicaciones, Servidores e Impresoras	Menos Grave	24 horas	N1
11		**Requerimientos en Seguridad de la Información**	Análisis de Vulnerabilidades	No Aplica	48 horas	N2
			Concepto técnico seguridad de la información	No Aplica	48 horas	N1-N2
			Análisis o solicitud de instalación de software	No Aplica	48 horas	N1

7.1.4 Definición de medidas y acciones para abordar el incidente

- El especialista de nivel 2 informa a las partes interesadas (jefe Inmediato, responsable(s) de Seguridad de la información y TI) sobre la ocurrencia del evento o incidente de seguridad

- El Profesional de seguridad de la información o jefe de Oficina TICs o quien haga sus veces, coordina y asigna las actividades del equipo (Especialistas) de respuesta.

- Se verifica la causa real del incidente y la afectación sobre el/los activo(s) de información.

7.1.5 Tipificación del incidente

Durante la evaluación del incidente se identifica el nivel de impacto con base en los insumos entregados por el análisis y la clasificación de activos de información de la entidad. A continuación, se plantea la escala de severidad del incidente:

- **Muy Grave y Grave**: El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales del Ministerio. 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.

- **Menos Grave y Menor**: El incidente de seguridad afecta a activos de información considerados de impacto moderado o menor que influyen directamente o no a los objetivos de un proceso determinado. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

El equipo de respuesta revisa y analiza los siguientes aspectos:

- Nivel de afectación de los activos de la entidad
- Nivel de Incidencia
- Priorización
- Tiempo de respuesta
- Clasificación
- Valoración del incidente

Una vez revisados y analizados los aspectos relevantes del incidente, y determinado su valor en la escala de impacto, el especialista de nivel 2 procederá a documentar detalladamente el caso correspondiente en la herramienta GEMA.

7.1.6 Criterios atención y gestión de incidentes de seguridad de la información

Tabla 2 Criterios Atención y Gestión de Incidentes de Seguridad de la Información

Muy Grave	El incidente de seguridad de la información debe atenderse de forma inmediata y menor a 2 horas, contadas a partir del reporte al CSIRT de Gobierno.	DoS, DDoS, Backdoor, ataques de diccionario y fuerza bruta, acceso, modificación/borrado de la información sensible, Ransomware, Intercepción de información, entre otros.
Grave	El incidente de seguridad de la información debe atenderse en un tiempo menor a 6 horas, contadas a partir del reporte al CSIRT de Gobierno.	Ataques a aplicativos webs, evidencia de malware y APT, ataques de red (MITM, Sesión Hijacking, Poisoning, manipulación de red), ataques de inyección SQL, XSS, RFI/LFI, SSL y certificados, basados en web, compromiso de cuenta, movimiento lateral, fuga de información, exposición pública, defacement.
Menos Grave	El incidente de seguridad de la información, debe atenderse en un tiempo menor a 24 horas.	Sabotaje, spam, contenido no autorizado, ingeniería social, técnicas OSINT, error Seguridad Perimetral, error Seguridad Endpoint, error Seguridad Red, error en Segmentación, error Arquitectura Seguridad.
Menor	El incidente de seguridad de la información, debe atenderse en un tiempo menor a 48 horas.	Fraudulento de recursos, Copyright y Marca, suplantación de entidades o de sus funcionarios en sitios web o en redes sociales, Phishing/ Spear Phishing, fallo de red cableada o Inalámbrica, fallo energía, fallo de dispositivos o sistemas.

7.1.7 Priorización del incidente

Todos los incidentes deben ser priorizados para garantizar que son atendidos de acuerdo con su nivel de criticidad. Para todos los incidentes se debe evaluar los siguientes factores:

- Efectos técnicos reales y potenciales del incidente
- Recursos críticos afectados por el incidente

Los incidentes que impactan directamente la continuidad de las actividades misionales de la entidad requieren atención prioritaria.

La primera tarea para priorizar los incidentes es calificar el nivel de los efectos. La siguiente tabla permite establecer el nivel de efectos del incidente.

Nivel de prioridad: Depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados.

Tabla 3 Niveles de Criticidad de Impacto

Valor	Escala cualitativa del efecto	Descripción
Inferior	0.10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	0.25	Sistemas que apoyan a una sola dependencia o proceso de una entidad.
Medio	0.50	Sistemas que apoyan más de una dependencias o proceso de la entidad.
Alto	0,75	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Crítico	1.00	Sistemas Críticos.

Impacto actual: Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

Impacto futuro: Depende de la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado.

Tabla 4 Niveles de Impacto Actual y Futuro

Nivel Impacto	Escala cualitativa del efecto	Definición
Inferior	0.10	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo.
Bajo	0.25	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo.
Medio	0.50	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo.
Alto	0.75	Impacto moderado en uno o más componentes de más de un sistema de Información.
Crítico	1.00	Impacto alto en uno o más componentes de más de un sistema de información.

Para determinar el nivel de severidad del incidente se debe calcular la siguiente formula:

NP = Nivel de Prioridad

IA = Impacto Actual

IF = Impacto Futuro

CS = Criticidad del Sistema

$$NP = (IA * 2.5) + (IF * 2.5) + (CS * 5)$$

Donde: ***Nivel Prioridad*** = *(Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)*

De los resultados obtenidos se deben compara con la siguiente tabla para determinar la prioridad de atención:

Tabla 5 Niveles de Prioridad del Incidente

Nivel de Prioridad	Valor
Inferior	00,00 – 02,49
Bajo	02,50 – 03,74
Medio	03,75 – 04,99
Alto	05,00 – 07,49
Crítico	07,50 – 10,00

7.1.8 Tiempos de respuesta

Para el caso de la atención de incidentes de seguridad de la información, se han establecido unos tiempos máximos de atención de estos, con el fin de atender adecuadamente los incidentes de acuerdo con su criticidad e impacto. Los tiempos expresados en la siguiente tabla son un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso.

Tabla 6 Tiempos Máximos de Atención de Incidentes

Nivel Prioridad	Tiempo de Respuesta
Inferior	3 horas
Bajo	1 hora
Medio	30 min.
Alto	15 min.
Crítico	5 min.

Una vez que el incidente ha sido analizado y priorizado se debe notificar a las instancias apropiadas y en los casos que determine el jefe de la Oficina TIC del Ministerio.

7.1.9 Clasificación de estado actual del incidente

Debido a que se deben mantener informadas a las partes pertinentes sobre la evolución del incidente, la siguiente tabla describe los estados definidos para los incidentes.

Tabla 7 Clasificación de estado actual del incidente

Estado	Descripción
Pendiente	Si bien el incidente ha sido reportado, aún no se lo ha comunicado al [Profesional de Seguridad de la información].
Informado	El incidente ha sido reportado al [Profesional de Seguridad de la información] pero aún no se lo ha tratado.
En curso	El incidente ha sido reportado al [Profesional de Seguridad de la información] y se encuentra en tratamiento.
Resuelto	El incidente ha sido resuelto.

Una vez valorado y clasificado el incidente de seguridad de la información si el mismo es catalogado como Muy Grave o Grave se deberá reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, para el respectivo apoyo y coordinación en la gestión de estos a través del formato de reporte establecido por el CSIRT.

- https://tinyurl.com/5xuf3dvm
- Contacto mesa de servicio 018000910742 opción 2
- Correo: csirtgob@mintic.gov.co

En caso de que el incidente sea catalogado como Menos Grave o Menor, deberá ser gestionado por los diferentes niveles de especialistas definidos en el **Procedimiento de Gestión de la Operación de Servicios Tecnológicos P-A-GTI-11.**

7.1.10 Contención

La contención, como su nombre lo indica, se refiere a la estrategia que permite tomar decisiones oportunas para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información. También busca detener el impacto o efecto que un incidente pueda tener dentro de la infraestructura y arquitectura de la entidad.

Las acciones de contención están relacionadas con el nivel de prioridad del incidente, que se determina en la fase de detección.

Durante la acción de contención, se debe registrar en el caso correspondiente de GEMA toda la información relacionada con el incidente que se está gestionando. Este registro debe incluir los detalles de la contención realizada, como parte de las medidas de control y seguimiento establecidas. La documentación adecuada no solo facilita el análisis y resolución de incidentes futuros, sino que también sirve como insumo para reforzar o diseñar nuevas políticas y procedimientos de seguridad de la información, contribuyendo así a la mejora continua del sistema de gestión.

Responsables de las Acciones de Contención deberá identificar y aplicar las estrategias pertinentes para evitar la propagación del incidente en otros activos de información de TI, que minimice el daño a los recursos de TI y la perdida de la confidencialidad, integridad y disponibilidad de la información. Las acciones de contención varían según el tipo de incidente y los criterios deben estar bien documentados por cada incidente. Algunos criterios que pueden ser tomados como base son:

- Daño potencial o sustracción de los activos de información.
- Acciones que permitan la preservación de evidencia digital
- Disponibilidad del servicio
- Tiempo y recursos para implementar la acción de contención.
- Efectividad de las acciones para contener el incidente de manera total o parcial
- Tiempo estimado de duración en dar solución a incidente.
- Criterio de peritos forenses

7.1.11 Erradicación y recuperación

7.1.12 Erradicación

Una vez contenido el incidente se procede con la erradicación, en esta actividad se procede a la eliminación de cualquier rastro dejado por el incidente y a la remoción de la causa de este.

Es pertinente que, durante esta actividad, se realicen las siguientes acciones:

- Determinar las causas del incidente, eliminándolas completamente.
- Mejorar los esquemas de protección actualmente implementados.
- Realizar pruebas de vulnerabilidad para revisar el estado posterior a la erradicación.
- Determinar y aplicar, en caso de ser necesario, la restauración del sistema.
- Revaluar las políticas y lineamientos existentes, con el fin de identificar e implementar posibles modificaciones.
- Implementar los controles
- Revisar y/o ajustar los indicadores de ser necesario.

7.1.13 Recuperación

Una vez erradicado el incidente, es necesario restaurar el funcionamiento normal de los sistemas y/o servicios dañados, así como aplicar medidas de seguridad que eviten que se repita una situación similar en el futuro. Estas medidas pueden incluir el endurecimiento del sistema, es decir, la implementación de controles técnicos y organizativos que reduzcan la vulnerabilidad y aumenten la resistencia ante posibles ataques.

- Velar por la recuperación de los datos y configuraciones.
- Aplicar las actualizaciones necesarias.
- Robustecer las actividades de auditoría.
- Garantizar el restablecimiento de los servicios e información afectados.

Las actividades de recuperación y la fecha de aplicación se deben registrar en las estadísticas de los incidentes.

7.1.14 Recolección de evidencia digital

Se realiza la recolección de información digital de ser necesario correspondiente al incidente de seguridad para su respectivo análisis de datos y generación del informe o reporte final de acuerdo con la Guía recolección evidencia digital G-A-GTI-06.

7.1.15 Lecciones Aprendidas

Una vez que el equipo de respuesta a incidentes sospeche que un incidente está ocurriendo u ocurrió, se debe iniciar la documentación de este. Es necesario documentar únicamente los hechos relacionados con el incidente, se debe evitar el registro de opiniones o subjetivas.

Todas las notas deben estar firmadas y fechadas por su autor, ya que pueden constituir evidencia en eventuales procesos legales. Asimismo, todas las actuaciones realizadas por el equipo de respuesta a incidentes deben registrarse en la herramienta GEMA, incluyendo:

- Estado actual del incidente
- Resumen del estado actual del incidente
- Acciones que se han tomado para dar respuesta al incidente
- Información de contacto de las personas que se han involucrado en el incidente
- Lista de la evidencia recolectada a la fecha

- Siguientes pasos que se deben realizar

El equipo (Especialistas) de respuesta a incidentes debe preservar toda la información de las acciones y evidencias recolectadas durante el proceso de atención del incidente debido a que muchas veces contiene información sensible como: vulnerabilidades no detectadas, acciones indebidas realizadas por usuarios o atacantes, brechas de seguridad en los sistemas o la plataforma tecnológica. Los correos, documentos, y reportes relacionados con el manejo del incidente deben ser cifrados para evitar acceso no autorizado a los mismos.

Registrar la información en la herramienta de mesa de ayuda para dar el respectivo cierre al caso respecto el cual debe contener la siguiente información:

- Descripción exacta de lo ocurrido (en qué momento) y como se gestionó el incidente.
- Medidas o acciones que podrían haber impedido la recuperación.
- Documentar acciones correctivas para prevenir incidentes similares.
- Documentar herramientas o recursos adicionales para detectar, analizar y mitigar los incidentes en el futuro.

8. CONTROL DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El control de incidentes relacionados con la seguridad y privacidad de la información, según lo establecido en el *Manual para la Gestión de Incidentes de Seguridad y Privacidad de la Información*, se llevará a cabo mediante un sistema de monitoreo y análisis en **Power BI**, permitiendo una visualización dinámica y en tiempo real del estado de los incidentes. Adicionalmente, se gestionará un indicador de control en la plataforma **SOMOSIG**, que permitirá centralizar la información y facilitar el seguimiento y reporte de los incidentes.