TIC

Lineamientos De Gestión de incidentes de seguridad de la información y seguridad digital

Ministerio de tecnologías de la información y las comunicaciones

MSPI

Julián Molina Gómez – Ministro de Tecnologías de la Información y las Comunicaciones
Yeimi Carina Murcia Yela - Viceministra de Transformación Digital
Lucy Elena Urón Rincón - Directora de Gobierno Digital
Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI
Danny Alejandro Garzón Aristizábal – Contratista Subdirección de Estándares y Arquitectura de TI
German García Filoth – Contratista Subdirección de Estándares y Arquitectura de TI
Johanna Marcela Forero Varela - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
Julio Andrés Sánchez Sánchez - Contratista Subdirección de Estándares y Arquitectura de TI
Lourdes María Acuña Acuña - Contratista de la Dirección de Gobierno Digital
Tairo Elías Mendoza Piedrahita - Profesional Especializado Dirección de Gobierno Digital
Andrés Díaz Molina- Jefe de la Oficina de Tecnologías de la Información
Nelson Barrios Perdomo – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Adriana María Pedraza - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Camilo Andrés Jiménez - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Emanuel Elberto Ortiz - Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
Angela Janeth Cortés Hernández - Oficial de Seguridad y Privacidad de la Información GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	**Observaciones**
Versión 5 21/04/2025	Lineamientos De Gestión de incidentes de seguridad de la información y seguridad digital Dirigida a las entidades del Estado

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Lineamientos De Gestión de incidentes de seguridad de la información y seguridad digital V 5.0
Este documento de la Dirección de Gobierno Digital se encuentra bajo una Licencia Creative Commons Atribución 4.0 Internacional

Tabla de contenido

Tabla de contenido 3
Listado de Tablas 4
Tabla de ilustraciones 4
Lineamientos De Gestión de incidentes de seguridad de la información y seguridad digital . 5
1. Derechos De Autor 5
2. Audiencia 5
3. Introducción 5
4. Justificación 5
5. Objetivos 6
6. Alcance 7
7. Adaptabilidad al ciclo de vida de la ciberseguridad NIST 7
8. Gestión De Incidentes 9
8.1. ¿Qué es la gestión De incidentes? 9
8.1.1. Evento 9
8.1.2. Incidente de seguridad digital 9
8.2. Objetivos 9
8.3. Despliegue de acciones adecuadas para la gestión de incidente. 10
9. Ciclo de vida de la gestión de incidentes 11
9.1. Preparación 12
9.1.1. Acciones de prevención: 13
9.2. Detección y Análisis 14
9.2.1. Identificación de incidentes 14
9.2.2. Análisis 15
9.2.3. Documentación del incidente. 16
9.2.4. Clasificación de Incidentes de seguridad de la información y seguridad digital 17
9.2.5. Priorización del incidente 21
9.2.6. Criterios de valoración del Nivel de Impacto 22
9.2.7. Criterios de valoración del nivel de recuperabilidad - urgencia del Incidente 23
9.2.8. Tiempos de Respuesta 24
9.3. Contención, Erradicación y Recuperación 25
9.3.1. Recopilación y preservación de evidencia 26
9.3.2. Erradicación y Recuperación 26

9.3.3. Recuperación 26
10. Actividades posteriores al Incidente. 27
10.1. Lecciones aprendidas. 27
10.2. Uso de datos e información recopilados del incidente. 28
10.2.1. Evaluación Objetiva: 29
10.2.2. Evaluación Subjetiva: 29
10.3. Retención de pruebas: 30
10.4. Lista de verificación para la gestión de incidentes. 30
11. Recomendaciones Generales 31
12. Coordinación e intercambio de información. 32
13. Lineamientos a considerar. 32
14. Referencias. 33

Listado de Tablas

Tabla 6 Taxonomía clasificación de incidentes 21
Tabla 7 Descripción categorías de impacto función y de compromisos de información 23
Tabla 8 Descripción de categorías de impacto de recuperabilidad de las operaciones 23
Tabla 9 Descripción de escalas de nivel de prioridad de atención de incidentes 24
Tabla 10 Descripción Tiempos Máximos de Atención de Incidentes por parte del IRT 25
Tabla 11 Pasos para seguir en la gestión del incidente 31
Tabla 12 Lineamientos a considerar 33

Tabla de ilustraciones

Ilustración 1 Figura adaptada al Modelo CSF NIST 2.0 – Funciones del CSF 8
Ilustración 2 Ciclo de vida de Gestión de incidentes- NIST.SP 800-61 r2 12

Lineamientos De Gestión de incidentes de seguridad de la información y seguridad digital

1. Derechos De Autor

Para el desarrollo de este lineamiento, se recogieron aspectos importantes de mejores prácticas y documentos de uso libre por parte del NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide Special Publication 800-61 Revisión 2) y el artículo 9 de la Resolución 500 de 2021 MinTIC.

2. Audiencia

Entidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno Digital, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de TI en el marco de la estrategia de seguridad digital.

3. Introducción

Este anexo entrega los lineamientos básicos para poner en marcha un Sistema de Planificación y Preparación de la Gestión de Incidentes de Seguridad Digital y de la información física impresa, a través de un modelo propuesto, el cual está concebido para que se puedan integrar los incidentes de seguridad sobre los activos de información, independiente del medio en el que se encuentren.

4. Justificación

El lineamiento expuesto en este documento es un complemento del Modelo de Seguridad y Privacidad de la Información MSPI y se constituye en un referente de planificación y preparación de la gestión de incidentes de seguridad de la información y seguridad digital, para las entidades del Estado.

La gestión de incidentes de seguridad digital (ciberseguridad) se ha convertido en una actividad relevante e indispensable de las áreas de tecnologías y seguridad de la información por el volumen de ataques a las infraestructuras tecnológicas y los nuevos métodos cada vez más sofisticados que afectan a mayor escala, así las cosas, las entidades y organizaciones necesitan capacidades de respuesta que permita detectar de manera rápida y oportuna los incidentes que puedan presentarse, minimizando el impacto y permitiendo restaurar los servicios afectados en el menor tiempo posible .

Estos lineamientos proporcionan recomendaciones y pautas que deben ser adoptadas por las entidades y organizaciones sin importar el tipo de infraestructura con las que se cuente, de igual manera, es necesario realizar una identificación de activos y gestión de riesgos para asegurar la infraestructura, compartir información con las comunidades para alertar sobre amenazas y establecer estrategias de respuesta contra los ataques más comunes.

Es fundamental establecer un criterio para la priorización de atención de los incidentes (Resolución 500 del 2021 – MinTIC), un procedimiento de lecciones aprendidas para realizar los ajustes y mejoras al proceso de gestión de incidentes. Finalmente, se debe revisar la matriz de riesgo y diseñar controles que permitan ajustar la postura de seguridad digital de la entidad/Organización.

5. Objetivos

El objetivo principal del presente documento de planificación y preparación de la gestión de incidentes de seguridad digital es tener un enfoque estructurado, consensuado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información / seguridad digital (Ciberseguridad).

Los objetivos específicos del presente documento son:

Identificar y Gestionar los incidentes de seguridad de la información /seguridad digital (Ciberseguridad) para ser evaluados y dar respuesta de la manera más eficiente y adecuada.

Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de una base de conocimiento y registro de incidentes y a través de los indicadores del sistema de gestión de seguridad de la información.

Definir roles y responsabilidades dentro de los sujetos obligados, para mejorar la postura de seguridad de la infraestructura tecnológica, mediante la identificación de activos de información, la gestión de riesgos, la gestión de incidentes que permitan la continuidad de las operaciones en el tiempo.

Establecer e implementar el procedimiento de gestión de incidentes de seguridad de la información y de seguridad digital (Ciberseguridad), según lo establecido en el presente documento, la Resolución 500 del 2021 del MinTIC, la norma ISO/IEC 27001:2022.

Gestionar los incidentes de seguridad de la información/seguridad digital (Ciberseguridad), que se presenten en la infraestructura tecnológica, infraestructura crítica ICC y servicios esenciales de manera eficiente y adecuada por parte del Equipo de Respuesta a Incidentes de Seguridad de la Información – IRT.

Minimizar los impactos adversos de los incidentes, mediante la oportuna gestión por parte del Equipo de Respuesta a Incidentes de Seguridad de la Información - IRT.

Consolidar las lecciones aprendidas producto de los incidentes de seguridad de la información/seguridad digital (Ciberseguridad), identificando de puntos de mejora, actualización de riesgos y ajustes de controles, para incrementar las oportunidades

de prevenir la ocurrencia de futuros incidentes, mejorar la postura de seguridad y el uso de las salvaguardas y mejorar el esquema global de la gestión de incidentes.

Definir los protocolos formales de reporte y escalamiento de los incidentes de seguridad de la información/seguridad digital (Ciberseguridad) clasificados como Muy Graves y Graves al CSIRT Gobierno/COLCERT, para su respectivo apoyo y coordinación de su gestión.

Garantizar que los incidentes de seguridad de la información y de seguridad digital (Ciberseguridad) se documenten de manera consistente, utilizando la taxonomía establecida por el COLCERT y estándares apropiados para la categorización, clasificación e intercambio de información producto de la gestión de incidentes.

Activar comités de crisis cuando se presenten incidentes que afecten infraestructura crítica y servicios esenciales e incidentes de impacto crítico y nacional, que involucren los diferentes lideres de proceso y articular las acciones que desde cada una de las áreas corresponda para la recuperación de las operaciones, las acciones jurídicas a desplegar, la asignación de recursos y las comunicaciones internas y externas entre otras.

6. Alcance

Estos lineamientos aplican a todos los incidentes de seguridad de información y seguridad digital que puedan afectar a la confidencialidad, integridad o disponibilidad de la información o los sistemas de información de entidades / organizaciones que forman parte de la Rama Ejecutiva, sin embargo, también puede ser aplicada a las demás ramas de poder público, teniendo en cuenta la adopción de buenas prácticas de seguridad digital. Además, debe comprender el relacionamiento de un efectivo tratamiento de la evidencia digital y la referenciación basada en la Resolución 500 del 2021 del MinTIC, la norma ISO/IEC 27001:2022 y la política de Gobierno Digital con el Modelo de Seguridad y Privacidad de la Información - MSPI.

Adicionalmente el presente lineamiento tiene como finalidad brindar a las entidades/ organizaciones una estructura y directrices claras para gestionar eficientemente los incidentes de seguridad digital y relacionar los efectos de cada uno de los factores de los Marcos de Trabajo del NIST Cybersecurity Framework (CSF) 2.0, el FIRST CSIRT Services Framework Version 2.1, 2019) y las mejores prácticas de gestión de incidentes.

7. Adaptabilidad al ciclo de vida de la ciberseguridad NIST

El Framework de Ciberseguridad (CSF) del NIST v4.0 es un marco integral de referencia para comenzar y mejorar los procedimiento y políticas de Seguridad digital (Ciberseguridad), con el propósito de mejorar la postura de Seguridad, incentivar la gobernanza, promover las comunicaciones y alinear los riesgos de Seguridad Digital con los riesgos de proceso.

El marco está organizado en seis funciones: gobernar, identificar, proteger, detectar, responder, recuperar, los cuales conjuntamente proporcionan una visión integral del ciclo de vida para la gestión del riesgo de ciberseguridad a lo largo del tiempo.

Gobernar: Incorporar en la estrategia de gestión de riesgos, actividades de gobernanza para conocer el contexto organizacional, el establecimiento de una estrategia de seguridad digital, gestión de riesgos en las cadenas de suministros, roles, responsabilidades, políticas y seguimiento.

Identificar: Desarrollar una comprensión organizacional para la gestión del riesgo de ciberseguridad de datos, hardware, software, sistemas, instalaciones, servicios, personas y capacidades.

Proteger: Desarrollar e implementar las protecciones apropiadas para garantizar la entrega de servicios.

Detectar: Desarrollar e implementar las actividades apropiadas para identificar cuando ocurra un evento de seguridad digital (ciberseguridad).

Responder: Desarrollar e implementar las actividades apropiadas para tomar acciones en relación con un incidente de seguridad digital (ciberseguridad) detectado.

Recuperar: Desarrollar e implementar las actividades necesarias para implementar y mantener planes de recuperación para reestablecer los servicios y capacidades que hayan sido afectados durante el incidente de seguridad digital (ciberseguridad).

Ilustración 1 Figura adaptada al Modelo CSF NIST 2.0 – Funciones del CSF

8. Gestión De Incidentes

8.1. ¿Qué es la gestión De incidentes?

La gestión de incidentes es un proceso sistemático para identificar, documentar, clasificar, priorizar, resolver y registrar incidentes de seguridad de la información y seguridad digital que puedan afectar la confidencialidad, integridad o disponibilidad de la información o los sistemas de información de una entidad u organización.

8.1.1. Evento

Un evento es cualquier suceso observable en un sistema o red, como un usuario que se conecta a un recurso compartido de archivos, un usuario que envía un archivo electrónico o un firewall que bloquea un intento de conexión, entre otros.

Igualmente, los eventos adversos, son aquellos que tienen consecuencias negativas, como fallos en un sistema, usos no autorizados de privilegios en un sistema, acceso no autorizados y ejecución de malware.

8.1.2. Incidente de seguridad digital

Un incidente es una violación o amenaza inminente a las políticas de seguridad digital, políticas de uso aceptable y o prácticas de seguridad básicas. (Fuente: NIST.SP 800-62r2.)

Teniendo en cuenta las Guías del Instituto Nacional de Tecnologías de la Comunicación y el Centro Nacional para la Protección de las Infraestructuras Computer Security Incident Handling Guide (Cichonski et al., 2012) y la Guía de Recomendaciones y Consideraciones para los riesgos de Ciberseguridad - NIST - Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (Publications, 2023).

8.2. Objetivos

Los objetivos de la Gestión de incidentes de Seguridad Digital son:

- Minimizar el impacto de los incidentes de seguridad.
- Identificar y corregir la causa raíz de los incidentes.
- Prevenir que se repitan los incidentes.

- Mejorar la postura de seguridad de las entidades/organizaciones.
- Identificar precursores e indicadores para evitar incidentes mediante la implementación de medidas preventivas y correctivas adecuadas. Además de:

Cumplir con las obligaciones legales y contractuales con relación a la gestión de incidentes de Seguridad Digital en Colombia de acuerdo con la Política de Seguridad Digital, de Gobierno Digital, el Decreto 1078 de 2015, adicionado por el Decreto 338 del 2022 y la Resolución 500 del 2021 del MinTIC.

Ayudar a las entidades/organizaciones a mitigar los riesgos de los incidentes de seguridad digital proporcionando pautas sobre cómo responder ante éstos de manera eficaz y eficiente.

Proporcionar lineamientos para establecer un programa efectivo de respuesta a incidentes, con un enfoque principal en la detección, análisis, priorización y manejo de incidentes

8.3. Despliegue de acciones adecuadas para la gestión de incidente.

Desarrollar una política de gestión de incidentes: La política de gestión de incidentes debe definir los objetivos del programa, los roles y responsabilidades de las diferentes partes involucradas, así como los procesos para identificar, clasificar, priorizar, resolver y registrar incidentes de seguridad.

Establecer un Equipo de Respuesta a Incidentes (IRT):

El IRT debe estar integrado en el Modelo de Seguridad de la Información MSPI o Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, cuya función principal es gestionar y mitigar los eventos no deseados que afectan la seguridad de la información/Seguridad digital. Este equipo centraliza la coordinación y supervisión de la respuesta a los incidentes, articulando cada una de las acciones de contención, erradicación y recuperación con el equipo técnico y administrativo, así mismo proporcionado directrices a las diferentes dependencias de la entidad encaminadas a gestionar los incidentes de manera adecuada.

El IRT debe estar integrado al Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, cuya función principal es gestionar y mitigar los eventos no deseados que afectan la seguridad de la información y la seguridad digital. Este equipo centraliza la coordinación y supervisión de la respuesta a los incidentes, articulando cada una de las acciones de contención, erradicación y recuperación con los equipos técnicos y administrativos. Además, proporciona directrices a las diferentes dependencias de la entidad para gestionar los incidentes de manera adecuada.

Crear un plan de respuesta a incidentes: El plan de respuesta a incidentes debe describir los pasos a seguir para gestionar los incidentes de seguridad, incluyendo aquellos relacionados

con la seguridad de la información y seguridad digital (Incident management, 2022). El plan debe incluir información sobre cómo desarrollar e implementar cada una de las etapas, como son: preparación, detección, análisis, contención, erradicación, recuperación y lecciones aprendidas.

Capacitar al personal en gestión de incidentes: El personal de la entidad/organización debe estar capacitado en los procesos de gestión de incidentes. La capacitación debe cubrir temas como el análisis e identificación de incidentes de seguridad, la comunicación de incidentes, la respuesta a incidentes, la recuperación de incidentes y la investigación de éstos.

Probar y actualizar regularmente el plan de respuesta a incidentes: El plan de respuesta a incidentes debe probarse y actualizarse de manera regular para garantizar su efectividad y para que refleje los cambios en el entorno de amenazas.

Reporte de Incidentes:

Una vez identificado un incidente de seguridad digital/ciberseguridad por el IRT, el responsable de seguridad digital de la entidad (CISO) debe reportar al CSIRT Gobierno/COLCERT, a través de los canales de atención, los incidentes catalogados como Muy Grave y Grave. Esto permitirá el despliegue del apoyo y la coordinación en la gestión del incidente. Para ello, se debe utilizar el formato de reporte establecido, disponible en el sitio web del COLCERT.

De igual manera, los incidentes catalogados como Menos Grave y Menor deben ser registrados en el formulario disponible en el portal web del COLCERT una vez gestionados, con el propósito de identificar los tipos de incidentes que afectan a las entidades y mantener una estadística de estos.

Asimismo, los incidentes de seguridad digital/ciberseguridad que afecten bases de datos y archivos con datos personales deben ser reportados a la Superintendencia de Industria y Comercio (SIC) a través del portal de Registro Nacional de Bases de Datos o por los canales de atención establecidos.

9. Ciclo de vida de la gestión de incidentes

Para la gestión de incidentes de seguridad de la información y seguridad digital (Ciberseguridad) y teniendo en cuenta el Marco de Ciberseguridad (CSF) del NIST v4.0, se tomará como estándar para desarrollar los lineamientos de gestión de incidentes el estándar NIST.SP.800-61r2, así las cosas, el procedimiento de gestión de incidentes contempla varias fases, las cuales corresponde Preparación, Detección y Análisis, Contención, Erradicación y Recuperación y Actividades Post-Incidente.

Ilustración 2 Ciclo de vida de Gestión de incidentes- NIST.SP 800-61 r2

Fuente: https://grupo-siayec.com.mx/images/blog/principal/thum31.jpg

9.1. Preparación

En esta fase inicial, se establece y capacita al Equipo de Respuesta a Incidentes (IRT) como parte del Modelo de Seguridad de la Información (MSPI) o Sistema de Gestión de Seguridad de la Información (SGSI), proporcionando directrices a las diferentes dependencias de la entidad para gestionar los incidentes de manera adecuada. Asimismo, esta etapa contempla la asignación de recursos y la adquisición de herramientas tecnológicas y de seguridad digital para identificar y mitigar los eventos no deseados que afectan la seguridad de la información y la seguridad digital. La implementación de esta fase contribuye a la gestión de riesgos y al fortalecimiento de la postura de seguridad de la infraestructura tecnológica, de acuerdo con los lineamientos definidos en el Modelo de Seguridad y Privacidad de la Información (MSPI).

Realizar periódicamente ejercicios de simulación de ciberataques con el propósito de evaluar la respuesta de los Equipos de Respuesta a Incidentes (IRT) y la resiliencia de los sistemas e infraestructura de la entidad ante incidentes de seguridad digital o cibernéticos. Asimismo, llevar a cabo ejercicios de mesas de crisis con simulaciones diseñadas para preparar a la entidad para enfrentar situaciones de emergencia o crisis, evaluando y mejorando la capacidad de respuesta y coordinación en todos los niveles estratégicos, tácticos y operacionales de la entidad.

Las siguientes son algunas herramientas y recursos para la gestión de incidentes por parte de las entidades/organizaciones.

Comunicaciones e Instalaciones: establecer un árbol telefónico con los miembros del equipo, lideres de proceso y entidades externas como el CSIRT Sectorial y el COLCERT, entre otros, para el apoyo y gestión. Este árbol debe incluir los datos de contacto básicos.

Mecanismos de reporte de incidentes: establecer un punto único de contacto para el reporte de eventos, habilitar buzones de correo, formulario en línea, números telefónicos y sistemas de mensajería instantánea.

Sala de crisis: Contar con un sitio para realizar reuniones y coordinaciones necesarias. Esta sala de crisis se utilizará para desarrollar las mesas estratégicas, táctica y operativas para

el abordaje integral de gestión de incidentes, con todos los líderes de proceso de la entidad/Organización.

Hardware y Software: Dotar de dispositivos para realizar respaldo para crear imágenes forenses, preservar archivos y log ´ s e información de los incidentes. Además, proporcionar computadoras portátiles con capacidad de procesamiento para análisis de datos e instalación herramientas especializadas en el manejo de la evidencia digital.

Recursos de análisis: Contar con Listados de puertos, diagramas de red, lista de activos de información y un inventario de la infraestructura tecnológica a recuperar. Este inventario debe incluir el detalle de las máquinas que soportan los sistemas de información, su ubicación, sus integraciones, sus mecanismos de autenticación y las observaciones necesarias para recuperar dichos servicios. También se debe disponer de documentación de sistemas operativos, aplicaciones, sistemas de información y herramientas de seguridad, así como procedimientos técnicos de recuperación de cada sistema de información.

Software de Mitigación de incidentes: construir y mantener un kit de herramientas especializadas para la investigación y análisis forense de incidentes. Además, mantener imágenes de sistemas operativos limpias y actualizadas para facilitar los procesos de restauración y recuperación operativa.

9.1.1. Acciones de prevención:

Realizar un ejercicio responsable de identificación de activos de información y gestión de riesgos, garantizará que los controles implementados sean lo suficientemente robustos para prevenir la materialización de riesgos.

Evaluación de riesgos: Realizar evaluaciones periódicas o cada vez que surjan cambios que puedan generar nuevos riesgos, a la matriz de riesgos de la entidad /organización, así como después de gestionar incidentes, para ajustar los controles de seguridad y minimizar los riesgos.

Seguridad de host: Gestionar vulnerabilidades para mantener los sistemas actualizados con las últimas actualizaciones de seguridad, habilitar la auditoria en los dispositivos y realizar un monitoreo constante para asegurar la visibilidad.

Seguridad de la Red: Bloquear y denegar cualquier actividad que no sea expresamente permitida, incluidas las VPN y conexiones dedicadas a otras entidades.

Prevención de Malware: Implementar software para detectar y detener malware en todos los equipos de cómputo, portátiles, servidores físicos y virtuales.

Sensibilización y formación de usuarios: Comunicar las políticas y procedimientos establecidos en el Modelo de Seguridad y Privacidad de la Información MSPI, y proporcionar información sobre los vectores de ataque identificados en incidentes previos.

9.2. Detección y Análisis

Los incidentes de seguridad pueden manifestarse de diversas formas, cada una requiriendo estrategias de respuesta específicas. Por ello, los Equipos de Respuesta a Incidentes (IRT) deben estar preparados para gestionar distintos escenarios, identificando y anticipando vectores de ataque comunes, tales como:

- Ataques desde medios extraíbles o periféricos.
- Fuerza bruta sobre credenciales.
- Correos electrónicos maliciosos.
- Suplantación de identidad.
- Uso indebido de la red institucional.
- Pérdida o robo de dispositivos.

La identificación y gestión adecuada de estos vectores es clave para garantizar una respuesta oportuna y eficaz ante los incidentes.

9.2.1. Identificación de incidentes

Para detectar y evaluar con precisión si ha ocurrido un incidente y conocer los niveles de detalle, se pueden utilizar diversas herramientas y soluciones, es así como la detección automatizada, soluciones de antivirus, correlaciones de eventos. Asimismo, los incidentes pueden ser detectados manualmente y comunicados por los usuarios a través de la mesa de servicios. Estas múltiples vías de detección permiten una evaluación más completa y precisa de los incidentes de seguridad.

Los signos de un incidente se dividen en Precursores e Indicadores, un precursor es una señal de que puede ocurrir un incidente en el futuro, mientras que un indicador es una señal de que un incidente pude haber ocurrido o puede estar desarrollándose.

Así las cosas, en muchos ataques no se evidencian precursores, ya que no siempre se conoce el objetivo del atacante. Sin embargo, algunos ejemplos de precursores pueden incluir:

- Logs del servidor web que muestran el uso de un escáner de vulnerabilidades.
- Anuncio de un nuevo "exploit" que puede ser explotado en un servidor de la entidad/organización.
- Amenaza de un grupo o actor de amenaza que anuncia un ataque.

Estos precursores pueden servir como alertas tempranas para preparar y reforzar las defensas contra posibles incidentes. Los indicadores son más fáciles de detectar. Algunos ejemplos incluyen:

- El software antivirus alerta cuando detecta que un equipo está infectado con malware.
- Una aplicación registra múltiples intentos fallidos de inicio de sesión.
- Un administrador de red evidencia una desviación de tráfico.

Por lo tanto, es esencial identificar las fuentes de precursores e indicadores en la infraestructura tecnológica. Estas fuentes pueden incluir:

- Firewall.
- Antivirus.
- NOC/SOC (Centro de Operaciones de Red/Centro de Operaciones de Seguridad).
- SIEM (Gestión de Información y Eventos de Seguridad).
- CVE (Common Vulnerabilities and Exposures).
- Registros e información pública disponible.
- Identificar y monitorear estas fuentes permite una detección temprana y una respuesta más efectiva a los incidentes de seguridad.

9.2.2. Análisis

Realizar un análisis inicial que proporcione suficiente información es crucial para que el IRT pueda priorizar actividades de contención y erradicación. Sin embargo, algunos incidentes no son fáciles de detectar debido a los signos mínimos que presentan. Por esta razón, es necesario trabajar en equipo con el personal técnico y de seguridad de la información para validar y tomar acciones necesarias para contener un incidente.

Una vez analizados los precursores e indicadores de manera eficientes y efectiva, el IRT debe realizar rápidamente un análisis detallado, identificando la ocurrencia de un incidente de seguridad de la información y seguridad digital, determinar el alcance de este, estableciendo que activos de información fueron afectados, cuál fue el vector de ataque y qué vulnerabilidades fueron explotadas. Esta información permitirá realizar acciones prioritarias de contención.

Las siguientes son recomendaciones para realizar análisis y validaciones iniciales.

- Perfiles de redes y sistemas: establecer una línea base de operación para detectar cambios fácilmente.

- Conocer los comportamientos normales: Comprender el comportamiento normal de redes, sistemas y aplicaciones, lo cual permitirá detectar actividades anormales.

- Crear políticas de retención de registros - Log ´ s: implementar una política de

- retención de registros - log ´ s de Firewall, IPS, servidores, aplicaciones bases de datos. Esta política debe especificar la duración de la retención de los datos con el propósito de:

    - Analizar las entradas de registros más antiguas, que pueden mostrar actividades de reconocimiento o ataques similares.

    - Revisar comportamientos y tácticas que los actores de amenaza utilizan antes de comprometer una infraestructura.

    - Realizar correlación de eventos: Para evidenciar un incidente, se debe revisar integralmente los eventos generados por las diferentes herramientas, sistemas y aplicaciones. Sin embargo, para hacerlo de manera constante, se recomienda utilizar herramientas de correlación de eventos (SIEM), las cuales proporcionan visibilidad completa de la infraestructura.

    - Mantener actualizados los relojes en todos los dispositivos y sistemas: para realizar una correcta correlación de eventos tanto manual como automatizada, es necesario que todos los componentes de la infraestructura estén sincronizados con servidores de hora (NTP). Esto puede hacerse utilizando equipos on-premise o servicios públicos, como los del Instituto Nacional de Metrología de Colombia (INM), a través de los dominios: ntp1.inm.gov.co y ntp2.inm.gov.co.

    - Instale analizadores de tráfico: Para realizar análisis de tráfico y complementar la información de precursores e indicadores, es fundamental contar con herramientas especializadas que monitoricen y analicen el tráfico de red. Esto permitirá una detección más precisa y una respuesta efectiva ante posibles accidentes de seguridad.

9.2.3. Documentación del incidente.

Una vez el IRT, identifique la ocurrencia de un incidente, debe comenzar a registrar todos los hechos y actividades realizadas en cada una de las fases el procedimiento

de gestión de incidentes, llevando una marca de tiempo. Además, todos los informes técnicos generados a nivel interno como para las autoridades judiciales deben ser fechados y firmados por el responsable del IRT. Es fundamental documentar minuciosamente las actividades y acciones realizadas para la preservación de la evidencia digital.

9.2.4. Clasificación de Incidentes de seguridad de la información y seguridad digital

La taxonomía de clasificación para los incidentes de seguridad digital empleada por COLCERT, se alinea a la utilizada por el CSIRT Américas (https://csirtamericas.org/) y por homólogos globales para la clasificación de los incidentes de seguridad de la información y seguridad digital.

TAXONOMÍA			
Clasificación	Definición	Tipo de incidente	Descripción
Contenido abusivo	Ataques destinados a dañar la imagen de la organización o utilizar sus recursos electrónicos para usos ilícitos (como publicidad, extorsión o ciberdelincuencia en general)	Spam	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje compartido.
		Delito de odio	Contenido difamatorio o discriminatorio. Ej: Ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos o grupos.
		Materiales de abuso/explotación sexual infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino	Incidentes relacionados con actividades maliciosas, aplicaciones y archivos dañinos para obtener acceso no	Sistema infectado	Sistema infectado con malware. Ej: Sistema, computador, dispositivos móviles infectado con un rootkit
		Servidor C&C	Conexión con servidor de Comando y Control (C&C) mediante malware o sistemas infectados.

TAXONOMÍA			
Clasificación	Definición	Tipo de incidente	Descripción
	autorizado al sistema para sustraer, exfiltrar, eliminar, modificar su información privada que pretenden acceder a sus datos u.	(Comando y Control)	
		Distribución de malware	Recurso usado para distribución de malware. Ej: Recurso de una organización empleado para distribuir malware.
		Configuración de malware	Recurso que aloje archivos de configuración de malware Ej: Ataque de webinjects para troyano.
Obtención de información	Incidentes relacionados con la identificación y recopilación de información de personas, infraestructura tecnológica y activos de información de una organización a través de técnicas no autorizadas con fines delictivos.	Escaneo de redes (scanning)	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: Peticiones DNS, ICMP, SMTP y escaneo de puertos.
		Análisis de paquetes (sniffing)	Observación y grabación del tráfico de redes.
		Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ej: Mentiras, trucos, sobornos, amenazas.
Intento de intrusión	Incidentes relacionados con la utilización de técnicas que intentan atacar una infraestructura tecnológica o un activo de información aprovechándose de una vulnerabilidad para obtener el control y privilegios administrativos o de ejecución.	Explotación de vulnerabilidades conocidas	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej: Desbordamiento de buffer, puertas traseras y cross site scripting (XSS).
		Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ej: Intentos de ruptura de contraseñas, ataque por fuerza bruta.
		Ataque desconocido	Ataque empleando exploit desconocido
Intrusión	Ataques que aprovechar las vulnerabilidades de diseño, funcionamiento o configuración de las	Compromiso de cuenta con privilegios	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
		Compromiso de cuenta	Compromiso de un sistema empleando cuentas sin privilegios.

TAXONOMÍA			
Clasificación	Definición	Tipo de incidente	Descripción
	diferentes tecnologías, para entrar de forma fraudulenta a los sistemas de una organización	sin privilegios	
		Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades del software. Ej: Inyección SQL y defacement.
		Robo	Intrusión física. Ej: acceso no autorizado a Centro de Procesamiento de Datos.
Disponibilidad	Interrupción de la capacidad de procesamiento y respuesta de los sistemas y redes para dejarlos inoperativos Acción premeditada para dañar un sistema, interrumpir un proceso, cambiar o borrar información.	DoS (Denegación de Servicio)	Ataque de denegación de servicio. Ej: Envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
		DDoS (Denegación Distribuida de Servicio)	Ataque de Denegación Distribuida de Servicio. Ej: Inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
		Mala configuración	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
		Sabotaje	Sabotaje físico. Ej: Cortes de cableados de equipos, desconexión de equipos o incendios provocados
		Interrupciones	Interrupciones por causas ajenas. Ej: Desastre natural.
Compromiso de Información	Incidentes relacionados con el acceso, filtraciones (confidencialidad), la modificación o el borrado (integridad) de información.	Acceso no autorizado a información	Acceso no autorizado a información. Ej: Robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
		Modificación no autorizada de información	Modificación no autorizada de información. Ej: Modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado

TAXONOMÍA			
Clasificación	Definición	Tipo de incidente	Descripción
			de datos mediante ransomware.
		Pérdida de datos	Pérdida de información Ej: Pérdida por fallo de disco duro o robo físico.
Fraude	Incidentes relacionados con la pérdida de bienes causada con intención fraudulenta o deshonesta en procura de un beneficio económico para sí mismo, para otra persona o empresa	Uso no autorizado de recursos	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.
		Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej: Warez
		Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
		Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
Vulnerable	Incidentes relacionados con la identificación del grado de debilidad inherente en un sistema de hardware o software que permitan a un atacante realizar actividades no autorizadas a la misma organización o en contra de otra.	Criptografía débil	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: Servidores web susceptibles de ataques POODLE/FREAK.
		Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej: DNS open-resolvers o Servidores NTP con monitorización monlist.
		Servicios con acceso potencial no deseado	Ej: Telnet, RDP o VNC.
		Revelación de información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej: SNMP o Redis.
		Sistema vulnerable	Sistema vulnerable.

TAXONOMÍA			
Clasificación	Definición	Tipo de incidente	Descripción
			Ej: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Otros	Incidentes no clasificados en la taxonomía existente o amenazas persistentes avanzadas	Incidente no clasificado	Incidentes que no se ajustan a la clasificación existente, actuando como indicador para la actualización de la clasificación.
		APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

Tabla 1 Taxonomía clasificación de incidentes

9.2.5. Priorización del incidente

La gestión de los incidentes no debe realizarse por orden de llegada. Este proceso es uno de los más críticos y debe priorizarse teniendo en cuenta los siguientes factores:

Impacto funcional del incidente: Este corresponde a las afectaciones de la operatividad y funcionalidad actual de las aplicaciones y servicios a los usuarios, tanto interno como externos. También se deben considerar el probable impacto funcional futuro si el incidente no se contiene de inmediato.

Impacto de la Información comprometida: Una vez Identificada la afectación a las funcionalidades de los activos en términos de confidencialidad, integridad y disponibilidad, se debe evaluar si el incidente ha causado una filtración de información. Es importante determinar el impacto de esta filtración tanto en la entidad/organización como en terceros, y cómo afecta la misionalidad de la entidad. La evaluación debe considerar el rol de la entidad como responsable y encargado de la información comprometida.

Recuperabilidad del incidente: La magnitud del incidente y los activos de información afectados determinarán el tiempo y los recursos necesarios para la recuperación de las operaciones. En algunos casos, un incidente puede requerir muchos más recursos de los que la entidad tiene disponible. Priorización atención de Incidentes y Tiempos de Respuesta.

Para permitir una gestión y respuesta a los incidentes, se debe determinar el nivel de prioridad para la atención por parte del IRT. A continuación, se definen algunas

variables que pueden ser utilizadas para realizar una adecuada priorización de los incidentes.

9.2.6. Criterios de valoración del Nivel de Impacto

Nivel	Valor	Descripción
Muy Grave	• 1,00	• Afecta activos de información de criticidad Alta y de Infraestructura crítica cibernética y servicios esenciales. • Afecta las funcionalidades a más del 75% de los sistemas de la organización. • Afecta la operación y funcionalidad de más del 75% de los usuarios internos y externos: • Afecta interdependencia de las operaciones y servicios en más de un 75% a otras entidades/organizaciones. • Compromete la confidencialidad de la información y los datos de la entidad, con filtración de cualquier porcentaje de Información pública Clasificada, Información pública Reservada, Información semi-privada e Información Privada. • Provoca daños reputacionales muy elevados y cobertura continua en medios de comunicación nacionales.
Grave	• 0,75	• Afecta activos de información de criticidad Media. • Afecta las operaciones y funcionalidades de más del 50% de los sistemas de la organización. • Afecta la operación y funcionalidad de más del 50% de usuarios internos y externos. • Afecta interdependencia de las operaciones y servicios en más del 50% de otras entidades/organizaciones. • Afecta a un servicio esencial. • Provoca daños reputacionales de difícil reparación, con amplia cobertura mediática y afectando la reputación de terceros. .
Menos Grave	• 0,50	• Afecta activos de información identificados de criticidad Baja. • Afecta las operaciones y funcionalidades de más del 25% de los sistemas de la organización. • Afecta la operación y funcionalidad de más del 25% de usuarios internos y externos. • Afecta interdependencia de las operaciones y servicios en más de un 25% a otras entidades/organizaciones.

Nivel	Valor	Descripción
		• Provoca daños reputacionales a menor escala, con mínima cobertura mediática y sin afectación a la reputación de terceros. .
Menor	• 0,25	• Afecta las operaciones y funcionalidades de los sistemas de la organización con interrupciones. • Afecta la operación y funcionalidad de hasta el 10% de usuarios internos. • Provoca daños reputacionales mínimo y puntuales, sin repercusión mediática en medios de comunicación
Sin Impacto	• 0.00	• No hay ningún impacto que afecte las operaciones, funcionalidades y reputación a la entidad.

Tabla 2 Descripción categorías de impacto función y de compromisos de información

9.2.7. Criterios de valoración del nivel de recuperabilidad - urgencia del Incidente

La Tabla 17, establece los criterios y categorías frente a los recursos y tiempo de recuperación de las operaciones.

Nivel	Valor	Descripción
Muy Grave	• 1,00	• Recuperación de las funcionalidades y operaciones de los activos afectados es superior a 24 horas. • La recuperación requiere recursos adiciones y ayuda externa.
Grave	• 0,75	• Recuperación de las funcionalidades y operaciones de los activos afectados es superior a 8 horas. • La recuperación requiere recursos adiciones.
Menos Grave	• 0,50	• Recuperación de las funcionalidades y operaciones de los activos afectados superior a 1 hora. • La recuperación se realiza con recursos propios.
Menor	• 0,25	• Recuperación de las funcionalidades y operaciones de los activos afectados superior a 15 minutos. • La recuperación se realiza utilizando mínimos recursos.

Tabla 3 Descripción de categorías de impacto de recuperabilidad de las operaciones

Luego de tener definidas las variables de impacto funcional actual, impacto funcional futuro y urgencia se obtiene la prioridad aplicando la siguiente formula:

Nivel de Prioridad = (Impacto funcional actual * 2) + (Impacto funcional futuro * 2) + (Urgencia * 4).

Impacto funcional actual: Se refiere al impacto actual del incidente, tomando en cuenta la afectación a los sistemas, usuarios, funcionalidades, interdependencia y reputación según los criterios establecidos en la Tabla 2.

Impacto funcional futuro: Se refiere al potencial impacto que podría tener el incidente si no se gestiona adecuadamente, evaluando la posible evolución y consecuencias adicionales, según los criterios establecidos en la Tabla 2.

Urgencia: Se refiere a la rapidez con la que debe ser resuelto el incidente, basada en la criticidad de la situación y los tiempos de respuesta necesarios, según los criterios establecidos en la Tabla 3.

Esta fórmula permite calcular una prioridad equilibrada considerando tanto el impacto inmediato como el potencial futuro del incidente, además de la urgencia de la respuesta necesaria.

Nivel de Prioridad	Nivel de Prioridad
Muy Grave	6,01 -8,00
Grave	4,01 – 6,00
Menos Grave	2,01 – 4,00
Menor	00,00 – 2,00

Tabla 4 Descripción de escalas de nivel de prioridad de atención de incidentes

9.2.8. Tiempos de Respuesta

Para la atención de incidentes, se han definido tiempos máximos de respuesta según la prioridad asignada, con el fin de asegurar una gestión oportuna y permitir la ejecución de acciones de contención, erradicación y recuperación. Estos tiempos aplican tanto al Equipo de Respuesta a Incidentes (IRT) como a las dependencias involucradas, conforme a sus responsabilidades.

Los plazos establecidos en la Tabla siguiente representan el tiempo máximo estimado para actuar según el nivel de criticidad del incidente. El IRT tiene a su cargo orientar, coordinar y supervisar la respuesta, garantizando que las dependencias cuenten con lineamientos y recursos para una gestión eficaz. Así, se asegura una atención proporcional al impacto del incidente sobre la seguridad de la organización.

Es importante aclarar que el tiempo de recuperación de las operaciones, varía dependiendo el impacto y los recursos disponibles, así las cosas, cada entidad está en la libertad de definir tiempos de atención a los incidentes como crean conveniente y dependiendo el nivel de criticidad de los activos impactados, los recursos disponibles, lo establecido en sus planes DRP Y BCP.

Nivel de Prioridad	Tiempo de Respuesta
Muy Grave	20 Minutos
Grave	45 Minutos
Menos Grave	1 Hora
Menor	2 Horas

Tabla 5 Descripción Tiempos Máximos de Atención de Incidentes por parte del IRT

9.3. Contención, Erradicación y Recuperación

Es fundamental para la entidad/organización diseñar estrategias que permitan tomar decisiones oportunas para evitar la propagación del incidente, acceso no autorizado, compromisos de otros sistemas y reducir el impacto en nivel la confidencialidad, integridad y disponibilidad de la información, así como los recursos tecnológicos.

Apagar un sistema, desconectar dispositivos de la red o desactivar funcionalidades son decisiones que pueden contemplarse en la estrategia a seguir durante el proceso de contención, con el objetivo de limitar el alcance y la afectación del incidente.

En este sentido, las estrategias y procedimientos establecidos para contener los diversos tipos de incidentes permiten facilitar la toma de decisiones y la implementación de acciones con mayor celeridad.

Los siguientes son algunos criterios que pueden ser adoptados para definir las estrategias de contención:

- Posibles daños y afectaciones.
- Necesidad de preservación de evidencia digital.
- Disponibilidad del servicio, interdependencia interna y externa.
- Tiempo y recursos necesarios para implementar la estrategia.
- Eficacia de la estrategia, determinando si la contención es parcial o total.
- Duración de la solución, evaluando si las acciones solucionar el incidente de manera parcial, temporal o total, si la solución es permanente o se eliminará después de un tiempo determinado.

9.3.1. Recopilación y preservación de evidencia

En paralelo con la gestión del incidente, se debe llevar a cabo una investigación de análisis forense para recopilar y preservar las evidencias, las cuales serán entregadas a las autoridades judiciales competentes (Fiscalía General de la Nación – Unidades de Policía Judicial). Es crucial documentar detalladamente como se han recolectado y preservado todas las evidencias para asegurar su admisibilidad en un proceso judicial. Por lo tanto, siempre que se transfiera la evidencia de una persona a otra, se debe diligenciar los formularios de cadena de custodia, que deben estar firmados por cada parte involucradas en el proceso.

Para la obtención de imágenes forenses, es recomendable que estás sean obtenidas antes de que los administradores de sistemas realicen cualquier actividad en el activo comprometido, utilizando las herramientas forenses recomendadas por la comunidad técnico-científica y documentando el proceso de acuerdo con los lineamientos establecidos por COLCERT para el manejo de la evidencia digital

Identificación de equipos atacantes: los IRT, deben centrar todas su acciones y actividades en la contención, erradicación y recuperación. Identificar un host atacante o paciente cero, puede ser un proceso que requiere mucho tiempo y, a veces, resulta inútil, impidiendo que el equipo minimice le impacto del incidente.

9.3.2. Erradicación y Recuperación

Una vez contenido el incidente, puede ser necesario realizar la erradicación para eliminar cualquier rastro dejado por el incidente y la amenaza a la infraestructura tecnológica, esto incluye eliminar el malware, deshabilitar cuentas comprometidas e identificar y mitigar las vulnerabilidades explotadas. Es crucial identificar todos los hosts y dispositivos afectados para llevar a cabo procesos de remediación y sanitización.

En algunos casos los incidentes, la erradicación se lleva a cabo durante la recuperación o simplemente no se realiza.

9.3.3. Recuperación

Los administradores de plataforma, sistemas, e infraestructura, deben restaurar el funcionamiento normal validando con las áreas funcionales la correcta operación. Así mismo, deben corregir las vulnerabilidades explotadas. Las restauraciones se pueden realizar a partir de copias de seguridad limpias, reconstruyendo sistemas y aplicaciones desde cero, reemplazando archivos comprometidos con versiones limpias, instalando parches de seguridad, renovación contraseñas, inactivando

usuarios con y sin perfiles de administrador, y ajustando las políticas en los equipos de seguridad perimetral.

En esta fase, es importante monitorear la infraestructura tecnológica para tener visibilidad, detectar precursores e indicadores y evitar futuros ataques.

En casos de incidentes clasificados como muy graves y grave la recuperación puede llevar meses, por esta razón, las estrategias de detección y las acciones de erradicación y recuperación deben estar orientadas a realizar cambios y ajustes rápidos, para evitar incidentes futuros.

Teniendo en cuenta los ajustes a la matriz de riesgos, los controles y ajustes a la postura de seguridad, deben realizarse a mediano y largo plazo, manteniendo las operaciones y la continuidad del negocio.

10. Actividades posteriores al Incidente.

10.1. Lecciones aprendidas.

La gestión de incidentes debe ser una oportunidad de aprendizaje y mejora para toda la entidad. Tanto el Equipo de Respuesta a Incidentes (IRT) como cada dependencia involucrada deben aprender de cada evento, independientemente de su gravedad. Por ello, es fundamental realizar reuniones de lecciones aprendidas con todas las partes involucradas, especialmente en incidentes clasificados como graves o muy graves. Para los de menor impacto, se recomienda programar espacios periódicos de revisión que fortalezcan la mejora continua.

Estas reuniones tienen como propósito no solo fortalecer la capacidad técnica del IRT, sino también mejorar las competencias de cada dependencia en la gestión de incidentes. En estos espacios se deben ajustar la matriz de activos y riesgos, mejorar controles, validar la eficacia de las acciones tomadas y revisar el procedimiento general.

Además, permiten formalizar el cierre del incidente, identificar a las partes interesadas y fortalecer la madurez institucional en seguridad de la información. Así, cada dependencia asume su rol en la gestión de incidentes y aporta activamente a la resiliencia organizacional.

Esta revisión permite establecer:

- ¿Qué pasó exactamente y en qué momentos?
- ¿Qué tan bien desempeñó el personal y la alta dirección en el abordaje del incidente?
- ¿Se siguieron los procedimientos y fueron adecuados?
- ¿Qué información se debía tener con antelación?

- ¿Qué acciones correctivas pueden prevenir incidentes similares en el futuro?
- ¿Qué precursores e indicadores se deben vigilar en el futuro para detectar incidentes?
- ¿Qué ajustes se deben realizar a la matriz de riesgos y qué controles deben ser ajustados e implementados para evitar futuros incidentes?
- ¿Qué herramientas o recursos adicionales se necesitan para detectar, analizar y mitigar incidentes futuros?

Igualmente, los temas abordados en las reuniones de lecciones aprendidas sirven como insumos para desarrollar campañas de concientización en seguridad de la información y seguridad digital y a capacitar a nuevos integrantes de los IRT. Asimismo, permite realizar ajustes a las políticas y procedimientos de gestión de incidentes.

En esta fase, se debe complementar los informes técnicos y de gestión del incidente, los cuales servirán como base de conocimiento para afrontar incidentes futuros.

10.2. Uso de datos e información recopilados del incidente.

Los datos permiten realizar una revisión a los riesgos y controles para realizar los ajustes correspondientes y fortalecer la postura de seguridad tanto a nivel del IRT como de las dependencias responsables de la gestión de incidentes.

Asimismo, los datos ayudan a establecer las capacidades y los recursos desplegados en la gestión del incidente, permitiendo identificar necesidades para justificar inversiones tanto en el IRT como en el fortalecimiento de las capacidades dentro de cada dependencia, asegurando que cuenten con los medios adecuados para responder de manera efectiva a los incidentes de seguridad de la información según su ámbito de responsabilidad.

Los datos obtenidos en la gestión de incidentes permiten cumplir con las obligaciones de reporte definidas en la **Resolución 500 de 2021 del MinTIC**. En particular, los incidentes clasificados como *Menos Grave* y *Menor* deben ser reportados al **Equipo COLCERT**, una vez gestionados, a través del siguiente enlace: https://www.colcert.gov.co/800/w3-article-198656.html#formulario_i__form_ReporteIncidentes_1.

Por su parte, los incidentes que involucren **datos personales** deben ser reportados a la **Superintendencia de Industria y Comercio (SIC)**, de conformidad con la normatividad vigente en protección de datos.

La recopilación estructurada de esta información facilita la clasificación y análisis de los incidentes, y permite identificar cómo las amenazas impactan los procesos institucionales.

Además, estos datos son clave para:

- Cumplir con los requisitos formales de notificación.
- Generar retorno de inversión en ciberseguridad.
- Detectar tendencias, nuevas amenazas y posibles vulnerabilidades.

Entre las métricas sugeridas para el monitoreo y mejora continua se encuentran:

- Número de incidentes gestionados.
- Tiempo total dedicado a su gestión.
- Tiempo de respuesta inicial del IRT.

Tiempo de notificación a la alta dirección y al CSIRT Gobierno/COLCERT

10.2.1. Evaluación Objetiva:

Busca determinar qué tan efectivas fueron las acciones y actividades desarrolladas por el IRT.

- Identificar los precursores e indicadores del incidente.
- Determinar si se identificó la causa raíz y el vector de ataque, las vulnerabilidades explotadas, y las características de la infraestructura afectada.
- Determinar si el incidente es producto de un incidente anterior.
- Medir la diferencia entre la evaluación de impacto inicial e impacto final.
- Identificar medidas y controles que se podrían haber implementados para evitar el incidente.

10.2.2. Evaluación Subjetiva:

Busca evaluar el desempeño de cada miembro del IRT y de las personas que intervinieron en cada una de las fases de la gestión del incidente, así como validar con el propietario del activo afectado si el incidente se gestionó de manera eficiente.

Igualmente, las entidades/organizaciones pueden realizar auditorías al procedimiento de gestión y respuesta a incidentes.

10.3. Retención de pruebas:

Para la retención de evidencia digital, la entidad/organización puede establecer un protocolo, en el cual indique que las evidencias preservadas se mantendrán resguardadas por el representante legal en un lugar seguro y que después de recolectadas y embaladas dentro del proceso de cadena de custodia (Manual cadena de custodia Fiscalía https://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf) y entregadas a las autoridades judiciales (CTI de la Fiscalía y Delitos Informáticos de la DIJIN), estas se mantendrán en custodia durante tres (3) meses contados a partir de la entrega.

Sin embargo y entendiendo las capacidades disponibles para el restablecimiento de los servicios afectados, la entidad puede ajustar estos tiempos, en virtud de la recuperación las operaciones.

10.4. Lista de verificación para la gestión de incidentes.

Los siguientes son los principales pasos para seguir en la gestión del incidente, sin embargo, estos pueden variar según el tipo y naturaleza de incidentes a gestionar.

Item	Acción	Terminado
	Detección y Análisis	
1	Determinar si ha ocurrido un incidente	
1.1	Analizar los precursores e indicadores	
1.2	Buscar información de diferentes fuentes y correlacionarla	
1.3	Realizar investigación en motores de búsqueda y base de conocimientos	
1.4	Documentar el incidente, las actividades de investigación y la recolección de evidencias.	
2	Priorizar el incidente según los criterios de Impacto funcional, de información afectada y recuperabilidad.	
3	Informar el incidente internamente y al COLCERT/CSIRT Gobierno	
	Contención Erradicación y Recuperación	
4	Adquirir, preservar, proteger y documentar	
5	Contener el incidente	
6	Erradicar la amenaza	
6.1	Identificar y mitigar todas las vulnerabilidades que fueron explotadas	
6.2	Eliminar el malware, sanitizar equipos y dispositivos.	
7	Recuperación del incidente	
7.1	Restablecer los sistemas afectados y restablecer los servicios.	
7.2	Confirmar con los funcionales de los aplicativos y sistemas el funcionamiento de estos.	

7.3	Implementar seguimientos adicionales en búsqueda de afectaciones sin restablecer.	
	Actividad Posteriores	
8	Elaborar un informe de seguimiento de las gestiones y actividades de investigación realizadas	
9	Realizar reunión de lecciones aprendidas obligatorias para incidentes muy graves y graves.	

Tabla 6 Pasos para seguir en la gestión del incidente

11. Recomendaciones Generales

- Adquirir herramientas y soluciones que puedan apoyar la gestión de los incidentes.
- Identificar precursores e indicadores a través de alertas generadas por equipos de seguridad.
- Solicitar registros y eventos de todos los sistemas a un nivel básico.
- Perfilar redes y sistemas.
- Entender los comportamientos normales de las redes, sistemas y aplicaciones.
- Realizar correlación de eventos.
- Mantenga sincronizados todos los relojes de equipos y dispositivos.
- Mantener y utilizar una base de conocimiento de información de incidentes.
- Registrar todas las informaciones una vez se identifique un incidente.
- Preservar las evidencias.
- Priorizar la gestión de los incidentes según el resultado del análisis.
- Divulgar el procedimiento de gestión de incidentes del COLCERT/CSIRT Gobierno.
- Establecer estrategias y procedimientos de contención.
- Capture datos volátiles de los sistemas y equipos como evidencia.
- Celebrar reuniones de lecciones aprendidas.

12. Coordinación e intercambio de información.

Las entidades/organizaciones deben trabajar conjuntamente durante la gestión de los incidentes. Se debe realizar una coordinación con las múltiples partes interesadas para el intercambio de información sobre amenazas, vulnerabilidades y ataques (Indicadores de Compromiso (IoC)- Indicadores de Ataque -(IoA) para que sea validada y ajustada la postura de seguridad.

Para el intercambio de información se deben establecer los canales de comunicación con los proveedores de servicios onpremise y nube, infraestructura tecnológica, PRST, cadenas de suministro, autoridades y el CISRT Gobierno/COLCERT, para reportar los incidentes y solicitar los apoyos y coordinar las acciones en cada una de las fases de la gestión de incidentes.

Con el propósito de recibir apoyo y coordinación en la gestión de los incidentes catalogados como muy graves y graves, estos deben ser reportados al COLCERT/CSIRT Gobierno, por los canales de comunicación establecidos como son contacto@colcert.gov.co – csirtgob@mintic.gov.co.

Los incidentes catalogados como Menos Grave y Menor deben ser reportados al COLCERT/CSIRT Gobierno en el formulario establecido una vez sea gestionado. El cual se encuentra publicado en la siguiente URL https://www.colcert.gov.co/800/w3-article-198656.html#formulario_i__form_ReporteIncidentes_1, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos.

La información de los incidentes debe ser protegida por el IRT, a través de accesos a los repositorios de manera restringida y controlada.

13. Lineamientos a considerar.

A continuación, se detallan lineamientos para ser considerados por las entidades:

Lineamiento Sugerido	Acciones Claves
- Los incidentes de seguridad relacionados con proveedores y terceros, como los servicios en la nube, deben ser abordados en los planes de respuesta, incluyendo cláusulas contractuales para notificación, gestión y mitigación oportuna, conforme al control A.5.19 de la ISO/IEC 27001:2022	- Actualizar los planes de respuesta a incidentes incluyendo procedimientos documentados y roles definidos para análisis, respuesta, recuperación y mejora continua.
- Los incidentes relacionados con datos personales deberán ser tratados	Definir protocolos de actuación diferenciados para incidentes que

conforme a la Ley 1581 de 2012 y las disposiciones de la ISO/IEC 27701, incluyendo la notificación oportuna a los titulares afectados y a la autoridad competente	involucren datos personales, incluyendo notificación a la SIC y a los titulares afectados.
- Se deben establecer procedimientos para la comunicación de incidentes relevantes a las partes interesadas, incluyendo notificación a autoridades regulatorias, terceros afectados y entes de control, según la criticidad del incidente y el tipo de información comprometida	Desarrollar una política de notificación de incidentes críticos con plazos, responsables y medios de comunicación hacia entes de control y ciudadanía.
- La entidad deberá articular su proceso de respuesta a incidentes con el CSIRT Gobierno, y cuando aplique, con otros CSIRT sectoriales o institucionales, a través de canales de reporte, protocolos de escalamiento y mecanismos de coordinación establecidos.	Incluir en el plan de respuesta procedimientos de escalamiento y cooperación con CSIRT Gobierno, incluyendo contacto permanente, roles compartidos y trazabilidad de casos.
Incluir la gestión de incidentes relacionados con proveedores o terceros, en especial en la cadena de suministro y servicios en la nube (control A.5.19).	Establecer cláusulas contractuales con proveedores que contemplen notificación, mitigación y reporte de incidentes; definir mecanismos de coordinación y seguimiento.

Tabla 7 Lineamientos a considerar

14. Referencias.

- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August 6). Computer Security Incident Handling Guide. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

- Computer Security Incident Handling Guide. (2012, August 6). https://doi.org/10.6028/NIST.SP.800-61r2

- CSIRT Services Framework Version 2.1. (2019, November). https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

- FIRST - Improving Security Together. (2015, January 1). https://www.first.org/

- Incident management. (2022, May 31). https://www.wikiwand.com/en/Incident_response

- National Institute of Standards and Technology This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29 February 26, 2024 The NIST Cybersecurity Framework (CSF) 2.0. (2024, February 29). NIST, 2.0. https://doi.org/https://doi.org/10.6028/NIST.CSWP.29

- Prácticas recomendadas y tutoriales de gestión de incidentes. (2023, January 1). https://www.atlassian.com/es/incident-management

- Publications. (2023, February 6). https://csrc.nist.gov/publications

- Ruefle, R., Dorofee, A., Mundie, D A., Householder, A D., Murray, M., & Perl, S J. (2014, September 1). Computer Security Incident Response Team Development and Evolution. https://doi.org/10.1109/msp.2014.89

- Şeker, E., & Ozbenli, H H. (2018, June 1). The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation. https://doi.org/10.1109/cybersecpods.2018.8560673