Contenido

VERSIONES

Versión	Elaborado por	Revisado por	Aprobado por	Fecha	Motivo
1	DIANA ROJAS LUIS MERLY TORRES BERNAL	LAURA MARCELA PERDOMO FONSECA	LAURA MARCELA PERDOMO FONSECA	20/11/2020	Versión inicial
2	JAKELINE SÁNCHEZ MERLY TORRES BERNAL	LAURA MARCELA PERDOMO FONSECA	COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	17/05/2022	Actualización

1 INTRODUCCIÓN

Hoy en día, la información, que es considerada uno de los activos principales de las organizaciones, está expuesta a una gran variedad de amenazas que pueden desencadenar incidentes de seguridad que atenten contra su confidencialidad, integridad y disponibilidad.

Según la norma ISO 27035, un incidente de seguridad de la información está representado por un evento o una serie de eventos de seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información. Las políticas y controles de seguridad de la información por sí solas no garantizan la protección total de la información, después de que los controles se han implementado, es posible que queden vulnerabilidades residuales que pueden hacer posible la ocurrencia de incidentes de seguridad de la información.

En la siguiente figura se describe la relación existente entre los distintos componentes de un incidente de seguridad de la información:

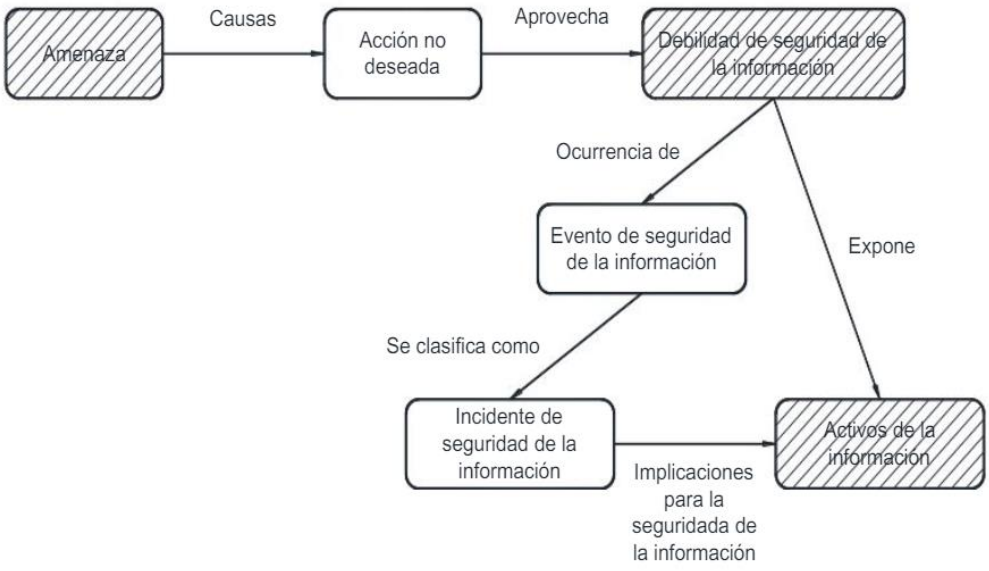

Figura 01: Relación entre los objetos en una cadena de incidentes de seguridad de la información
Fuente: GTC-ISO 27035 2012

Por lo anteriormente expuesto, es esencial que toda organización cuente con un enfoque estructurado y planificado para:

- ✓ Detectar, reportar y evaluar incidentes de seguridad de la información
- ✓ Responder a incidentes de seguridad de la información
- ✓ Reportar, evaluar y tratar las vulnerabilidades de seguridad de la información que puedan causar eventos de seguridad de la información, y posiblemente incidentes de seguridad de la información.
- ✓ Aprender de las vulnerabilidades e incidentes de seguridad de la información con el fin de fortalecer la prevención.

RTVC, como entidad pública cumpliendo con la normativa y estándares vigentes que dictan las entidades del Gobierno Nacional, compila en este documento los lineamientos para la gestión de incidentes de seguridad de la información en la entidad.

La expresión "gestión de incidentes de seguridad" se utilizará en el presente documento para referirse a incidentes de seguridad de la información, incidentes de seguridad informática e incidentes de seguridad digital.

2 OBJETIVO

Establecer los lineamientos básicos que deben ser utilizados por las dependencias y sus funcionarios, colaboradores y/o terceros de RTVC para gestionar incidentes de seguridad y privacidad de la información o seguridad digital, a través de una oportuna identificación, atención y respuesta, con el fin de mitigar el impacto asociado a la pérdida de la confidencialidad, Integridad y Disponibilidad de la información de RTVC.

3 ALCANCE

Este documento cubre todos los aspectos para la gestión de los incidentes de seguridad de la información que se puedan presentar sobre la infraestructura tecnológica, los sistemas de información y repositorios físicos o lógicos de RTVC.

4 NORMATIVIDAD

Ley, norma o decreto	Ámbito de aplicación del procedimiento
ISO 27001:2013	Sistema de Gestión de Seguridad de la Información
ISO 27035:2016	Incidentes de Seguridad de la Información
CONPES-3701	Lineamientos de Política para ciberseguridad y ciberdefensa.
CONPES 3854	Política Nacional de Seguridad Digital
Ley Estatutaria 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Ley 1266 de 2008	Define el manejo de la información contenida en bases de datos personales desde sistemas como registro, credenciales y otros.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "*de la protección de la información y de los datos*" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Artículo 269A	Acceso abusivo a un sistema informático.
Artículo 269B:	Obstaculización ilegítima de sistema informático o red de telecomunicación
Artículo 269C:	Interceptación de datos informáticos.
Artículo 269D:	Daño Informático.
Artículo 269E:	Uso de software malicioso.
Artículo 269F:	Violación de datos personales.
Artículo 269G:	Suplantación de sitios web para capturar datos personales
Artículo 269H:	Agravación punitiva.
Artículo 269I:	Hurto por medios informáticos y semejantes.
Artículo 269J:	Transferencia no consentida de activos.
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 078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Ley 1928 de 2018	Por medio de la cual se aprueba el “Convenio sobre la ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest
Directiva Presidencial No. 03 de 2021	Donde se dictan lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos
Resolución No. 500 de 2021 MinTIC	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 GLOSARIO

- **Activo de información:** 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.[1]

- **Acceso no autorizado**: consiste en intentos no autorizados para utilizar incorrectamente un sistema, servicio o red.

- **Amenaza**: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad. [2]

- **Ataque cibernético:** Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio.

- **Ataque de diccionario**: es un método que consiste en intentar averiguar una contraseña probando todas (o casi todas) las palabras posibles o recogidas en un diccionario.

- **Ataque de fuerza bruta**: es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta.

- **Ataque Man-in-the-middle**: Es un tipo de ataque basado en interceptar la comunicación entre 2 o más interlocutores, pudiendo suplantar la identidad de uno u otro según lo requiera para ver la información y modificarla a su antojo, de tal forma que las respuestas recibidas en los extremos pueden estar dadas por el atacante y no por el interlocutor legítimo. [3]

- **Bomba lógica:** Tipo de virus en forma de código que es insertado intencionalmente en un programa informático y que permanece oculto hasta

[1] CONPES 3854:2016, pág.56
[2] Glosario de términos de ciberseguridad - Incibe
[3] Glosario de términos de ciberseguridad - Incibe

cumplirse una o más condiciones preprogramadas, en ese momento se ejecuta una acción maliciosa.

- **CCOC:** Comando Conjunto Cibernético del Comando General de las Fuerzas Militares de Colombia. [4]

- **Ciberdefensa:** es la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.[5]

- **Ciberdelito:** Actividad delictiva de las acciones en Internet o relacionadas, llevada a cabo mediante equipos informáticos o a través de Internet.

- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.[6]

- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.[7]

- **Cross-site Scripting – XSS**: Se trata de una vulnerabilidad existente en algunas páginas web generadas dinámicamente (en función de los datos de entrada). Dado que los sitios web dinámicos dependen de la interacción del usuario, es posible insertar en un formulario un pequeño programa malicioso, ocultándolo entre solicitudes legítimas y hacer que éste se ejecute. [8]

- **Defacement**: es un tipo de ataque que se realiza contra un sitio web, en el que se modifica la apariencia de alguna de sus páginas, para llevar a cabo algún tipo de acción fraudulenta o de vandalismo. [9]

- **DoS – Denegación de servicios**: ataque cuyo objetivo es consumir los recursos de máquina o de la red destino causando la indisponibilidad de sus servicios.

- **DDoS – Denegación distribuida de servicios**: ataque de DoS, pero ejecutado de forma coordinada entre varios equipos, que pueden estar siendo utilizados para este fin sin el conocimiento de sus legítimos dueños.

[4] CONPES 3854. Pág.13
[5] CONPES 3701
[6] CONPES 3701
[7] Norma ISO 27000 Términos y definiciones
[8] Glosario de términos de ciberseguridad - Incibe
[9] Glosario de términos de ciberseguridad - Incibe

- **Disponibilidad:** Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.[10]

- **Evento de seguridad de la información**: Es la presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación a la política de seguridad de la información o a la falla de las salvaguardas o una condición desconocida previamente que puede ser pertinente a la seguridad. [11]

- **Gusano informático:** Es un programa malicioso que tiene como característica principal su alto y rápido nivel de propagación.

- **Incidente de Seguridad de la información:** evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.[12]

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad. [13].

- **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014[14].

- **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo de esta ley[15].

- **Ingeniería Social:** son tácticas utilizadas para obtener información datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima. [16]

[10] Glosario de términos de ciberseguridad - Incibe
[11] GTC-ISO/IEC 27035 2012
[12] GTC-ISO/IEC 27035 2012
[13] Tomado de la Ley 1712 del 2014
[14] Tomado de la Ley 1712 del 2014
[15] Tomado de la Ley 1712 del 2014
[16] Glosario de términos de ciberseguridad - Incibe

- **Integridad:** es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales. [17]

- **Inyección SQL**: tipo de ataque que aprovecha una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que puede permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web. [18]

- **Pharming:** consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una web falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad. [19]

- **Phishing:** estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta. [20]

- **Ransomware:** ataque en el que el ciberdelincuente, toma control del equipo infectado y secuestra la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos. [21]

- **Rootkits:** Programa malicioso que genera un acceso privilegiado continuo a una computadora pero que mantiene su presencia activa oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.

- **Software Malicioso:** Programa o parte de un programa destinado a perturbar, alterar o destruir la totalidad o parte de los elementos de un sistema de información.

[17] Glosario de términos de ciberseguridad - Incibe
[18] Glosario de términos de ciberseguridad - Incibe
[19] Glosario de términos de ciberseguridad - Incibe
[20] Glosario de términos de ciberseguridad - Incibe
[21] Glosario de términos de ciberseguridad - Incibe

- **Troyano:** Paquete de software que presenta al usuario como un programa aparentemente legítimo e inofensivo, pero al ejecutarlo ocasiona daños a los sistemas de información.

- **Virus informático:** Es un malware que tiene por objeto alterar el normal funcionamiento de una computadora, sin el permiso o el conocimiento del usuario.

- **Vulnerabilidad:** Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. Las debilidades de seguridad pueden ser aprovechadas por atacantes mediante exploits, para acceder a los sistemas con fines maliciosos.[22]

- **Vulnerabilidad Zero-day**: es aquella vulnerabilidad en sistemas o programas informáticos que es únicamente conocida por determinados atacantes y es desconocida por los fabricantes y usuarios. Al ser desconocida por los fabricantes, no existe un parche de seguridad para solucionarla. [23]

[22] Glosario de términos de ciberseguridad - Incibe
[23] Glosario de términos de ciberseguridad - Incibe

6 FASES DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La gestión de incidentes de seguridad de la información en RTVC involucra las siguientes etapas:

- ✓ Prevención
- ✓ Preparación
- ✓ Detección y análisis
- ✓ Respuesta, contención y erradicación
- ✓ Recuperación y aprendizaje

6.1 PREVENCIÓN

En esta etapa se encuentran todas las actividades que debe realizar la entidad para prevenir la ocurrencia de incidentes de seguridad de la información:

Control de acceso: el control de acceso a los sistemas de información, servidores y equipos de comunicaciones debe realizarse según establecido en la Política para la administración de la infraestructura de TI y la Política de Seguridad de la información formalizadas en el Sistema integrado de Gestión para el proceso Gestión de Tecnologías de la información.

Actualizaciones de seguridad: mediante la herramienta centralizada, se debe mantener actualizado el sistema operativo de todos los equipos de cómputo de usuarios de los servicios de RTVC. Así mismo, los encargados de administrar la infraestructura y las redes velarán por mantener los sistemas operativos y/o firmware de servidores y equipos de comunicaciones actualizados.

Prevención de código malicioso: todos los equipos de la infraestructura, tanto servidores como equipos de cómputo de usuarios, deben tener activo el software antivirus con las firmas de actualización al día.

Seguridad en redes: las políticas definidas en el firewall deben ser revisadas con frecuencia con el objetivo de ajustarlas si es necesario tomando en cuenta los cambios en el entorno, así mismo deben seguirse los lineamientos establecidos en la Política para la administración de la infraestructura de TI y la Política de Seguridad de la información formalizadas en el Sistema integrado de Gestión para el proceso Gestión de Tecnologías de la información.

Sensibilización y entrenamiento de usuarios: todos los usuarios de la entidad incluidos los administradores de tecnologías deben ser sensibilizados de acuerdo con

las tecnologías utilizadas, las políticas y los procedimientos existentes relacionados con el uso apropiado de redes, sistemas y aplicaciones en concordancia con los estándares de seguridad de la entidad.

Gestión de riesgos de seguridad de la información: se debe ejecutar análisis de riesgos de seguridad de la información y seguridad digital al menos una vez al año o cuando se presenten cambios en los activos de información con el fin de identificar los riesgos presentes y establecer los controles necesarios para su mitigación.

Escaneo de vulnerabilidades: se deben realizar de manera periódica escaneo para identificar y remediar vulnerabilidades en los distintos dispositivos sobre los cuales se soportan los servicios tecnológicos que ofrece.

Monitoreo: a través del centro de operaciones de red (NOC) y el centro de operaciones de seguridad (SOC), así como mediante la revisión de logs de servidores y equipos de comunicaciones, se debe efectuar monitoreo continuo para detectar, analizar e informar sobre eventos e incidentes de seguridad se debe identificar cualquier actividad inusual en los dispositivos y/o servicios, así como detectar tráfico malicioso que pudiera estar ingresando o intentando ingresar en la red.

6.2 PREPARACIÓN

Esta fase involucra contar con todo lo que se requiere para que la gestión de incidentes de seguridad de la información se lleve a cabo de manera exitosa:

Equipo de respuesta a incidentes de Seguridad de la información y seguridad digital (ERISID)

El equipo de respuesta a incidentes de Seguridad de la información y Seguridad digital de RTVC es un grupo creado para atender eventos e incidentes de seguridad de la información con el fin de proteger la infraestructura tecnológica y los activos de información y mitigar el impacto ocasionado por la materialización de un incidente. Este equipo, con el apoyo de la Coordinación de Tecnologías de la información, generará planes de contención y recuperación de los servicios y sistemas afectados para garantizar la continuidad de las operaciones, está conformado por los siguientes actores:

- ✓ Apoyo al Monitoreo y control de la infraestructura
- ✓ Administradores del Firewall
- ✓ Administradores de infraestructura y redes
- ✓ Apoyo al aseguramiento de la infraestructura tecnológica

- ✓ Oficial de Seguridad de la información
- ✓ Apoyo a Seguridad de la información

6.2.1 CONTACTOS

Se debe contar con una lista de contactos de cada una de las personas que conforman el equipo de respuesta a incidentes de Seguridad de la información y Seguridad digital y del equipo de soporte de T.I.

Así mismo, se debe contar con información de contacto para el escalamiento de incidentes según la estructura de la entidad:

- Información de contacto de los administradores de la plataforma tecnológica (Servicios, Servidores) y del soporte externo de esta, en caso de que aplique.
- Contacto con áreas interesadas o grupos de interés:

Entidad	Contacto
ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia	contacto@colcert.gov.co Teléfono: (+571) 2959897
CSIRT Gobierno (Equipo de Respuesta a Incidentes de Seguridad Digital)	csirtgob@mintic.gov.co
Centro cibernético Policial	https://caivirtual.policia.gov.co/
CSIRT Ponal	https://cc-csirt.policia.gov.co/

Tabla 01: Contacto entidades externas
Fuente: Coordinación de T.I.

6.2.2 RECURSOS

- Diagrama de red físico y lógico, actualizado, para tener la ubicación rápida de los recursos existentes.
- Listado detallado de servidores y servicios activos: Nombre, IP, Aplicaciones, Sistema operativo, Usuarios Configurados, administrador.
- Línea base sobre el comportamiento de la red en condiciones normales de operación, que permita identificar una conducta sospechosa en algún elemento de la plataforma, por ejemplo la presencia de un patrón de tráfico anormal que pueda ser indicativo de un problema de rendimiento de una aplicación o de una violación de seguridad, recomendable incluir, entre otras cosas, los puertos utilizados, horarios de utilización, direcciones IP con que generan mayor tráfico, direcciones IP que reciben mayor número de peticiones. Esta línea base debe revisarse y actualizarse de forma regular en el tiempo, toda vez que la red no es una entidad estática.

- Copias de respaldo de Información, configuraciones e imágenes de servidores, y cualquier información base que pueda recuperar el funcionamiento normal del sistema.
- Investigación constante para generar una base de conocimientos con información relacionada con nuevas vulnerabilidades y ataques.

6.3 DETECCIÓN Y ANÁLISIS

Esta etapa involucra la identificación de la ocurrencia de eventos de seguridad de la información y el análisis de la información asociada, por lo tanto, se deben tomar en cuenta las siguientes actividades:

6.3.1 DETECCIÓN

La detección de eventos o incidentes de seguridad puede realizarse a través de las siguientes fuentes:

a) **Reporte de usuarios**: una de las fuentes para la detección de eventos e incidentes son los funcionarios o colaboradores que hacen uso de los diferentes servicios de Tecnologías de Información para realizar sus labores de generación y actualización de información. Los servidores públicos, colaboradores o terceras partes deberán informar, tan pronto como sea posible, debilidades, eventos o incidentes que puedan tener un impacto en la seguridad de los activos de la organización.

b) M**onitoreo de infraestructura**: el monitoreo constante de la infraestructura es requerido para detectar:
   - Alertas del SOC
   - Salida de operación de servidores
   - Alertas e informes del software antivirus
   - Comportamientos fuera de la línea base de operación normal de la infraestructura y sistemas.
   - Análisis de auditorías de los sistemas y de las infraestructuras tecnológicas, basados en:
     - Logs de servidores
     - Logs de aplicaciones
     - Logs de herramientas de seguridad
     - Cualquier otra herramienta que permita la identificación de un incidente de seguridad.

6.3.2 ANÁLISIS

Para el análisis de los eventos o incidentes se pueden emplear diferentes fuentes de información:

- **A nivel de red:**

  - Notificaciones del SOC
  - Registros de conexiones realizadas.
  - Registros de conexiones autorizadas por el firewall
  - Registros de intentos de conexión que han sido bloqueadas en el firewall
  - Trazas de red que muestren conexiones a destinos, puertos o a través de protocolos no esperados, así como picos de tráfico anómalos o en horarios no habituales.
  - Conexiones que tengan como origen o destino IPs reportadas en listas de reputación como potencialmente maliciosas.

- **A nivel de equipos (servidores o estaciones de trabajo):**

  - Cuentas de usuario inusuales en el sistema, especialmente aquellas con privilegios de administrador.
  - Archivos ocultos o con tamaños, nombres o ubicaciones sospechosas
  - Entradas sospechosas en el registro, principalmente en el caso de infecciones por malware en sistemas Windows, ésta es una de las técnicas habituales utilizadas para asegurar la persistencia en el sistema comprometido.
  - Registros de auditoría y accesos no autorizados.
  - Procesos y servicios inusuales activos y/o ejecutándose
  - Una carga excesiva de disco o memoria puede estar producida por un incidente de seguridad como malware, denegaciones de servicio o intrusiones.
  - Sesiones abiertas en la máquina desde otros equipos, anomalías en las tablas ARP, carpetas compartidas inusuales o con permisos excesivos, o un elevado número de conexiones.
  - Comportamiento anómalo de alguna aplicación, ventanas emergentes del navegador, conexiones muy lentas, reinicios o aplicaciones que se cierran sin motivo.
  - Registros de la consola del software antivirus

- Otros comportamientos sospechosos reportados por otros usuarios

- **A nivel de aplicación:**

  - Registros de auditoría y accesos no autorizados
  - Registros o *logs* de aplicaciones que puedan recoger información de interés, como fechas, transacciones o actividad de los usuarios.

6.3.3 EVALUACIÓN

Según lo expresado por el CSIRT Gobierno, los incidentes de seguridad pueden clasificarse de la siguiente manera:

Clasificación	Evento o incidente
Muy grave	Denegación de servicios - DoS, Denegación distribuida de servicios – DDoS, ataques de diccionario y fuerza bruta, acceso, modificación/borrado de información
Grave	Ataques a aplicaciones Web, evidencia de Malware y APT, Ataques de Red (Hombre en el medio - MITM, Sesión Hijacking, Poisoning, manipulación de red), ataques de inyección SQL, Cross-site scripting – XSS, compromisos de cuentas, fuga de información, defacement.
Menos grave	Sabotaje, Spam, contenido no autorizado, ingeniería social, técnicas OSINT, error en seguridad perimetral, seguridad Endpoint, seguridad de red, segmentación.
Menor	Uso fraudulento de recursos, suplantación de entidades o de algún funcionario, phishing, fallo de red cableada o inalámbrica, fallo de energía, fallo de dispositivos o sistemas

Tabla 02: Valoración de los incidentes
Fuente: CSIRT Gobierno

6.3.4 TIEMPOS DE ATENCIÓN

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.

Clasificación	Tiempo de atención
Muy grave	Menor o igual a 12 horas
Grave	12 a 24 horas
Menos grave	2 a 4 días
Menor	5 a 8 días

Tabla 03: Tiempos de atención
Fuente: Coordinación de T.I.

Los incidentes clasificados como Muy grave y Grave deben reportarse al CSIRT Gobierno, a través Formato Reporte de Incidentes, para el respectivo apoyo y coordinación en la gestión de estos.

Los incidentes catalogados como Menos Grave y Menor deben ser comunicados al CSIRT Gobierno a través del Formato Reporte de eventos, una vez sean gestionados, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos.

6.4 RESPUESTA, CONTENCIÓN Y ERRADICACIÓN

El objetivo de esta fase es evitar más daños y reducir el impacto inmediato del incidente eliminando el acceso del atacante. El escenario particular determinará el tipo de estrategia de contención que se utilice, sin embargo, algunas de las acciones que se pueden tomar en primer lugar consisten en:

- Desconectar el equipo o segmento de red del resto de la red de la organización.
- Reubicación del recurso comprometido en una VLAN aislada.
- Si se conocen los detalles técnicos del tipo de incidente se pueden aplicar medidas de contención más ajustadas a cada situación (bloqueo de determinados correos electrónicos, aplicación o ajuste de las reglas en el firewall, bloqueo de acceso a unidades compartidas, etc.).
- Bloquear remitentes de correo o cuentas de usuario
- Restablecimiento de contraseñas en cuentas comprometidas
- Aplicar actualizaciones de seguridad para remediar vulnerabilidades
- Reemplazo de archivos comprometidos con versiones limpias
- Monitoreo de cualquier signo de respuesta del atacante a las actividades de contención
- Escalar el incidente a las entidades del estado correspondientes las cuales pueden ofrecer ayuda en la contención.

Algunos ejemplos de estrategias de contención a incidentes se presentan en la siguiente tabla (Guía 21 del MinTIC – Gestión de incidentes):

Incidente	Ejemplo	Estrategia de contención
Acceso no autorizado	Sucesivos intentos fallidos de login	Bloqueo de cuenta
Código Malicioso	Infección con virus	Desconexión de la red del equipo afectado
Acceso no autorizado	Compromiso del Root	Desconexión de la red del equipo afectado
Reconocimiento	Scanning de puertos	Incorporación o ajuste de reglas de filtrado en el firewall

Tabla 04: Ejemplo de estrategias de contención
Fuente: Guía 21 del MinTIC – Gestión de incidentes

Las actividades de contención deben realizarse cuidando de no destruir información valiosa. La documentación de cada paso que se tome o cada actividad que se observe durante esta fase resulta de gran importancia para incluir en el informe post-incidente.

Luego de una contención exitosa (es decir, sin nuevos signos de compromiso), se debe conservar la evidencia para referencia o investigación policial en caso de ser necesario, ajustar las herramientas de detección y avanzar hacia la siguiente fase de recuperación y aprendizaje.

6.5 RECUPERACIÓN Y APRENDIZAJE

6.5.1 RECUPERACIÓN

La finalidad de la fase de recuperación consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante que antes de la puesta en producción de los sistemas o tecnologías afectadas por el incidente, se realice una auditoría de seguridad de estos para garantizar que el nivel de protección es aceptable y su puesta en producción se puede realizar de forma segura.

Las estrategias de recuperación dependen del incidente y de las estrategias de contención y erradicación tomadas, no obstante, se mencionan a continuación algunas actividades que se pueden ejecutar:

- Reinstalación de servidores
- Restauración de información a partir de copias de respaldo
- Reconexión de sistemas reconstruidos/nuevos a la red.
- Fortalecimiento de la seguridad del perímetro (por ejemplo, conjuntos de reglas de firewall, listas de control de acceso en switches core).
- Fortalecimiento del control de acceso a los servidores y servicios
- Monitorear las operaciones para detectar comportamientos anormales

Algunos ejemplos para la recuperación se mencionan en la siguiente tabla:

Incidente	Ejemplo	Estrategia de Recuperación
DoS (denegación de servicio)	SYN Flood	Restitución del servicio caído
Virus	Gusano en la red	Corrección de efectos producidos. Restauración desde copias de respaldo
Vandalismo	Defacement a un sitio web	Reparar el sitio web
Intrusión	Instalación de un rootkit	Reinstalación del equipo y recuperación de datos

Tabla 05: Ejemplo de estrategias de recuperación
Fuente: Guía 21 del MinTIC – Gestión de incidentes

Un aspecto clave de la recuperación es tener una mayor vigilancia y controles para validar que el plan de recuperación se ha ejecutado con éxito y que no existen signos de actividad adversa en el entorno.

La documentación de cada paso que se tome o cada actividad que se observe durante esta fase resulta de gran importancia para incluir en el informe post-incidente.

6.5.2 APRENDIZAJE

Una vez el incidente se ha tratado exitosamente se debe generar un informe post-incidente, a partir del cual se puedan analizar las lecciones aprendidas. Cada miembro del equipo implicado en la gestión del incidente debe realizar sus aportes y estos deben ser compilados en un informe general que puede incluir un breve resumen ejecutivo y anexos técnicos.

Los principales objetivos del análisis incluyen:

- Asegurarse de que se haya eliminado la causa raíz.
- Identificar problemas de infraestructura a resolver.
- Identificar los problemas u obstáculos al ejecutar el procedimiento de gestión de incidentes.
- Revisar y actualizar roles y responsabilidades.
- Identificar las necesidades de formación técnica u operativa.
- Revisar, identificar y hacer mejoras a la implementación de controles de seguridad de la información.
- Mejorar las herramientas necesarias para realizar acciones de protección, detección, análisis o respuesta.