INSTRUCTIVO: Gestión de Incidentes de Seguridad de la Información			
FECHA DE APLICACIÓN: 2023-12-05	**CÓDIGO:** IN.0720.06	**VERSIÓN:** 001	
ELABORADO POR: FABIAN EDUARDO ROJAS GALLEGO PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION CAROLA DUQUE JIMENEZ TECNICO ADMINISTRATIVO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION JUAN CARLOS CAMACHO CASTILLO PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	**REVISADO POR:** PAMELA KATHERINE ENRIQUEZ PAZ PROFESIONAL DE APOYO GRUPO GESTIÓN AMBIENTAL Y DE CALIDAD EDWIN RUANO GAMBOA PROFESIONAL ESPECIALIZADO DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	**APROBADO POR:** DIEGO ALEXANDER MILLAN LONDOÑO JEFE DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACION	

1. OBJETIVO

Describir en detalle las actividades que se deben realizar para gestionar los incidentes de seguridad de la información, conforme al procedimiento Gestión de Incidentes de Seguridad de la Información PT.0720.29.

2. DEFINICIONES

Las definiciones que aplican a este instructivo pueden ser consultadas en el siguiente enlace **GLOSARIO DE TERMINOS Y DEFINICIONES OTI.**

3. DESARROLLO

3.1 POLÍTICAS Y CONDICIONES GENERALES

1. Todos los incidentes de seguridad de la información deben ser reportados en el menor tiempo posible con el fin de acelerar la detección, restauración y reparación de cualquier daño causado y facilitar la obtención de cualquier evidencia asociada.
2. La información suministrada debe indicar fecha y hora del evento/incidente, breve descripción del hecho (alcance, qué ocurrió, efectos producidos como impacto o daño en un recurso o servicio).
3. Todas las partes interesadas deben reportar los incidentes de seguridad de la información a través de los funcionarios y medios definidos por la Corporación Autónoma Regional del Valle del Cauca – CVC.
4. Si se determina que el evento es un incidente de seguridad de la información, se debe identificar y aplicar de forma inmediata una solución temporal que garantice la integridad, confidencialidad y disponibilidad de la información.
5. Se deben reportar los incidentes de seguridad que afecten a los activos de información de la CVC con las entidades correspondientes cuando sea necesario.
6. Los delitos Informáticos deben ser denunciados a la Policía Nacional, Unidad de Delitos Informáticos o a la entidad que corresponda.
7. Cuando una acción de seguimiento contra una persona u organización, después de un incidente de seguridad de la Información implique acciones legales, la evidencia se debe recolectar, retener y presentar ante las autoridades competentes, dando cumplimiento a las normas de custodia de evidencia en la jurisdicción pertinente.
8. La CVC para prevenir incidentes de seguridad, debe aplicar buenas prácticas para el aseguramiento de redes, sistemas y aplicaciones, tales como:
    a. **Gestión de parches de seguridad:** La CVC debe contar con herramientas de gestión de vulnerabilidades en Sistemas Operativos, Bases de Datos y Aplicaciones, para ayudar a los administradores en la identificación, adquisición, prueba e instalación de los parches.
    b. **Aseguramiento de plataforma:** la CVC debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos. Se deben revisar configuraciones por defecto (usuarios, contraseñas y archivos compartidos). Cada recurso que pueda ser accedido por externos e incluso por usuarios internos debe desplegar alguna advertencia. Los servidores deben tener habilitados sus sistemas de auditoría para permitir el registro de eventos.
    c. **Seguridad en redes:** Se deben gestionar constantemente los elementos de seguridad. Las reglas configuradas en equipos de seguridad deben ser revisadas continuamente. Las firmas y actualizaciones de dispositivos como IDS (Sistema de Detección de Intrusos) o IPS (Sistema de Prevención de Intrusos) deben

encontrarse a la última versión estable. Todos los elementos de seguridad y de red deben encontrarse sincronizados y sus registros de actividades deben ser consolidados y analizados constantemente.

d. **Prevención de código malicioso:** Todos los equipos de cómputo que hacen parte de la red corporativa de la CVC deben tener activo y actualizado su antivirus y antimalware.
e. **Sensibilización y entrenamiento de usuarios:** Todos los funcionarios y contratistas de la CVC, deben ser sensibilizados y capacitados en las políticas y procedimientos existentes relacionados con el uso adecuado de la infraestructura tecnológica y la protección y seguridad de la información.

9. La CVC debe identificar y proporcionar la información y los recursos necesarios para la gestión de incidentes como:
   a. **Políticas y procedimientos:** Para la correcta ejecución del proceso, incluyendo roles, responsabilidades y formatos requeridos.
   b. **Información de contacto:** Lista de información de contacto de cada una de las personas que conforman el equipo de gestión de incidentes.
   c. **Información de escalamiento:** Información de contacto para el escalamiento de incidentes según la estructura de la CVC.
   d. Información de los administradores de la plataforma tecnológica (Sistemas de Información, Infraestructura y Servicios)
   e. Contacto con el área de talento humano o quien realice sus funciones (por si se realizan acciones disciplinarias).
   f. Contacto con áreas interesadas o grupos de interés (Centro Cibernetico Policial, ColCert, Policía Nacional, Fiscalía, entre otras)
   g. **Política de comunicación:** Política de comunicación de los incidentes de seguridad para definir qué incidente puede ser comunicado a los medios y cuál no.
   h. **Recursos hardware y software.** En caso de ser necesario y para una correcta y eficiente gestión de incidentes, la CVC se deberá soportar en herramientas como:
      - Equipos Forenses
      - Analizadores de protocolos.
      - Software de adquisición.
      - Software para recolección de evidencia.
      - Kit de respuesta a incidentes.
      - Software de análisis forense.
      - Medios de almacenamiento
   i. **Recursos para el análisis de incidentes:**
      - Listado de los puertos conocidos y de los puertos vulnerables a un ataque informático.
      - Diagrama de red para tener la ubicación rápida de los recursos existentes
      - Una línea base de Información de servidores (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios). Esta información siempre debe estar actualizada para poder conocer el funcionamiento normal del mismo y realizar una identificación más acertada de un incidente.
      - Análisis del comportamiento de red que incluya puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones, entre otras.
   j. **Recursos para la mitigación y remediación.**Para la contención de un posible incidente se deben contar con elementos basicos como copias de seguridad de la Información, imágenes de servidores y cualquier información base que pueda recuperar el funcionamiento normal del sistema.
   k. **Detección de incidentes**. Para la detección de incidentes de seguridad de la información se deben tener en cuenta las siguientes fuentes:
      - Alertas en sistemas de seguridad.
      - Caídas de servidores.
      - Reportes de usuarios.
      - Alerta de antivirus.
      - Comportamiento anormal de la infraestructura.
      - Registros de actividades de servidores.
      - Registros de actividades de aplicaciones.
      - Registros de actividades de herramientas de seguridad.
      - Cualquier otra herramienta que permita la identificación de un incidente de seguridad.
   l. **Funcionarios que sospechen sobre posibles incidentes de seguridad.** Al detectarse la posible materialización de un incidente de seguridad, el funcionario deberá notificarlo al primer punto de contacto definido por la CVC a través de los siguientes canales de comunicación:
      - Telefónico.
      - Correo.
      - Verbalmente.
   m. **Evaluación de incidentes de seguridad.** Para realizar la evaluación de un incidente de seguridad se debe tener en cuenta los niveles de impacto con base en los insumos entregados por el análisis de riesgos y la clasificación de activos de información de la CVC.
   n. **Estrategias para la toma de decisiones.** La CVC implementará estrategias que permitan tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.
   o. **Registro de lecciones aprendidas.** La CVC debe mantener registro de las lecciones aprendidas donde se evidencie:
      - Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
      - Si se tomaron las medidas o acciones necesarias para la recuperación.

- Cuál sería la gestión del personal y que debería hacerse la próxima vez que ocurra un incidente similar.
- Que acciones correctivas pueden prevenir incidentes similares en el futuro.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

10. **Prevención de incidentes de seguridad de la información:** Establecer acciones para prevenir los incidentes de seguridad de la información, a través de las siguientes actividades:
    a. Establecer contacto con grupos de interés especial para compartir y actualizar conocimientos.
    b. Analizar los comunicados y boletines emitidos por los grupos de interés especial.
    c. Implementar las medidas preventivas necesarias en seguridad.
    d. Realizar periodicamente análisis de seguridad para identificar fuentes de riesgo y diseñar controles que reduzcan la posibilidad de ocurrencia de incidentes.
    e. Las actividades de gestión de riesgos se deben realizar empleando la metodología de gestión de riesgos de seguridad adoptada por la CVC.
    f. El Profesional Especializado con funciones de seguridad de la información, mantendrá contacto con grupos de interés especial, foros y asociaciones profesionales especializadas en seguridad, con el fin de prevenir incidentes de seguridad de la información y también:
        - Ampliar y actualizar el conocimiento en mejores prácticas en seguridad de la información.
        - Recibir advertencias tempranas de las alertas, avisos y parches de seguridad frente a ataques y vulnerabilidades.
        - Obtener acceso a asesoría especializada en seguridad de la información.
        - Compartir e intercambiar información de nuevas tecnologías, productos, amenazas o vulnerabilidades.
    g. Analizar los comunicados emitidos por los grupos de interés especial. Cuando los grupos de interés especial emitan comunicados y alertas, es deber del Profesional Especializado responsable del sistema de gestión de seguridad de la información o a quien haga sus veces, analizar su aplicabilidad en la CVC y en caso de ser necesario tomar las acciones pertinentes.
    h. Tomar las medidas preventivas necesarias para que no se vea afectada la plataforma tecnológica de la CVC y sus usuarios. El resultado de la implementación de las medidas preventivas debe ser notificado a los interesados.
11. **Roles y perfiles necesarios para la gestión de incidentes de seguridad**
    - A continuación, se presenta una descripción de los actores que intervienen y conforman el proceso de atención de Incidentes, para cada actor se presenta una breve descripción sobre su perfil y la función dentro del proceso de respuesta a Incidentes de Seguridad de la información.
        - **Equipo de respuesta a incidentes de seguridad de la información:** Provee a la CVC la capacidad adecuada para evaluar, aprender y respondera un incidente de seguridad de forma coordinada, gestionando y comunicando las acciones necesarias de respuesta a un incidente de seguridad.
        - **Detección de Incidentes de Seguridad:** Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
        - **Atención de Incidentes de Seguridad:** Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
        - **Recolección y Análisis de Evidencia Digital:** Toma, preserva, documenta y analiza la evidencia cuando sea requerida.
        - **Anuncios de Seguridad:** Deben mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación (Web, Intranet, Correo).
        - **Auditoria y trazabilidad de Seguridad Informática:** El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.
        - **Certificación de productos:** El equipo verifica la implementación de las nuevas aplicaciones en producción para que se ajusten a los requerimientos de seguridad informática definidos por el equipo.
        - **Configuración y Administración de Dispositivos de Seguridad Informática:** Se encargarán de la administración adecuada de los elementos de seguridad informática.
        - **Clasificación y priorización de servicios expuestos:** Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
        - **Investigación y Desarrollo:** Deben realizar la búsqueda constante de nuevos productos en el mercado o desarrollo de nuevas herramientas de protección para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad de la información.

    El equipo de respuesta a incidentes de seguridad de la información se recomienta que esté integrado por:

    1. **Jefe de Oficina de Tecnologías de la Información:** Líder del Equipo, responsable de velar por el cumplimiento de las políticas y objetivos de la gestión de incidentes de forma que se encuentren alineados con los requerimientos de normas y leyes vigentes. Lidera y convoca las reuniones del equipo y reporta a la dirección sobre la gestión de incidentes de seguridad de la información y su impacto.
    2. **Líder de Seguridad de la Información:** Responsable por gestionar las respuestas a los eventos/incidentes dentro de los parámetros de tiempo, cubrimiento y precisión esperados. Periódicamente según se defina, presenta informes sobre los eventos e incidentes de seguridad de la información, así como contramedidas a adoptar en razón a las lecciones aprendidas que se obtuvieron en el periodo. Responsable por buscar el mejoramiento continuo del proceso de gestión de incidentes de seguridad de la información. Responde a las consultas sobre los incidentes de seguridad que impacten de forma inmediata y es el encargado de revisar y evaluar los indicadores de gestión

correspondientes a la atención de incidentes de seguridad para poder ser presentados a los directivos. Estará en la capacidad de convocar la participación de otros funcionarios de la institución cuando el incidente lo amerite. También debe estar al tanto del cumplimiento de los perfiles mencionados y de revisar el cumplimiento de los procedimientos y mejores prácticas, así como también de los indicadores de gestión, y en capacidad de disparar planes de contingencia y/o continuidad. Finalmente será el responsable del modelo de Gestión de incidentes y debe estar en la capacidad de revisar todos los incidentes de seguridad y los aspectos contractuales que se manejen en la institución.

3. **Oficial de seguridad informática:** Es el apoyo para la definición de estrategias o medidas de respuesta que se decidan. Realiza seguimiento al correcto manejo de los incidentes de seguridad informática y generación de lecciones aprendidas. Lidera la infraestructura tecnológica y coordina para que se mantenga actualizada toda la información de contacto de los principales proveedores de tecnología, bien sea que tengan contrato vigente con la entidad o aquellos que pueden ser llamados para detener los ataques o recuperarse de los mismos.
4. **Administradores de plataforma tecnológica:** Responsable por desarrollar las principales actividades encaminadas a detectar, informar, evaluar, decidir y responder en relación con un evento/incidente.
5. **Otros procesos de la Institución:** se debe contar con varias personas que traten y respondan a incidentes concretos. Los miembros asociados provienen de varios procesos de la institución y pueden implicarse directamente en un incidente o servir de punto de entrada para delegar o escalar la responsabilidad a alguien más apropiado. Según se requiera se podría invitar entre otras a las siguientes áreas o procesos: a. Planeación y desarrollo institucional, b. Bienes y servicios, c. Oficina Jurídica, d. Control interno.

6. **Usuario sensibilizado:** Es un funcionario, con acceso a la infraestructura de la CVC, quien debe estar educado y concientizado sobre las instructivos implementados sobre la seguridad de la información y en particular el instructivo de atención de incidentes. Estos usuarios serán muchas veces quienes reporten los problemas siguiendo los lineamientos establecidos.

7. **Agente Primer Punto de Contacto:** Es el encargado de recibir las solicitudes por parte de los usuarios sobre posibles incidentes, también debe registrarlos en la base de conocimiento y debe ser el encargado de escalarlos a la persona encargada de la atención de incidentes. Este Agente debe contar adicionalmente con capacitación en Seguridad de la Información (con un componente tecnológico fuerte) y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes. Adicionalmente debe contar con una capacitación básica en técnicas forenses, específicamente en recolección y manejo de evidencia.

8. **Administrador del Sistema:** Se define como la persona encargada para configurar y mantener un activo informático. También debe ser notificado por el agente de primer punto de contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al agente de primer punto de contacto sobre el incidente la solución del mismo. Se recomienda que los administradores cuenten con capacitación en Seguridad de la Información (con un componente tecnológico fuerte no solo en su plataforma si no en Redes y erradicación de vulnerabilidades) y debe conocer perfectamente la clasificación de Incidentes y los procesos de escalamiento de Incidentes. Adicionalmente debe contar con una capacitación en técnicas forenses, específicamente en recolección y manejo de evidencia.

9. **Administrador de los sistemas de Seguridad:** Personas encargadas de configurar y mantener un activo informático relacionado con la seguridad de la plataforma ej. Firewall, Sistemas de Prevención de Intrusos, Routers, Sistemas de Gestión y Monitoreo. También debe ser notificado por el agente de primero contacto sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar un incidente de seguridad. Este debe documentar y notificar al agente de primer contacto sobre el incidente y la solución del mismo. Se recomienda que los administradores de esta tecnología sean expertos en Seguridad de la Información (con un componente tecnológico fuerte en Redes y erradicación de vulnerabilidades, Ethical Hacking y técnicas forenses) y debe conocer perfectamente la clasificación de Incidentes de la CVC.

10. **Analista Forense:** Es un experto en el tema forense, quien debe estar disponible en caso de que un incidente de impacto alto (o uno que amerite acciones disciplinarias o legales o investigación profunda) requiera una investigación completa para solucionarlo y determinar los siguientes Ítems:

    - Que Sucedio
    - Donde sucedió.
    - Cuando Sucedió.
    - Quien fue el responsable.
    - Como sucedió.

3.2 REPORTAR EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

1. Todos los servidores públicos de la CVC deben reportar presuntos incidentes de seguridad de la información cuando puedan afectar la confidencialidad, integridad y/o disponibilidad de la información.
2. Los canales de comunicación definidos para el reporte de eventos de seguridad son:
    a. Correo electrónico: itmesaintegral.principal@cvc.gov.co
    b. Línea telefónica PBX: 602 620 66 00 - 602 318 17 00 extensión 5555 - 1286
3. Los eventos y/o debilidades que se pueden reportar para su respectiva investigación, análisis y gestión, deben ser los que atenten contra la confidencialidad, disponibilidad e integridad de la información. Algunos de ellos son:
    a. Accesos no autorizados a los sistemas de información.

b. Uso indebido de los recursos informáticos de la CVC.
c. Divulgación de información a quien no tiene derecho a conocerla.
d. Uso de la información con el fin de obtener beneficio propio o de terceros.
e. Hacer pública la información sin la debida autorización.
f. Realización de copias no autorizadas de software.
g. Descargar software a través de Internet sin la debida autorización.
h. Intentar modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización.
i. Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad.
j. Enviar cualquier comunicación electrónica fraudulenta.
k. Violación de cualquier ley o regulación nacional respecto al uso de sistemas de información.
l. Robo de información sensible.
m. Robo y pérdida de equipos de cómputo con información sensible.
n. Denegación de servicio sobre equipos de la red, afectando la operación diaria de la CVC.
o. Denegación de servicio por el ingreso y propagación de virus que explotan vulnerabilidades.
p. Amenazas a través de diferentes medios de comunicación, que generen un impacto directo sobre la seguridad de la información.
q. Cambios o modificaciones en registros de bases de datos sin previa autorización.
r. Generación o distribución de código malicioso.
s. Fallas en los sistemas de información y pérdidas de servicio.
t. Reinicio inesperado de los equipos de cómputo.

3.3 ANALIZAR EL EVENTO REPORTADO

Cuando se presente un evento de seguridad se debe recolectar la mayor cantidad de evidencia posible para determinar las causas del mismo y buscar alternativas de solución. Se pueden seguir las etapas:

1. Analizar si el evento es un posible incidente de seguridad, para proceder a registrarlo en el Reporte y Gestión de Incidentes de Seguridad de la Información FT.0720.05 formato de reporte y gestión de incidentes. Si no es un incidente se debe hacer el cierre del evento como se indica en este instructivo.
2. Se debe conformar un equipo de personas para investigar y documentar las causas del incidente de seguridad.
3. Se debe realizar un análisis rápido para determinar el alcance del incidente en la infraestructura o servicios afectados.
4. Clasificar el incidente de seguridad para desarrollar las actividades de gestión de incidentes y la generación de estadísticas de acuerdo a:
    a. **Acceso no autorizado:** Cuando un agente interno o externo, persona o sistema, gana acceso lógico o físico a un recurso de información y tecnología (equipo, dato, software, red , etc) sobre el cual no tiene derechos.
    b. **Denegación de servicio:** Cuando un atacante interno o externo a la entidad impide el uso autorizado de servicios informáticos, redes o sistemas de información mediante el consumo excesivo de recursos de la plataforma o sistema bajo ataque.
    c. **Código malicioso:** Software como virus troyanos, RAT, Rootkit, Ransomware, gusanos y demás formas de código malicioso donde infectan exitosamente un recurso de información y tecnología.
    d. **Uso inapropiado:** Cuando las partes interesadas (interno o externo, persona o sistema) incumplen la política de seguridad de la información.
    e. **Multicomponente:** Son incidentes en los cuales se presentan más de una de las formas de incidentes antes descritos.
5. Detectar cual fue la fuente del incidente de seguridad.
6. Detectar que herramientas se están utilizando para realizar el ataque y las vulnerabilidades que se está explotando.
7. Verificar los perfiles o registros del comportamiento de los diferentes dispositivos y sistemas, para identificar comportamientos no esperados o irregulares.
8. Estudiar las redes, sistemas y aplicaciones para obtener un conocimiento detallado de lo que se considera un comportamiento normal y así identificar comportamientos anormales y reconocer fácilmente la ocurrencia de incidentes.
9. Verificar los registros de eventos de los diferentes dispositivos de red, sistemas de información, servidores y servicios.
10. Consultar en información adicional relacionada para apoyar el análisis del incidente de seguridad.
11. Utilizar rastreadores de red para recolectar información complementaria.
12. Utilizar diferentes criterios de filtrado de datos de acuerdo con la naturaleza del incidente para facilitar su análisis.
13. Utilizar herramientas de diagnóstico de incidentes en formatos comprensibles para los grupos de mesa de ayuda, administradores y otras personas que participen en las actividades de respuesta a riesgos.
14. En las actividades de análisis de incidentes, es recomendable tener en cuenta los siguientes recomendaciones:
    a. Tener conocimientos de las características normales a nivel de red y de los sistemas.
    b. El personal debe tener conocimientos sobre los comportamientos de la Infraestructura que están administrando.
    c. Toda información que permita realizar análisis al incidente debe estar centralizada en un solo punto de acopio (Registros de actividades de servidores, redes, aplicaciones).
    d. Es importante efectuar correlación de eventos, ya que por medio de este proceso se pueden descubrir patrones de comportamiento anormal y poder identificar de manera más fácil la causa del incidente.
    e. Para un correcto análisis de un incidente debe existir una única fuente de tiempo (Sincronización de Relojes)

ya que esto facilita la correlación de eventos y el análisis de información.
   f. Se debe mantener y usar una base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados y experiencias con incidentes anteriores.
15. Registrar en el formato de reporte y gestión de Incidentes, la información obtenida en el análisis

3.4 EVALUAR Y CLASIFICAR EL INCIDENTE DE SEGURIDAD

Se debe evaluar y clasificar el incidente de seguridad, teniendo en cuenta los niveles de impacto y priorización del mismo.

3.4.1 Clasificación de incidentes de seguridad de la información

Los incidentes de seguridad de la información se clasifican de acuerdo a las siguientes categorías y subcategorías:

1. **Acceso no autorizado:** El acceso no autorizado va desde el uso no autorizado de credenciales hasta la modificación o cambio de archivos y directorios almacenados en un sistema o medio de almacenamiento. Adicionalmente se puede lograr acceso a otros sistemas a través de programas o herramientas de "Captura de tráfico de red" que pueden ser instalados para capturar información confidencial que este moviéndose por la red. Con un acceso no autorizado se pone en riesgo:
   a. Robo de información.
   b. Alteración de la información.
   c. Robo de contraseñas.
   d. Robo de información web mediante Cross-Site-Scripting o SQL Injection.
   e. Divulgación no autorizada de información.
   f. Intrusión física a las instalaciones
   g. Modificación, instalación o eliminación no autorizada de software.
   h. Intento fallido de conexión VPN de clientes.
   i. Robo o pérdida de un recurso informático.
   j. Pérdida o eliminación no autorizada de backups de la información.
   k. Robo de backups de la información.
   l. Consultas no autorizadas mediante Telnet.
   m. Intento de acceso no autorizado en Base de Datos.
   n. Acceso no autorizado a carpetas privadas en el servidor compartido.
   o. Creación de usuarios administrativos sin autorización.
   p. Robo, pérdida o destrucción no autorizada de manuales de funcionamiento de servidores internos.
   q. Robo de cookies.
   r. Deficiencias en la protección de la confidencialidad de la información.
   s. Modificación o eliminación no autorizada de datos.
   t. Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales.
2. **Denegación de servicio:** Los ataques de denegación de servicio se refieren al uso específico de ciertas herramientas por parte de intrusos con el fin de causar que las redes y/o sistemas dejen de operar apropiadamente. Esto incluye:
   a. Tiempos de respuesta muy bajos sin razones aparentes.
   b. Servicio(s) interno(s) inaccesibles sin razones aparentes.
   c. Servicio(s) Externo(s) inaccesibles sin razones aparentes.
   d. Interrupción prolongada en un sistema o servicio de red.
   e. Caída de Base de Datos.
   f. Caída del servicio de internet.
3. **Código malicioso:** Pueden ser programas como virus, gusanos, troyanos, spyware o scripts utilizados por intrusos para lograr acceso privilegiado, capturar contraseñas o información confidencial.
4. **Mal uso de recursos tecnológicos:** Ocurren cuando un usuario lleva a cabo acciones que violan las políticas de uso aceptable de los recursos computacionales. Esto incluye:
   a. Violación de las normas de acceso a Internet.
   b. Mal uso y/o Abuso del correo electrónico.
   c. Violación de las políticas, normas y procedimientos de seguridad de la información.
   d. Destrucción o alteración de la información de configuración.
   e. Destrucción o alteración física de los componentes de la red.
   f. Uso prohibido de un recurso informático o de red.
   g. Uso indebido de información crítica.
   h. Modificación no autorizada de un sitio o página web.
   i. Afectación en la disponibilidad de dispositivos como Switches/Router/Core-Router/AP
5. Escaneos, pruebas o intentos de obtención de la información. Esto incluye:
   a. Rastreadores de red.

b. Detección de Vulnerabilidades.
c. Ataques Hombre en el Medio.
d. Cracking de passwords.
e. Email bombing.
f. Email Spamming.
g. Intento de conexiones arbitrarias a través del mismo puerto.
h. Intento de escalar privilegios de usuarios.
i. Instalación de Keyloggers/capturadores de caracteres introducidos por teclado.
j. Intento de seguimiento de conexiones mediante consultas “ping”.

6. **Ingeniería Social:** Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Describe un método de ataque, donde alguien hace uso de la persuasión, muchas veces abusando de la ingenuidad o confianza de un usuario, para obtener información que pueda ser utilizada para tener acceso autorizado a la información de los computadores. Esta actividad puede ser realizada a través de mensajes de correo, llamadas telefónicas o redes sociales.

3.4.2 Priorización de incidentes de seguridad de la información y tiempos de respuesta

Con el fin de permitir una atención adecuada a los incidentes (análisis, contención y erradicación) se debe determinar el nivel de prioridad del mismo y de esta manera atenderlos adecuadamente según la necesidad.

La severidad del incidente puede ser:

1. **Alto Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor, que influyen directamente a los objetivos misionales de la CVC. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.
2. **Medio Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.
3. **Bajo Impacto:** El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

Las variables a considerar para realzar la evaluación de los incidentes son:

1. Prioridad
2. Criticidad de impacto
3. Impacto Actual
4. Impacto Futuro

Nivel de Prioridad: Depende del valor o importancia dentro de la CVC y del proceso que soporta el o los sistemas afectados:

Nivel de criticidad	Valor	Definición
Inferior	0,10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	0,25	Sistemas que apoyan a una sola dependencia o proceso de la CVC.
Medio	0,50	Sistemas que apoyan más de una dependencias o proceso de la CVC.
Alto	0,75	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	1	Sistemas Críticos.

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

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

Nivel de	Valor	Definición

impacto		
Inferior	0,10	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo.
Bajo	0,25	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo.
Medio	0,50	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo.
Alto	0,75	Impacto moderado en uno o más componentes de más de un sistema de información.
Superior	1	Impacto alto en uno o más componentes de más de un sistema de información.

Luego de tener definidas las variables se obtiene la *prioridad* mediante la siguiente formula:

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

Y los resultados obtenidos se deben comparar con la siguiente tabla para determinar la prioridad de atención:

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

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

Nivel de prioridad	Valor
Inferior	3 horas
Bajo	1 hora
Medio	30 minutos
Alto	15 minutos

Superior	5 minutos

3.4.3 Registrar en el formato de reporte y gestión de incidentes la información generada en la evaluación y clasificación para complementar los datos requeridos en todo el proceso.

3.5 IMPLEMENTAR ESTRATEGIAS Y ACCIONES PARA CONTENER EL INCIDENTE DE LA SEGURIDAD DE LA INFORMACIÓN

Es importante para la CVC implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

Esta fase se descompone en tres componentes:

1. **Contención:** Una vez analizado el incidente, el Profesional Especializado asignado debe ejecutar acciones para evitar la propagación del inicidente que pueda afectar a otros sistemas. Las posibles acciones de contención deben ser analizadas por el equipo de atención de incidentes. Cada incidente tiene su forma particular de contención que debe ser estudiada, definida y adoptada por el equipo de respuesta a incidentes, algunas de las opciones de contención incluyen:

Incidente	Ejemplo	Estrategia de contención
Acceso no autorizado	Sucesivos intentos fallidos de login	Bloqueo de cuenta Desconectar el sistema de redes (cableada o inalámbrica)
Código Malicioso	Infección con virus	Desconexión de la red del equipo afectado Apagar el sistema afectado
Acceso no autorizado	Compromiso del Root	Apagado del sistema Deshabilitar funciones del sistema Apagar servicios
Reconocimiento	Scanning de puertos	Incorporación de reglas de filtrado en el firewall

La estrategia de contención varía según el tipo de incidente y los criterios deben estar bien documentados para facilitar la rápida y eficaz toma de decisiones. Algunos criterios que pueden ser tomados como base son:

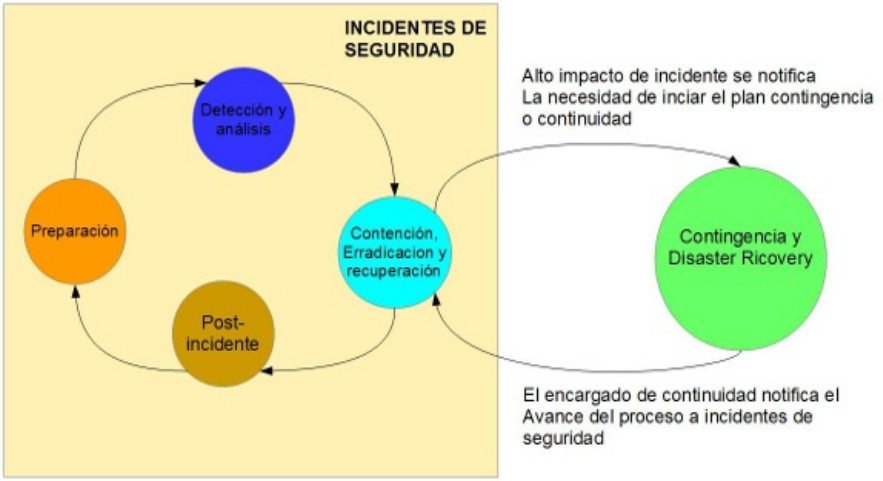
a. Daño potencial y pérdida de recursos.
b. Necesidad de preservación de evidencias.
c. Disponibilidad del servicio.
d. Tiempo y recursos necesarios para implementar la estrategia de manejo del incidente de seguridad.
e. Efectividad de la estrategia seleccionada.
f. Duración de la solución.

2. **Erradicación y Recuperación:** Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el administrador de TI o quien haga sus veces deben restablecer la funcionalidad de los sistemas afectados, y realizar un fortalecimiento del sistema que permita prevenir incidentes similares en el futuro.

Incidente	Ejemplo	Estrategia de erradicación
DoS (denegación de servicio)	SYN Flood	Restitución del servicio caído

Virus	Gusano en la red	Corrección de efectos producidos. Restauración
Vandalismo	Defacement a un sitio web	Reparar el sitio web
Intrusión	Instalación de un rootkit	Reinstalación del equipo y recuperación de datos

En algunas ocasiones durante el proceso de atención de incidentes de seguridad informática específicamente en la fase de “Contención, Erradicación y Recuperación” se puede hacer necesario activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres) en el caso que un incidente afecte gravemente a un determinado sistema.



3. Se debe generar las acciones para implementar las medidas preventivas o correctivas con el fin de contener el incidente de seguridad del activo de información de la CVC comprometido, a través de las siguientes actividades:

a. Definir la solución del incidente.
b. Implementar la solución al incidente.
c. Notificar la solución del incidente.
d. Establecer contacto con las autoridades cuando sea necesario.
e. Identificar y documentar las lecciones aprendidas. El Profesional Especializado designado para la solución del incidente, debe identificar las lecciones aprendidas después de presentarse un incidente, lo cual es sumamente útil en la mejora de las medidas de seguridad y el proceso de gestión de incidentes. Para mantener un adecuado registro de lecciones aprendidas la documentación de la lección aprendida debe permitir conocer:
   - Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
   - Si se tomaron las medidas o acciones que facilitaron la recuperación eficiente.
   - Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
   - Las acciones correctivas que pueden prevenir incidentes similares en el futuro.
   - Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

3.6 RECOLECTAR Y CONSERVAR LA EVIDENCIA DIGITAL DEL INCIDENTE DE SEGURIDAD

1. Se debe determinar si es necesario la recolección de evidencia digital, en cuyo caso, si se cuenta con personal especializado para la recolección de la evidencia forense en la CVC se realiza el proceso, de lo contrario se debe contratar el servicio si es necesario, con el propósito que éste realice la recolección de la evidencia. En general se tienen que considerar los lineamientos de las buenas prácticas de la cadena de custodia de evidencias digitales, tomando como marco general la legislación colombiana; en tal sentido, se deberán desarrollar las siguientes actividades como parte de la recolección y conservación de evidencias:
   a. El primer paso comprende la captura de la evidencia, que será realizada por el Profesional Especializado designado para el caso junto a las personas a cargo del proceso.
   b. Se debe garantizar integridad y veracidad de la evidencia. Se debe recoger la evidencia volátil antes de apagar o reiniciar el equipo, es decir información contenida en la memoria RAM, procesos activos, aplicaciones en ejecución, puertos abiertos o en escucha, usuarios conectados. El otro tipo de evidencia es la información contenida en el disco duro y se puede obtener incluso después de apagar el equipo con acceso físico al disco duro.
   c. Determinar de manera exacta el Incidente: Es necesario definir bien el problema, estudiar el caso, recopilar datos sobre el incidente, recuperar información borrada y/o oculta, analizar la evidencia, generar un informe, presentar las pruebas.
   d. Obtener información basada en el equipo como la fecha y hora del sistema, aplicaciones corriendo, puertos abiertos, conexiones de red, entre otras y realizar un backup de archivos copiados recientemente, información en portapapeles, etc. También es importante recolectar la información de red, registros de

actividades (de identificadores, monitoreo, routers, autenticación, firewalls, etc.), recolectar información mediante sniffers y obtener el testimonio de las personas que reportan el incidente o están vinculadas a los activos.

e. Se debe garantizar la autenticidad e integridad de la evidencia recolectada, llevar una cadena de custodia con el registro detallado del tratamiento de la evidencia asignando responsables y llevando un registro del proceso realizado.
f. Se debe proceder a realizar la captura de la evidencia con herramientas que no modifiquen ni el entorno ni la prueba en sí, salvaguardando su integridad.
g. Se debe actuar con precaución a la hora de recolectar la evidencia; dado que se debe garantizar la no alteración de la misma para soportar su validez en un proceso legal. Para ello se pueden utilizar los siguientes elementos:
    - Bolsas antiestáticas, que permitan la correcta manipulación de medios de almacenamiento.
    - Bolsas de seguridad, para almacenar los elementos físicos, que permitan garantizar que una vez depositados, se tenga la certeza que la bolsa no ha sido abierta.
    - Embalaje, para almacenar los discos duros y evitar que una eventual caída o maltrato al elemento ocasione una afectación a la integridad de la información, que en este caso sería perdida de la evidencia.
    - Etiquetas o rótulos, para marcar los elementos físicos, con el fin de identificarlos. Esta etiqueta debe tener la información necesaria que identifique al elemento. Por ejemplo, si se habla de un disco duro, se debería incluir por lo menos la siguiente información:
        - Un consecutivo
        - Número del incidente.
        - Descripción del elemento (marca, modelo, serial, capacidad, tipo de conector (IDE, SCSI, SATA o SSD), configuración física, particiones, sistema operativo).
        - Fecha y hora.
        - Lugar.
        - Nombre y firma de quién recolecta el elemento. Si es posible nombre y firma de un testigo.
h. Las tareas de recolección, así como las de análisis posteriores se realizan en conjunto entre la OTI y el tercero contratado si es el caso. Si se encuentra un servidor público involucrado como sospechoso de la causa del incidente, el Grupo de trabajo de Control Disciplinario Interno también podrá participar en las actividades de análisis de la evidencia. Para la recolección y retención de las evidencias que puedan ser presentadas ante las autoridades competentes, se deberán seguir los procedimientos e instructivos indicados por el Profesional Especializado del Sistema de Seguridad de Seguridad de la Información, o quien él delegue, o el tercero contratado y los lineamientos de las buenas prácticas de la cadena de custodia de evidencias digitales, tomando como marco general la legislación colombiana.
i. Los incidentes de seguridad de la información sobre los cuales se va a requerir la toma de evidencia digital, serán aquellos cuya valoración de severidad sea alta y que adicionalmente deberá corresponder a algún incidente de los incluidos en la siguiente lista:
    - Cuando el equipo originador del incidente o afectado por el incidente sea un servidor que cumple una labor misional o un elemento de red:
        - Modificación no autorizada de sitios web (Website Defacement).
        - Ataques de denegación de servicio (Denial of Service Attacks).
        - Ataques de código malicioso (Malicious Code virus/worm).
        - Hackeo o intrusión (Intrusion/Hack).
        - Notificaciones de IDS (IDS alert notifications).
        - Espionaje (Unauthorized Electronic Monitoring).
        - Acceso no autorizado a sistemas de información.
        - Robo de propiedad intelectual.
j. Aunque la razón principal para la recolección de evidencias es la gestión del incidente también es necesaria para eventuales procesos legales, es fundamental que esta etapa se realice cumpliendo con la regulación y recomendaciones de la oficina Jurídica de forma que la evidencia sea admisible para procesos legales, algunas recomendaciones son:
    - Manejo de computadores forenses:
        - Seguir procedimientos forenses aprobados para poder recolectar evidencias validas en procesos legales.
        - Antes de generar las imágenes forenses se deben recolectar los datos volátiles (conexiones de red activas, procesos en ejecución, registros de sesiones activas, archivos abiertos, configuración de las interfaces de red y contenidos de memoria), que no quedarán registrados en los filesystem del sistema afectado.
        - Tener en cuenta que cualquier acción que se ejecute sobre el servidor puede afectar sustancialmente las evidencias, de igual forma el atacante puede estar aún dentro del equipo y la recolección de la evidencia en esas circunstancias puede tener consecuencias técnicas irreparables para el equipo y la información.
        - Es indispensable que las actividades de recolección de la evidencia sean realizadas por personal debidamente entrenado y que se emplee el mínimo de comandos para evitar la modificación de la evidencia.
        - Recolectar evidencias generadas de otros dispositivos como firewall, DNS los registros de estos dispositivos también deben ser almacenados es dispositivos de solo lectura, la segunda copia de esos registros puede ser empleada para análisis del incidente.
    - Manejo forense de dispositivos móviles:
        - El manejo forense de dispositivos móviles como smartphones implica el uso de equipo

especializado, conocimiento y procedimientos específicos. Lo ideal es que el equipo de respuesta a incidentes solicite apoyo especializado para el manejo de este tipo de evidencias.

- Identificación del atacante
  - Para identificar el atacante se debe considerar:
    - Validación de la dirección IP del atacante
    - Explorar el sistema del atacante
    - Recolectar evidencias del atacante mediante motores de búsqueda
    - Usar bases datos de incidentes
    - Supervisar los posibles canales de comunicación del atacante

2. Iniciar proceso legal

Cuando se requiera puede iniciarse un proceso legal, a través de la siguiente actividad:

Iniciar el proceso legal. En caso de que el análisis de la evidencia digital recopilada determine que se ameritan el inicio de acciones legales, el Profesional Especializado del Sistema de Seguridad de la Información o quien él delegue, procederá a comunicar el hecho al Jefe de la OTI vía correo electrónico. La solicitud de inicio de un proceso legal está a cargo del Jefe de la OTI, o de quien él delegue.

3.7 DOCUMENTAR INCIDENTE DE SEGURIDAD

Diligenciar el formato Formato de Reporte y Gestión de Incidentes.

3.8 CIERRE Y NOTIFICACIÓN DEL INCIDENTE DE SEGURIDAD A LAS PARTES INTERESADAS

- De acuerdo con el incidente se seguridad mitigado se da respuesta a las partes interesadas mediante los siguientes métodos que incluyen:
  - Correo electrónico
  - Llamada telefónica
  - En persona
  - Papel

4. ANEXOS

Anexo 1: **Documento digital Autoridades y Grupos de Interés.**

Anexo 2: FT.0720.05 Reporte y Gestión de Incidentes de Seguridad de la Información