ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA RECREACION Y DEPORTE
Instituto Distrital de las Artes

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

PLAN DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

GTI-P-08

V.1

19/08/2026

Instituto Distrital de las Artes -IDARTES-
Carrera 8 No. 15 - 46 - Bogotá
+57 (601) 379 5750
Código postal: 111711

BOGOTÁ

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

TABLA DE TABLAS

1. INTRODUCCIÓN

El Instituto Distrital de las Artes – IDARTES, en los últimos años, ha fortalecido significativamente su ecosistema tecnológico y digital, ampliando la cobertura de servicios institucionales dirigidos tanto a los funcionarios y contratistas como a la ciudadanía en general. Este crecimiento ha implicado el incremento de plataformas tecnológicas, sistemas de información, servicios en nube, herramientas colaborativas, infraestructura de red, canales virtuales de atención y mecanismos de interoperabilidad, elementos que actualmente soportan gran parte de la operación administrativa, misional y estratégica de la Entidad.

La Oficina Asesora de Planeación y Tecnologías de la Información – OAPTI, como dependencia encargada de liderar la gestión tecnológica institucional, ha venido desarrollando procesos de modernización orientados a garantizar la disponibilidad, continuidad, integridad y seguridad de los servicios TI del Instituto. En consecuencia, el aumento en la dependencia tecnológica también ha incrementado la exposición a amenazas de ciberseguridad, riesgos operacionales y vulnerabilidades asociadas al uso de herramientas digitales, correo electrónico, servicios web, acceso remoto y manejo de información institucional.

Actualmente, las entidades públicas enfrentan amenazas constantes relacionadas con ransomware, malware, ataques de phishing, compromiso de credenciales, fuga de información, explotación de vulnerabilidades, accesos no autorizados y demás incidentes que pueden afectar la confidencialidad, integridad y disponibilidad de la información institucional. Estos eventos no solo impactan los activos tecnológicos, sino también la continuidad de la prestación de servicios a la ciudadanía, la confianza institucional y el cumplimiento de obligaciones legales y regulatorias.

Teniendo en cuenta lo anterior, el Instituto Distrital de las Artes – IDARTES requiere contar con lineamientos formales, procedimientos estandarizados y mecanismos de actuación coordinada que permitan responder de manera oportuna y eficiente ante incidentes de seguridad de la información, minimizando el impacto operativo, financiero, legal y reputacional que estos puedan generar.

El presente Plan de Respuesta ante Incidentes de Seguridad de la Información define las directrices, roles, responsabilidades, niveles de severidad, criterios de escalamiento, manejo de evidencias digitales y procedimientos de atención necesarios para la gestión integral de incidentes de ciberseguridad dentro del IDARTES. Así mismo, establece playbooks específicos para la atención de eventos críticos como ransomware, phishing/BEC, credenciales comprometidas, malware y exfiltración de información, permitiendo una respuesta organizada, trazable y alineada con las buenas prácticas internacionales de seguridad de la información y continuidad operativa.

De igual manera, este documento busca fortalecer la capacidad institucional de prevención, detección, contención, erradicación y recuperación frente a incidentes de seguridad, promoviendo una cultura de gestión del riesgo y mejora continua en los procesos tecnológicos administrados por la Oficina Asesora de Planeación y Tecnologías de la Información.

2. OBJETIVO

Establecer el marco metodológico, operativo y técnico para la gestión integral de incidentes de seguridad de la información en el Instituto Distrital de las Artes – IDARTES, definiendo los lineamientos, responsabilidades, procedimientos y mecanismos de respuesta necesarios para identificar, analizar, contener, erradicar, recuperar y documentar incidentes que puedan afectar los activos de información y los servicios tecnológicos institucionales.

2.1 Objetivos Específicos

- Definir un plan institucional para la atención y gestión de incidentes de seguridad de la información.
- Establecer roles y responsabilidades claras para los actores involucrados en la respuesta a incidentes.
- Asegurar la adecuada clasificación, priorización y escalamiento de incidentes de acuerdo con su impacto y criticidad.
- Minimizar el impacto operativo, financiero, legal y reputacional derivado de incidentes de ciberseguridad.
- Establecer mecanismos para la preservación y manejo adecuado de evidencias digitales.
- Definir playbooks específicos para la atención de amenazas comunes como ransomware, phishing, malware, compromiso de credenciales y fuga de información.
- Garantizar la trazabilidad de las actividades ejecutadas durante el ciclo de vida del incidente.
- Fortalecer las capacidades institucionales de detección, análisis y respuesta frente a amenazas cibernéticas.
- Promover la mejora continua mediante procesos de lecciones aprendidas y actualización de controles de seguridad.
- Contribuir al cumplimiento de requisitos normativos, regulatorios y de buenas prácticas en materia de seguridad de la información.

3. ALCANCE

El presente Plan de Respuesta ante Incidentes de Seguridad de la Información aplica a todos los funcionarios, contratistas, terceros, proveedores y personal autorizado que hagan uso de los activos tecnológicos y recursos de información del Instituto Distrital de las Artes – IDARTES.

Así mismo, el alcance comprende todos los activos tecnológicos institucionales, incluyendo, pero sin limitarse a:

- Equipos portátiles y dispositivos móviles institucionales.
- Servidores físicos y virtuales.
- Infraestructura de red y telecomunicaciones.
- Plataformas en nube.
- Sistemas de información institucionales.
- Correo electrónico corporativo.
- Bases de datos institucionales.
- Aplicaciones web y servicios digitales.
- Herramientas colaborativas y de acceso remoto.
- Sistemas de almacenamiento y respaldos.
- Activos críticos de información.
- Servicios tecnológicos administrados por terceros.

El presente documento cubre todas las etapas del ciclo de gestión de incidentes de seguridad de la información, iniciando desde la detección, reporte o identificación de un evento de seguridad, continuando con su análisis, clasificación, contención, erradicación y recuperación, y finalizando con el cierre formal del incidente, documentación de evidencias, generación de lecciones aprendidas y definición de acciones de mejora.

El plan aplica a incidentes que afecten o puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional, incluyendo eventos asociados a:

- Ransomware.
- Malware.
- Phishing.
- Business Email Compromise (BEC).
- Compromiso de credenciales.
- Accesos no autorizados.
- Exfiltración o fuga de información.
- Denegación de servicio.
- Vulnerabilidades críticas.
- Uso indebido de activos tecnológicos.
- Intrusiones y actividades maliciosas.

4. MARCO NORMATIVO

El presente Plan de Respuesta ante Incidentes de Seguridad de la Información se fundamenta en los siguientes lineamientos normativos, regulatorios y de buenas prácticas aplicables a entidades públicas y a la gestión de seguridad de la información:

4.1 Normatividad Nacional

- Constitución Política de Colombia.
- Ley 1273 de 2009 – Protección de la información y de los datos.
- Ley 1581 de 2012 – Protección de Datos Personales.
- Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública.
- Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC.
- Política de Gobierno Digital – MinTIC.
- Modelo de Seguridad y Privacidad de la Información – MSPI.
- Guía de Gestión de Incidentes de Seguridad Digital – MinTIC.
- Lineamientos de Seguridad Digital para entidades públicas.

4.2 Estándares y Buenas Prácticas Internacionales

- ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27002 – Controles de Seguridad de la Información.
- ISO/IEC 27035 – Gestión de Incidentes de Seguridad de la Información.
- NIST Cybersecurity Framework.
- NIST SP 800-61 – Computer Security Incident Handling Guide.
- CIS Controls.
- OWASP Top 10.

5. RESPONSABLES

La gestión y respuesta ante incidentes de seguridad de la información en el Instituto Distrital de las Artes – IDARTES será coordinada por la Oficina Asesora de Planeación y Tecnologías de la Información – OAPTI, con apoyo de las áreas involucradas según la naturaleza y criticidad del incidente.

Oficina Asesora de Planeación y Tecnologías de la Información – OAPTI

- Liderar la estrategia institucional de respuesta ante incidentes.
- Coordinar la gestión técnica y operativa de incidentes de seguridad.
- Definir mecanismos de monitoreo y contención.
- Autorizar escalamiento de incidentes críticos.
- Garantizar la actualización del presente documento.
- Coordinar actividades de recuperación tecnológica.

Mesa de Servicios TI

- Recibir y registrar reportes de incidentes.
- Escalar eventos al equipo correspondiente.
- Realizar seguimiento inicial.
- Mantener trazabilidad de los casos.
- Documentar tiempos de atención y cierre.

Responsable de Seguridad de la Información / Ciberseguridad

- Analizar eventos e indicadores de compromiso.
- Ejecutar actividades de contención.
- Coordinar procesos de erradicación.
- Realizar análisis forense cuando aplique.
- Gestionar evidencias digitales.
- Emitir recomendaciones de mitigación.

Funcionarios y Contratistas

- Reportar oportunamente eventos sospechosos.
- Cumplir las políticas institucionales de seguridad.
- Cooperar con los procesos de investigación y contención.
- Proteger las credenciales y activos asignados.

Subdirección Jurídica

- Evaluar implicaciones legales y regulatorias.
- Apoyar procesos de denuncia o notificación.
- Revisar obligaciones asociadas a protección de datos personales.
- Gestionar requerimientos de autoridades competentes.

Comité Institucional de Gestión y Desempeño

- Aprobar decisiones estratégicas relacionadas con incidentes críticos.
- Autorizar activación de planes de continuidad.
- Aprobar notificaciones externas de alto impacto.
- Realizar seguimiento a incidentes críticos institucionales.

6. CRITERIOS DE SEVERIDAD

La severidad permite determinar el nivel de impacto que tiene un incidente sobre la operación del Instituto Distrital de las Artes – IDARTES y definir la prioridad con la que debe ser atendido.

6.1 Severidad Baja

Corresponde a incidentes con impacto mínimo y controlado, que afectan uno o pocos usuarios sin comprometer servicios críticos ni información sensible.

Ejemplos

- Malware detectado en un solo equipo.
- Correo sospechoso reportado a tiempo.
- Bloqueo temporal de una cuenta.

Impacto: No afecta la operación institucional.
Tiempo de respuesta: Hasta 72 horas.

6.2 Severidad Media

Corresponde a incidentes que afectan parcialmente procesos o áreas específicas y requieren atención prioritaria para evitar propagación.

Ejemplos

- Campaña de phishing a varios usuarios.
- Malware en varios equipos.
- Caída parcial del correo institucional.

Impacto: Afecta temporalmente una dependencia o servicio.
Tiempo de respuesta: Hasta 24 horas.

6.3 Severidad Alta

Corresponde a incidentes que afectan servicios críticos, información sensible o múltiples áreas de la entidad.

Ejemplos

- Ransomware en servidores.
- Compromiso de cuentas administrativas.
- Fuga parcial de información.

Impacto: Genera interrupción importante de la operación institucional.
Tiempo de respuesta: Máximo 4 horas.

6.4 Severidad Critica

Corresponde a incidentes que afectan gravemente la operación institucional o comprometen información crítica de IDARTES.

Ejemplos

- Exfiltración masiva de información.
- Caída total de servicios tecnológicos.
- Ataque generalizado de ransomware.

Impacto: Puede impedir total o parcialmente la operación de la entidad.

Tiempo de respuesta: Inmediato.

6.5 Matriz de Severidad

Impacto	Urgencia	Severidad	Tiempo de Respuesta
Bajo	Baja	Baja	72 horas
Medio	Media	Media	24 horas
Alto	Alta	Alta	4 horas
Crítico	Crítica	Crítica	Inmediato

Tabla 1. Matriz de severidad de incidentes de SI, Fuente elaboración propia

7. IMPLEMENTACIÓN DEL PLAN - PLAYBOOKS DE RESPUESTA

Los playbooks de respuesta ante incidentes corresponden a guías operativas que establecen las actividades, responsables y acciones que deben ejecutarse frente a diferentes tipos de incidentes de seguridad de la información en el Instituto Distrital de las Artes – IDARTES.

Estos playbooks permiten estandarizar la atención de eventos de ciberseguridad, garantizando una respuesta organizada, rápida y adecuada ante situaciones que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.

Cada playbook define las fases de identificación, contención, erradicación, recuperación y lecciones aprendidas, así como ejemplos prácticos y acciones específicas para incidentes como ransomware, phishing/BEC, compromiso de credenciales, malware y exfiltración de información. Su propósito es facilitar la comprensión y correcta actuación del personal involucrado, incluso para usuarios que no cuentan con conocimientos técnicos especializados en seguridad informática.

Nota: Los playbooks se encuentran alojados en el repositorio institucional de Tecnologías de la Información.

7.1 Phishing / BEC

Descripción: Este tipo de incidente ocurre cuando un atacante envía correos falsos haciéndose pasar por áreas internas, directivos o entidades confiables con el fin de robar contraseñas, información o engañar al usuario.

Ejemplo: Un funcionario recibe un correo aparentemente enviado por Talento Humano solicitando actualizar la contraseña institucional mediante un enlace.

¿Cómo identificarlo?

- El remitente tiene pequeñas variaciones.
- El mensaje genera urgencia.
- Tiene errores ortográficos.
- Solicita contraseñas o información sensible.
- El enlace dirige a páginas extrañas.

Fases:

1. **Identificación:** Se analiza el correo recibido, el remitente, enlaces y archivos adjuntos para determinar si representa una amenaza.
2. **Contención:** Se bloquea el remitente, se eliminan los correos maliciosos y se suspenden

accesos comprometidos.

3. **Erradicación:** Se eliminan reglas maliciosas, accesos sospechosos o archivos descargados.
4. **Recuperación:** Se restablecen credenciales y se valida que el usuario pueda operar normalmente.
5. **Lecciones aprendidas:** Se capacita al personal y se fortalecen filtros de seguridad.

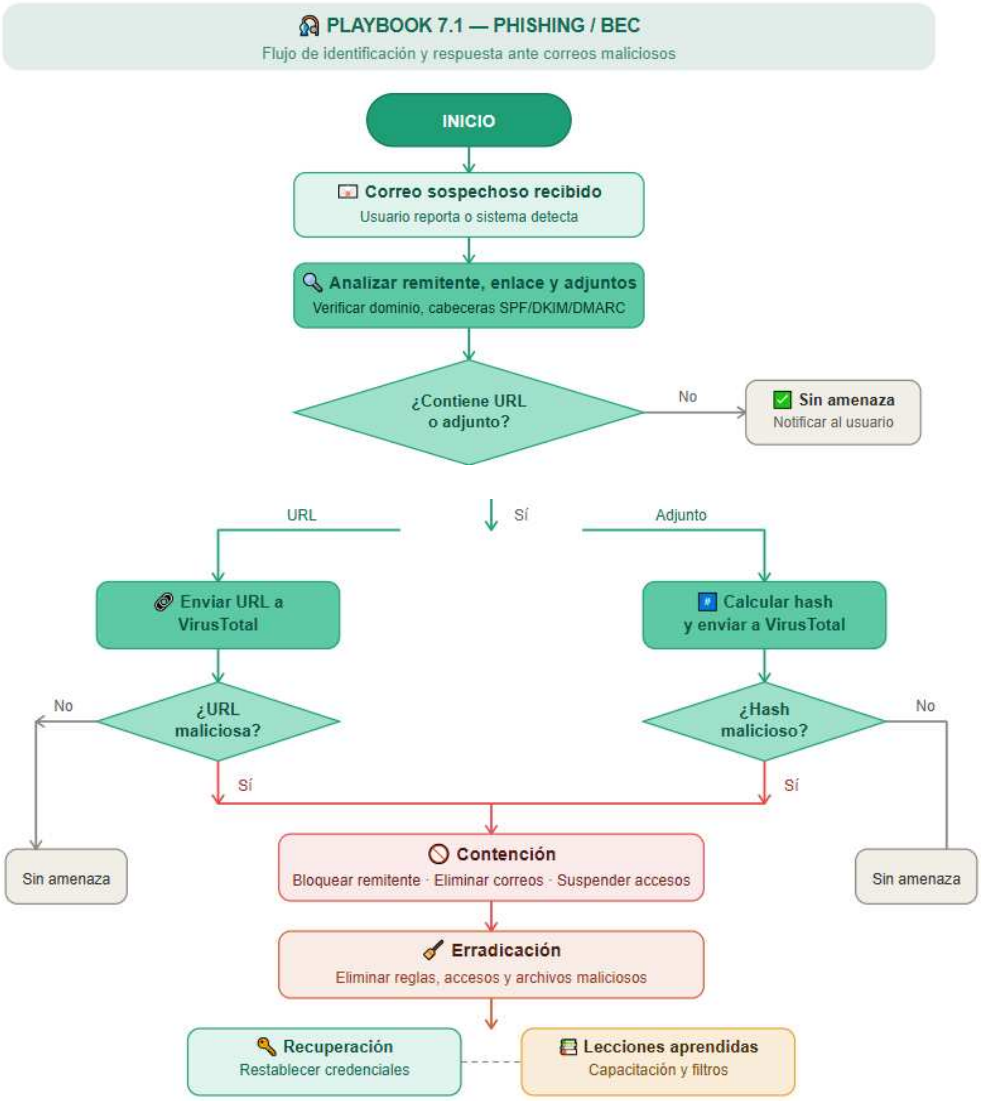

Ilustración 1. Playbook PHISHING, Fuente elaboración propia

7.2 Ransomware

Descripción: Es un tipo de ataque donde un software malicioso cifra archivos o sistemas para exigir un pago económico a cambio de recuperar la información.

Ejemplo: Un servidor institucional presenta archivos bloqueados y un mensaje solicitando dinero para recuperar la información.

¿Cómo identificarlo?

- Archivos con extensiones extrañas.
- Equipos lentos o bloqueados.

- Mensajes de rescate.
- Imposibilidad de abrir documentos.

Fases:

1. **Identificación:** Se detectan equipos o servidores afectados por cifrado de información.
2. **Contención:** Se aíslan los dispositivos afectados para evitar propagación.
3. **Erradicación:** Se elimina el malware y se corrigen vulnerabilidades utilizadas por el atacante.
4. **Recuperación:** Se restauran respaldos y servicios afectados.
5. **Lecciones aprendidas:** Se fortalecen políticas de backup y segmentación de red.

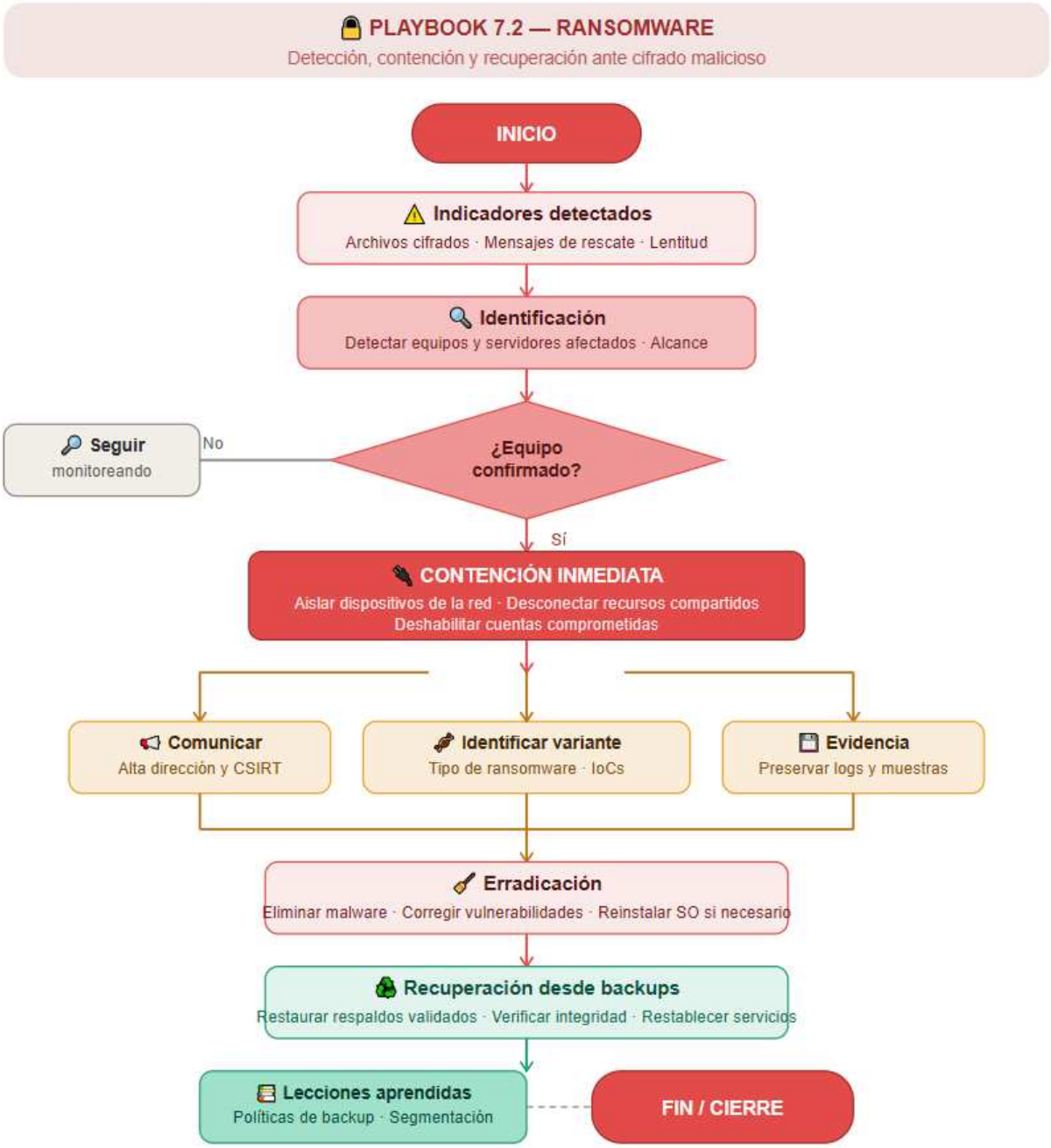

Ilustración 2. Playbook Ransomware, fuente elaboración propia.

7.3 Credenciales Comprometidas

Descripción: Ocurre cuando un atacante obtiene acceso no autorizado a las credenciales institucionales de un usuario.

Ejemplo: Se detecta inicio de sesión desde otro país usando una cuenta institucional.

¿Cómo identificarlo?

- Accesos desde ubicaciones desconocidas.
- Bloqueos frecuentes de cuenta.
- Actividades que el usuario no reconoce.
- Alertas de autenticación sospechosa.

Fases:

1. **Identificación:** Se detectan accesos inusuales o sospechosos.
2. **Contención:** Se bloquean cuentas y sesiones activas.
3. **Erradicación:** Se eliminan accesos persistentes o no autorizados.
4. **Recuperación:** Se restablecen contraseñas y mecanismos de autenticación.
5. **Lecciones aprendidas:** Se fortalece el uso de doble autenticación y controles de acceso.

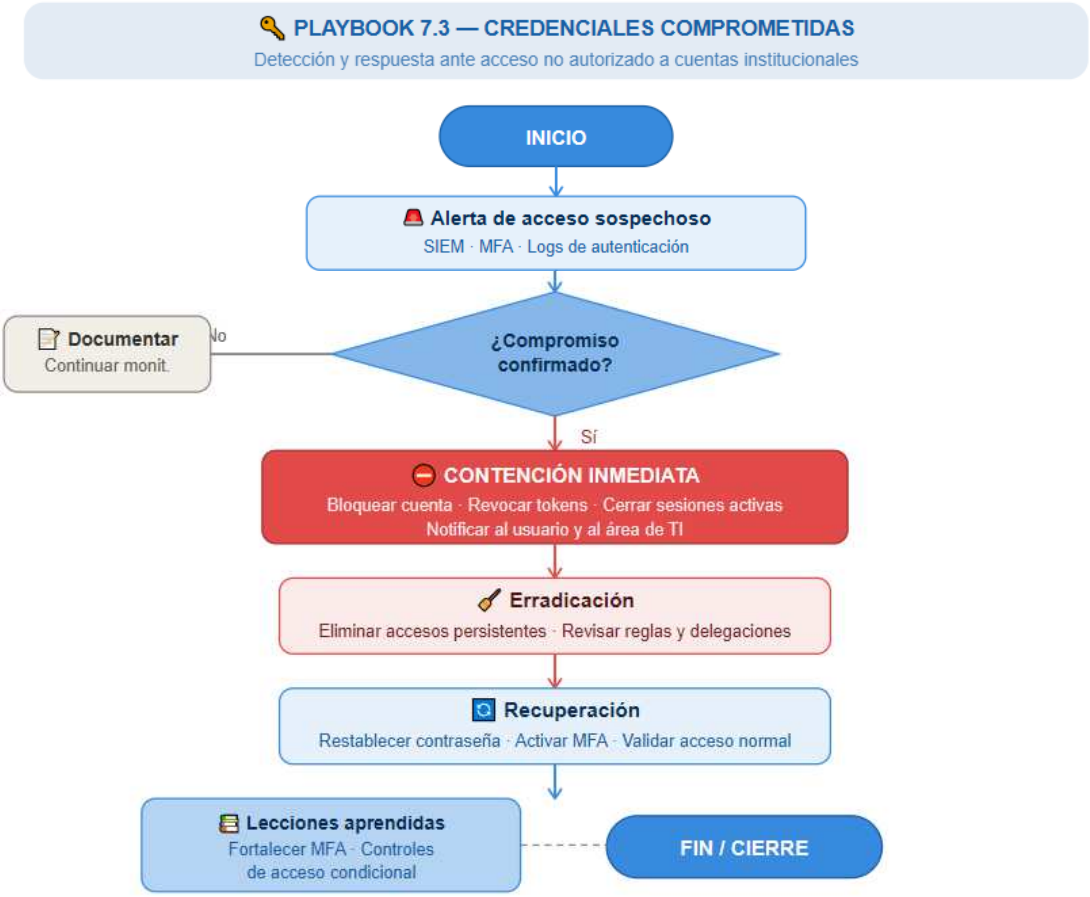

Ilustración 3.Playbook Credenciales Comprometidas, fuente elaboración propia.

7.4 Malware

Descripción: Corresponde a software malicioso que puede afectar equipos, robar información o permitir accesos no autorizados.

Ejemplo: El antivirus detecta un troyano descargado desde un sitio web no autorizado.

¿Cómo identificarlo?

- Lentitud en el equipo.
- Ventanas emergentes extrañas.
- Antivirus deshabilitado.
- Procesos desconocidos.

Fases:

1. **Identificación:** Se detecta comportamiento sospechoso o alertas del antivirus.
2. **Contención:** Se aísla el dispositivo afectado.
3. **Erradicación:** Se eliminan archivos y procesos maliciosos.
4. **Recuperación:** Se valida el correcto funcionamiento del equipo.
5. **Lecciones aprendidas:** Se actualizan controles de seguridad y políticas de navegación.

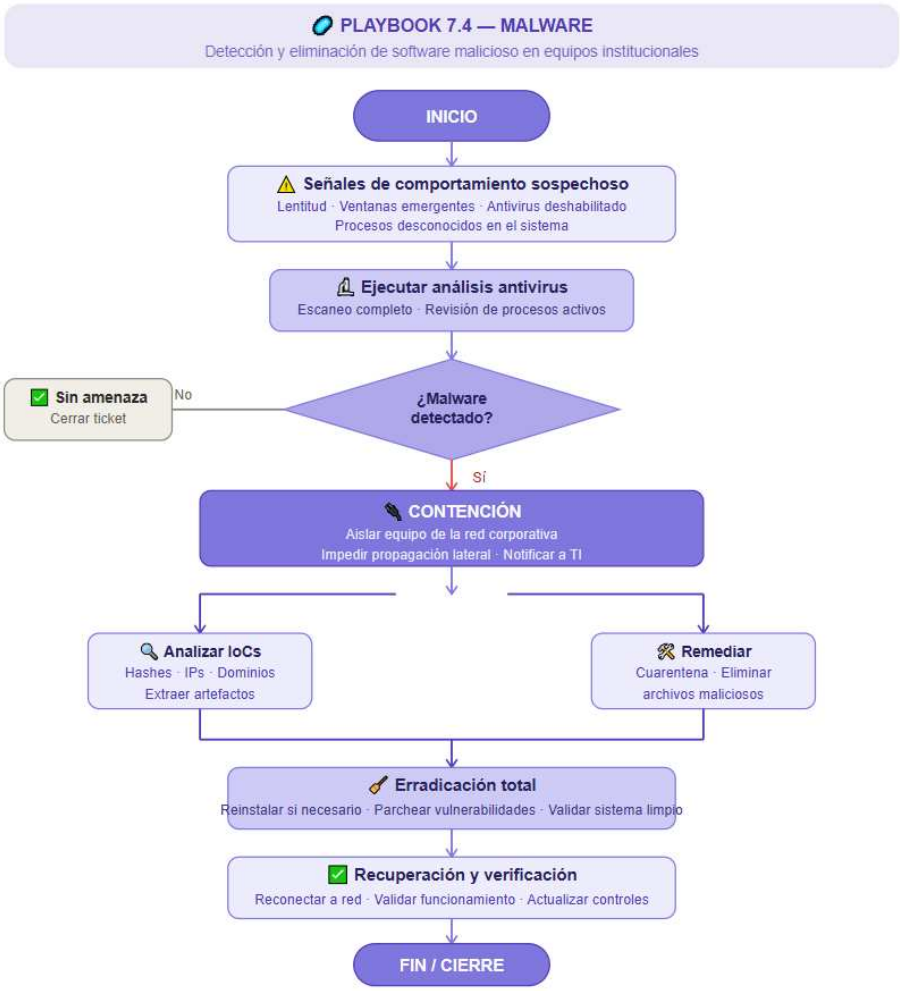

Ilustración 4.Playbook Malware, fuente elaboración propia.

7.5 Exfiltración de Información

Descripción: Consiste en la extracción no autorizada de información institucional hacia medios externos.

Ejemplo: Se detecta transferencia masiva de archivos institucionales hacia una plataforma no autorizada.

¿Cómo identificarlo?

- Alto tráfico de red.
- Descargas o transferencias inusuales.
- Acceso masivo a archivos.
- Conexiones externas sospechosas.

Fases:

1. **Identificación:** Se detectan movimientos inusuales de información.
2. **Contención:** Se bloquean conexiones y accesos sospechosos.
3. **Erradicación:** Se eliminan accesos no autorizados.
4. **Recuperación:** Se restablecen servicios y se valida integridad de información.

5. **Lecciones aprendidas:** Se fortalecen controles DLP y monitoreo institucional.

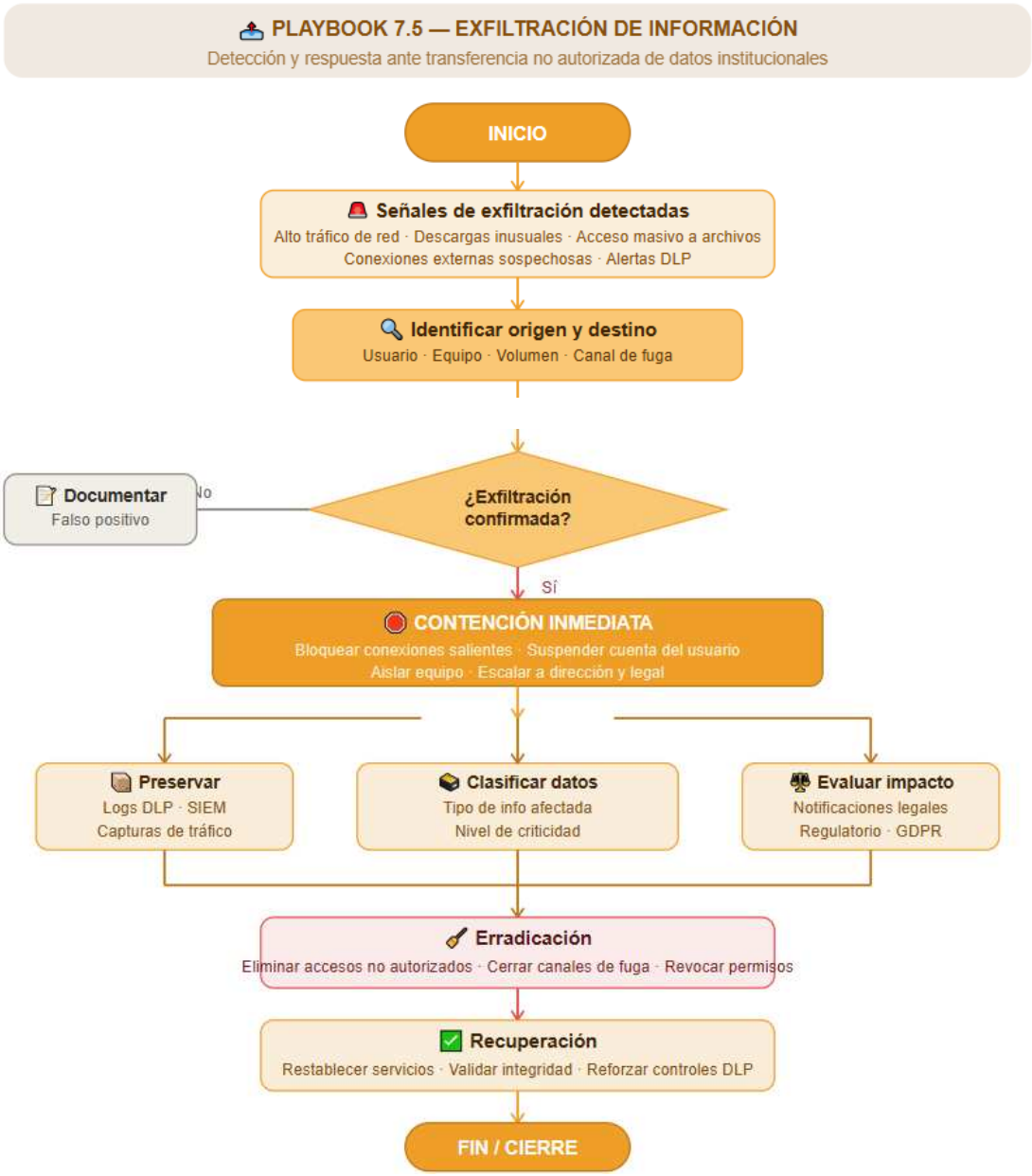

Ilustración 5. Exfiltración de Información, fuente elaboración propia

8. ESCALAMIENTO

El proceso de escalamiento permite garantizar que los incidentes de seguridad de la información sean atendidos por el personal adecuado según su nivel de criticidad e impacto sobre la operación del Instituto Distrital de las Artes – IDARTES. Este proceso busca asegurar una respuesta rápida, organizada y oportuna, evitando que un incidente aumente su nivel de afectación o se propague hacia otros servicios institucionales.

Inicialmente, todos los eventos o incidentes reportados deberán ser recibidos y registrados por la Mesa de Servicios TI, quien realizará una validación preliminar y determinará si el caso requiere escalamiento al Equipo de Seguridad TI. Cuando el incidente presente afectación sobre servicios

críticos, información sensible o múltiples áreas de la entidad, el caso deberá ser escalado al Líder de la Oficina Asesora de Planeación y Tecnologías de la Información – OAP-TI y, en situaciones críticas, a la Alta Dirección para la toma de decisiones institucionales y activación de protocolos de crisis.

Los tiempos máximos de escalamiento definidos permiten establecer prioridades de atención y asegurar que cada incidente sea gestionado dentro de un tiempo adecuado según su nivel de severidad, minimizando el impacto operativo, reputacional y tecnológico para la entidad.

Nivel	Responsable	Tiempo Máximo
Nivel 1	Mesa de Servicios	15 minutos
Nivel 2	Equipo Seguridad TI	30 minutos
Nivel 3	Líder OAP-TI	1 hora
Nivel 4	Alta Dirección	Inmediato

Tabla 2. Matriz de Escalamiento, Fuente elaboración propia

9. MANEJO DE EVIDENCIAS

Durante la atención de incidentes de seguridad de la información es fundamental garantizar la adecuada preservación de las evidencias digitales, ya que estas permiten analizar lo ocurrido, identificar la causa del incidente, determinar el impacto generado y soportar procesos técnicos, administrativos o legales que puedan derivarse del evento presentado.

Las evidencias pueden incluir registros de acceso, capturas de pantalla, correos electrónicos, archivos sospechosos, logs de sistemas, direcciones IP, registros de firewall, alertas de antivirus o cualquier otra información relacionada con el incidente. Toda evidencia recolectada deberá mantenerse íntegra, evitando modificaciones, alteraciones o eliminación accidental que puedan afectar su validez o trazabilidad.

Así mismo, el acceso a las evidencias deberá estar restringido únicamente al personal autorizado, manteniendo registro de la fecha, hora y responsable de cada actividad realizada sobre la información recolectada, garantizando la cadena de custodia y la confidencialidad de la información institucional.

- Preservar integridad de la evidencia.
- Mantener cadena de custodia.
- Restringir acceso únicamente al personal autorizado.
- Registrar fecha, hora y responsable.

10. LECCIONES APRENDIDAS

Al finalizar la atención de un incidente de seguridad de la información, se deberá realizar un proceso de análisis y revisión con el fin de identificar las causas que originaron el evento, evaluar la efectividad de las acciones ejecutadas y determinar oportunidades de mejora para fortalecer la capacidad de respuesta institucional del IDARTES.

Este proceso permitirá identificar fallas técnicas, vulnerabilidades, debilidades en controles de seguridad o errores operativos que hayan facilitado la ocurrencia del incidente. Así mismo, permitirá validar si los procedimientos, tiempos de atención y mecanismos de escalamiento fueron adecuados o requieren ajustes para mejorar la gestión futura de incidentes similares.

Como resultado de las lecciones aprendidas, deberán documentarse las mejoras identificadas en un informe interno de TI con carácter confidencial , actualizar procedimientos o controles de seguridad cuando sea necesario y definir planes de acción preventivos orientados a reducir la probabilidad de reincidencia y fortalecer la seguridad de la información institucional.

- Identificar causa raíz.
- Actualizar controles.
- Documentar mejoras.
- Generar plan de acción preventivo.

CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS
1	2026-08-19	Emisión inicial.

CONTROL DE APROBACIÓN

ESTADO	FECHA	NOMBRE	CARGO
ELABORÓ	2026-08-11	MARYURY FORERO BOHORQUEZ	ENLACE MIPG
REVISÓ	2026-08-11	MARYURY FORERO BOHORQUEZ	REFERENTE MIPG
REVISÓ	2026-08-11	MARYURY FORERO BOHORQUEZ	REFERENTE MIPG
APROBÓ	2026-08-19	DANIEL SANCHEZ ROJAS	LIDER DE PROCESO
AVALÓ	2026-08-19	DANIEL SANCHEZ ROJAS	JEFE DE LA OFICINA ASESORA DE PLANEACIÓN Y TECNOLOGÍAS DE LA INFORMACIÓN

COLABORADORES

NOMBRE
ANDRES FELIPE CUBILLOS GARCIA