SOLUCION LABORATORIO SESIÓN 3

Objetivos del Laboratorio:

1. Identificar el vector de ataque inicial (e.g., phishing, explotación de vulnerabilidad).
2. Analizar los logs del sistema para encontrar evidencias de actividad maliciosa.
3. Determinar el alcance del compromiso y los sistemas afectados.
4. Proponer medidas de contención y recuperación.

RESUMEN DE LOS MALWARE

Tipo de Malware	Concepto	¿Cómo funciona?
Virus	Código que se adjunta a archivos legítimos y se propaga.	Se activa al ejecutar el archivo infectado y se copia a otros archivos o programas.
Gusano (Worm)	Malware que se replica por sí mismo sin ayuda del usuario.	Se propaga por redes, correo electrónico o dispositivos, explotando vulnerabilidades.
Troyano (Trojan)	Programa malicioso disfrazado de legítimo.	Engaña al usuario para instalarlo, abriendo puertas traseras o robando información.
Ransomware	Secuestra archivos del usuario y exige un rescate.	Cifra datos y muestra un mensaje pidiendo dinero para recuperarlos.
Spyware	Programa espía que recolecta información del usuario.	Monitorea actividades, capturando datos como contraseñas o hábitos de navegación.
Adware	Muestra publicidad no deseada.	Inyecta anuncios o redirige el navegador para generar ingresos a los atacantes.
Rootkit	Oculta otros malware o procesos maliciosos.	Se instala a nivel del sistema operativo y evita la detección por antivirus.
Keylogger	Registra lo que el usuario escribe.	Captura pulsaciones del teclado para obtener contraseñas, mensajes o datos privados.
Botnet	Red de dispositivos infectados bajo control de un atacante.	Los dispositivos (bots) se usan para enviar spam, hacer ataques DDoS, etc.
Backdoor (Puerta trasera)	Permite el acceso remoto no autorizado al sistema.	El atacante entra sin ser detectado, incluso si otras medidas de seguridad fallan.
Scareware	Finge ser un antivirus o alerta de virus para asustar al usuario.	Obliga al usuario a comprar software falso o descargar malware real.
Fileless Malware	Malware que no se instala como archivo en disco.	Se ejecuta directamente en la memoria RAM usando herramientas legítimas del sistema.
Rogue Software	Software fraudulento que simula ser útil.	Se presenta como una herramienta de limpieza o seguridad, pero en realidad es dañino.

Polymorphic Malware	Cambia su código para evitar detección.	Se modifica automáticamente cada vez que se replica, eludiendo los antivirus.
Metamorphic Malware	Se reescribe a sí mismo completamente para evitar detección.	Va más allá del polimórfico, cambiando su lógica interna.
Logic Bomb	Código que se activa solo cuando se cumplen ciertas condiciones.	Puede destruir archivos, apagar sistemas o lanzar otros malware al activarse.
RAT (Remote Access Trojan)	Troyano que otorga control remoto total sobre el equipo.	Permite al atacante ver pantalla, grabar cámara, extraer archivos, etc.
Malvertising	Uso de publicidad en línea para distribuir malware.	Inyecta código malicioso en anuncios legítimos, infectando a quienes los ven.
Crimeware	Malware diseñado para cometer delitos financieros.	Se enfoca en robar datos bancarios, clonar tarjetas, etc.
Mobile Malware	Malware diseñado para dispositivos móviles.	Infecta apps, roba datos, espía llamadas o mensajes, y puede controlar el dispositivo.
Wiper Malware	Diseñado para borrar datos del sistema de forma irreversible.	Borra el disco duro o sobrescribe archivos críticos, dejándolos inutilizables.
ATM Malware	Infecta cajeros automáticos.	Permite al atacante dispensar efectivo, robar datos de tarjetas o acceder al backend.
Clicker Trojan	Realiza clics automáticos en anuncios sin el conocimiento del usuario.	Genera ingresos por publicidad a costa del sistema del usuario.
Cryptojacker	Malware que mina criptomonedas usando recursos del sistema infectado.	Afecta rendimiento, consume CPU/GPU y electricidad sin permiso del usuario.
Exploit Kit	Conjunto de herramientas que busca vulnerabilidades en el sistema.	Se usa para instalar malware aprovechando fallos en el software del usuario.
Firmware Malware	Se instala en el firmware de hardware (como BIOS o UEFI).	Difícil de detectar y eliminar; persiste incluso tras formatear el disco.
Stealer	Especializado en robar credenciales y datos personales.	Extrae información de navegadores, apps, y carteras de criptomonedas.

LAS TECNICAS O METODOS DE ATAQUES

Técnica de ataque	Concepto	¿Cómo funciona?
Phishing	Engaño mediante correos o sitios falsos para robar información.	El atacante suplanta una entidad legítima (banco, red social, etc.) para obtener credenciales.

Spear Phishing	Variante de phishing dirigida a una persona o grupo específico.	Usa información personalizada para parecer más creíble.
Smishing	Phishing por mensajes SMS.	Envía enlaces maliciosos o códigos falsos por mensajes de texto.
Vishing	Phishing por llamadas telefónicas.	El atacante se hace pasar por un representante legítimo para obtener datos.
Spoofing	Suplantación de identidad digital.	Falsifica direcciones IP, correos o sitios web para engañar al usuario.
Ingeniería social	Manipulación psicológica para obtener acceso o información.	Engaña a las personas para que revelen contraseñas, den clic o permitan accesos.
Fuerza bruta	Intento masivo de adivinar contraseñas.	Prueba miles de combinaciones posibles hasta encontrar la correcta.
Ataque de diccionario	Variante de fuerza bruta usando palabras comunes.	Usa una lista de contraseñas comunes o probables para adivinar claves.
Ataque de día cero (Zero-day)	Aprovecha una vulnerabilidad no conocida aún por el proveedor.	Se ejecuta antes de que exista un parche de seguridad.
Man-in-the-Middle (MitM)	Intercepción de comunicación entre dos partes.	El atacante se posiciona entre el usuario y un servidor para espiar o modificar los datos.
Sniffing	Captura de datos que viajan por la red.	Usa software para escuchar el tráfico de red y robar información.
SQL Injection	Inyección de código malicioso en formularios SQL.	Permite acceder, modificar o eliminar datos en bases de datos mal protegidas.
Cross-site Scripting (XSS)	Inserción de scripts en sitios web para afectar a los usuarios.	El atacante ejecuta código en el navegador del usuario a través de formularios o URL.
Cross-site Request Forgery (CSRF)	Hace que el usuario ejecute acciones sin querer en un sitio web legítimo.	Aprovecha sesiones activas para enviar solicitudes maliciosas.
Denegación de servicio (DoS)	Saturación de un sistema para impedir su funcionamiento.	Envía un alto volumen de peticiones hasta que el sistema colapsa.
DDoS (Distributed DoS)	DoS distribuido desde múltiples dispositivos (botnet).	Multiplica el ataque desde miles de IPs para hacerlo más efectivo.
Escalada de privilegios	Obtención de más permisos de los que debería tener el atacante.	Aprovecha errores en el sistema para pasar de usuario común a administrador.
Ataque por repetición (Replay)	Reutilización de datos válidos capturados anteriormente.	Se intercepta y reutiliza una comunicación legítima para obtener acceso.

Clickjacking	Truco visual para hacer que el usuario haga clic en algo diferente a lo que cree.	Usa capas invisibles sobre botones legítimos.
Rogue software (falso antivirus)	Software que se presenta como útil, pero es malicioso.	Intenta que el usuario lo instale y pague para eliminar amenazas falsas.
Ataque a la cadena de suministro	Compromete software o hardware desde el origen.	Se inserta código malicioso en actualizaciones, proveedores o dispositivos antes de que lleguen al usuario final.
Social engineering vía USB	Dejar memorias USB infectadas en lugares públicos.	La curiosidad hace que la víctima la conecte, ejecutando el malware.
Password spraying	Probar una contraseña común contra múltiples cuentas.	A diferencia de fuerza bruta, evita bloqueos por intentos fallidos consecutivos.
Eavesdropping	Escucha pasiva de comunicaciones privadas.	Similar al sniffing, busca capturar conversaciones sin alterar datos.
DNS Spoofing	Falsificación de registros DNS para redirigir tráfico.	El usuario accede a sitios falsos creyendo que son legítimos.
Rogue access point	Punto de acceso WiFi falso que imita uno legítimo.	El usuario se conecta y el atacante puede espiar o redirigir el tráfico.

PASO 2: COMO AFECTAN A LOS SISTEMAS

Tipo de Malware	¿Cómo afecta el sistema?	Impacto si sucede
Virus	Infecta y modifica archivos ejecutables.	Pérdida de información, mal funcionamiento del sistema, propagación a otros equipos.
Gusano (Worm)	Se replica a través de redes y consume recursos.	Colapso de la red, lentitud del sistema, saturación de ancho de banda.
Troyano (Trojan)	Se oculta en programas aparentemente legítimos.	Acceso remoto no autorizado, robo de información o instalación de más malware.
Ransomware	Cifra archivos del sistema y bloquea el acceso.	Pérdida de datos críticos, interrupción del negocio, posibles costos de rescate.
Spyware	Espía las actividades del usuario sin consentimiento.	Violación de privacidad, robo de contraseñas, datos financieros o confidenciales.
Adware	Muestra anuncios no deseados e interfiere con el navegador.	Experiencia del usuario degradada, redireccionamiento a sitios maliciosos.
Rootkit	Oculta procesos maliciosos y desactiva antivirus.	El atacante puede controlar el sistema sin ser detectado, difícil de eliminar.
Keylogger	Registra pulsaciones del teclado.	Robo de credenciales, fraudes financieros, espionaje corporativo.

Backdoor	Abre una puerta oculta en el sistema.	Control remoto permanente del sistema por parte del atacante.
Botnet	Convierte el equipo en parte de una red controlada.	El sistema puede ser usado para enviar spam, lanzar ataques DDoS, o minar criptomonedas.
Scareware	Muestra alertas falsas para engañar al usuario.	Puede inducir a instalar más malware o pagar por software inútil o malicioso.
Fileless Malware	Se ejecuta desde la memoria RAM sin dejar rastros.	Difícil de detectar, permite ataques rápidos y altamente evasivos.
Cryptojacker	Usa los recursos del sistema para minar criptomonedas.	Degradación del rendimiento del equipo, sobrecalentamiento y aumento en el consumo eléctrico.
Wiper	Borra archivos o discos duros por completo.	Daño irreversible, pérdida total de datos, interrupción de operaciones.
Rogue Software	Finge ser un software útil como antivirus o limpiador.	Pérdida de dinero, instalación de malware adicional, pérdida de confianza.

Paso 1: Identificar el Vector de Ataque Inicial

1.1 Revisión de Indicadores Iniciales:

• Actividad: Recolectar información sobre los primeros signos del incidente. Algunos indicadores comunes pueden incluir:

- Correo electrónico (Email phishing)

Es el más común. El atacante envía un correo que parece legítimo (de una entidad bancaria, una red social, una empresa conocida, etc.), con enlaces o archivos adjuntos maliciosos.

- Mensajería instantánea y SMS (Smishing)

El atacante envía un mensaje de texto con un enlace fraudulento. Similar al correo electrónico, pero usando SMS o apps como WhatsApp, Telegram, etc.

- Llamadas telefónicas (Vishing)

El atacante llama haciéndose pasar por una entidad confiable para pedir credenciales o convencer a la víctima de ejecutar una acción.

- Redes sociales y mensajería en plataformas

  Links maliciosos o mensajes falsos enviados a través de plataformas como Facebook, Instagram, LinkedIn, etc.

- Sitios web comprometidos o falsos (Pharming)

El atacante manipula el tráfico web (por ejemplo, envenenando el DNS) para redirigir al usuario a un sitio falso que imita a uno legítimo.

- Fallos en sistemas específicos: Interrupciones repentinas, ralentización del sistema, inicios de sesión fallidos.

Identificadores clave

- Indican urgencia o amenazas

Mensajes que te presionan a actuar rápido ("Tu cuenta será bloqueada", "Verifica en 24 horas").

- Presentan Errores ortográficos o gramaticales
- Remitentes sospechosos
- Direcciones de correo extrañas o que no coinciden con el dominio de la organización real.
- Enlaces sospechosos: Al pasar el mouse por el enlace, la dirección URL es diferente a la que aparenta ser. Ej: https://banco.com en realidad apunta a http://banco.seguridad-falsa.ru.
- Solicitudes inusuales: solicitud de tu contraseña, código de verificación o número de tarjeta.
- Archivos adjuntos inesperados

Pueden contener malware. Cuidado con archivos .exe, .zip, .docm, entre otros.

Posibles vectores de ataque:

1. Ingeniería social

Phishing (correo electrónico), Smishing (mensajes SMS) ,Vishing (llamadas telefónicas)

Spear phishing (dirigido a una persona específica), Pretexting (el atacante finge una identidad con un pretexto creíble), Baiting (engañar con algo atractivo, como un USB con malware).

2. Correo electrónico malicioso: Enlaces a sitios falsos, Archivos adjuntos infectados (PDF, Word, Excel, ZIP, etc.), Scripts ocultos o macros maliciosas

3. Software vulnerable o sin parches: Sistemas operativos o aplicaciones desactualizadas, Plugins y frameworks sin mantenimiento, Drivers y bibliotecas con exploits conocidos

4. Dispositivos externos y medios removibles: USBs infectados, Discos externos comprometidos, Smartphones conectados a la red

5. Navegación web: Sitios web comprometidos o falsos (pharming), Drive-by downloads (instalación automática de malware al visitar una página), Malvertising (publicidad maliciosa)

6. Redes inseguras: Conexión a redes Wi-Fi públicas sin protección, Redes internas sin segmentación, Acceso físico no controlado a la infraestructura

7. Credenciales débiles o filtradas: Contraseñas fáciles de adivinar, Reutilización de contraseñas, Uso de contraseñas filtradas en la dark web.

8. Acceso físico: Robo de dispositivos (laptops, móviles), Acceso no autorizado a salas de servidores o estaciones de trabajo

9. Aplicaciones y APIs expuestas: Interfaces web mal configuradas, APIs sin autenticación o sin validación de entradas, Errores de lógica en aplicaciones.

10. Servicios de nube mal configurados: Buckets públicos en Amazon S3, Claves API expuestas, Contenedores sin autenticación.

11. Amenazas internas (insider threat): Empleados malintencionados, Errores humanos (envío accidental de datos sensibles), Uso indebido de privilegios.

12. Ataques por red: Man-in-the-Middle (MitM), Sniffing o espionaje de tráfico, Spoofing (suplantación de identidad), DDoS (ataques de denegación de servicio)

Otros vectores menos comunes pero peligrosos:

Ataques a la cadena de suministro (vulnerabilidades en proveedores de software o hardware)

Ataques a dispositivos IoT (conectados pero mal protegidos)

Ataques por Bluetooth o NFC

Uso de inteligencia artificial para automatizar ataques o imitar voces/personas (deepfakes)

1.2 Evaluación de la Evidencia:

• Actividad: Evaluar la evidencia para identificar el vector de ataque.

o Si se sospecha phishing: Busca correos electrónicos con enlaces sospechosos, archivos adjuntos maliciosos o remitentes falsificados.

o Si se sospecha explotación de vulnerabilidades: Revisa registros de actividad no habitual en aplicaciones o sistemas, y busca informes de vulnerabilidades recientes que puedan haber sido explotadas.

Paso 2: Analizar los Logs del Sistema para Encontrar Evidencias de Actividad Maliciosa

2.1 Recolección de Logs:

• Actividad: Describir los logs que deben revisarse en los sistemas afectados.

o Logs del Servidor de Correo Electrónico: Busca correos electrónicos sospechosos enviados o recibidos, cuentas que enviaron múltiples correos no solicitados, o accesos inusuales.

o Logs del Sistema de Bases de Datos: Identifica actividades anómalas, como consultas no autorizadas, modificaciones masivas o acceso en momentos no habituales.

o Logs de Seguridad: Revisa alertas de seguridad relacionadas con accesos fallidos, cambios en las configuraciones del sistema, o patrones inusuales de tráfico de red.

2.2 Análisis de la Actividad Maliciosa:

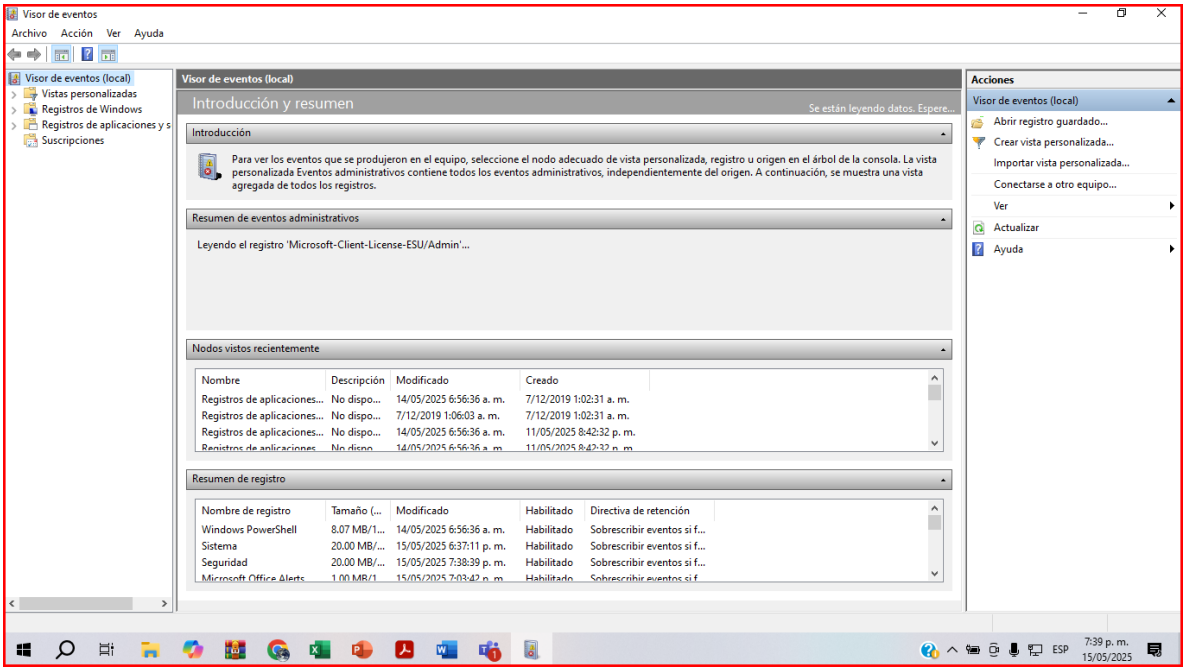
• Actividad: Analiza los logs en busca de patrones inusuales.

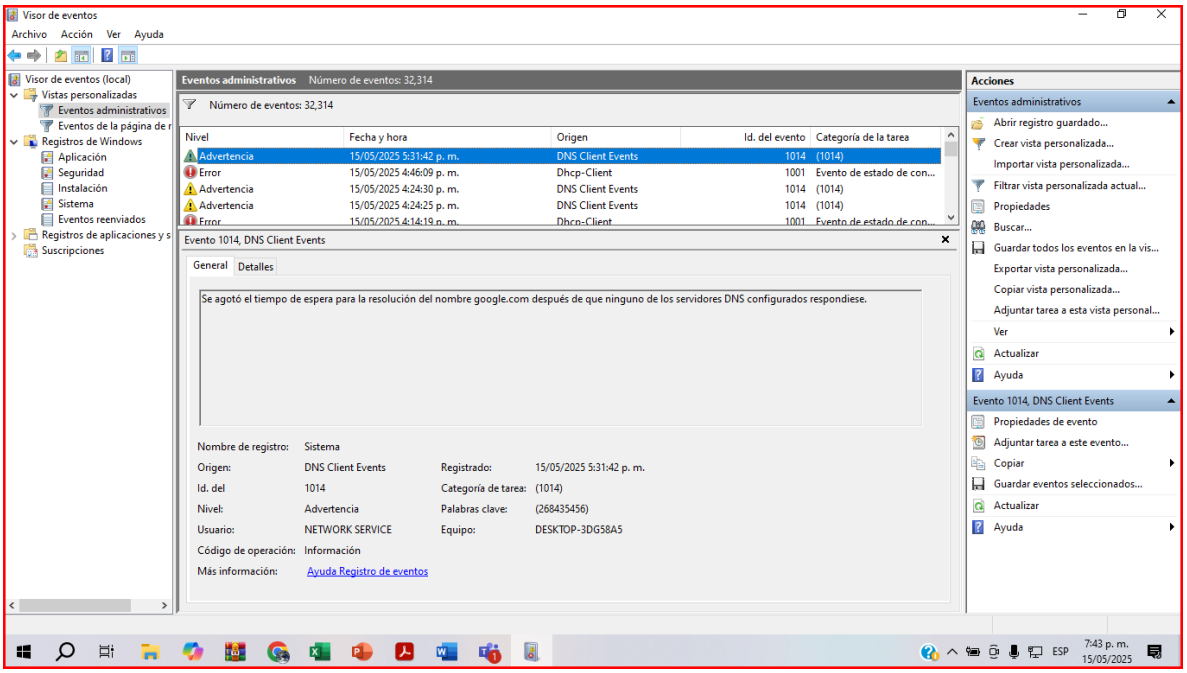
o Ejemplos de análisis: Buscar múltiples intentos fallidos de inicio de sesión, tráfico elevado de IPs externas o archivos descargados desde ubicaciones inusuales.

• Herramientas de Análisis:

o Herramientas para analizar los logs: Utiliza herramientas como Splunk, Wireshark, o Graylog para visualizar y analizar los registros.

REVISÍON DE LOGS VISOR DE EVENTOS DE WINDOWS 11





Paso 3: Determinar el Alcance del Compromiso y los Sistemas Afectados

3.1 Identificación de Sistemas Comprometidos:
• **Actividad**: Cuando se identifican sistemas comprometidos, realiza lo siguiente:
o **Revisa los sistemas interconectados**: Determina si otros sistemas conectados al afectado pueden haber sido comprometidos.
o **Evalúa el impacto en la infraestructura crítica**: Determina si sistemas clave, como servidores de bases de datos o aplicaciones críticas, se ven afectados.

3.2 Evaluación del Impacto:
• **Actividad**: Evalúa cómo el incidente ha afectado la disponibilidad, integridad y confidencialidad de los datos.
o **Disponibilidad**: ¿El incidente ha interrumpido el acceso a sistemas o datos críticos?
o **Integridad**: ¿Ha habido alguna modificación no autorizada de los datos?
o **Confidencialidad**: ¿Se han expuesto datos confidenciales o sensibles a usuarios no autorizados?

Paso 4: Proponer Medidas de Contención y Recuperación

4.1 Medidas de Contención Inmediatas:
• **Actividad**: Implementar medidas para detener el ataque y prevenir una mayor propagación.
o **Desconectar sistemas comprometidos**: Aislar los sistemas afectados para evitar que el malware o atacante se propague a otras partes de la red.
o **Actualización de sistemas**: Parchear vulnerabilidades conocidas en sistemas críticos.
o **Cambio de credenciales**: Restablecer las contraseñas y credenciales de acceso de los sistemas comprometidos.

4.2 Plan de Recuperación:

• **Actividad**: Desarrollar un plan para restaurar los sistemas y volver a la operación normal.

1. Objetivo y alcance del plan

Descripción del propósito del plan.
Extensión (qué sistemas, procesos y lugares abarca).
Tipos de desastres considerados (naturales, ciberataques, errores humanos, fallos de hardware, etc.).

2. Análisis de Impacto al Negocio (BIA):

Identificación de activos críticos.
Impacto financiero y operacional si se encuentran en interrupción.
Determinación de:
RTO (Recovery Time Objective): Tiempo máximo para uno de los sistemas
RPO (Recovery Point Objective): Pérdida máxima de datos aceptable (en tiempo).

3. Evaluación de riesgos y amenazas:

Análisis de vulnerabilidades.
Identificación de amenazas probables.
Evaluación del nivel de exposición al riesgo.

4. Estrategias de recuperación

Procedimientos específicos para restaurar:
Sistemas operativos.
Bases de datos.
Aplicaciones críticas.
Infraestructura de red y telecomunicaciones.
Entornos de nube (si aplica).
Uso de respaldos (backups) y réplicas.
Uso de sitios alternos:
Sitio caliente (activo con replicación en tiempo real).
Sitio tibio (recursos preparados, pero no activos).
Sitio frío (infraestructura mínima que requiere configuración)

5. Plan de respaldo (backups)

Frecuencia y tipos de backups (completas, incrementales, diferenciales).
Ubicación (local, en la nube, híbrido).
Procedimientos de restauración testeados.

6. Procedimientos de respuesta y recuperación

Instrucciones paso a paso para:
Contener el daño y evaluar el daño.
Informar a los equipos responsables.
Dar inicio a la restauración de servicios y sistemas.
Verificar la integridad de los procesos..

4.3 Comunicación:

• • **Actividad**: Determina a quién se debe informar sobre la situación y las medidas tomadas.

1. Internamente (en el seno de la organización):

Equipo de respuesta a incidentes (CSIRT / equipo de IR)

Grupo que es responsable de evaluar, contener y gestionar el incidente.

Área de TIC o Seguridad de la información

Grupo que se encarga de investigar, mitigar y recuperar los sistemas afectados.

Alta dirección o Comité de crisis

Deben ser conocedores del incidente para tomar decisiones estratégicas, legales y financieras.

Área de legal y compliance

Que evaluará el impacto en el ámbito legal, el cumplimiento normativo (GDPR, ISO 27001, etc.) y de notificaciones obligatorias.

Área de Comunicaciones / RRPP

En caso de producirse una comunicación oficial (a usuarios, medios de comunicación, partners, etc.).

Recursos Humanos

En caso de que el incidente afecte a personas de la organización o necesite una concienciación.

2. Externamente (según el caso):

Clientes y usuarios afectados

Si el incidente comporta una ruptura de datos personales, una interrupción de servicios a clientes definidos u o bien una violación de las cuentas de sus usuarios.

Proveedores o partners estratégicos

Si en el incidente de seguridad se ven directa o indirectamente afectados por el mismo.

Autoridades reguladoras y gubernamentales (en función de la jurisdicción)

Por ejemplo:

Autoridad de protección de datos (por ejemplo, Superintendencia de Industria y Comercio en Colombia).

CERT nacional o sectorial.

Entidades financieras (si aplica).

Policía o Fiscalía (en el marco de investigaciones penales).

Medios de comunicación (solo en caso que sea necesario y a su control)

Para no disparar rumores y consolidar la reputación de la institución, se ha de hacer a través del área de comunicaciones.

¿Qué medidas se deben llevar a cabo después de haber pasado por un incidente?

Fase 1: Detección y evaluación.

Confirmación de que el incidente es auténtico.

Clasificación de su nivel de severidad/alcance.

Recoger información de todo tipo (logs, evidencias, comportamiento...).

Fase 2: Contención:

Aislamiento de sistemas comprometidos (segmentación de red, cierre de accesos).

Cambio de credenciales implicadas.

Parada de procesos maliciosos o de usuarios comprometidos.

Fase 3: Erradicación:

Hallazgo del origen del ataque (vector de entrada).

Eliminación de malware o accesos no permitidos.

Poner en marcha los parches de seguridad y mejoras.

Fase 4: Recuperación:

Restauración de los servicios y sistemas comprometidos.

Restaurar la información desde backups seguros.

Controlar de nuevo la integridad de la información.

Monitorear comportamientos anómalos de forma posterior.

Fase 5: Reporte de incidentes y lecciones aprendidas.

Documentar el incidente y su tratamiento.

Generar informes técnicos y ejecutivos.

Realización de evaluaciones de los fallos de controles y cambios de políticas o configuraciones.

Realizar sesiones de feedback y aprendizaje organizacional.