

LABORATORIO – El Incidente Crítico

Paso 1: Identificar el Vector de Ataque Inicial

1.1 Revisión de Indicadores Iniciales

Debemos recolectar información sobre los primeros signos del incidente, que pueden incluir:

- **Mensajes extraños o sospechosos:** Correos electrónicos con enlaces o archivos adjuntos sospechosos, solicitudes inusuales de credenciales, mensajes urgentes que buscan presionar al usuario.
- **Fallos en sistemas específicos:** Desempeño inesperado, accesos no autorizados, cambios en configuraciones sin razón aparente.
- **Registros de actividad anómala:** Intentos de acceso fallidos, cambios en permisos, tráfico de red inusual.

Posibles vectores de ataque

1. Phishing:

- Indicadores clave: Correos electrónicos fraudulentos, URLs alteradas, remitentes desconocidos.
- Evidencia por buscar: Enlaces a sitios maliciosos, patrones de envío de correos a múltiples usuarios.

2. Explotación de vulnerabilidad:

- Indicadores clave: Accesos inesperados, ejecución de procesos desconocidos, actividad anormal en logs.
- Evidencia por buscar: Exploits identificados en software desactualizado, actividad en puertos abiertos.

3. Acceso no autorizado:

- Indicadores clave: Cambios en credenciales sin autorización, nuevos usuarios con privilegios elevados.
- Evidencia por buscar: Registros de acceso no habituales, uso de cuentas comprometidas.

4. Manipulación psicológica (ingeniería social):

Estrategias como el *phishing* (fraudes vía correo electrónico), *smishing* (mensajes SMS engañosos) y *vishing* (suplantación por llamadas). También se incluyen ataques dirigidos como el *spear phishing*, el *pretexting* (el atacante se hace pasar por otra persona con un motivo

creíble) y el *baiting* (atracción mediante elementos maliciosos, como USBs infectados).

5. **Correos electrónicos peligrosos:** Contienen enlaces fraudulentos, archivos adjuntos infectados (*PDF, Word, Excel, ZIP*), así como scripts ocultos o macros diseñadas para ejecutar código malicioso.
6. **Software sin actualizar o con fallas:** Sistemas operativos y aplicaciones obsoletas, plugins y frameworks sin mantenimiento, además de *drivers* y bibliotecas con vulnerabilidades explotables.
7. **Dispositivos externos y almacenamiento portátil:** Peligros como *USBs* comprometidos, discos duros externos alterados y *smartphones* conectados a redes inseguras.
8. **Navegación en sitios web inseguros:** Riesgos incluyen páginas falsificadas (*pharming*), descargas automáticas de malware (*drive-by downloads*) y publicidad maliciosa (*malvertising*).
9. **Uso de redes no protegidas:** Conexión a *Wi-Fi* públicas sin cifrado, redes internas sin segmentación y acceso físico sin restricciones a infraestructura crítica.
10. **Credenciales débiles o comprometidas:** Contraseñas fáciles de descifrar, reutilización de credenciales y el uso de claves filtradas en la *dark web*.
11. **Accesos físicos no autorizados:** Robo de dispositivos como *laptops* y teléfonos móviles, además de ingreso sin permiso a salas de servidores o estaciones de trabajo.
12. **Vulnerabilidades en aplicaciones y APIs:** Interfaces web mal configuradas, APIs sin mecanismos de autenticación o validación de entrada y errores lógicos en aplicaciones.
13. **Configuraciones inseguras en la nube:** *Buckets* de almacenamiento público sin restricciones, exposición de claves *API* y contenedores sin autenticación adecuada.
14. **Amenazas internas:** Empleados con intenciones maliciosas, errores humanos que exponen datos sensibles y el uso indebido de privilegios de acceso.
15. **Ataques basados en red:** Técnicas como *Man-in-the-Middle (MitM)*, *sniffing* (espionaje de tráfico), *spoofing* (suplantación de identidad) y ataques de denegación de servicio (*DDoS*).

Otros vectores menos comunes pero peligrosos:

- Vulnerabilidades en la cadena de suministro (fallos en software o hardware de proveedores).
- Ataques dirigidos a dispositivos *IoT* con medidas de seguridad deficientes.
- Explotación de *Bluetooth* o *NFC* para infiltrarse en sistemas.
- Uso de *inteligencia artificial* para automatizar ataques o falsificar voces/imágenes (*deepfakes*).

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

2.1 Revisión de Registros del Sistema

Objetivo: Identificar los registros clave de los sistemas afectados para detectar actividad sospechosa.

- **Registros del servidor de correo electrónico:** Examinar mensajes enviados y recibidos que puedan ser sospechosos, detectar cuentas que han enviado múltiples correos no solicitados y revisar accesos inusuales al sistema.
- **Registros de bases de datos:** Identificar anomalías como consultas realizadas sin autorización, modificaciones masivas de datos o accesos en horarios poco frecuentes.
- **Registros de seguridad:** Analizar alertas sobre intentos de acceso fallidos, cambios en la configuración del sistema y tráfico de red fuera de lo habitual.

2.2 Evaluación de Actividad Maliciosa

Objetivo: Analizar los registros para detectar patrones de comportamiento anómalo.

- **Ejemplos de actividad sospechosa:** Revisar intentos reiterados de inicio de sesión sin éxito, tráfico excesivo proveniente de direcciones IP externas y descargas de archivos desde ubicaciones desconocidas.
- **Herramientas de análisis de registros:** Utilizar soluciones como *Splunk*, *Wireshark* o *Graylog* para interpretar los registros y visualizar posibles amenazas.

REVISION DE LOGS VISOR DE EVENTOS DE WINDOWS 10

Visor de eventos

Archivo Acciones Ver Ayuda

Visor de eventos (local)

Introducción y resumen

Última actualización: 23/05/2025 10:55:05 a. m.

Para ver los eventos que se produjeron en el equipo, seleccione el nodo adecuado de vista personalizada, registro u origen en el árbol de la consola. La vista personalizada Eventos administrativos contiene todos los eventos administrativos, independientemente del origen. A continuación, se muestra una vista agregada de todos los registros.

Resumen de eventos administrativos

Tipo de evento	Id. del e...	Origen	Registro	Última hora	24 horas	7 días
Crítico	-	-	-	0	0	4
Error	-	-	-	26	140	1381
Advertencia	-	-	-	4	210	1,278
Información	-	-	-	50	343	4,888
Auditoría cor...	-	-	-	933	5,452	27,706
Error de aud...	-	-	-	0	0	2

Nodos vistos recientemente

Nombre	Descripción	Modificada	Creado
--------	-------------	------------	--------

Resumen de registro

Nombre de registro	Tamaño (L...	Modificado	Habilitado	Directiva de retención
Windows PowerShell	6,07 MB/L...	23/05/2025 3:25:45 p. m.	Habilitado	Subscribir eventos si f...
Sistema	13,07 MB/L...	23/05/2025 9:58:20 a. m.	Habilitado	Subscribir eventos si f...
Seguridad	20,00 MB/L...	23/05/2025 10:38:59 a. m.	Habilitado	Subscribir eventos si f...
Microsoft Office Alerts	60 KB/L...	23/05/2025 10:15:06 a. m.	Habilitado	Subscribir eventos si f...
Servicios de administración	60 KB/L...	19/02/2025 10:59:52 a. m.	Habilitado	Subscribir eventos si f...
Internet Explorer	60 KB/L...	19/02/2025 10:59:52 a. m.	Habilitado	Subscribir eventos si f...
Eventos de hardware	60 KB/L...	19/02/2025 10:59:52 a. m.	Habilitado	Subscribir eventos si f...
Aplicación	6,07 MB/L...	23/05/2025 10:15:06 a. m.	Habilitado	Subscribir eventos si f...
Microsoft-Windows-Np...	0 Bytes/L...		Deshabilita...	Subscribir eventos si f...

Acciones

Visor de eventos (local)

Abir registro guardado...

Crear vista personalizada...

Importar vista personalizada...

Conectar a otro equipo...

Ver

Actualizar

Ayuda

Error

Ver todas las instancias de este evento

Ayuda

Visor de eventos

Archivo Acciones Ver Ayuda

Visor de eventos (local)

Eventos administrativos

Número de eventos: 11,010

Número de eventos: 11,010

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Advertencia	23/05/2025 9:49:24 a. m.	DistributedCOM	10016	Ninguno
Error	23/05/2025 9:49:04 a. m.	DistributedCOM	10005	Ninguno
Error	23/05/2025 9:49:04 a. m.	Service Control Manager	7001	Ninguno
Error	23/05/2025 9:46:54 a. m.	Kernel-EventTracing	2	Session
Error	23/05/2025 9:44:23 a. m.	DistributedCOM	10005	Ninguno
Error	23/05/2025 9:44:23 a. m.	Service Control Manager	7001	Ninguno
Error	23/05/2025 9:44:23 a. m.	DistributedCOM	10005	Ninguno
Error	23/05/2025 9:44:23 a. m.	Service Control Manager	7001	Ninguno
Error	23/05/2025 9:44:22 a. m.	DistributedCOM	10005	Ninguno
Error	23/05/2025 9:44:22 a. m.	Service Control Manager	7001	Ninguno
Error	23/05/2025 9:44:22 a. m.	DistributedCOM	10005	Ninguno
Error	23/05/2025 9:44:13 a. m.	Service Control Manager	7001	Ninguno
Error	23/05/2025 9:44:13 a. m.	DistributedCOM	10005	Ninguno
Error	23/05/2025 9:44:06 a. m.	Service Control Manager	7001	Ninguno
Error	23/05/2025 9:44:06 a. m.	DistributedCOM	10005	Ninguno
Error	23/05/2025 9:44:04 a. m.	Service Control Manager	7001	Ninguno
Error	23/05/2025 9:44:04 a. m.	DistributedCOM	10005	Ninguno
Error	23/05/2025 9:44:03 a. m.	Service Control Manager	7001	Ninguno
Error	23/05/2025 9:44:03 a. m.	DistributedCOM	10005	Ninguno
Advertencia	23/05/2025 9:43:58 a. m.	User Device Registration	360	Ninguno
Error	23/05/2025 9:43:57 a. m.	DistributedCOM	10005	Ninguno
Error	23/05/2025 9:43:57 a. m.	Service Control Manager	7001	Ninguno
Error	23/05/2025 9:43:57 a. m.	DistributedCOM	10005	Ninguno
Error	23/05/2025 9:43:57 a. m.	Service Control Manager	7001	Ninguno

Evento 10005, DistributedCOM

General Detalles

Error de DCOM "10005" al intentar iniciar el servicio cdprvc con argumento: "No disponible" para ejecutar el servidor: {7798046-795-651-8C66-AA8CAB2280}

Nombre de registro: Sistema

Origen: DistributedCOM

Registrado: 23/05/2025 9:49:04 a. m.

Id. del: 10005

Categoría de tarea: Ninguno

Nivel: Error

Palabra clave: Crítico

Usuario: DESKTOP-TR08450\delni

Equipo: DESKTOP-TR08450

Código de operación: Información

Más información: [Ayuda Registro de eventos](#)

Acciones

Eventos administrativos

Abir registro guardado...

Crear vista personalizada...

Importar vista personalizada...

Filtrar vista personalizada actual...

Propiedades

Buscar...

Guardar todos los eventos en la vista personalizada co...

Exportar vista personalizada...

Copiar vista personalizada...

Adjuntar tareas a esta vista personalizada...

Ver

Actualizar

Ayuda

Evento 10005, DistributedCOM

Propiedades de evento

Adjuntar tareas a este evento...

Copiar

Guardar eventos seleccionados...

Actualizar

Ayuda

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

3.1 Detección de Sistemas Afectados

Acción: Una vez identificados los sistemas comprometidos, tenemos que seguir estos pasos:

- Verifica los sistemas conectados: Examina si otros dispositivos o plataformas vinculadas al sistema afectado también han sido comprometidos.
- Analiza el impacto en la infraestructura esencial: Determina si servidores de bases de datos, aplicaciones críticas u otros componentes clave han sido afectados por el incidente.

3.2 Análisis del Alcance del Impacto

Acción: evaluamos cómo el incidente ha afectado aspectos fundamentales de la seguridad de los datos:

- Disponibilidad: ¿Se ha visto afectado el acceso a sistemas o información esencial?
- Integridad: ¿Existen modificaciones no autorizadas en los datos almacenados?
- Confidencialidad: ¿Se han filtrado o expuesto datos sensibles a personas no autorizadas?

Paso 4: Proponer Medidas de Contención y Recuperación.

4.1 Acciones de Contención Rápida

Objetivo: Aplicar medidas inmediatas para frenar el ataque y evitar su propagación.

- Aislamiento de sistemas afectados: Desconectar los dispositivos comprometidos para impedir que el malware o el atacante se extienda a otras áreas de la red.
- Corrección de vulnerabilidades: Implementar actualizaciones y parches de seguridad en sistemas críticos para cerrar posibles brechas explotadas.
- Restablecimiento de credenciales: Modificar contraseñas y accesos de los sistemas comprometidos para evitar un uso no autorizado.

4.2 Estrategia de Restauración

Objetivo: Diseñar un plan estructurado para restablecer los sistemas y reanudar las operaciones normales.

1.Propósito y alcance del plan

- Definir el objetivo principal del plan.
- Especificar qué sistemas, procesos y ubicaciones están incluidos.
- Considerar distintos tipos de incidentes, como desastres naturales, ciberataques, errores humanos y fallos de hardware.

2.Evaluación del impacto en el negocio (BIA)

- Identificar los activos esenciales para la operación.
- Analizar las consecuencias financieras y operativas de una interrupción.

Determinar:

- RTO (Recovery Time Objective): Tiempo máximo permitido para la recuperación de un sistema.
- RPO (Recovery Point Objective): Límite de pérdida de datos aceptable en términos de tiempo.

3.Análisis de riesgos y amenazas

- Examinar vulnerabilidades existentes.
- Identificar posibles amenazas que puedan afectar la infraestructura.
- Evaluar el nivel de exposición y riesgo asociado.

4.Estrategias de recuperación

Definir procedimientos específicos para restaurar:

- Sistemas operativos.
- Bases de datos.
- Aplicaciones críticas.
- Infraestructura de red y telecomunicaciones.

Entornos en la nube (si aplica).

- Implementar respaldos y réplicas para garantizar la recuperación.

Considerar el uso de sitios alternos:

- Sitio caliente: Operativo con replicación en tiempo real.
- Sitio tibio: Recursos preparados, pero no activos.
- Sitio frío: Infraestructura mínima que requiere configuración.

5. Plan de respaldo (backups)

- Establecer la frecuencia y tipos de copias de seguridad (completas, incrementales, diferenciales).
- Definir la ubicación de los respaldos (local, nube, híbrido).
- Garantizar que los procedimientos de restauración han sido probados y validados.

6. Protocolos de respuesta y recuperación

Pasos detallados para:

- Contener y evaluar el daño.
- Notificar a los equipos responsables.
- Iniciar la restauración de servicios y sistemas.
- Verificar la integridad de los procesos antes de la reactivación completa.

4.3 Estrategia de Comunicación

Objetivo: Definir a quién se debe informar sobre el incidente y las acciones tomadas.

1. Comunicación interna dentro de la organización

- **Equipo de respuesta a incidentes (CSIRT / IR):** Encargado de evaluar, contener y gestionar el incidente.
- **Área de TIC o Seguridad de la Información:** Responsable de investigar, mitigar y restaurar los sistemas afectados.
- **Alta dirección o Comité de crisis:** Debe estar informado para tomar decisiones estratégicas, legales y financieras.
- **Área legal y compliance:** Evalúa el impacto normativo y legal, asegurando el cumplimiento de regulaciones como *GDPR* o *ISO 27001*.
- **Área de Comunicaciones / RRPP:** Maneja la comunicación oficial hacia usuarios, medios y socios estratégicos.

- **Recursos Humanos:** Interviene si el incidente afecta a empleados o requiere medidas de concienciación.

2. Comunicación externa según el caso

- **Clientes y usuarios afectados:** Se les informa si hubo filtración de datos personales, interrupción de servicios o vulneración de cuentas.
- **Proveedores o socios estratégicos:** Se les notifica si el incidente impacta sus operaciones directa o indirectamente.
- **Autoridades reguladoras y gubernamentales:** Dependiendo de la jurisdicción, puede incluir:
 - Autoridad de protección de datos (*Superintendencia de Industria y Comercio en Colombia*).
 - CERT nacional o sectorial.
 - Entidades financieras (si aplica).
 - Policía o Fiscalía (para investigaciones penales).
- **Medios de comunicación:** Solo si es necesario y bajo control del área de comunicaciones para evitar rumores y proteger la reputación institucional.

Medidas posteriores a un incidente

Fase 1: Detección y evaluación

- Confirmar la autenticidad del incidente.
- Clasificar su nivel de severidad y alcance.
- Recopilar información relevante (*logs, evidencias, comportamiento*).

Fase 2: Contención

- Aislar los sistemas comprometidos (*segmentación de red, cierre de accesos*).
- Cambiar credenciales afectadas.
- Detener procesos maliciosos o accesos no autorizados.

Fase 3: Erradicación

- Identificar el origen del ataque (*vector de entrada*).
- Eliminar malware o accesos indebidos.
- Aplicar parches de seguridad y mejoras.

Fase 4: Recuperación

- Restaurar servicios y sistemas comprometidos.
- Recuperar información desde respaldos seguros.
- Verificar la integridad de los datos y monitorear actividad sospechosa.

Fase 5: Reporte y aprendizaje

- Documentar el incidente y su resolución.
- Generar informes técnicos y ejecutivos.
- Evaluar fallos en controles y ajustar políticas de seguridad.
- Realizar sesiones de retroalimentación y aprendizaje organizacional.