MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL

SERVICIO PÚBLICO DE EMPLEO ESTATAL
SEPE
SERVEI PÚBLIC D'OCUPACIÓ ESTATAL

MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

Generalitat de Catalunya
SOC Servei d'Ocupació de Catalunya

IRON HACK SPAIN

# Gestión de incidentes de seguridad informática

IFCT0109 – Seguridad informática

MF0488_3 (90 horas)

# Proceso de notificación y gestión de intentos de intrusión

- Introducción
- Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones
- Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial
- Criterios para la determinación de las evidencias objetivas en las que se soportará la gestión del incidente
- Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones
- Guía para la clasificación y análisis inicial del intento de intrusión o infección contemplando el impacto previsible del mismo
- Establecimiento del nivel de intervención requerido en función del impacto previsible
- Guía para la investigación y diagnóstico del incidente de intento de intrusión o infecciones
- Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección
- Proceso para la comunicación del incidente a terceros, si procede
- Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente
- Resumen

# Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones

## Introducción

Intrusión: un evento en el que un usuario no autorizado intenta acceder a equipos y/o dispositivos de una red para comprometer la seguridad de la información.

Herramientas para prevenir intrusiones:

- Cortafuegos
- Sistemas de detección y prevención de intrusiones (IDS/IPS)

Criterios para elegir un IDS/IPS:

- Escalabilidad: capacidad de adaptarse a los cambios de tráfico de la red.
- Firmas de ataque utilizadas: mayor número de firmas para reducir falsos positivos y negativos.
- Capacidad de administración y gestión: funciones de autogestión, examen de logs, archivo, gestión de alarmas, consola centralizada, etc.
- Tipo de estructura de hardware utilizada: topología de la red y disposición de equipos y cortafuegos.

Ubicación del IDS/IPS:

- Antes del cortafuegos: detecta intrusiones desde el exterior.
- Después del cortafuegos: detecta intrusiones internas.

# Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones

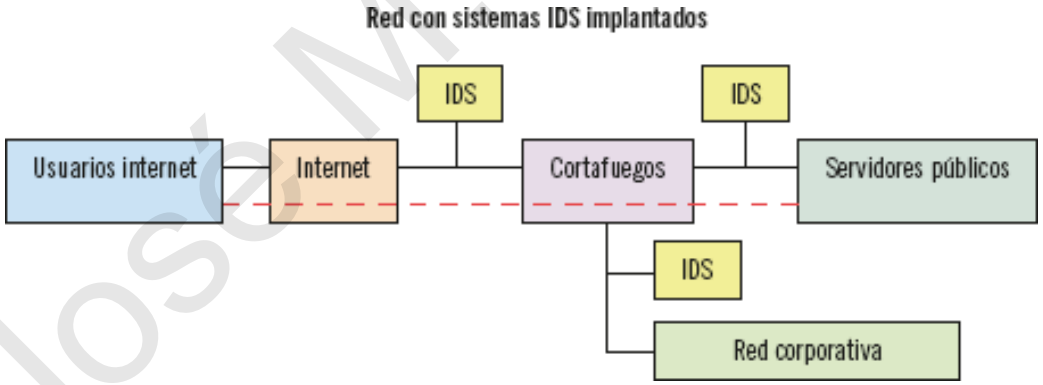
## Introducción

Responsabilidades en la gestión de intrusiones e infecciones:

- Equipo de seguridad: responsable de la detección, análisis y respuesta a las intrusiones e infecciones.
- Usuarios: responsables de informar sobre cualquier actividad sospechosa.

Beneficios de una gestión eficaz de intrusiones e infecciones:

- Minimiza los daños causados por intrusiones e infecciones.
- Reduce el tiempo de respuesta ante un ataque.
- Mejora la capacidad de recuperación de la organización.
- Permite aprender de los incidentes para mejorar las medidas de seguridad.



# Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones

## Responsabilidades de gestión y notificación de intrusiones

Importancia del procedimiento:

Un buen IDS/IPS no es suficiente si no hay un procedimiento adecuado para gestionar y notificar las intrusiones.
Las organizaciones deben establecer un procedimiento para minimizar el tiempo de respuesta y los daños.

Responsables. Designar responsables para:

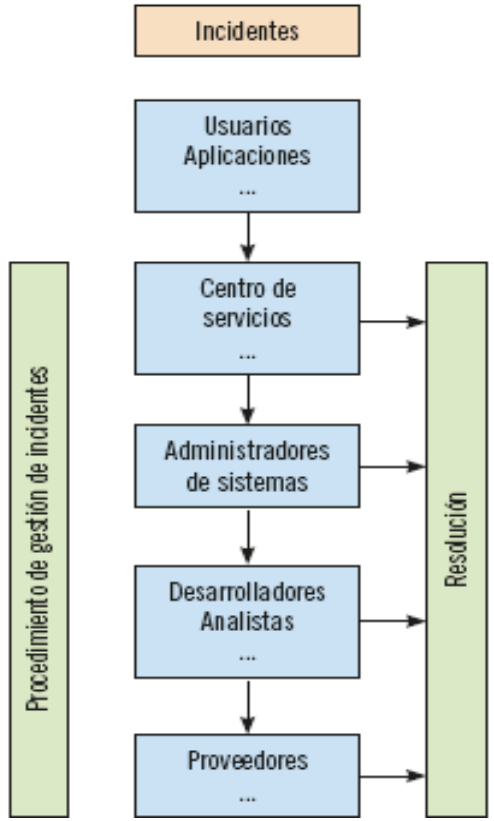
- Localizar las intrusiones detectadas.
- Remitir la información a las personas adecuadas.
- Tomar medidas de respuesta.

Estructura. Formar una estructura integrada por varias áreas para:

- Detectar alteraciones en los servicios.
- Registrar y clasificar incidentes.
- Restaurar la situación al punto previo al incidente.
- Proceso de gestión de incidentes:

**Seguir una estructura similar a la siguiente imagen >>>>>**

Estructura del proceso de gestión de incidentes



# Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones

## Responsabilidades de gestión y notificación de intrusiones

**Gestión de intrusiones: áreas responsables.**
**Niveles de gestión:**

Centro de servicios: primer nivel, contacto con usuarios.

- Registra y monitoriza incidentes.
- Aplica soluciones temporales.
- Colabora en la elaboración de bases de datos de intrusiones.

Administradores de sistemas: conocimiento más profundo de las intrusiones. Desarrollan respuestas rápidas a ataques complejos.

Desarrolladores y analistas: conocimientos avanzados sobre intrusiones. Desarrollan herramientas de contraataque y protección.

Proveedores: último escalón, cuando la organización no puede combatir el incidente. Consultan bases de datos para facilitar una solución.

**Derivación de la intrusión:**

- Nivel de complejidad: determina la derivación a un nivel u otro de la organización.
- Mayor complejidad: mayores conocimientos de los responsables.
- Notificación adecuada: influye en el tiempo de respuesta.

# Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones

## Responsabilidades de gestión y notificación de intrusiones

**Gestión de intrusiones:**

Ejemplo. Intrusión compleja derivada al centro de servicios:
Solo pueden tomar medidas provisionales.
Se pierde tiempo fundamental.
La infección se puede expandir o los daños pueden ser mayores.

Consideraciones:

- Nivel de seguridad y necesidad de protección: definen las áreas de respuesta a incidentes.
- Empresa pequeña: puede no necesitar desarrolladores.

# Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones

## Obligaciones legales de gestión y notificación de incidentes de seguridad e intrusiones

**Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD 3/2018):**

- Protege los datos de carácter personal.
- Establece pautas sobre los incidentes de ciberseguridad que afecten a datos personales.
- Designa responsables de su detección, notificación y gestión.

Violación de seguridad. Según el RGPD, es toda brecha de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales.

**Comunicaciones ante una violación de seguridad:**

- A las autoridades de control:
  - En España, la Agencia Española de Protección de Datos (AEPD) o la autoridad autonómica competente.
  - Debe realizarse antes de 72 horas si la brecha supone un riesgo para los derechos y libertades de los usuarios.
- A los afectados:
  - Para informarles del incidente y que puedan tomar medidas para mitigar sus efectos.

# Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones

## Obligaciones legales de gestión y notificación de incidentes de seguridad e intrusiones

**La comunicación a los afectados debe contener:**

- Descripción de la naturaleza de la brecha.
- Alcance y número de afectados (si es posible).
- Posibles consecuencias.
- Medidas tomadas para solventar la brecha.
- Recomendaciones a los afectados.
- Datos de contacto del Delegado de Protección de Datos.

**Registro interno de violaciones de seguridad.**

- El RGPD obliga al responsable de protección de datos a tener un registro interno de cualquier violación de seguridad.
- Permite estudiar cada brecha de seguridad y mejorar la respuesta ante futuros incidentes.

**¿Cuándo no es necesario comunicar una incidencia a los afectados?**

- Si los datos comprometidos son ininteligibles (por ejemplo, mediante técnicas de cifrado).
- Si se reacciona de manera rápida y eficaz, adoptando medidas para evitar que se produzca un riesgo para los derechos y libertades de los interesados.
- Si la comunicación supone un esfuerzo desproporcionado, se puede optar por una comunicación pública equivalente.

# Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones

## Obligaciones legales de gestión y notificación de incidentes de seguridad e intrusiones

**Sanciones por el incumplimiento del deber de notificar una brecha de seguridad.**

- Multa de hasta 10 millones de euros o el 2% de los ingresos totales anuales de la entidad.

**Recomendaciones:**

- Las entidades, tanto públicas como privadas, deben ser proactivas en materia de protección de datos.
- Es importante contar con una serie de procedimientos claros para estudiar cada brecha de seguridad.

# Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial

## Introducción

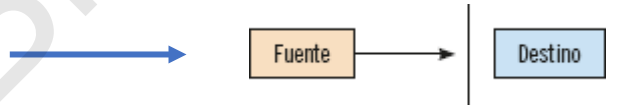
**Categorización de incidentes por impacto potencial:**

- Objetivo: Recopilar información para la resolución y restauración del sistema.
- Proceso de clasificación:
  - Categorización del incidente. Asignar categoría (y subcategoría) según el tipo de incidente y los responsables.
  - Nivel de prioridad. Asignar según los daños causados y la urgencia.
  - Asignación de recursos. Designar técnicos especializados y recursos específicos si el centro de servicios no puede resolver la incidencia.
  - Monitorización. Asociar un estado (detectado, activo, resuelto, etc.) y un tiempo de respuesta y resolución según la prioridad y la criticidad.

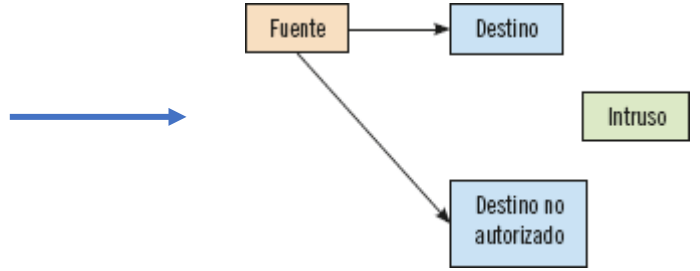
# Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial

Tipos de ataques. **Según el impacto en las propiedades de la información:**

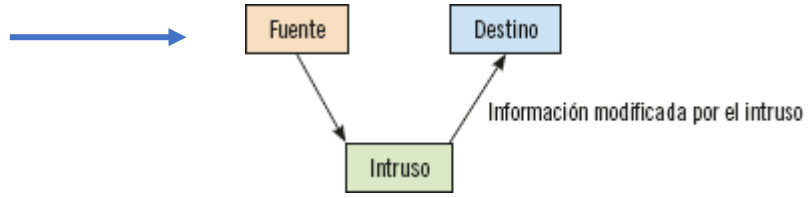
Interrupción: Destruyen o inutilizan la información y afectan a la accesibilidad y/o disponibilidad (destrucción de dispositivos, saturación del procesador).



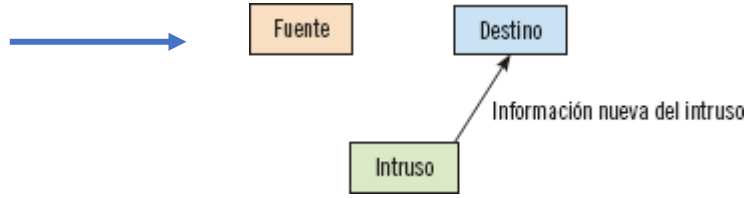

Intercepción: Usuarios no autorizados acceden a los datos del sistema. Afecta a la confidencialidad (copias de información no autorizadas, obtención de contraseñas).




Modificación: Usuarios no autorizados modifican la información contenida en los equipos. Afecta a la integridad (cambio de contenido de bases de datos, aplicaciones, datos bancarios).




Fabricación: Usuarios no autorizados falsifican la información del sistema. Afecta a la autenticidad (adición de campos, registros, virus en aplicaciones).



# Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial

Tipos de ataques. **Según la actividad del atacante:**

- Pasivos: El atacante solo escucha/monitoriza el tráfico de red (difíciles de detectar).
- Activos: El atacante modifica o crea tráfico falso.

**Tipos de ataques activos:**

- Reacción: Repetición de mensajes legítimos para producir efectos no deseados (transferencias a cuentas no autorizadas).
- Modificación de mensajes: Alteración de mensajes legítimos para confundir al receptor (modificación de cuentas bancarias).
- Suplantación de identidad (phishing): El intruso simula ser otra entidad (duplicación de páginas web bancarias).
- Degradación fraudulenta del servicio: Interrumpe el uso normal de las comunicaciones y recursos informáticos (saturación de redes).

| Clasificación de los ataques | Tipos de ataques |
|---|---|
| Ataques pasivos | Ataques de intercepción |
| Ataques activos | Ataques de interrupción |
| | Ataques de modificación |
| | Ataques de fabricación |

Así, los ataques de intercepción (o interceptación) se consideran ataques pasivos al no alterar el tráfico de red, mientras que los ataques de interrupción, modificación y fabricación son ataques activos al alterar la información que se pretende transmitir.

# Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial

## Categorización de los incidentes.

**Importancia de la categorización**

- La categorización de los incidentes es un factor clave para una recuperación rápida y completa de la actividad normal tras un incidente.
- Permite priorizar la respuesta a los incidentes en función de su impacto potencial.
- Facilita la toma de decisiones sobre la asignación de recursos y la implementación de medidas de respuesta.

**Criterios para la categorización**

- Impacto potencial: El daño que el incidente puede causar a la organización, sus activos y sus operaciones.
- Urgencia: La rapidez con la que se debe responder al incidente para evitar daños mayores.
- Probabilidad: La probabilidad de que el incidente ocurra.
- Las implicaciones legales que pueden acarrear

El impacto de un incidente no tiene que ver con su complejidad. Un incidente de lo más simple puede causar numerosos daños irreparables, siendo su nivel de impacto muy elevado.

# Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial

## Categorización de los incidentes.

**Clasificación de incidentes por impacto:**

- **Alto impacto:** Afecta considerablemente la actividad y el servicio al cliente de la organización.
- **Impacto medio:** Afecta significativamente la actividad y los servicios de la organización, o tiene un impacto potencialmente elevado.
- **Bajo impacto:** No afecta significativamente la organización, pero tiene el potencial de hacerlo.

**Incidentes de alto impacto:**

Ejemplos:

Infecciones por ransomware.
Fuga de datos confidenciales.
Ataques de denegación de servicio (DoS) a gran escala.

Respuesta:

Movilización inmediata del equipo de respuesta a incidentes.
Implementación de medidas de contención y recuperación.
Comunicación clara y transparente a los stakeholders.

**Incidentes de impacto medio:**

Ejemplos:

Intentos de intrusión no exitosos.
Robo de credenciales de bajo nivel.
Interrupciones menores del servicio.

Respuesta:

Investigación y análisis del incidente para determinar su alcance y impacto.
Implementación de medidas de mitigación y recuperación.
Comunicación a los stakeholders según sea necesario.

# Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial

## Categorización de los incidentes.

**Incidentes de bajo impacto:**

Ejemplos:

Escaneos de puertos no autorizados.
Phishing dirigido a empleados no críticos.
Errores de software sin impacto significativo.

Respuesta:

Monitoreo del incidente y análisis de su evolución.
Implementación de medidas de prevención y educación.
Notificación a los stakeholders si hay riesgo potencial de escalada.

**Consideraciones adicionales**

- El impacto de un incidente no siempre es evidente de inmediato. Es importante realizar un análisis exhaustivo para determinar su alcance total.
- La categorización de los incidentes debe ser un proceso flexible y adaptable a las necesidades específicas de cada organización.
- Es importante contar con un plan de respuesta a incidentes que defina las acciones a tomar para cada categoría de incidente.

# Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial

## Categorización de los incidentes.

**Ejemplo de categorización de incidentes**

| Impacto | Urgencia | Categoría | Ejemplo |
|---|---|---|---|
| Alto | Alta | Crítico | Ataque de ransomware que cifra todos los datos de la organización. |
| Alto | Media | Alto | Fuga de datos confidenciales de clientes. |
| Medio | Alta | Medio | Intento de intrusión en el sistema financiero de la organización. |
| Medio | Media | Medio | Robo de credenciales de un usuario con acceso limitado a información sensible. |
| Bajo | Baja | Bajo | Escaneo de puertos no autorizados en un servidor web público. |

# Criterios para la determinación de las evidencias objetivas en las que se soportará la gestión del incidente

**Importancia de las evidencias objetivas**

- Las evidencias objetivas son fundamentales para identificar la causa del incidente, determinar su alcance y tomar las medidas adecuadas para solucionarlo.
- Permiten reconstruir lo que sucedió durante el incidente y identificar las vulnerabilidades que lo permitieron.
- Son esenciales para demostrar que se ha tomado la debida diligencia en la gestión del incidente.

**Criterios para la selección de las evidencias objetivas**

- Relevancia: Las evidencias deben ser relevantes para el incidente que se está investigando.
- Fiabilidad: Las evidencias deben ser confiables y precisas.
- Suficiencia: Las evidencias deben ser suficientes para permitir una investigación completa del incidente.
- Admisibilidad: Las evidencias deben ser admisibles en un proceso legal o administrativo.

**Tipos de evidencias objetivas**

- Registros: Registros del sistema, registros de aplicaciones, registros de seguridad, etc.
- Archivos: Archivos de datos, archivos de configuración, archivos de correo electrónico, etc.
- Testimonios: Declaraciones de testigos, entrevistas con empleados, etc.
- Huellas digitales: Huellas dactilares, ADN, registros de acceso, etc.

# Criterios para la determinación de las evidencias objetivas en las que se soportará la gestión del incidente

**Recolección de evidencias objetivas**

- La recolección de evidencias debe realizarse de manera metódica y cuidadosa para evitar su alteración o destrucción.
- Se debe utilizar una cadena de custodia para documentar la recolección, manejo y almacenamiento de las evidencias.
- Se deben utilizar herramientas forenses para recuperar datos de dispositivos dañados o eliminados.

**Análisis de las evidencias objetivas**

- Las evidencias deben ser analizadas por un experto para determinar su significado e importancia.
- El análisis debe ser objetivo e imparcial.
- Los resultados del análisis deben ser documentados en un informe.

**Obtención de archivos de registro para detectar intrusiones**

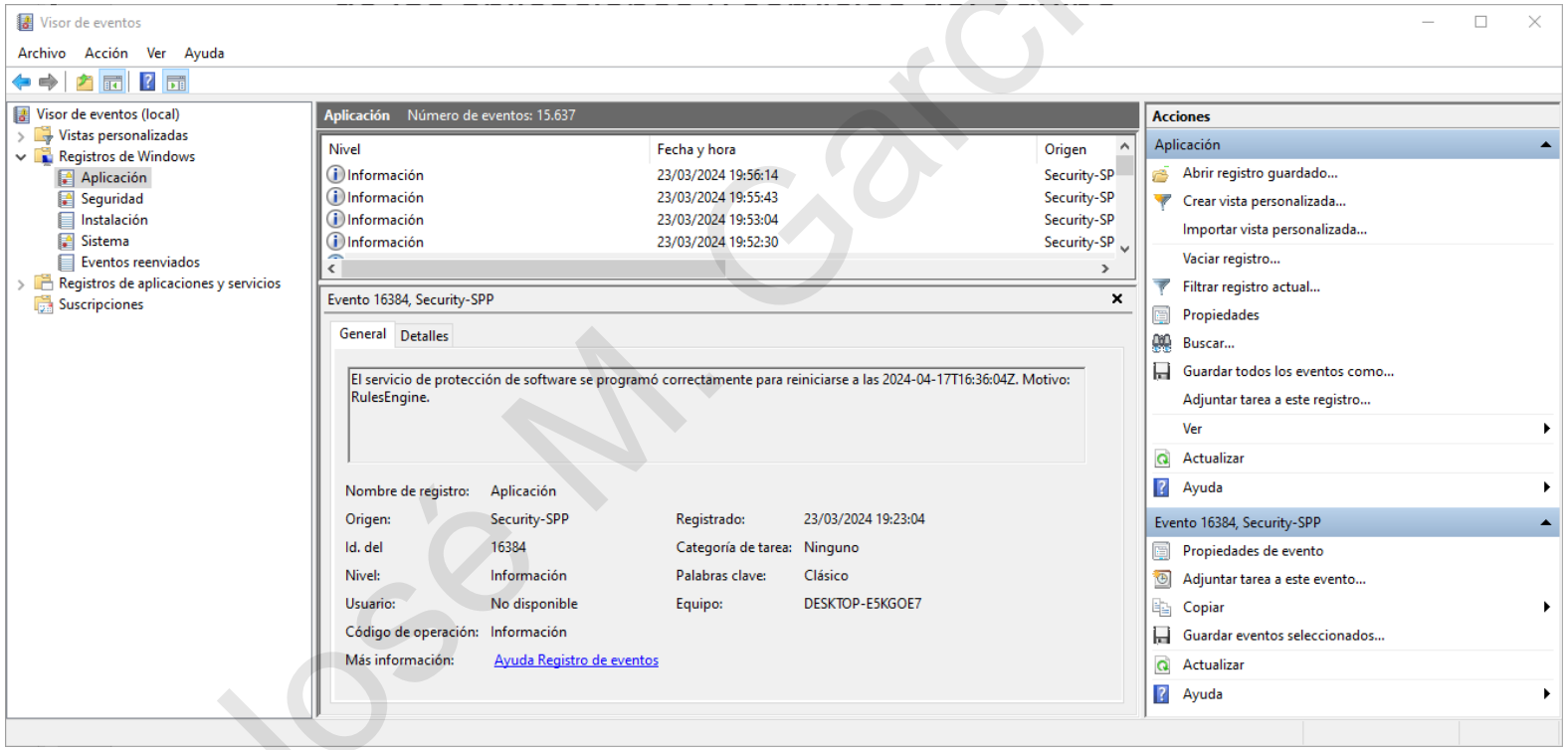
- Importancia: Los archivos de registro son una fuente crucial de información para detectar intrusiones y comprender su alcance.
- Tipos de archivos de registro:
  - Registros del sistema: Contienen información sobre eventos del sistema operativo, aplicaciones y servicios.
  - Registros de seguridad: Registran eventos relacionados con la seguridad, como inicios de sesión, intentos de acceso fallidos y actividades sospechosas.
  - Registros de aplicaciones: Registran información específica de las aplicaciones.

# Criterios para la determinación de las evidencias objetivas en las que se soportará la gestión del incidente

**Revisión de archivos de registro en Windows**

Visor de eventos: Herramienta central para revisar registros de Windows.

- Permite ver eventos del sistema, aplicaciones y servicios.
- Ofrece opciones de filtrado y búsqueda para facilitar la investigación.



# Criterios para la determinación de las evidencias objetivas en las que se soportará la gestión del incidente

**Revisión de archivos de registro en Linux**

No se dispone de interfaz gráfica que permita ver los eventos del sistema y para ello utilizamos comandos sobre archivos de registro.

Comandos:

- **tail**: Ver las últimas líneas de un archivo de registro.
- **less**: Ver un archivo de registro completo.
- **grep**: Buscar texto específico en un archivo de registro.

Archivos de registro importantes:

- **/var/log/syslog**: Mensajes generales del sistema.
- **/var/log/auth.log**: Registros de autenticación y seguridad.
- /**var/log/wtmp**: Historial de inicios y cierres de sesión.
- **/var/log/btmp**: Intentos de inicio de sesión fallidos.

Detección de evidencias en archivos adicionales

- **/etc/passwd**: Información de las claves del sistema.
- **/etc/shadow**: Información de los usuarios.
- **/etc/group**: Información sobre los grupos del sistema.

**Limitaciones de la revisión de archivos de registro**

La revisión de archivos de registro no siempre es suficiente para confirmar intrusiones.

Se requiere un análisis más profundo y exhaustivo para determinar el tipo de ataque, su alcance y las medidas a tomar.

# Criterios para la determinación de las evidencias objetivas en las que se soportará la gestión del incidente

## Criterios para la recolección de evidencas

**Sensores basados en equipo (Host Based Sensors)**

- Función: Obtener información de eventos a nivel del sistema operativo (intentos de conexión, accesos, etc.).
- Ventajas: Información de calidad, Fácil configuración, Alta precisión.
- Desventajas: Alto consumo de recursos del sistema.

**Sensores basados en aplicación (Application Based Sensors)**

- Función: Obtener información de las aplicaciones que se ejecutan en el sistema.
- Ventajas e inconvenientes: Mismos que los sensores basados en equipo.

**Sensores basados en red (Network Based Sensors)**

- Función: Recolectar información de eventos en el tráfico de datos de la red.
- Ventajas: No afectan a los recursos del equipo ni a la infraestructura de red, Mayor nivel de seguridad porque no tienen que estar instalados sobre el equipo a analizar, Información que no se puede obtener con otros sensores.
- Desventaja: Requiere mayor inversión en infraestructura.

**Soluciones híbridas (propias en los IDS/IPS)**

- Combinan las tres opciones (información de equipos, aplicaciones y red).
- Ofrecen información más completa y extensa.

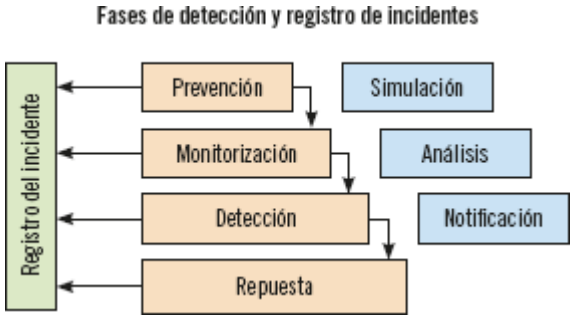
# Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones

## Detección de incidentes

Herramientas como IDS/IPS se complementan con firewall, antimalwares y herramientas de análisis de logs.

El proceso de detección conlleva:

- Recopilación de datos: Se recopilan datos de las diferentes herramientas de seguridad.
- Análisis de datos: Se analizan los datos para identificar posibles incidentes.
- Investigación: Se investiga la causa del incidente y su impacto.
- Escalada: Se informa del incidente a los responsables correspondientes.



# Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones

**Fase de Prevención de Incidentes**

La prevención es clave para evitar intrusiones e infecciones en las redes. Los sistemas de prevención de intrusiones son esenciales para esta tarea, realizando simulaciones con el tráfico de red para identificar posibles amenazas. Estas herramientas se clasifican según el modo en que detectan el tráfico malicioso.

| Método de Detección | Descripción |
|---|---|
| Basada en Firmas | Busca elementos reconocidos como intrusiones en su base de datos. |
| Basada en Políticas | Detecta intrusiones siguiendo las directrices de seguridad de la organización. |
| Basada en Anomalías | Analiza actividad inusual para detectar posibles amenazas. |
| Honey Pot o Jarra de Miel | Utiliza señuelos para desviar la atención de los intrusos. |
| **¿Cómo detectan?** | |
| Basadas en firmas | Buscan elementos reconocidos en su base de datos como intrusiones. |
| Basadas en políticas | Siguen directrices marcadas por la política de seguridad. |
| Basadas en anomalías | Buscan actividad anómala para su análisis y detección de intrusiones. |
| Honey pot o jarra de miel | Utilizan señuelos para atraer intrusiones. |

# Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones

**Fase de monitorización de Incidentes**

- Cuando, a pesar de implementar medidas preventivas, se detecta actividad inusual o sospechosa, es esencial proceder con su monitorización.
- En esta etapa, se observa el tráfico de red del sistema para analizar su comportamiento y asegurar su adecuado funcionamiento. La monitorización permite detectar intentos de intrusión y facilita la implementación de respuestas rápidas para evitar daños graves.
- Para mejorar la eficacia de esta tarea, se recomienda configurar un sistema de alertas que notifique cualquier actividad sospechosa, como procesadores sobrecargados o consumo excesivo de recursos, mediante mensajes en pantalla, correos electrónicos u otros métodos.
- La utilización de sistemas de alertas garantiza una reacción más rápida y eficaz, lo que resulta en una contención y eliminación más ágil de la intrusión, minimizando los daños ocasionados.
- Recuerde que los sistemas de detección y prevención de intrusiones (IDS/IPS) son herramientas fundamentales para monitorear los procesos y servicios de los equipos y sistemas, identificando anomalías y posibles intrusiones.

# Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones

**Fase de detección de la intrusión**

Con la monitorización del tráfico de red y de los procesos que se están ejecutando ya habrá indicios suficientes que determinarán si la actividad sospechosa es realmente una intrusión o no.

En este caso la configuración de los IDS/IPS debe realizarse por técnicos experimentados que prueben la sensibilidad de la herramienta y encuentren el punto de equilibrio entre la detección de amenazas reales y la detección de falsas alarmas.

Este punto puede ser un hándicap para las organizaciones, ya que una mayor sensibilidad evita que algunas intrusiones pasen desapercibidas, pero también detecta como posible intrusión un mayor número de falsas alarmas.

Por el contrario, una configuración de poca sensibilidad detectará pocas intrusiones que sean falsas alarmas pero, sin embargo, dejará de detectar otras intrusiones reales que pueden tener graves efectos sobre el sistema al que accedan.

Respuesta

- Los sistemas IDS, en general, no pueden combatir y eliminar la amenaza, simplemente se limitan a su detección y a la generación de alertas que permitan a los responsables la toma de medidas reactivas.
- Sin embargo, en la actualidad hay sistemas IDS más sofisticados que incluyen medidas de contingencia o cuarentena para evitar daños mayores ante la detección de intrusiones: cierre de puertos, bloqueo de tráfico de red, etc.

# Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones

## Fase de detección de la intrusión

Las respuestas que pueden generar los sistemas IDS se pueden clasificar en:

- Respuestas pasivas: Notificación a los responsables de seguridad de la intrusión o ataque detectado.
- Respuestas activas: Realización de acciones automáticas configuradas específicamente para que obtengan más información sobre el posible ataque. Otro tipo de respuestas activas también serían las medidas de contingencia o cuarentena mencionadas anteriormente como: filtrado de información en el router, cierre de sesión del sistema, bloqueo de la dirección IP del intruso, etc.

Las respuestas activas intentan bloquear la intrusión o, por lo menos, evitar en todo lo posible la propagación de los daños. Sin embargo, con las respuestas pasivas la intrusión se sigue extendiendo y produciendo daños. Estas se limitan simplemente a avisar a los administradores y responsables de seguridad.

## Registro del incidente

Esta fase del proceso de gestión de incidentes no tiene un momento temporal específico, sino que se debe producir a lo largo de todo el incidente, desde la detección previa de posibles indicios de intrusión hasta el momento en el que se restaura la situación incluyendo el momento anterior de la entrada de la intrusión.

El procedimiento de registro del incidente consiste en la generación de un archivo de registro en el que se vayan almacenando todos los detalles detectados de la intrusión y todas las acciones tomadas a cabo para su contención, erradicación y restauración del sistema.

# Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones

**Registro del incidente**

Además de toda la información relativa a la intrusión, también debe incluirse en los archivos de registro cualquier información que pueda ser relevante para la resolución del incidente. En el caso de que la intrusión pueda afectar a otros usuarios, estos deberán ser avisados para que sean conocedores de la incidencia y de las medidas a tomar en caso de detectarla.

Con un análisis profundo de los archivos de registro los analistas forenses pueden conocer con detalle cómo y por dónde ha conseguido acceder la intrusión y qué es lo que ha podido fallar en su detección y prevención.

De este modo y mediante el análisis forense de la información aportada por los archivos de registro se puede realizar un proceso de aprendizaje que culmine en el diseño de nuevas medidas que eviten que incidentes futuros parecidos a los ya sucedidos no puedan volver a acceder a los sistemas de la organización.

# Guía para la clasificación y análisis inicial del intento de intrusión o infección contemplando el impacto previsible del mismo

**Impacto previsible**

El impacto previsible de un intento de intrusión o infección es el daño potencial que puede causar al sistema o a la organización. Este daño puede ser de tipo:

- Financiero: pérdida de datos, robo de información financiera, etc.
- Reputacional: daño a la imagen de la organización, pérdida de confianza de los clientes, etc.
- Operativo: interrupción del servicio, pérdida de productividad, etc.

**Clasificación de la intrusión** en función de su naturaleza:

- Intrusiones de uso erróneo: intrusiones diseñadas para atacar los puntos débiles de un sistema. Se pueden detectar con la observación de acciones sucedidas en dicho sistema.
- Intrusiones de anomalía: intrusiones que atacan desviando las acciones de un sistema de su utilización habitual. Se pueden detectar guardando los perfiles del sistema en situaciones normales y comparándolas periódicamente para detectar alteraciones y anomalías importantes.

El modo de acceso al sistema:

- Intrusión física: el intruso accede al equipo a través de un medio físico (por ejemplo, con el teclado).
- Intrusión del sistema: el intruso utiliza una cuenta de usuario del sistema con pocos privilegios sobre la que actuará para que se le asignen otros privilegios más significativos y poder atacar en consecuencia.
- Intrusión alejada: el intruso accede al sistema con acceso remoto a través de la red.

# Guía para la clasificación y análisis inicial del intento de intrusión o infección contemplando el impacto previsible del mismo

**Análisis inicial de la intrusión**, debe incluir:

- Identificación del tipo de intrusión: ¿Qué tipo de ataque se ha producido?
- Identificación del origen de la intrusión: ¿De dónde ha provenido el ataque?
- Identificación del objetivo de la intrusión: ¿Qué se ha intentado obtener con el ataque?
- Evaluación del impacto de la intrusión: ¿Qué daño ha causado el ataque?
- Definición de las medidas de respuesta: ¿Qué medidas se deben tomar para responder al ataque?

| Clasificación | Tipo |
|---|---|
| Según su naturaleza | Intrusiones de uso erróneo |
| | Intrusiones de anomalía |
| Según el modo de acceso al sistema | Intrusión física |
| | Intrusión del sistema |
| | Intrusión alejada |

# Guía para la clasificación y análisis inicial del intento de intrusión o infección contemplando el impacto previsible del mismo

## Clasificación de los intentos de intrusión según su impacto

**Tipos de intrusiones en atención al impacto sobre los activos:**

- Intentos de entrada: Impacto alto. El atacante busca acceso no autorizado y obtener privilegios apropiados. Puede dañar el sistema.
- Ataques enmascarados: Impacto medio. El atacante utiliza un usuario ya registrado con menos privilegios. El impacto puede ser igual o mayor que otras intrusiones si el atacante accede como administrador.
- Penetraciones en el sistema de control: Impacto alto. El atacante busca alterar las herramientas de control del sistema.
    - Internas: Se producen desde el mismo sistema.
    - Externas: Proceden de otro equipo o de la red.
- Fuga: Impacto bajo. El atacante busca saturar el sistema para impedir su funcionamiento normal. El impacto puede conllevar costes por la pérdida de calidad del servicio, pero no se elimina información.
- Denegación de servicio: Impacto bajo. El atacante busca limitar o impedir el acceso a los recursos y servicios de la organización. Lo habitual es que estos ataques se lleven a cabo para dañar la imagen y reputación de las organizaciones al impedir que los clientes puedan acceder a ellas y que estas no puedan ofrecer sus servicios con facilidad. Su prevención es dificultosa.
- Uso malicioso: Impacto variable. Depende del tipo de malware utilizado. Se suele detectar por los modelos de comportamiento atípico del sistema o de alguna aplicación o proceso concreto. El impacto será distinto: desde saturación de servidores, borrado de datos, aparición de ventanas molestas, observación de actividad, envío de spam, etc.

# Establecimiento del nivel de intervención requerido en función del impacto previsible

El impacto previsible de una intrusión se determina por los efectos negativos producidos o potenciales y la criticidad de los recursos afectados.

**Clasificación de los incidentes según su nivel de criticidad**

Los efectos negativos y la criticidad de los recursos determinan el nivel de criticidad del incidente.

**Niveles de criticidad:**

- Crítico. Intrusiones con impacto muy significativo en la confidencialidad, disponibilidad o integridad de datos críticos. Suelen afectar a servicios esenciales, recursos críticos y pueden provocar pérdidas irrecuperables de información crítica.
- Muy Alto. Intrusiones con impacto considerable en recursos críticos, amenazando la integridad, disponibilidad y confidencialidad de datos. Requieren contención y resolución laboriosa.
- Alto. Impacto considerable en recursos no críticos. Afectan a sistemas limitados sin información relevante. Suelen afectar en exclusiva a un equipo.
- Medio. Impacto limitado en recursos no críticos. Las organizaciones deben tener capacidad para combatir estas intrusiones sin recurrir a agentes externos. No es necesario reportar estos incidentes, si bien es recomendable la elaboración de informes periódicos para llevar un control y comprobar la efectivad de las salvaguardas.
- Bajo. Impacto nulo o insignificante. Son detectadas y erradicadas por sistemas de seguridad.

Cuanto más nivel de criticidad tenga el intento de intrusión o infección, menos deberá tardarse en su notificación y menor deberá ser el tiempo de respuesta para la toma de medidas y su erradicación.

# Establecimiento del nivel de intervención requerido en función del impacto previsible

## Nivel de Intervención en Función del Impacto y Criticidad de la Intrusión

Es esencial reaccionar adecuadamente ante una intrusión confirmada, considerando su criticidad. Cada intrusión debe registrarse y gestionarse según los recursos afectados y su impacto: a mayor criticidad, menor tiempo desde la detección hasta el registro.

- Intrusiones Críticas: Notificar en una hora.
- Nivel Muy Alto: Notificar en 12 horas.
- Nivel Alto: Notificar en 24-48 horas.
- Nivel Medio: Notificar dentro de una semana.
- Nivel Bajo: Notificar en un mes.

**Intervención para la Contención y Erradicación**

Las organizaciones deben establecer tiempos "objetivo" máximos para contener y erradicar intrusiones, manteniendo la restauración del sistema. Aunque son objetivos, se pueden exceder en circunstancias justificadas.

Además la correcta clasificación de las intrusiones es fundamental, ya que retrasos en la respuesta pueden tener consecuencias graves para la organización

# Establecimiento del nivel de intervención requerido en función del impacto previsible

## Nivel de Intervención en Función del Impacto y Criticidad de la Intrusión

**Tiempos máximos de contención y erradicación**

| Nivel de Criticidad | Plazo Máximo de Contención | Plazo Máximo de Erradicación |
|---|---|---|
| Crítico | 8 horas | 24 horas |
| Muy Alto | 48 horas | 72 horas |
| Alto | 4 días naturales | 14 días naturales |
| Medio | 1 mes | 1 mes |
| Bajo | 3 meses | 3 meses |

# Guía para la investigación y diagnóstico del incidente de intento de intrusión o infecciones

## Introducción

Al sospechar de una intrusión, es crucial evaluar si es una amenaza real, si ha tenido éxito y el nivel de compromiso del sistema.

**Consideraciones Iniciales:**

- Identificar la Amenaza: Determinar si se trata de un ataque exitoso o fallido y evaluar los daños y el nivel de compromiso del sistema afectado.
- Usuarios Internos como Amenaza: No subestimar la posibilidad de ataques de "insiders", tanto actuales como ex empleados. Mantener un estricto control sobre las cuentas de usuario inactivas es esencial para la seguridad.

**Procedimiento de Investigación:**

- Visualizar Usuarios Logueados: Identificar quiénes están usando el sistema, las aplicaciones en uso y su actividad temporal. Comportamientos inusuales pueden indicar posibles causantes del incidente.
- Examinar Procesos Activos: Observar la actividad de los procesos en ejecución, prestando atención a aquellos que llevan mucho tiempo activos, inician en horas no habituales, consumen recursos excesivos o no son ejecutados desde una terminal.

Estas medidas son cruciales mientras el intruso permanece en el sistema. Una vez que salga, se requerirá utilizar otras técnicas para rastrear posibles huellas dejadas.

La detección temprana y la respuesta eficiente son fundamentales para mitigar el impacto de los intentos de intrusión. Además, mantener un monitoreo continuo de usuarios y procesos puede prevenir futuros incidentes y fortalecer la seguridad informática organizacional.

# Guía para la investigación y diagnóstico del incidente de intento de intrusión o infecciones

## Investigación y diagnóstico de una incidencia ya ocurrida

Cuando surge una incidencia en el sistema a pesar del control ejercido sobre usuarios y procesos, es esencial realizar una investigación exhaustiva para identificar posibles intrusiones. **Se deben seguir los siguientes pasos**:

- Examen de archivos de registro o logs: Analizar registros para detectar actividades inusuales o conexiones a lugares poco frecuentes
- Comprobación de permisos del sistema: Verificar que los usuarios tienen permisos adecuados, evitando asignar privilegios de administrador a usuarios sin necesidad
- Chequeo de archivos binarios: Revisar archivos binarios en busca de alteraciones que puedan indicar intrusiones.
- Comprobación de puertos abiertos: Identificar puertos abiertos no autorizados que podrían indicar intrusiones pasadas
- Comprobar la existencia de sniffers: Detectar la presencia de sniffers no autorizados para monitorear el tráfico de red
- Comprobar servicios no autorizados: Verificar la existencia de servicios activos no autorizados en el sistema
- Comprobar contraseñas del sistema: Revisar todas las contraseñas para detectar cambios no autorizados
- Comprobar la configuración del sistema y de la red: Examinar los archivos de configuración en busca de accesos no autorizados
- Buscar archivos ocultos o poco habituales: Investigar archivos ocultos donde los intrusos podrían esconderse
- Examinar equipos de la red local: No limitarse al equipo afectado inicialmente, sino examinar todos los dispositivos de la red para identificar posibles expansiones del ataque

Este enfoque sistemático permite detectar intrusiones pasadas y prevenir futuros ataques, fortaleciendo así la seguridad de la organización.

# Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección

## Introducción

Una vez confirmado y diagnosticado un incidente de seguridad derivado de un intento de intrusión o infección, es crucial iniciar el proceso de resolución y recuperación para restaurar los sistemas a su estado previo.

## Proceso de resolución y recuperación de incidentes

### Contención del incidente

En esta fase inicial, se debe desarrollar una estrategia para contener el incidente y evitar su propagación. Esto implica tomar medidas rápidas para minimizar los riesgos y daños al sistema. Se pueden desconectar equipos de la red o desactivar servicios para evitar daños mayores. Sin embargo, en ocasiones, retrasar la contención puede ser beneficioso para recopilar más detalles sobre la incidencia y recoger evidencias para acciones legales

### Medidas de erradicación

Una vez contenido el incidente, se procede a su eliminación. Se realizan actividades para asegurar que el incidente ya no está presente en los equipos y recursos afectados. Esto implica buscar y eliminar archivos introducidos por el intruso, revisar servicios y procesos afectados, y asegurar la erradicación completa de la intrusión en toda la red

### Recuperación

Una vez confirmada la eliminación del incidente, se inicia la fase de recuperación. Esto implica restaurar los sistemas a su funcionamiento habitual mediante la utilización de copias de respaldo para reinstalar el sistema operativo y las aplicaciones. Además, se recomienda actualizar las medidas de seguridad y definir nuevas contraseñas para minimizar el riesgo de futuras intrusiones.

# Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección

## El Plan de Recuperación Ante Desastres

En el ámbito empresarial, se aconseja la implementación de un Plan de Recuperación Ante Desastres (DRP, por sus siglas en inglés) para establecer los procedimientos de recuperación de información en caso de incidentes y desastres.

El término "desastre" en el contexto de la tecnología de la información abarca cualquier causa, natural, intencionada o involuntaria, que afecte la infraestructura de una organización (datos, aplicaciones, hardware) y detenga su actividad.

**Este plan se desarrolla con una serie de objetivos:**

- Identificar y prevenir vulnerabilidades que puedan interrumpir el servicio.
- Evaluar el impacto financiero, de imagen y otras consecuencias de la interrupción.
- Determinar las necesidades inmediatas y a largo plazo de recuperación.
- Seleccionar las alternativas más rentables para la copia de seguridad y restauración.
- Establecer planes de contingencia para medidas inmediatas y a largo plazo.

Un DRP de calidad minimiza el tiempo de inactividad y la pérdida de datos. Se debe realizar un análisis de impacto en el negocio para priorizar las etapas de recuperación según la criticidad de los recursos y la clasificación de riesgos.

# Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección

## El Plan de Recuperación Ante Desastres

**La estructura mínima del plan incluye:**

- Plan de trabajo para la recuperación de la información.
- Informes de evaluación de seguridad y vulnerabilidad.
- Análisis de impacto en el negocio.
- Definición de requisitos, objetivos y responsables.
- Programa de pruebas y mantenimiento.

Es crucial actualizar periódicamente el plan para adaptarse a cambios organizativos y tecnológicos.

La correcta implementación de un DRP ofrece numerosos beneficios, como la reducción de daños, protección de sistemas críticos y minimización de interrupciones, responsabilidades legales y garantía de la fiabilidad de los sistemas reserva.

Con estos planes, las organizaciones pueden recuperar su actividad sin pérdidas graves de información en caso de desastre.

# Proceso para la comunicación del incidente a terceros, si procede

Cuando se logra controlar un incidente y restaurar la situación inicial, se debe considerar la comunicación de los hechos a terceros no relacionados con la organización. El plan de respuesta a incidentes debe incluir aspectos clave sobre esta comunicación, detallando los efectos, causas y posibles consecuencias de la incidencia.

**Proceso con implicación de terceros:**

Asesoramiento: Se aconseja buscar la opinión de profesionales especializados para evaluar las acciones tomadas y mejorar en futuros incidentes

Proveedores: Es crucial informar a los proveedores sobre fallos en las herramientas de detección y prevención de incidentes para mejorar su eficacia. Además, se debe evaluar la posibilidad de cambiar de proveedor si es necesario.

Comunicación a Terceros: Se debe comunicar a terceros afectados por la incidencia, como proveedores o clientes, las acciones tomadas y las posibles repercusiones para colaborar en la recuperación de la situación original.

Fabricantes de Software y Hardware: Informar a los fabricantes sobre los daños causados por la incidencia y evaluar posibles vulnerabilidades en sus productos.

Comunicación a Terceros Perjudicados: Evaluar los daños a terceros y comunicarles la situación para que tomen medidas de seguridad adicionales.

Comunidad General: En casos graves, comunicar a la comunidad los incidentes y sus consecuencias a través de medios de comunicación para evitar especulaciones innecesarias.

Fuerzas de Seguridad y Organismos de Respuesta: Informar a las autoridades competentes y mantener contacto con organismos de respuesta a incidentes para evaluar y combatir la incidencia de manera efectiva.

La comunicación efectiva con terceros es esencial para mitigar los impactos de los incidentes y restaurar la confianza en la seguridad de la organización.

# Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

Durante todo el ciclo de vida del incidente hay que elaborar y mantener un registro sobre todas las acciones que se van tomando y su evolución para que los agentes encargados de la solución y los usuarios afectados dispongan de información actualizada sobre el estado del incidente.

Cuando ya se ha solucionado hay que llevar a cabo una serie de acciones que permitan cerrar el incidente:

- Comprobación con los usuarios de la resolución del incidente.
- Incorporación de las acciones y medidas a la base de datos del histórico.
- Reclasificación del incidente como resuelto o cerrado.
- Actualización de la información de las configuraciones del sistema.
- Cierre del incidente.

Registro y documentación del incidente. Se debe realizar a lo largo de toda su gestión. Se recomienda realizar revisiones periódicas que actualicen el registro.

Resuelto y cerrado el incidente se deben elaborar informes, aportan información básica:

- Gestión de los niveles de servicio: Informar a los clientes sobre los servicios y su nivel de cumplimiento.
- Monitorización del rendimiento del centro de servicios: Encuestas y entrevistas a los clientes para conocer su nivel de satisfacción.
- Optimización de la asignación de recursos: Evaluar el proceso de gestión del incidente para evitar duplicidades.
- Identificación de los errores: Adoptar medidas correctivas para que no se repitan en el futuro.
- Disposición de información estadística: Incluir información estadística sobre la organización (consumo de recursos, costes del servicio, tiempo de respuesta, etc.).

# Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

Además de la realización del informe se recomienda la utilización de métricas e indicadores que sirvan de guía de comparación con futuras actuaciones para un correcto seguimiento del incidente. Los principales aspectos a considerar son los siguientes:

- Cantidad de incidentes clasificados temporalmente y por prioridades.
- Ratio en porcentaje de los incidentes resueltos en una primera instancia.
- Nivel de cumplimiento de la oferta de servicios a clientes.
- Costes asociados a la aparición y resolución de la incidencia.
- Recursos utilizados para la resolución de la incidencia.
- Nivel de satisfacción de los clientes.
- Tiempos de respuesta y resolución según el impacto y la urgencia de los incidentes.

Los incidentes graves con daños significativos deben contener un registro más profundo y detallado.

# Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

## Soporte de incidentes

El soporte de incidentes abarca desde su detección hasta su cierre, con una serie de pasos para un control adecuado:

**Reporte del incidente:**

- Comunicación inmediata de las sospechas de incidente a los responsables.
- Se puede realizar por correo electrónico, teléfono, personalmente o cualquier otro medio de comunicación establecido.

**Registro y documentación:**

- El responsable de la gestión del incidente identifica el tipo de incidente y lo clasifica según su prioridad.
- Se registra toda la información del incidente y se documenta de forma detallada.

**Preparación de la solución:**

- Se asigna un tiempo máximo de respuesta, contención y resolución.
- Se consulta la base de datos de incidentes antiguos para buscar soluciones similares.

**Aplicación de soluciones con software de apoyo:**

- Se envían alertas y notificaciones a los usuarios responsables de la resolución.
- Se realizan tareas internas para completar y apoyar las medidas de resolución.
- Se comunica periódicamente el avance en la resolución a los usuarios implicados.

# Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

## Soporte de incidentes

**Identificación y solución de problemas:**

- Se comprueba el histórico de incidencias para detectar causas comunes.
- Se toman medidas para evitar incidencias futuras y mejorar la seguridad de la organización.

**Cierre del incidente con éxito:**

- Se comunica el cierre del incidente a los usuarios afectados.
- Se incluyen las soluciones aplicadas en la base de datos de incidentes para futuras referencias.

Es importante que las organizaciones aprendan de las acciones tomadas y de los errores cometidos para mejorar la gestión de incidentes en el futuro.

# Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

## Soporte de incidentes

| Pasos de soporte de incidentes | Descripción |
|---|---|
| Reporte del incidente | Comunicación de las sospechas de incidente a los responsables. |
| Registro y documentación | Obtención de información adicional y clasificación de la incidencia. |
| Preparación de la solución | Asignación de tiempos máximos de contención y respuesta. |
| Aplicación de soluciones mediante software de apoyo | Remisión a los interesados de información referente a la evolución del incidente. |
| Identificación y solución de problemas | Búsqueda de causa común con incidentes anteriores. |
| Cierre del incidente con éxito | Comunicación del cierre exitoso del incidente a todos los interesados. |

# Resumen

Las intrusiones son accesos no autorizados al sistema. Las organizaciones deben establecer herramientas y controles para prevenirlas.

**Si se detecta una posible intrusión:**

- Recopilar información adicional para verificar la amenaza.
- Si la amenaza es real:
  - Analizar la incidencia y clasificarla según su criticidad e impacto.
  - Definir tiempos máximos de contención y resolución.
  - Tomar medidas correctivas y resolver la incidencia.
- Valorar la posibilidad de comunicar la incidencia a terceros.
- Registrar toda la información sobre la incidencia, las medidas tomadas, los errores cometidos y sus soluciones.

Un correcto registro permite a las organizaciones aprender de las acciones tomadas y evitar nuevos incidentes similares.