3. Protección de la información almacenada.

La **protección de la información almacenada** se centra en garantizar que los datos mantengan su **confidencialidad, integridad y disponibilidad** a lo largo del tiempo, con independencia del soporte en el que residan y del entorno en el que se utilicen. A diferencia de otras capas de seguridad, aquí el foco no está en el sistema en ejecución, sino en **los datos en reposo**, que continúan existiendo incluso cuando los equipos están apagados o desconectados.

Proteger la información almacenada implica anticiparse a incidentes frecuentes —pérdidas, robos, accesos indebidos, fallos técnicos— y aplicar **controles proporcionales al valor y sensibilidad de los datos**. Un mismo dispositivo puede albergar información de muy distinta criticidad; por ello, la protección debe diseñarse a partir del análisis del riesgo y no de supuestos genéricos.

Recuerda

La información más sensible suele ser la que permanece almacenada durante más tiempo y la que se copia, mueve o reutiliza con mayor frecuencia.

3.1. Riesgos sobre la información almacenada.

La información almacenada está expuesta a una variedad de **riesgos específicos** que no siempre se manifiestan de forma inmediata. Muchos de ellos actúan de manera silenciosa, acumulativa o indirecta, y se descubren cuando la recuperación ya es compleja o imposible.

- **Riesgos de acceso no autorizado.** Uno de los riesgos más críticos es el **acceso indebido** a los datos almacenados. Puede producirse por:
  - Dispositivos perdidos o robados sin protección.
  - Permisos excesivos o mal configurados.
  - Credenciales comprometidas.
  - Almacenamientos compartidos sin control.
  - Accesos físicos a los soportes.

Este riesgo afecta directamente a la **confidencialidad** y suele tener consecuencias legales y reputacionales, especialmente cuando se trata de datos personales o sensibles.

Nota

El acceso no autorizado no siempre implica un ataque externo; con frecuencia se produce dentro del propio entorno por errores de configuración o uso.

- **Riesgos de pérdida de información.** La **pérdida de datos** puede tener causas muy diversas:
  - Fallos físicos de los dispositivos.

  - Errores humanos (borrados accidentales).
  - Incidentes eléctricos o ambientales.
  - Fallos durante traslados o migraciones.
  - Uso de soportes inadecuados o degradados.

Este riesgo compromete la **disponibilidad** de la información y, en muchos casos, la continuidad de la actividad.

- **Riesgos de alteración o corrupción de datos.** La **integridad** de los datos puede verse afectada por:
  - Fallos del sistema de archivos.
  - Apagados bruscos.
  - Errores de escritura.
  - Malware.
  - Manipulación intencionada.

La alteración de datos es especialmente peligrosa cuando pasa desapercibida, ya que puede conducir a decisiones erróneas basadas en información incorrecta.

- **Riesgos derivados de la portabilidad y la replicación.** La facilidad para copiar y mover información incrementa el riesgo:
  - Dispositivos USB sin control.
  - Copias no autorizadas.
  - Envío de datos a ubicaciones inseguras.
  - Almacenamiento duplicado sin protección coherente.

Cuantas más copias existen, **mayor es la superficie de exposición** y más complejo resulta aplicar medidas homogéneas de protección.

- **Riesgos a medio y largo plazo.** Existen riesgos que no se manifiestan de inmediato:
  - Obsolescencia de soportes.
  - Degradación de dispositivos.
  - Pérdida de compatibilidad.
  - Falta de documentación sobre los datos almacenados.

Estos riesgos afectan a la **recuperabilidad futura** de la información, incluso aunque esté aparentemente protegida en el presente.

Esta tabla relaciona **tipos de riesgo con su impacto principal**, facilitando la identificación de prioridades de protección:

Riesgo identificado	Impacto principal
Acceso no autorizado	Confidencialidad
Pérdida de datos	Disponibilidad
Alteración de información	Integridad
Replicación descontrolada	Exposición
Obsolescencia	Recuperabilidad

Recuerda

Identificar los riesgos es el paso previo imprescindible para elegir las medidas de protección adecuadas.

3.2. Cifrado de discos y dispositivos.

El **cifrado de discos y dispositivos** es una de las medidas más eficaces para proteger la información almacenada frente a accesos no autorizados. Su función principal es **hacer ininteligible la información** para cualquier persona que no disponga de las credenciales o claves adecuadas, incluso aunque tenga acceso físico al dispositivo.

Desde el punto de vista de la seguridad, el cifrado transforma incidentes potencialmente críticos —como la pérdida o el robo de un equipo— en **incidentes de impacto limitado**.

Dispositivo de almacenamiento cifrado que requiere autenticación para acceder a la información almacenada.

El cifrado consiste en aplicar un **algoritmo matemático** que transforma los datos originales en un formato ilegible. Solo mediante una **clave de cifrado** es posible revertir este proceso y acceder a la información.

En el caso del almacenamiento, el cifrado puede aplicarse:

- A **discos completos**.
- A **particiones concretas**.
- A **dispositivos extraíbles**.
- A **archivos o contenedores específicos**.

El cifrado suele ser transparente para el usuario una vez autenticado, pero actúa de forma automática cuando el dispositivo está apagado o desconectado.

Cifrado de disco completo

El **cifrado de disco completo** protege todo el contenido del dispositivo, incluyendo:

- Sistema operativo.
- Archivos de usuario.
- Archivos temporales.
- Espacio libre.

Esta modalidad es especialmente recomendable en:

- Portátiles.
- Equipos utilizados fuera de entornos controlados.
- Dispositivos con información sensible.
- Sistemas expuestos a robo o pérdida.

Nota

El cifrado de disco completo protege los datos cuando el sistema no está en uso; no sustituye al control de accesos durante la sesión activa.

Cifrado de dispositivos extraíbles

Los **dispositivos extraíbles** presentan un riesgo elevado por su facilidad de pérdida. El cifrado en estos soportes es una medida clave para:

- Proteger la información transportada.
- Cumplir requisitos normativos.
- Reducir el impacto de extravíos.
- Permitir el uso seguro en distintos entornos.

El cifrado puede implementarse mediante:

- Software de cifrado.
- Dispositivos con cifrado hardware integrado.
- Contenedores cifrados dentro del dispositivo.

Gestión de claves y contraseñas

La eficacia del cifrado depende directamente de la **gestión de las claves**:

- Uso de contraseñas robustas.
- Almacenamiento seguro de claves de recuperación.
- Procedimientos claros ante pérdida de credenciales.
- Separación entre usuario y clave de cifrado cuando sea posible.

Una mala gestión de claves puede inutilizar los datos incluso para los usuarios legítimos.

Esta tabla explica el uso recomendado de cada modalidad de cifrado:

Modalidad de cifrado	Uso recomendado
Disco completo	Equipos portátiles y de trabajo
Partición cifrada	Datos sensibles específicos
Dispositivo extraíble	Transporte de información
Contenedor cifrado	Compartición controlada

3.3. Cifrado de archivos y carpetas.

El **cifrado de archivos y carpetas** es una medida de protección selectiva que permite **asegurar información concreta** sin necesidad de cifrar todo el dispositivo. A diferencia del cifrado de disco completo, esta modalidad resulta especialmente útil cuando solo una parte de los datos requiere un nivel de protección elevado o cuando se trabaja en entornos compartidos donde no todos los usuarios deben acceder a la misma información.

El cifrado a nivel de archivo o carpeta aporta **flexibilidad**, pero exige mayor disciplina en su uso y en la gestión de claves, ya que la protección deja de ser global y pasa a depender de decisiones más finas y conscientes.

Este tipo de cifrado resulta especialmente apropiado en escenarios como:

- Equipos compartidos por varios usuarios.
- Carpetas con información sensible dentro de sistemas más amplios.
- Necesidad de compartir datos de forma controlada.
- Protección adicional sobre datos críticos ya almacenados.

En estos casos, el cifrado selectivo permite **limitar el acceso incluso dentro del propio sistema**, reduciendo la exposición innecesaria.


Nota

Cifrar solo lo necesario reduce el impacto en la usabilidad, pero incrementa la importancia de una buena organización y gestión de claves.

El cifrado de archivos y carpetas se aplica de forma explícita sobre los elementos seleccionados. Solo quienes disponen de las credenciales adecuadas pueden acceder a su contenido, aunque el resto del sistema sea accesible.

Entre sus características principales se encuentran:

- Protección granular de la información.
- Posibilidad de compartir claves o credenciales de forma controlada.
- Dependencia directa del sistema operativo o de herramientas específicas.
- Necesidad de copias de seguridad compatibles con el cifrado.

Un aspecto crítico es garantizar que las **copias de seguridad preserven el cifrado** o se realicen de forma segura, evitando copias en claro de información sensible.

El uso incorrecto de esta modalidad puede introducir nuevos riesgos:

- Pérdida de acceso por olvido de claves.
- Cifrado parcial que deja información sensible expuesta.
- Dificultad para recuperar datos en situaciones de emergencia.
- Dependencia excesiva de una sola persona usuaria.

Se introduce a continuación una tabla que relaciona **uso del cifrado de archivos con beneficios y riesgos**, facilitando la toma de decisiones:

Uso del cifrado selectivo	Beneficio principal	Riesgo asociado
Carpetas sensibles	Acceso restringido	Pérdida de claves
Archivos concretos	Protección puntual	Olvidos de cifrado
Compartición cifrada	Control del acceso	Gestión compleja
Protección adicional	Defensa en profundidad	Dependencia del usuario

El cifrado selectivo es eficaz solo si se integra en una **política clara y conocida** por quienes lo utilizan.

3.4. Protección frente a accesos no autorizados.

La **protección frente a accesos no autorizados** es un objetivo central de la seguridad de la información almacenada. No basta con cifrar los datos: es necesario **controlar de forma activa quién puede acceder a ellos, en qué condiciones y desde qué entornos**. Muchos incidentes no se producen por ataques externos sofisticados, sino por accesos indebidos facilitados por configuraciones laxas o prácticas inadecuadas.

La protección eficaz combina **medidas técnicas, organizativas y de uso**, aplicadas de forma coherente.

Control de accesos y autenticación

El primer nivel de protección frente a accesos no autorizados es la **autenticación**, que permite verificar la identidad de la persona usuaria. Este control debe ser adecuado al valor de la información protegida.

Entre las medidas habituales se encuentran:

- Autenticación individual y no compartida.
- Contraseñas robustas y únicas.
- Uso de autenticación multifactor cuando sea posible.
- Bloqueo tras intentos fallidos repetidos.

La autenticación debe complementarse con una **gestión correcta de sesiones**, evitando accesos persistentes innecesarios.

Autorización y permisos efectivos

Una vez autenticado, el sistema debe controlar **qué puede hacer cada usuario**. Esto se logra mediante permisos bien definidos y revisados periódicamente.

Una protección eficaz implica:

- Aplicar el principio de mínimo privilegio.
- Evitar permisos globales o heredados sin revisión.
- Revisar accesos tras cambios de función.
- Retirar accesos obsoletos.

Nota

La mayoría de accesos indebidos internos se producen porque nadie retiró permisos que ya no eran necesarios.

Protección frente a accesos físicos a los soportes

El acceso no autorizado no siempre se produce a través del sistema en funcionamiento. El acceso físico a los dispositivos puede permitir:

- Extracción de discos.
- Lectura de datos sin pasar por el sistema operativo.
- Copia masiva de información.

Por ello, las medidas de control de accesos deben complementarse con:

- Cifrado de discos y dispositivos.
- Custodia física de soportes.
- Control de acceso a salas y equipos.

Para aportar una visión operativa, se presenta a continuación una tabla que relaciona **medidas de control con el riesgo que mitigan**, aportando criterios prácticos:

Medida aplicada	Riesgo mitigado
Autenticación individual	Uso indebido
Permisos restrictivos	Acceso excesivo
Cifrado	Lectura no autorizada
Bloqueo de sesión	Accesos accidentales
Revisión periódica	Privilegios obsoletos

Recuerda

Proteger la información no consiste solo en impedir el acceso externo, sino en controlar correctamente el acceso legítimo.

3.5. Buenas prácticas en el uso de dispositivos extraíbles.

Los **dispositivos extraíbles** representan uno de los vectores de riesgo más frecuentes en la protección de la información almacenada. Su facilidad de uso y portabilidad los convierte en herramientas útiles, pero también en **puntos críticos de exposición** si no se gestionan adecuadamente.

Las buenas prácticas en su uso buscan **reducir riesgos sin eliminar su utilidad**, estableciendo normas claras y hábitos responsables.

Entre los riesgos más habituales se encuentran:

- Pérdida o robo del dispositivo.
- Acceso no autorizado a la información.
- Introducción de malware en el sistema.
- Uso en equipos no confiables.
- Copias no controladas de datos sensibles.

Estos riesgos se agravan cuando los dispositivos se utilizan sin cifrado ni control.

Las buenas prácticas recomendadas incluyen:

- Cifrar siempre los dispositivos con información sensible.

- Utilizar dispositivos corporativos o controlados.
- Evitar el uso en equipos públicos o desconocidos.
- Desconectar el dispositivo cuando no se esté usando.
- Almacenar los dispositivos en lugares seguros.

Nota

Un dispositivo extraíble sin cifrar debe considerarse información expuesta en potencia.

Además de las medidas técnicas, es esencial establecer **normas claras de uso**, especialmente en entornos compartidos:

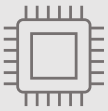
- Definir qué información puede copiarse.
- Registrar el uso de dispositivos cuando sea necesario.
- Prohibir dispositivos personales en determinados contextos.
- Informar sobre riesgos y responsabilidades.

La concienciación reduce significativamente los incidentes derivados de errores humanos.

Esta tabla relaciona **prácticas habituales con su impacto en la seguridad**, aportando criterios claros de actuación:

Práctica	**Impacto en la seguridad**
Uso sin cifrado	Riesgo elevado
Uso cifrado	Riesgo reducido
Dispositivos controlados	Mayor trazabilidad
Uso en equipos públicos	Riesgo crítico
Custodia segura	Prevención de pérdidas

La seguridad de los dispositivos extraíbles depende menos de la tecnología y más de **cómo se utilizan en la práctica diaria**.



Actividad 7

Describe tres riesgos físicos que pueden afectar a una sala técnica mal protegida y propón una medida preventiva para cada uno.

4. Gestión segura de soportes de almacenamiento.

La **gestión segura de los soportes de almacenamiento** aborda el conjunto de **medidas técnicas, organizativas y de uso** destinadas a minimizar los riesgos asociados a dispositivos que pueden **extraerse, transportarse o reutilizarse** con facilidad. Estos soportes —especialmente memorias USB y discos externos— concentran un riesgo elevado porque combinan **portabilidad, capacidad y facilidad de conexión** a múltiples sistemas.

Una gestión segura no pretende eliminar su uso, sino **encuadrarlo dentro de normas claras y controles proporcionales** al valor de la información. Cuando estos dispositivos se utilizan sin reglas ni seguimiento, se convierten en uno de los vectores más frecuentes de fugas de información y de introducción de software malicioso.

Recuerda

El riesgo de un soporte extraíble no está en el dispositivo en sí, sino en su capacidad de moverse fuera del entorno controlado.

4.1. Uso seguro de memorias USB y discos externos.

Las **memorias USB y los discos externos** son herramientas habituales para el transporte de datos, copias de seguridad puntuales y ampliación de almacenamiento. Su uso seguro requiere combinar **medidas técnicas básicas con hábitos responsables**, ya que gran parte de los incidentes asociados a estos dispositivos se producen por descuidos o prácticas rutinarias inadecuadas.

Dispositivo de almacenamiento externo con mecanismos de protección mediante autenticación para un uso seguro de datos transportables.

El uso cotidiano de estos dispositivos implica riesgos bien definidos:

- **Pérdida o robo** durante desplazamientos.
- **Acceso no autorizado** a la información almacenada.
- **Introducción de malware** al conectarlos a distintos equipos.
- **Uso en sistemas no confiables**.
- **Copias no controladas** de información sensible.

Estos riesgos aumentan cuando el dispositivo carece de cifrado o se utiliza de forma indistinta en entornos personales y profesionales.

Para reducir estos riesgos, es imprescindible aplicar una serie de medidas técnicas mínimas:

- **Cifrado del dispositivo completo**, especialmente si contiene información sensible.
- Uso de contraseñas robustas o mecanismos de autenticación integrados.
- Desactivación de la ejecución automática de contenidos.
- Análisis del dispositivo antes de su uso, cuando sea posible.
- Extracción segura para evitar corrupción de datos.

Estas medidas convierten un soporte potencialmente inseguro en una herramienta controlada.

La seguridad también depende del **comportamiento del usuario**. Entre las buenas prácticas recomendadas se encuentran:

- No dejar dispositivos desatendidos en espacios públicos.
- Evitar su uso en equipos ajenos o públicos.
- Guardarlos en lugares seguros cuando no se utilicen.
- No reutilizarlos sin revisión previa.
- Limitar la información almacenada a la estrictamente necesaria.

Esta tabla sintetiza las **formas habituales de uso y su impacto en la seguridad**, ayudando a identificar conductas de riesgo:

Forma de uso	Nivel de riesgo
Dispositivo cifrado y custodiado	Bajo
Uso ocasional sin cifrado	Medio
Uso frecuente en equipos ajenos	Alto
Transporte sin control	Crítico

4.2. Control de dispositivos extraíbles en entornos corporativos.

En **entornos corporativos**, educativos o institucionales, el control de los dispositivos extraíbles adquiere una dimensión adicional. No se trata solo de proteger la información individual, sino de **preservar la seguridad global del sistema**, evitando que un único dispositivo comprometa múltiples equipos o datos compartidos.

La ausencia de control sobre los dispositivos extraíbles en entornos compartidos puede dar lugar a:

- Fugas masivas de información.
- Infecciones de malware propagadas internamente.
- Pérdida de trazabilidad sobre los datos.
- Incumplimientos normativos.

Por ello, resulta imprescindible establecer **criterios comunes y verificables** sobre su uso.

El control puede aplicarse mediante configuraciones y herramientas que permitan:

- Autorizar o bloquear el uso de dispositivos extraíbles.
- Permitir solo dispositivos identificados o cifrados.
- Restringir tipos de dispositivos o funciones (lectura/escritura).
- Registrar conexiones y transferencias.
- Integrar el control con sistemas de seguridad del endpoint.

Estas medidas reducen la dependencia del comportamiento individual y aportan **coherencia y trazabilidad**.

El control técnico debe apoyarse en **normas claras de uso**, conocidas por todas las personas usuarias:

- Definir cuándo está permitido el uso de dispositivos extraíbles.
- Establecer responsabilidades sobre su custodia.
- Regular la transferencia de información sensible.
- Prohibir el uso de dispositivos personales en determinados contextos.
- Establecer procedimientos ante incidentes o pérdidas.

Recuerda

Sin normas claras, incluso las mejores herramientas técnicas pierden eficacia.

El control no debe percibirse como una restricción arbitraria, sino como una **medida de protección colectiva**. La concienciación ayuda a:

- Reducir resistencias al control.
- Mejorar el cumplimiento de las normas.
- Detectar usos indebidos de forma temprana.
- Integrar la seguridad en la cultura organizativa.

Para visualizar el impacto del control en entornos corporativos, se presenta a continuación una tabla que relaciona **grado de control aplicado con el riesgo resultante**:

Nivel de control	**Riesgo residual**
Sin control	Muy alto
Normas sin control técnico	Alto
Control técnico básico	Medio
Control técnico y organizativo	Bajo

En entornos corporativos, un solo dispositivo sin control puede comprometer **mucho más que un solo equipo**.

4.3. Riesgos de pérdida y robo de información.

La **pérdida y el robo de información** constituyen dos de los incidentes más graves asociados a la gestión de soportes de almacenamiento, especialmente cuando estos son **extraíbles o portátiles**. A diferencia de otros riesgos, sus consecuencias no dependen únicamente del valor económico del soporte, sino del **valor intrínseco de los datos** que contiene y de la facilidad con la que pueden ser explotados por terceros.

Estos riesgos no se limitan a escenarios de ataque deliberado. Con frecuencia se producen por **descuidos, prácticas rutinarias inseguras o falta de control**, lo que los convierte en una amenaza persistente y difícil de erradicar sin medidas estructurales.

Pérdida de información: causas habituales

La pérdida de información puede producirse incluso sin intervención maliciosa. Entre las causas más frecuentes se encuentran:

- Extravío de dispositivos extraíbles durante desplazamientos.
- Daños físicos en soportes (golpes, humedad, calor).
- Borrados accidentales.
- Uso de dispositivos defectuosos o degradados.
- Falta de copias de seguridad actualizadas.

En estos casos, la información puede desaparecer sin posibilidad de recuperación, afectando directamente a la **disponibilidad** y, en muchos contextos, a la continuidad del servicio.

Robo de información y explotación de los datos

El **robo de información** implica un riesgo adicional: la posible **explotación de los datos por terceros**. Cuando un soporte es sustraído, el impacto depende de factores como:

- Existencia o no de cifrado.
- Tipo de información almacenada.
- Nivel de acceso que proporcionan los datos.
- Capacidad de identificar a personas, sistemas o procesos.

Un soporte robado sin protección puede dar lugar a:

- Fugas de datos personales.
- Accesos indebidos a sistemas.
- Suplantación de identidad.
- Incumplimientos legales y sanciones.


Nota

El impacto real de un robo no se mide por el dispositivo perdido, sino por lo que permite hacer la información contenida en él.

Riesgos indirectos asociados

Además de la pérdida directa de datos, existen riesgos indirectos:

- Daño reputacional.
- Pérdida de confianza de clientes o usuarios.
- Interrupción de proyectos o procesos.
- Costes de notificación y mitigación.
- Investigación interna y responsabilidades disciplinarias.

Esta tabla vincula el **nivel de protección del soporte con las consecuencias previsibles**:

Nivel de protección	Consecuencia habitual
Sin cifrado ni control	Fuga grave de información
Cifrado sin control de uso	Impacto limitado
Cifrado y control de accesos	Incidente material
Cifrado, control y backups	Recuperación viable


Recuerda

La diferencia entre un incidente crítico y uno asumible suele estar en las medidas aplicadas antes de que ocurra.

4.4. Políticas de uso de soportes extraíbles.

Las **políticas de uso de soportes extraíbles** establecen el marco normativo interno que regula **quién puede usar estos dispositivos, en qué condiciones y con qué finalidad**. Su función principal es reducir la dependencia del criterio individual y asegurar una **gestión coherente del riesgo** en todo el entorno.

Sin una política definida, el uso de soportes extraíbles queda expuesto a decisiones improvisadas, lo que incrementa significativamente la probabilidad de incidentes.

Una política bien diseñada persigue varios objetivos:

- Proteger la información sensible.
- Reducir la superficie de exposición.

- Establecer responsabilidades claras.
- Facilitar el cumplimiento normativo.
- Unificar criterios técnicos y organizativos.

Estas políticas no deben entenderse como restricciones arbitrarias, sino como **herramientas de protección colectiva**.

Para que sea operativa, una política de uso de soportes extraíbles debe definir, al menos:

- Qué tipos de dispositivos están permitidos.
- En qué situaciones se autoriza su uso.
- Qué información puede almacenarse.
- Requisitos de cifrado y protección.
- Procedimientos de alta, uso y retirada.
- Actuación ante pérdidas o incidentes.

Por otra parte, las políticas deben adaptarse al **tipo de entorno**:

- En entornos educativos, puede priorizarse la concienciación.
- En entornos corporativos, el control técnico.
- En entornos críticos, la prohibición casi total salvo excepciones justificadas.

La rigidez excesiva puede generar incumplimientos informales; la laxitud, incidentes previsibles.

Para aportar una visión operativa, se presenta a continuación una tabla que relaciona **elementos de la política con el riesgo que ayudan a reducir**:

Elemento de la política	Riesgo mitigado
Dispositivos autorizados	Uso de soportes inseguros
Cifrado obligatorio	Fuga de información
Restricción de contenidos	Exposición innecesaria
Procedimiento ante pérdida	Impacto descontrolado
Responsables definidos	Falta de trazabilidad

4.5. Registro y control de accesos al almacenamiento.

El **registro y control de accesos al almacenamiento** permite conocer **quién accede a la información, cuándo y qué acciones realiza**. Esta capacidad es fundamental no solo para prevenir incidentes, sino también para **detectarlos, investigarlos y demostrar diligencia** en la gestión de la seguridad.

Sin registros adecuados, la seguridad se vuelve opaca: los incidentes pueden producirse sin dejar rastro claro, dificultando la respuesta y la mejora posterior.

El registro de accesos cumple varias funciones esenciales:

- Detección de comportamientos anómalos.
- Investigación de incidentes.
- Verificación del cumplimiento de políticas.
- Identificación de usos indebidos.
- Soporte en auditorías y revisiones.

No se trata de vigilar indiscriminadamente, sino de **disponer de información objetiva** cuando es necesaria.

Un sistema de registro eficaz debe contemplar:

- Accesos a información sensible.
- Intentos de acceso fallidos.
- Cambios de permisos.
- Conexión de dispositivos de almacenamiento.
- Transferencias relevantes de datos.

Recuerda

El nivel de detalle debe ser proporcional al riesgo y al volumen de información gestionada.

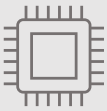
Además del registro, el **control de accesos** actúa de forma preventiva:

- Limita quién puede acceder al almacenamiento.
- Restringe acciones según rol o perfil.
- Impide accesos fuera de contexto.
- Reduce el impacto de credenciales comprometidas.

El control y el registro deben funcionar de forma coordinada para ser realmente eficaces.

Para mostrar cómo el control y el registro influyen en la capacidad de respuesta ante incidentes, se presenta a continuación una tabla que relaciona **nivel de control con efecto operativo**, aportando criterios claros de gestión:

Nivel de control y registro	Capacidad de respuesta
Sin registro	Nula
Registro básico	Investigación limitada
Registro y control selectivo	Detección eficaz
Registro avanzado y auditoría	Respuesta y mejora continua



Actividad 8

En una organización que dispone de zonas con distinto nivel de criticidad (oficinas, aulas técnicas y sala de servidores), se plantea implantar un sistema de control de accesos mediante tarjetas electrónicas para regular la entrada del personal.

Indica:

Dos ventajas de este sistema desde el punto de vista de la seguridad física.

Una limitación o riesgo asociado a su uso.

5. Borrado y destrucción segura de datos.

El **borrado y la destrucción segura de datos** constituyen la fase final del ciclo de vida de la información y de los soportes de almacenamiento. Aunque a menudo se perciben como tareas secundarias, son **críticas para la seguridad**, ya que muchos incidentes graves se producen cuando dispositivos supuestamente "vacíos" conservan información recuperable.

Eliminar datos de forma segura no significa simplemente borrar archivos o formatear un dispositivo. Implica **asegurar que la información no pueda ser recuperada**, ni por usuarios legítimos ni por terceros, incluso utilizando herramientas especializadas. Esta fase es especialmente relevante cuando los soportes se reutilizan, se ceden, se venden, se reciclan o se desechan.

Recuerda

La información no deja de existir cuando deja de utilizarse; deja de existir cuando no puede recuperarse.

5.1. Importancia del borrado seguro de la información.

La **importancia del borrado seguro** reside en que los sistemas operativos y los sistemas de archivos no eliminan los datos de forma inmediata cuando se realiza un borrado convencional. En la mayoría de los casos, lo que se elimina es la **referencia al archivo**, no su contenido real en el soporte.

Esto significa que:

- Los datos pueden recuperarse con herramientas de análisis.
- La información permanece accesible durante un tiempo indeterminado.
- El soporte puede contener restos de datos antiguos.
- El riesgo persiste incluso tras un formateo rápido.

El borrado seguro resulta crítico en situaciones como:

- Reutilización de equipos dentro de la organización.
- Cesión o devolución de dispositivos.
- Venta de equipos usados.
- Reciclaje de soportes defectuosos.
- Baja de equipos al finalizar su vida útil.
- Sustitución de discos por avería o actualización.

En todos estos casos, un borrado convencional es **claramente insuficiente**.

Nota

Muchos casos de fuga de información proceden de discos vendidos o reciclados sin borrado seguro previo.

La falta de un borrado seguro puede tener consecuencias graves:

- Exposición de datos personales o confidenciales.
- Acceso indebido a información histórica.
- Incumplimientos legales y sanciones.
- Daño reputacional.
- Pérdida de confianza de clientes o usuarios.

Estas consecuencias pueden producirse **mucho tiempo después** de haber dejado de usar el dispositivo, lo que dificulta la detección y la atribución del incidente.

Para comprender el impacto real de las distintas prácticas de borrado, se presenta a continuación una tabla que relaciona **acción realizada con el nivel de protección obtenido**:

Acción realizada	Nivel de protección
Borrado de archivos	Muy bajo
Formateo rápido	Bajo
Formateo completo	Medio
Borrado seguro	Alto
Destrucción física	Máximo

Recuerda

El borrado seguro no es una opción avanzada: es una exigencia básica cuando la información ha tenido valor.

5.2. Métodos de borrado lógico.

Los **métodos de borrado lógico** consisten en técnicas que sobrescriben o eliminan la información de un soporte **sin destruir físicamente el dispositivo**, permitiendo su reutilización posterior. Estos métodos son especialmente adecuados cuando los soportes siguen siendo funcionales y se desea mantenerlos en uso.

Borrado por sobrescritura de datos

La **sobrescritura** consiste en escribir nuevos datos sobre las áreas del soporte donde se encontraba la información original. Este proceso dificulta o impide la recuperación mediante herramientas convencionales.

Características principales:

- Puede realizarse en una o varias pasadas.
- Es aplicable a discos mecánicos y, con limitaciones, a SSD.
- Permite reutilizar el soporte tras el proceso.
- Requiere tiempo proporcional al tamaño del dispositivo.

La sobrescritura múltiple incrementa la seguridad, aunque también el tiempo necesario.

Borrado seguro mediante herramientas específicas

Existen herramientas diseñadas específicamente para realizar **borrados seguros**, que:

- Identifican todas las áreas del soporte.
- Gestionan sectores ocultos o reasignados.
- Verifican el resultado del borrado.
- Generan registros del proceso.

Estas herramientas permiten aplicar políticas homogéneas y documentables, especialmente en entornos profesionales.

Nota

Un borrado sin verificación final no garantiza que la información haya sido realmente eliminada.

Borrado lógico en unidades de estado sólido (SSD)

En los **SSD**, el borrado lógico presenta particularidades debido a su funcionamiento interno:

- La sobrescritura tradicional puede no afectar a todas las celdas.
- El sistema gestiona internamente la ubicación de los datos.
- Existen comandos específicos de borrado seguro (*secure erase*).

Por ello, en SSD es fundamental utilizar **métodos compatibles con su tecnología**, recomendados por el fabricante o el sistema operativo.

Unidad de estado sólido (SSD), cuyo funcionamiento interno condiciona los métodos de borrado lógico aplicables.

Aunque eficaz en muchos escenarios, el borrado lógico tiene limitaciones:

- No siempre garantiza la eliminación total en dispositivos dañados.
- Puede ser insuficiente para información extremadamente sensible.
- Depende de la correcta ejecución del proceso.
- Requiere confianza en las herramientas utilizadas.

En casos de alta criticidad, puede ser necesario recurrir a **métodos de destrucción física**, que se abordarán en el epígrafe siguiente.

Esta tabla vincula el **método de borrado lógico con su uso recomendado**, aportando criterios de decisión:

Método	Uso recomendado
Sobrescritura simple	Reutilización interna
Sobrescritura múltiple	Cesión controlada
Herramientas certificadas	Entornos profesionales
Secure erase en SSD	Reutilización de SSD

5.3. Sobrescritura y herramientas de eliminación segura.

La **sobrescritura** y el uso de **herramientas de eliminación segura** constituyen los métodos más habituales y controlables para garantizar que la información almacenada **no pueda ser recuperada** cuando un soporte va a reutilizarse o a salir del entorno habitual. Estas técnicas se basan en un principio sencillo: sustituir los datos originales por otros irrelevantes hasta que la recuperación resulte inviable.

A diferencia del borrado convencional, estos métodos permiten **documentar el proceso**, verificar su correcta ejecución y aplicar criterios homogéneos en distintos dispositivos.

La sobrescritura consiste en escribir nuevos patrones de datos sobre los sectores donde se encontraba la información original. Su eficacia depende de:

- El tipo de soporte.
- El número de pasadas.
- El estado del dispositivo.
- La tecnología de almacenamiento utilizada.

En discos mecánicos tradicionales, la sobrescritura bien ejecutada ofrece un **nivel de protección elevado** frente a la recuperación mediante herramientas convencionales.

Nota

La sobrescritura no "borra" archivos: borra la posibilidad práctica de reconstruirlos.

Número de pasadas y nivel de seguridad

Durante años se promovieron esquemas de múltiples pasadas como garantía absoluta. En la práctica actual:

- Una sobrescritura completa bien ejecutada suele ser suficiente para la mayoría de escenarios.
- Pasadas adicionales incrementan la seguridad marginalmente, pero aumentan el tiempo.
- La elección debe basarse en la **sensibilidad de la información**, no en automatismos.

Herramientas de eliminación segura

Las herramientas de eliminación segura automatizan y verifican el proceso de borrado. Su uso aporta ventajas claras:

- Identificación de todo el espacio direccionable.
- Gestión de sectores ocultos o reasignados.
- Verificación posterior del borrado.
- Generación de informes o registros.
- Aplicación repetible de políticas internas.

En entornos profesionales, estas herramientas permiten **demostrar diligencia** y trazabilidad en la eliminación de datos.

Particularidades en unidades SSD

En unidades SSD, la sobrescritura clásica puede no afectar a todas las celdas físicas debido a la gestión interna del almacenamiento. Por ello:

- Deben utilizarse comandos específicos de borrado seguro compatibles con SSD.
- Es recomendable seguir las directrices del fabricante.
- La verificación cobra especial importancia.

Para orientar la elección práctica, se presenta a continuación una tabla que relaciona **método aplicado con su idoneidad**:

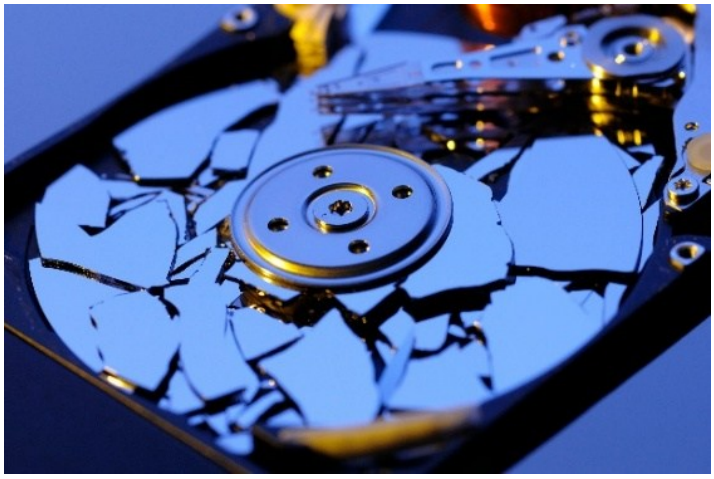
Método de eliminación	Escenario adecuado
Sobrescritura simple	Reutilización interna
Sobrescritura verificada	Cesión controlada
Herramientas certificadas	Entornos regulados
Secure erase SSD	Reutilización de SSD

Recuerda

La eliminación segura no termina cuando el proceso finaliza, sino cuando se verifica y se documenta.

5.4. Destrucción física de soportes.

La **destrucción física de soportes** es el método más contundente para garantizar la eliminación definitiva de la información. Se utiliza cuando la sensibilidad de los datos o el estado del dispositivo **no permiten confiar en métodos lógicos**.



Este enfoque elimina cualquier posibilidad razonable de recuperación, incluso mediante técnicas avanzadas.

Disco duro mecánico con los platos destruidos, ejemplo de eliminación definitiva de la información mediante destrucción física del soporte.

La destrucción física se considera adecuada en situaciones como:

- Información extremadamente sensible.
- Soportes defectuosos o inestables.
- Incumplimiento del borrado lógico.
- Final de vida útil sin reutilización prevista.
- Requisitos normativos estrictos.

Recuerda

En estos casos, preservar el soporte carece de sentido frente al riesgo potencial.

Entre los métodos más utilizados se encuentran:

- Triturado industrial.
- Perforación y fragmentación.
- Desmagnetización (en soportes magnéticos).
- Destrucción térmica controlada.

Cada método tiene implicaciones distintas en términos de coste, trazabilidad y gestión ambiental.

Nota

La destrucción improvisada o doméstica rara vez garantiza la eliminación completa de la información.

En entornos profesionales, la destrucción física debe:

- Realizarse por personal autorizado o empresas especializadas.
- Documentarse mediante registros o certificados.
- Asociarse a inventarios de activos.
- Integrarse en el ciclo de vida del hardware.

Esta trazabilidad es clave para **auditorías y cumplimiento normativo**.

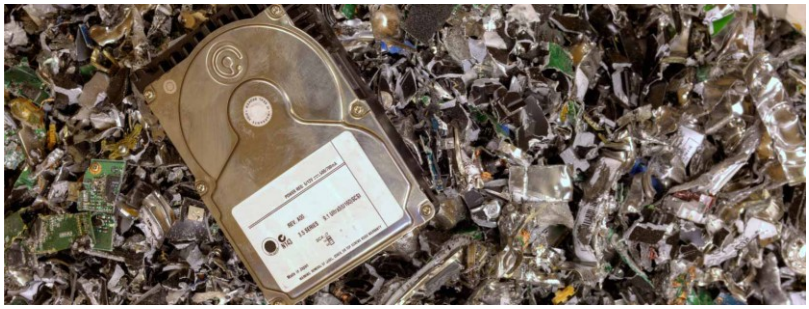
En función de la criticidad de la información se sintetiza, a continuación, el método recomendado:

Criticidad de los datos	Método recomendado
Media	Borrado lógico verificado
Alta	Borrado lógico + control
Muy alta	Destrucción física
Irrecuperable	Destrucción inmediata

Recuerda

Cuando el riesgo de recuperación es inaceptable, la destrucción física no es exagerada: es proporcional.

5.5. Gestión responsable del reciclaje de dispositivos.



La **gestión responsable del reciclaje de dispositivos** cierra el ciclo de vida del hardware integrando **seguridad de la información y protección ambiental**. Un reciclaje incorrecto puede anular todas las medidas de seguridad aplicadas previamente y generar impactos negativos tanto legales como ecológicos.

Cuando el reciclaje se realiza sin control, pueden producirse:

- Recuperación de datos por terceros.
- Pérdida de trazabilidad de los dispositivos.
- Incumplimientos legales.
- Daños reputacionales.
- Impacto ambiental innecesario.

El reciclaje debe considerarse una **fase de seguridad**, no solo de gestión de residuos.

Una gestión responsable del reciclaje implica:

- Borrado o destrucción previa de los datos.
- Selección de gestores autorizados.
- Documentación del proceso.
- Separación adecuada de componentes.
- Cumplimiento de la normativa ambiental vigente.

Recuerda

Reciclar sin eliminar datos equivale a entregar información a terceros sin control.

El reciclaje debe integrarse en los procedimientos habituales:

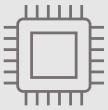
- Actualización del inventario.
- Registro de la retirada del dispositivo.
- Asociación del método de eliminación de datos aplicado.
- Archivo de certificados o evidencias.

Esta integración permite cerrar el ciclo de vida del dispositivo de forma **ordenada, segura y responsable**.

Las prácticas de reciclaje tienen efectos directos:

Práctica aplicada	Efecto principal
Borrado previo	Eliminación del riesgo de fuga
Gestor autorizado	Cumplimiento legal
Documentación	Trazabilidad
Reciclaje selectivo	Protección ambiental

Un dispositivo solo deja de ser un riesgo cuando **sus datos han sido eliminados y su destino está controlado**.



Actividad 9

Relaciona cada situación con su riesgo principal:

- Portátil sin anclaje en aula compartida
- Equipo con ventiladores obstruidos
- Dispositivo sin inventariar

6. Resumen.

La gestión de los dispositivos de almacenamiento constituye un eje central de la seguridad informática, ya que es en estos soportes donde la información reside de forma persistente y, por tanto, donde permanece expuesta incluso cuando los sistemas no están en funcionamiento. La protección del almacenamiento no depende únicamente del tipo de dispositivo utilizado, sino del conjunto de decisiones técnicas, organizativas y de uso que determinan cómo se guardan, acceden, trasladan y eliminan los datos. Una gestión deficiente convierte al almacenamiento en uno de los puntos más vulnerables del sistema, independientemente del nivel de seguridad aplicado en otras capas.

Los sistemas de almacenamiento y los sistemas de archivos desempeñan un papel clave en la organización y protección de la información. A través de ellos se establecen estructuras lógicas, se controlan accesos, se asignan permisos y se preserva la integridad de los datos. La elección del sistema de archivos y la correcta organización del almacenamiento permiten aplicar el principio de mínimo privilegio, reducir errores humanos y facilitar tanto las copias de seguridad como la recuperación ante incidentes. Sin una estructura clara y permisos bien definidos, la información queda expuesta a accesos indebidos y pérdidas accidentales.

La protección de la información almacenada exige identificar los riesgos asociados —pérdida, robo, acceso no autorizado, alteración y obsolescencia— y aplicar medidas proporcionales a la sensibilidad de los datos. El cifrado de discos, dispositivos, archivos y carpetas se configura como una de las herramientas más eficaces para proteger los datos en reposo, especialmente en entornos donde existe portabilidad o acceso físico al soporte. No obstante, el cifrado debe complementarse con controles de acceso, gestión adecuada de credenciales y políticas claras de uso para ser realmente efectivo.

Los soportes extraíbles representan un riesgo especialmente elevado debido a su facilidad de transporte y conexión a múltiples sistemas. Su uso seguro requiere combinar medidas técnicas, como el cifrado y el control de dispositivos, con normas organizativas y concienciación de las personas usuarias. En entornos corporativos, el control centralizado y el registro de accesos al almacenamiento resultan esenciales para reducir la superficie de exposición, garantizar la trazabilidad y responder de forma eficaz ante incidentes.

Finalmente, la eliminación segura de la información cierra el ciclo de vida del almacenamiento y es tan crítica como su protección durante el uso. El borrado lógico verificado, la sobrescritura adecuada o, cuando es necesario, la destrucción física de los soportes evitan que datos aparentemente eliminados puedan ser recuperados. Integrar estos procesos en una gestión responsable del reciclaje permite proteger la información, cumplir con las obligaciones legales y reducir el impacto ambiental, consolidando una visión completa y coherente de la seguridad del almacenamiento.

7. Prueba de autoevaluación.

1. ¿Por qué los dispositivos de almacenamiento son un objetivo prioritario desde el punto de vista de la seguridad informática?

a) Porque determinan el rendimiento del sistema

b) Porque mantienen la información incluso cuando los equipos están apagados

c) Porque requieren mayor mantenimiento técnico

d) Porque solo se utilizan en entornos corporativos

2. ¿Cuál es uno de los riesgos específicos asociados al almacenamiento externo frente al almacenamiento local?

a) Menor velocidad de acceso a los datos

b) Mayor consumo energético

c) Mayor dificultad para cifrar la información

d) Mayor riesgo de pérdida o robo por su portabilidad

3. ¿Qué característica de los sistemas de archivos como NTFS, ext4 o APFS aporta una mejora directa en la seguridad?

a) Alta compatibilidad entre sistemas operativos

b) Ausencia de estructura jerárquica

c) Permisos avanzados y registro de transacciones

d) Menor consumo de espacio en disco

4. ¿Cuál es la principal limitación de sistemas de archivos como FAT32 o exFAT desde el punto de vista de la seguridad?

a) Su bajo rendimiento

b) La falta de permisos avanzados y registro de transacciones

c) La imposibilidad de realizar copias de seguridad

d) Su incompatibilidad con dispositivos externos

5. ¿Qué medida resulta más eficaz para proteger la información almacenada en caso de pérdida o robo de un dispositivo?

a) Incrementar la frecuencia de copias de seguridad

b) Limitar el uso de dispositivos portátiles

c) Aplicar cifrado de discos o dispositivos

d) Utilizar únicamente almacenamiento local

6. ¿Qué riesgo se incrementa cuando existen múltiples copias no controladas de la misma información?

a) Pérdida de rendimiento del sistema

b) Aumento de la superficie de exposición de los datos

c) Dificultad para clasificar la información

d) Reducción de la disponibilidad

7. ¿Cuál es una buena práctica recomendada para el uso seguro de dispositivos extraíbles?

a) Usarlos solo en equipos públicos

b) Mantenerlos conectados permanentemente

c) Evitar cualquier tipo de cifrado

d) Cifrar los dispositivos que contengan información sensible

8. ¿Qué ventaja aporta una organización lógica adecuada del almacenamiento?

a) Incrementa automáticamente la capacidad del sistema

b) Elimina la necesidad de permisos de acceso

c) Reduce errores humanos y facilita el control de la información

d) Sustituye la necesidad de copias de seguridad

9. ¿Cuál es la principal finalidad de la eliminación segura de los datos al final del ciclo de vida de un soporte de almacenamiento?

a) Reducir el tamaño del inventario

b) Mejorar la reutilización del hardware

c) Cumplir únicamente criterios medioambientales

d) Evitar la recuperación de datos por terceros

10. ¿Por qué una copia de seguridad que no se ha probado periódicamente carece de valor real?

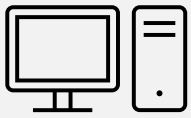
a) Porque ocupa espacio innecesario

b) Porque puede ralentizar el sistema

c) Porque no garantiza que la información pueda restaurarse

d) Porque no protege frente a accesos no autorizados

Unidad 3



Aplicación de medidas de seguridad activa

La seguridad activa se orienta a la **detección, prevención y respuesta** ante amenazas que actúan sobre los sistemas informáticos de forma continua. A diferencia de la seguridad pasiva, este enfoque implica una actuación dinámica, capaz de adaptarse a un entorno cambiante en el que las amenazas evolucionan constantemente.

En esta unidad se aborda la seguridad activa como un conjunto de mecanismos y herramientas diseñados para **identificar comportamientos anómalos, bloquear ataques y gestionar incidentes** de manera eficaz. La seguridad activa se entiende no como una solución aislada, sino como un componente integrado dentro de una estrategia global de protección, en la que la vigilancia y la respuesta rápida resultan esenciales.

1. Introducción a la seguridad activa.

La **seguridad activa** representa la dimensión **dinámica y reactiva** de la seguridad informática. Mientras que la seguridad pasiva se orienta a reducir vulnerabilidades estructurales y prevenir incidentes, la seguridad activa asume una realidad fundamental: **no todas las amenazas pueden evitarse**, y algunas lograrán atravesar las barreras preventivas. Su función, por tanto, es **detectar, bloquear, contener y responder** ante eventos de seguridad en tiempo real o casi real.

En los entornos actuales, caracterizados por una conectividad permanente, sistemas expuestos a Internet, trabajo remoto y amenazas automatizadas, la seguridad activa deja de ser una capa opcional para convertirse en un **componente imprescindible**. No se limita a "instalar herramientas", sino que implica un **modelo de vigilancia continua**, análisis de comportamiento y capacidad de reacción organizada.

Desde una perspectiva profesional, la seguridad activa introduce una lógica distinta a la pasiva: ya no se trata solo de "hacer las cosas bien", sino de **observar lo que ocurre**, interpretar señales, discriminar entre eventos normales y anómalos, y actuar con rapidez para limitar el impacto.


Nota

La seguridad activa no sustituye a la pasiva: la compensa cuando esta falla o resulta insuficiente frente a amenazas cambiantes.

Un sistema sin seguridad activa puede estar correctamente configurado y, aun así, **ser comprometido sin que nadie lo detecte**. Por el contrario, un sistema con seguridad activa mal diseñada puede generar alertas constantes sin aportar protección real. La clave está en el **equilibrio entre detección, respuesta y control del ruido**.

1.1. Concepto de seguridad activa.

La **seguridad activa** se define como el conjunto de **medidas, mecanismos y procedimientos** que permiten **detectar comportamientos anómalos o maliciosos**, **bloquear acciones no autorizadas** y **responder ante incidentes de seguridad** mientras estos se producen o inmediatamente después de su inicio.

A diferencia de la seguridad pasiva, que actúa principalmente **antes** del incidente, la seguridad activa interviene **durante y después**, cuando el riesgo ya se ha materializado o está en proceso de hacerlo.

Desde un punto de vista funcional, la seguridad activa cumple tres grandes funciones interrelacionadas:

- **Detección**: identificar eventos anómalos, patrones sospechosos o actividades no esperadas.
- **Respuesta**: bloquear, aislar o mitigar el evento detectado.
- **Aprendizaje**: registrar lo ocurrido para mejorar los controles futuros.

Este enfoque convierte la seguridad en un **proceso vivo**, no en un estado estático.

En términos operativos, la seguridad activa permite responder a situaciones como:

- ejecución de malware desconocido,

- intentos de acceso reiterados o anómalos,
- comportamientos fuera del patrón habitual de un usuario,
- tráfico de red sospechoso,
- modificaciones no autorizadas en el sistema.

Lo relevante no es solo la amenaza externa, sino también los **incidentes internos**, ya sean errores humanos, usos indebidos o fallos de configuración que generan comportamientos anómalos.

Recuerda

La seguridad activa no se centra solo en "ataques", sino en desviaciones del comportamiento esperado.

Desde el punto de vista de los tipos de control, la seguridad activa se sitúa principalmente en los **controles detectivos y correctivos**, aunque puede incorporar elementos preventivos dinámicos.

Para aportar un criterio operativo claro, la siguiente tabla relaciona **función de la seguridad activa con su efecto real**, ayudando a distinguirla de otros enfoques:

Función de la seguridad activa	Efecto operativo
Detección de anomalías	Visibilidad del incidente
Bloqueo automático	Reducción del impacto
Alerta al personal	Activación de respuesta
Registro del evento	Análisis posterior
Ajuste de reglas	Mejora continua

Esta lógica explica por qué la seguridad activa requiere **supervisión**, **criterios de ajuste** y, en muchos casos, **intervención humana cualificada**.

1.2. Diferencias entre seguridad pasiva y activa.

Aunque seguridad pasiva y seguridad activa persiguen el mismo objetivo —proteger los sistemas y la información—, lo hacen desde **enfoques claramente distintos**. Comprender esta diferencia es esencial para evitar errores habituales, como confiar excesivamente en herramientas reactivas para compensar un diseño deficiente, o asumir que una buena configuración inicial elimina la necesidad de vigilancia.

Nota

La diferencia fundamental no está en la tecnología utilizada, sino en el momento y la lógica de actuación.

La seguridad pasiva se orienta a **reducir la probabilidad** de que ocurra un incidente. La seguridad activa se orienta a **reducir el tiempo y el impacto** cuando el incidente ya está ocurriendo.

Dicho de otro modo:

- la seguridad pasiva intenta que el incidente **no llegue a producirse**;
- la seguridad activa asume que **alguno se producirá** y se prepara para gestionarlo.

En la práctica diaria, ambas implican tareas muy distintas:

- la seguridad pasiva se trabaja principalmente en fases de diseño, configuración y mantenimiento;
- la seguridad activa exige observación continua, análisis de eventos y capacidad de respuesta.

Esto explica por qué la seguridad activa suele introducir **alertas, logs, reglas dinámicas y decisiones en tiempo real**, mientras que la pasiva se apoya en configuraciones estables.

Otra diferencia clave es el papel del factor humano:

- una seguridad pasiva bien diseñada puede funcionar durante largos periodos con poca intervención;
- la seguridad activa requiere supervisión, interpretación y ajuste, especialmente para evitar falsos positivos o puntos ciegos.

Nota

Un sistema que genera alertas constantemente sin capacidad de análisis termina siendo ignorado, lo que equivale a no tener seguridad activa.

La siguiente tabla aporta **criterios prácticos de decisión**, útiles para entender qué esperar de cada enfoque en un entorno real:

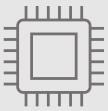
Criterio	Seguridad pasiva	Seguridad activa
Momento de actuación	Antes del incidente	Durante / después
Objetivo principal	Reducir vulnerabilidades	Detectar y responder
Tipo de control	Preventivo	Detectivo y correctivo
Dependencia humana	Baja si está bien diseñada	Media-alta
Ejemplos típicos	Hardening, cifrado, backups	Antivirus, firewall, IDS, EDR
Riesgo si falla	Sistema frágil	Incidente no detectado

Complementariedad real, no sustitución

Un error frecuente es pensar que una capa puede compensar la ausencia de la otra. En realidad:

- la seguridad pasiva sin activa genera sistemas **ciegos**;
- la seguridad activa sin pasiva genera sistemas **ruidosos y frágiles**.

La seguridad activa **no corrige un mal diseño**, y la seguridad pasiva **no detecta lo que ya está ocurriendo**.



Actividad 10

En un sistema informático se registran los siguientes eventos observados durante una jornada de trabajo:

- Se detectan múltiples intentos de inicio de sesión fallidos desde una misma dirección IP en un intervalo corto de tiempo.

- Un proceso desconocido intenta ejecutarse y acceder a archivos del sistema.

- Un usuario legítimo accede al sistema fuera de su horario habitual y descarga un volumen elevado de información.

- Se registra tráfico de red saliente hacia un destino no habitual tras la apertura de un archivo adjunto.

- El sistema genera un registro detallado del evento y ajusta automáticamente una regla de bloqueo.

Clasifica cada evento según la función de la seguridad activa implicada y describe la acción esperable del sistema, atendiendo a la lógica de detección, respuesta y aprendizaje.

1.3. Amenazas actuales en sistemas informáticos.

Las **amenazas actuales** en los sistemas informáticos se caracterizan por su **dinamismo, automatización y capacidad de adaptación**. A diferencia de escenarios anteriores, en los que predominaban ataques aislados y relativamente simples, el contexto actual combina actores humanos, herramientas automatizadas y economías ilícitas organizadas que explotan cualquier debilidad técnica u organizativa disponible.

Una amenaza no es únicamente un software malicioso concreto, sino **cualquier circunstancia capaz de provocar un incidente de seguridad**. En este sentido, las amenazas contemporáneas integran factores técnicos, humanos y contextuales: desde malware avanzado hasta errores de configuración, uso indebido de credenciales o dependencia excesiva de servicios externos.

El entorno de amenazas está marcado por varias tendencias estructurales. En primer lugar, la **automatización de los ataques** permite lanzar campañas masivas sin intervención humana directa, explorando redes y sistemas en busca de vulnerabilidades conocidas. En segundo lugar, la **comercialización del cibercrimen** ha profesionalizado los ataques: existen mercados de herramientas, accesos comprometidos y servicios de ataque “bajo demanda”.

A estas dinámicas se suman factores organizativos como el **teletrabajo**, la proliferación de dispositivos personales y la externalización de servicios, que amplían la superficie de exposición y dificultan el control centralizado.

Muchas amenazas actuales no “apuntan” a una organización concreta: buscan sistemas mal protegidos, independientemente de quién sea su propietario.