Facultad de Ingeniería

Unidad 1. Introducción a la Seguridad Informática

Apunte de cátedra

Contenido

1. Introducción a la Seguridad Informática
1.1. Introducción

La información se ha convertido en uno de los activos más valiosos de cualquier organización. A diferencia de los activos físicos tradicionales, como edificios o maquinaria, la información posee características particulares: puede copiarse en segundos, transmitirse a cualquier parte del mundo, modificarse de manera imperceptible y destruirse sin dejar evidencia física. Estas características la convierten en un recurso estratégico, pero también en un objetivo atractivo para atacantes con motivaciones económicas, políticas, ideológicas o personales.

La creciente digitalización de los procesos organizacionales ha incrementado significativamente la superficie de exposición frente a amenazas informáticas. El uso de Internet, la computación en la nube, los dispositivos móviles, el Internet de las Cosas (IoT), la inteligencia artificial y el trabajo remoto han ampliado las posibilidades de acceso a la información, pero también han generado nuevos riesgos que deben ser gestionados de forma adecuada.

En este escenario surge la Seguridad Informática, una disciplina que reúne conocimientos técnicos, metodologías de gestión, normativas y buenas prácticas destinadas a proteger los sistemas informáticos y la información frente a accesos no autorizados, alteraciones, pérdidas o interrupciones del servicio.

Es importante destacar que la seguridad informática no consiste únicamente en instalar un antivirus o configurar un firewall. Se trata de un proceso continuo que involucra personas, procesos, tecnologías y políticas organizacionales. La seguridad debe ser concebida como una estrategia integral que permita reducir los riesgos y garantizar la continuidad de las operaciones.

Asimismo, la seguridad absoluta no existe. Todo sistema presenta algún grado de vulnerabilidad y, por lo tanto, siempre existe un riesgo residual. El objetivo no es eliminar completamente los riesgos, sino administrarlos de manera que resulten aceptables para la organización, equilibrando el costo de las medidas de protección con el impacto potencial de los incidentes.

1.2. Evolución histórica de la Seguridad Informática

La seguridad informática ha evolucionado en paralelo con el desarrollo de las tecnologías de la información. A medida que los sistemas se volvieron más complejos e interconectados, también lo hicieron las amenazas y las técnicas de protección.

1.2.1. Décadas de 1950 y 1960: la era de las computadoras centrales

Durante los primeros años de la informática, las computadoras eran equipos de gran tamaño utilizados principalmente por organismos gubernamentales, universidades y grandes empresas. El acceso físico a estos sistemas estaba estrictamente controlado, por lo que la seguridad se enfocaba casi exclusivamente en proteger el hardware y restringir el acceso a las instalaciones. En esta etapa, las amenazas provenían principalmente de errores operativos o fallas del equipamiento, más que de ataques deliberados.

1.2.2. Década de 1970: aparición de los primeros mecanismos de control de acceso

Con la incorporación de sistemas multiusuario comenzaron a surgir mecanismos para identificar y autenticar a los usuarios. Se introdujeron las primeras contraseñas y modelos básicos de control de acceso, sentando las bases de la seguridad lógica moderna.

1.2.3. Década de 1980: nacimiento del malware

La expansión de las computadoras personales permitió la aparición de los primeros virus informáticos. Uno de los más conocidos fue **Brain** (infectaba el sector de arranque de los disquetes), desarrollado en 1986, considerado el primer virus para computadoras personales basado en MS-DOS.

Durante esta década comenzaron a desarrollarse los primeros programas antivirus comerciales.

1.2.4. Década de 1990: expansión de Internet

La popularización de Internet transformó completamente el panorama de la seguridad informática. Los sistemas dejaron de estar aislados y comenzaron a estar permanentemente conectados, lo que incrementó considerablemente la exposición a ataques externos.

En esta etapa aparecieron nuevas amenazas, como:

- Gusanos informáticos.
- Ataques de denegación de servicio.
- Robo de contraseñas.
- Intrusiones remotas.
- Ingeniería social.

También comenzaron a difundirse tecnologías como los firewalls y las redes privadas virtuales (VPN).

1.2.5. Siglo XXI: ciberseguridad global

Actualmente, la seguridad informática constituye una preocupación estratégica para gobiernos, empresas y ciudadanos.

Las amenazas actuales incluyen:

- Ransomware.
- Ataques patrocinados por Estados.
- Ciberespionaje.
- Ataques a infraestructuras críticas.
- Robo masivo de información.
- Ataques a servicios en la nube.
- Amenazas dirigidas mediante inteligencia artificial.

La seguridad ha dejado de ser una responsabilidad exclusiva del área técnica para convertirse en un componente esencial de la gestión organizacional y del gobierno corporativo.

1.3. Concepto de Seguridad Informática

1.3.1. Introducción

En el ámbito cotidiano suele asociarse la seguridad informática con el uso de la criptografía, la instalación de un antivirus, el uso de contraseñas robustas o la configuración de un firewall. Sin embargo, estas medidas representan solo una pequeña parte de una disciplina mucho más amplia.

La seguridad informática involucra el conjunto de **políticas, procedimientos, tecnologías, controles y buenas prácticas** destinados a proteger los sistemas informáticos y la información frente a amenazas que puedan comprometer su funcionamiento o la confiabilidad de los datos.

Es importante destacar que la seguridad informática no constituye un producto que pueda adquirirse e instalarse una única vez, sino un **proceso continuo de gestión**, adaptación y mejora. A medida que evolucionan las tecnologías y aparecen nuevas amenazas, también deben evolucionar las estrategias de protección.

1.3.2. Definición de Seguridad Informática

No existe una única definición universalmente aceptada, pero sí numerosos enfoques propuestos por organismos internacionales y autores especializados.

Definición conceptual

La seguridad informática puede definirse como:

La disciplina que estudia, diseña e implementa mecanismos destinados a proteger los sistemas informáticos, los recursos tecnológicos y la información contra accesos no autorizados, modificaciones indebidas, pérdidas, interrupciones del servicio y cualquier otro evento que comprometa la continuidad o el correcto funcionamiento de dichos sistemas.

Esta definición resalta tres aspectos fundamentales:

- Protección de la información.
- Protección de los sistemas informáticos.
- Protección de los servicios que estos ofrecen.

Definición según el NIST

El National Institute of Standards and Technology (NIST) define la seguridad informática como:

La protección de los sistemas de información frente al acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

Esta definición introduce explícitamente los tres principios clásicos de la seguridad, conocidos como la **Tríada CIA**, que serán desarrollados más adelante en este capítulo.

1.3.3. ¿Qué protege la Seguridad Informática?

Una idea frecuente entre los estudiantes es pensar que la seguridad informática protege únicamente computadoras. En realidad, protege un conjunto mucho más amplio de activos.

Entre ellos se encuentran:

Información

Es el activo más importante de cualquier organización.

Ejemplos:

- Historias clínicas.
- Datos bancarios.
- Patentes.
- Planos industriales.
- Bases de datos.
- Información personal.
- Expedientes judiciales.

Sin información, la mayoría de las organizaciones no podría operar.

Hardware

Incluye todos los dispositivos físicos.

Ejemplos:

- Servidores.
- Computadoras.
- Routers.
- Switches.
- Discos rígidos.
- Equipos de almacenamiento.
- Dispositivos móviles.

Aunque estos equipos pueden reemplazarse, su pérdida puede generar importantes costos económicos y operativos.

Software

Comprende todos los programas utilizados por la organización.

Ejemplos:

- Sistemas operativos.
- Sistemas de gestión.
- Aplicaciones web.
- Bases de datos.
- Software de control industrial.

La alteración de un software puede provocar consecuencias tan graves como la pérdida de información o la interrupción de un servicio crítico.

Servicios

Hoy en día muchas organizaciones dependen completamente de determinados servicios tecnológicos.

Por ejemplo:

- Correo electrónico.
- Sitios web.
- Sistemas de facturación.
- Plataformas educativas.
- Servicios en la nube.
- Sistemas bancarios.

Si alguno de estos servicios deja de funcionar, las actividades de la organización pueden verse seriamente afectadas.

Personas

Las personas forman parte del sistema de seguridad. No solo utilizan los sistemas, sino que también:

- administran la infraestructura,
- desarrollan aplicaciones,
- gestionan información sensible,
- toman decisiones.

La mayoría de los incidentes de seguridad involucran, de alguna manera, el factor humano.

1.3.4. ¿Por qué es necesaria la Seguridad Informática?

Existen múltiples razones que justifican la implementación de mecanismos de seguridad.

Crecimiento exponencial de la información digital

Las organizaciones producen enormes cantidades de información cada día.

Ejemplos:

- transacciones bancarias,
- expedientes electrónicos,
- historias clínicas,
- imágenes médicas,
- correos electrónicos,
- documentos digitales.

Toda esa información debe protegerse.

Aumento de los ataques informáticos

Actualmente se producen millones de ataques diarios alrededor del mundo. Los ciberdelincuentes utilizan herramientas cada vez más sofisticadas para:

- robar información,
- secuestrar datos,
- obtener beneficios económicos,
- interrumpir servicios.

Dependencia tecnológica

Hoy prácticamente todas las organizaciones dependen de sistemas informáticos.

Algunos ejemplos son:

- hospitales,
- bancos,
- universidades,
- aeropuertos,
- industrias,
- organismos gubernamentales.

La indisponibilidad de estos sistemas puede ocasionar pérdidas económicas e incluso poner en riesgo la vida de las personas.

Obligaciones legales

Muchos países poseen leyes relacionadas con:

- protección de datos personales,
- privacidad,
- firma digital,
- delitos informáticos.

Las organizaciones deben cumplir estas normativas para evitar sanciones legales.

Protección de la reputación

Una filtración de información puede afectar seriamente la imagen institucional. Muchos clientes dejan de confiar en empresas que sufren incidentes graves de seguridad. En numerosas ocasiones, el daño reputacional resulta mayor que las pérdidas económicas directas.

1.3.5. Seguridad como proceso y no como producto

Uno de los errores conceptuales más frecuentes consiste en creer que la seguridad informática puede resolverse comprando una determinada herramienta.

Es común escuchar afirmaciones como:

"La empresa ya tiene antivirus", "Compramos un firewall", "Instalamos un sistema de monitoreo"

Estas herramientas son importantes, pero por sí solas **no garantizan la seguridad**.

La seguridad depende de numerosos factores:

- políticas organizacionales,

- procedimientos,
- capacitación,
- controles,
- auditorías,
- gestión de riesgos,
- actualización permanente.

Por esta razón suele afirmarse que:

La seguridad informática es un proceso continuo de mejora y gestión del riesgo.

1.3.6. Ejemplo práctico

Supongamos una universidad que almacena:

- datos personales de los alumnos,
- calificaciones,
- títulos,
- información financiera,
- investigaciones.

Si un atacante obtiene acceso al sistema podría:

- modificar notas,
- eliminar registros,
- robar datos personales,
- cifrar toda la información mediante ransomware,
- vender la información en la dark web.

Para evitarlo, la universidad deberá implementar múltiples medidas:

- políticas de seguridad;
- control de acceso;
- autenticación multifactor;
- copias de seguridad;
- capacitación a usuarios;
- monitoreo continuo;
- auditorías;
- gestión de incidentes.

Este ejemplo demuestra que **ninguna medida aislada es suficiente**. La protección eficaz surge de la combinación de controles técnicos, administrativos y organizacionales.

1.4. Seguridad Informática, Seguridad de la Información y Ciberseguridad

1.4.1. Introducción

En los últimos años, el crecimiento de las tecnologías digitales ha provocado la aparición de numerosos términos relacionados con la protección de la información. Entre los más utilizados se encuentran:

- Seguridad Informática (*Computer Security*).
- Seguridad de la Información (*Information Security*).
- Ciberseguridad (*Cybersecurity*).

Aunque en muchos contextos estos términos se utilizan indistintamente, desde el punto de vista académico y profesional poseen alcances diferentes.

1.4.2. Seguridad de la Información

Definición

La **Seguridad de la Información** es la disciplina que protege la información, independientemente del medio en el que se encuentre almacenada, procesada o transmitida.

Esta definición implica que la información debe protegerse tanto si está en formato digital como si se encuentra en papel, en una conversación verbal o en cualquier otro soporte.

La norma **ISO/IEC 27000** define la seguridad de la información como:

La preservación de la confidencialidad, la integridad y la disponibilidad de la información. Adicionalmente, pueden incluirse otras propiedades como la autenticidad, la responsabilidad, el no repudio y la fiabilidad.

En consecuencia, el objeto principal de protección es la **información**, no la tecnología.

Ejemplos

- Un contrato impreso guardado en un archivo físico.
- Una historia clínica en formato papel.
- Una conversación confidencial entre directivos.
- Un expediente judicial.
- Una base de datos digital.
- Un respaldo almacenado en una cinta magnética.

Todos estos casos forman parte del ámbito de la Seguridad de la Información.

Objetivos

La Seguridad de la Información busca:

- Proteger la confidencialidad de la información.
- Garantizar su integridad.

- Asegurar su disponibilidad cuando sea necesaria.
- Evitar pérdidas, alteraciones o divulgaciones no autorizadas.
- Preservar el valor estratégico de la información para la organización.

1.4.3. Seguridad Informática

Definición

La **Seguridad Informática** es la disciplina encargada de proteger los sistemas informáticos y los recursos tecnológicos utilizados para almacenar, procesar y transmitir información.

Mientras la Seguridad de la Información tiene como objeto principal la información, la Seguridad Informática se concentra en la infraestructura tecnológica que la soporta.

Incluye la protección de:

- Computadoras.
- Servidores.
- Sistemas operativos.
- Aplicaciones.
- Bases de datos.
- Redes de comunicación.
- Dispositivos móviles.
- Equipos de almacenamiento.

Su propósito es impedir que estos sistemas sean utilizados, modificados, destruidos o interrumpidos por personas no autorizadas.

Ejemplos

Son actividades propias de la Seguridad Informática:

- Configurar permisos de acceso a un servidor.
- Instalar actualizaciones de seguridad.
- Implementar autenticación multifactor.
- Realizar copias de seguridad.
- Cifrar discos duros.
- Gestionar certificados digitales.
- Monitorear registros de eventos.

Todas estas acciones tienen como finalidad proteger los sistemas informáticos y, por extensión, la información que contienen.

1.4.4. Ciberseguridad

Definición

La **Ciberseguridad** es la disciplina dedicada a proteger las personas, las organizaciones, los sistemas y los servicios que operan en el **ciberespacio**, frente a amenazas originadas en entornos digitales.

A diferencia de la Seguridad Informática, la Ciberseguridad pone el foco en los riesgos derivados de la conectividad y de Internet.

El término comenzó a popularizarse a partir del crecimiento de:

- Internet.
- Computación en la nube.
- Dispositivos móviles.
- Internet de las Cosas (IoT).
- Infraestructuras críticas conectadas.
- Comercio electrónico.
- Servicios digitales.

¿Qué es el ciberespacio?

El **ciberespacio** puede definirse como el entorno virtual generado por la interconexión mundial de sistemas informáticos, redes de comunicación, dispositivos electrónicos y servicios digitales.

En este entorno ocurren diariamente millones de actividades:

- transacciones bancarias,
- compras electrónicas,
- comunicaciones,
- almacenamiento de información,
- servicios gubernamentales,
- educación virtual.

También es el escenario donde se producen los ciberataques.

Ejemplos de actividades relacionadas con la Ciberseguridad

- Protección frente a ransomware.
- Defensa contra ataques distribuidos de denegación de servicio (DDoS).
- Protección de infraestructuras críticas.
- Seguridad en la nube.
- Seguridad del Internet de las Cosas.
- Inteligencia de amenazas (*Threat Intelligence*).
- Respuesta ante incidentes cibernéticos.

1.4.5. Relación entre las tres disciplinas

Aunque poseen diferencias, estas disciplinas no compiten entre sí. Se complementan.

Puede entenderse la relación mediante el siguiente esquema.

Relación conceptual entre Seguridad de la Información, Seguridad Informática y Ciberseguridad. La Ciberseguridad integra elementos de ambas disciplinas cuando la información y los sistemas operan en entornos conectados.

1.4.6. Comparación entre los conceptos

Aspecto	**Seguridad de la Información**	**Seguridad Informática**	**Ciberseguridad**
¿Qué protege?	La información	Los sistemas informáticos	El ciberespacio y los activos digitales
Medio	Digital y no digital	Principalmente digital	Entornos conectados
Alcance	Más amplio	Tecnológico	Tecnológico y estratégico
Incluye documentos en papel	Sí	No	Generalmente no
Incluye redes e Internet	Puede incluirlas	Sí	Sí
Incluye infraestructura tecnológica	Parcialmente	Sí	Sí
Incluye personas y procesos	Sí	Parcialmente	Sí

Ejemplo integrador

Imaginemos un hospital.

La información que administra incluye:

- historias clínicas,
- resultados de laboratorio,
- estudios por imágenes,
- datos personales,
- información administrativa.

Seguridad de la Información

Se ocupa de proteger toda esa información, independientemente de si está:

- en una base de datos,
- impresa,
- archivada,
- comunicada verbalmente entre profesionales.

Seguridad Informática

Protege los sistemas utilizados por el hospital:

- servidores,
- computadoras,
- bases de datos,
- aplicaciones médicas,
- dispositivos de almacenamiento.

Ciberseguridad

Protege al hospital frente a amenazas provenientes del ciberespacio:

- ransomware,
- ataques a la red,
- robo de credenciales,
- ataques a servicios en la nube,
- accesos remotos no autorizados.

1.5. Activo, Vulnerabilidad, Amenaza y Riesgo

Uno de los errores más frecuentes consiste en confundir estos conceptos.

1.5.1. Activo

Es aquello que posee valor para la organización.

Ejemplos:

- bases de datos;
- servidores;
- documentos;
- sistemas;
- personal;
- infraestructura.

1.5.2. Vulnerabilidad

Es una debilidad que puede ser explotada.

Ejemplos:

- contraseña débil;
- software desactualizado;
- ausencia de copias de seguridad;
- mala configuración.

1.5.3. Amenaza

Es cualquier circunstancia, evento o actor con capacidad para explotar una vulnerabilidad y causar daño a un activo de información.

Ejemplos:

- un atacante;
- un malware;
- un incendio;
- un error humano.

1.5.4. Riesgo

Es la posibilidad de que una amenaza explote una vulnerabilidad y genere un impacto negativo.

Relación conceptual entre los principales elementos de la gestión de la seguridad.

Ejemplo completo

Activo: Sistema académico universitario.

Vulnerabilidad: Contraseñas débiles.

Amenaza: Ataque de fuerza bruta.

Riesgo: Acceso no autorizado a información académica.

1.6. Principios Fundamentales de la Seguridad

1.6.1. Introducción

¿Qué características debe conservar la información para que podamos considerarla adecuadamente protegida?

La respuesta se encuentra en los **principios fundamentales de la seguridad**, también denominados **atributos de seguridad u objetivos de la seguridad**.

Estos principios representan las propiedades que deben preservarse para garantizar que la información continúe siendo útil, confiable y accesible para quienes están autorizados a utilizarla.

Por ejemplo, proteger la información implica asegurar que:

- solo puedan acceder a ella quienes estén autorizados;
- no pueda modificarse sin autorización;
- esté disponible cuando sea necesaria.

Estas tres propiedades constituyen la conocida **Tríada CIA**, considerada el fundamento de toda la seguridad informática moderna.

Con el paso del tiempo, la evolución de los sistemas de información hizo necesario incorporar otros principios complementarios, como la **autenticidad**, el **no repudio** y la **trazabilidad**, que permiten responder a nuevas necesidades relacionadas con el comercio electrónico, la firma digital, las auditorías y el análisis de incidentes.

1.6.2. La Tríada CIA

La **Tríada CIA** (Confidentiality, Integrity, Availability) constituye el modelo clásico utilizado para describir los tres principios esenciales de la seguridad de la información.

Fue adoptada por numerosos organismos internacionales y continúa siendo la base conceptual de normas como **ISO/IEC 27001**, **ISO/IEC 27002** y de múltiples publicaciones del **NIST**.

Los tres principios son: Confidencialidad, Integridad, Disponibilidad.

Cada uno de estos principios responde a una pregunta diferente:

Principio	Pregunta que responde
Confidencialidad	¿Quién puede acceder a la información?
Integridad	¿La información ha sido modificada?
Disponibilidad	¿La información puede utilizarse cuando se necesita?

Los tres son igualmente importantes. La ausencia de cualquiera de ellos compromete la seguridad de la información.

Por ejemplo:

- Una base de datos perfectamente protegida contra accesos no autorizados, pero inaccesible durante una emergencia, carece de disponibilidad.
- Una base de datos disponible para todos los usuarios, incluso los no autorizados, pierde la confidencialidad.
- Una base de datos cuyos registros pueden modificarse sin control pierde la integridad.

1.6.3. Confidencialidad

Definición

La **confidencialidad** es el principio que garantiza que la información solo pueda ser conocida, utilizada o divulgada por personas, procesos o sistemas debidamente autorizados.

En términos simples:

Solo deben acceder a la información quienes tienen autorización para hacerlo.

La confidencialidad busca impedir que la información sea revelada accidental o deliberadamente a individuos no autorizados. Este principio resulta especialmente importante cuando la información posee un carácter sensible, confidencial o estratégico.

Importancia de la confidencialidad

Las organizaciones administran información cuyo acceso debe estar restringido.

Algunos ejemplos son:

- historias clínicas;
- datos bancarios;
- declaraciones juradas;
- expedientes judiciales;
- salarios del personal;
- estrategias comerciales;
- diseños industriales;
- investigaciones científicas;
- credenciales de acceso;
- claves criptográficas.

Si esta información fuera divulgada sin autorización, las consecuencias podrían ser muy graves.

Ejemplo cotidiano

Supongamos que una universidad almacena las calificaciones de sus estudiantes. Cada alumno puede consultar únicamente sus propias notas. El docente puede consultar las calificaciones de las materias que dicta. El secretario académico puede acceder a información de todas las carreras. Cada usuario posee distintos niveles de acceso.

La confidencialidad consiste precisamente en garantizar que cada persona vea únicamente la información que le corresponde.

Amenazas que afectan la confidencialidad

Existen numerosas situaciones que pueden comprometer este principio.

Accesos no autorizados

Cuando un usuario obtiene acceso a información para la cual no posee permisos.

Ejemplo:

Un empleado consulta los salarios de otro departamento utilizando una cuenta con privilegios indebidos.

Robo de credenciales

El atacante obtiene nombres de usuario y contraseñas mediante técnicas como:

- phishing;
- malware;
- fuerza bruta;
- ingeniería social.

Espionaje

La información es obtenida con fines económicos, políticos o militares.

Interceptación de comunicaciones

Si una comunicación no se encuentra protegida, un atacante puede capturar la información durante su transmisión.

Pérdida de dispositivos

La pérdida o robo de computadoras portátiles, teléfonos móviles o memorias USB también puede provocar filtraciones de información.

Mecanismos para proteger la confidencialidad

La confidencialidad puede preservarse mediante diversos controles.

Control de acceso

Consiste en permitir el acceso únicamente a usuarios autorizados.

Ejemplos:

- usuarios;
- contraseñas;
- permisos;
- roles.

Autenticación multifactor

Combina dos o más mecanismos de autenticación.

Ejemplo:

- contraseña;
- código enviado al teléfono móvil.

Cifrado

El cifrado transforma la información en un formato ilegible para quienes no poseen la clave correspondiente. Es uno de los mecanismos más eficaces para proteger la confidencialidad durante el almacenamiento y la transmisión de datos.

Clasificación de la información

No toda la información posee el mismo nivel de sensibilidad.

Una organización puede clasificarla como:

- Pública.
- Uso interno.
- Confidencial.
- Secreta.

Cada categoría requiere distintos niveles de protección.

Capacitación del personal

Muchas filtraciones de información se producen por errores humanos. La capacitación permite reducir significativamente este tipo de incidentes.

Ejemplo

Una empresa pierde una computadora portátil perteneciente al gerente financiero.

Situación A

El disco no estaba cifrado.

Cualquier persona que encuentre el equipo puede acceder a:

- balances;
- cuentas bancarias;
- contratos;
- información tributaria.

La confidencialidad queda completamente comprometida.

Situación B

El disco estaba cifrado mediante una herramienta de cifrado completo.

Aunque el equipo sea robado, la información permanece inaccesible para quien no posea la clave correspondiente.

En este caso, la confidencialidad se mantiene.

1.6.4. Integridad

Introducción

En el apartado anterior se estudió el principio de **Confidencialidad**, cuyo objetivo es impedir que personas no autorizadas accedan a la información.

Sin embargo, aunque una información permanezca confidencial, aún puede existir otro problema igualmente grave: **que la información haya sido alterada**.

Imaginemos los siguientes casos:

- Un estudiante modifica ilegalmente su calificación en el sistema académico.
- Un empleado cambia el número de cuenta bancaria de un proveedor antes de realizar un pago.
- Un atacante altera la dosis de un medicamento registrada en una historia clínica electrónica.
- Un error de software modifica automáticamente los saldos de miles de cuentas bancarias.

En todos estos ejemplos, la información puede seguir siendo confidencial (nadie ajeno tuvo acceso), pero ha perdido una propiedad esencial: **su integridad**.

La integridad garantiza que la información permanezca correcta, completa y confiable durante todo su ciclo de vida.

Definición de Integridad

La **integridad** es el principio que garantiza que la información no sea modificada, destruida o alterada de forma no autorizada o accidental.

En términos sencillos:

La información debe mantenerse exactamente como fue creada o como fue autorizadamente modificada.

La norma **ISO/IEC 27000** define la integridad como:

La propiedad de exactitud y completitud de los activos.

Esta definición destaca dos conceptos fundamentales:

- **Exactitud**: la información debe ser correcta.
- **Completitud**: la información no debe estar incompleta ni haber perdido partes esenciales.

¿Por qué es importante la integridad?

Las organizaciones toman decisiones basadas en la información que almacenan. Si esa información es incorrecta, las decisiones también lo serán.

Ejemplo 1: Banco

Supongamos que el saldo de una cuenta bancaria es de **$850.000**. Un error modifica el saldo a **$8.500.000**. Aunque nadie haya robado la información ni el sistema haya dejado de funcionar, la integridad se ha perdido.

Las consecuencias pueden incluir:

- transferencias incorrectas;
- pérdidas económicas;
- demandas judiciales;
- pérdida de confianza.

Ejemplo 2: Hospital

Un médico prescribe:

5 mg de un medicamento. Un atacante modifica la historia clínica y cambia el valor a: 50 mg. La confidencialidad sigue intacta. La disponibilidad también. Sin embargo, la pérdida de integridad puede poner en riesgo la vida del paciente.

Ejemplo 3: Universidad

En el sistema académico aparece registrada la siguiente nota:

Base de datos → 4

Un estudiante logra modificarla a:

Base de datos → 9

El sistema continúa funcionando normalmente. La información sigue siendo confidencial. Pero la integridad ha sido completamente comprometida.

Características de la Integridad

Para que una información mantenga su integridad debe cumplir ciertas condiciones.

Exactitud

Los datos deben reflejar fielmente la realidad.

Ejemplo:

La fecha de nacimiento registrada debe coincidir con la documentación oficial.

Completitud

La información debe encontrarse completa.

Ejemplo:

Una factura sin el importe total no posee integridad.

Consistencia

Los datos deben mantener coherencia entre sí.

Ejemplo:

Un empleado no puede figurar simultáneamente como "Activo" y "Jubilado".

Validez

Los datos deben cumplir las reglas establecidas.

Ejemplo:

Una nota universitaria no puede ser 18 cuando la escala válida es de 0 a 10.

Amenazas que afectan la Integridad

La pérdida de integridad puede originarse por múltiples causas.

Error humano

Es una de las causas más frecuentes.

Ejemplos:

- eliminación accidental de registros;
- carga incorrecta de datos;
- modificaciones involuntarias.

Fallas de software

Errores de programación pueden alterar información automáticamente.

Ejemplo:

Un error en un algoritmo de cálculo de intereses modifica miles de registros bancarios.

Malware

Algunos programas maliciosos modifican archivos deliberadamente.

Ejemplos:

- ransomware;
- virus infectores;
- troyanos.

Ataques informáticos

Los atacantes pueden alterar información para:

- obtener beneficios económicos;
- ocultar evidencias;
- sabotear organizaciones.

Fallas de hardware

Sectores defectuosos de un disco rígido o errores de memoria pueden corromper información.

Errores durante la transmisión

Problemas en una comunicación pueden modificar datos durante su envío.

Mecanismos para preservar la Integridad

La integridad puede protegerse mediante distintos controles.

Validación de datos

Antes de almacenar información deben verificarse reglas como:

- tipo de dato;
- longitud;
- rango permitido;
- obligatoriedad.

Ejemplo:

No permitir edades negativas.

Control de cambios

Toda modificación importante debe quedar registrada.

Esto permite conocer:

- quién realizó el cambio;
- cuando;
- qué información fue modificada.

Copias de seguridad

Si la información resulta alterada accidentalmente, puede restaurarse una versión íntegra.

Auditoría

Los registros de auditoría permiten identificar modificaciones indebidas.

1.6.5. Diferencias entre Confidencialidad e Integridad

Es frecuente que se confundan ambos principios.

Confidencialidad	**Integridad**
Protege el acceso a la información	Protege el contenido de la información
Evita divulgaciones	Evita modificaciones indebidas
Pregunta principal: ¿Quién puede verla?	Pregunta principal: ¿La información sigue siendo correcta?
Se protege con autenticación, autorización y cifrado	Se protege con validaciones, hash, firmas digitales y auditoría

Ejemplo

Una empresa farmacéutica desarrolla un nuevo medicamento. Un atacante logra modificar la fórmula almacenada en la base de datos. No roba información. No elimina archivos. No interrumpe el sistema. Simplemente cambia algunos componentes de la fórmula.

Consecuencias:

- producción defectuosa;
- pérdidas millonarias;
- retiro del producto del mercado;
- riesgos para la salud pública;
- pérdida de prestigio.

En este caso el principio vulnerado fue la **Integridad**.

1.6.6. Disponibilidad

Introducción

Hasta el momento se ha estudiado dos principios fundamentales: confidencialidad e integridad. Sin embargo, aún falta responder una pregunta esencial:

¿De qué sirve que la información sea confidencial e íntegra si no puede utilizarse cuando se la necesita?

Una organización puede proteger perfectamente sus datos mediante cifrado y controles de acceso. No obstante, si un usuario autorizado no puede acceder a ellos en el momento oportuno debido a una falla del sistema, un corte eléctrico o un ataque informático, la organización sufrirá igualmente un problema de seguridad.

Por esta razón, la **disponibilidad** constituye el tercer pilar de la Tríada CIA.

Definición de Disponibilidad

La **disponibilidad** es el principio que garantiza que la información, los sistemas y los servicios se encuentren accesibles y utilizables por los usuarios autorizados en el momento en que los necesiten.

En otras palabras:

La información debe estar disponible cuando se la requiere.

La norma **ISO/IEC 27000** define la disponibilidad como:

La propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada.

Esta definición enfatiza dos aspectos importantes:

- La información debe estar **accesible**.
- Solo debe estar disponible para quienes estén **autorizados**.

Por lo tanto, disponibilidad no significa acceso irrestricto, sino acceso oportuno para los usuarios legítimos.

Importancia de la Disponibilidad

La mayoría de las organizaciones actuales dependen de sistemas informáticos para desarrollar sus actividades diarias.

Algunos ejemplos son:

- bancos que procesan transferencias;

- hospitales que consultan historias clínicas;
- universidades que gestionan inscripciones;
- aerolíneas que administran reservas;
- industrias que controlan líneas de producción;
- comercios electrónicos que reciben pedidos.

Cuando estos sistemas dejan de estar disponibles, las consecuencias pueden ser inmediatas y, en algunos casos, muy graves.

Ejemplo

Supongamos que una guardia hospitalaria necesita acceder a la historia clínica electrónica de un paciente en estado crítico.

La información:

- no fue robada;
- no fue modificada.

Simplemente **no puede consultarse** porque el servidor dejó de funcionar.

En este caso, la confidencialidad y la integridad permanecen intactas, pero la disponibilidad ha sido comprometida.

¿Qué debe estar disponible?

La disponibilidad no se limita únicamente a los datos. Una organización necesita que estén disponibles distintos recursos.

Información

- Bases de datos.
- Documentos.
- Expedientes.
- Archivos.

Sistemas

- Sistemas de gestión.
- Sistemas académicos.
- Plataformas web.

Infraestructura

- Servidores.
- Equipos de almacenamiento.
- Redes.

- Enlaces de comunicación.
- Centros de datos.

Servicios

- Correo electrónico.
- Sitios web.
- DNS.
- Servicios de autenticación.
- Plataformas en la nube.

Personal

La disponibilidad también depende de que existan personas capacitadas para operar los sistemas y responder ante incidentes.

Amenazas que afectan la Disponibilidad

Existen múltiples factores que pueden impedir el acceso a la información o a los servicios.

Fallas de hardware

Los componentes físicos poseen una vida útil limitada.

Ejemplos:

- discos rígidos dañados;
- fuentes de alimentación defectuosas;
- fallas de memoria RAM;
- averías en servidores.

Errores humanos

Muchas interrupciones del servicio son consecuencia de acciones involuntarias.

Ejemplos:

- eliminación accidental de archivos;
- configuración incorrecta de servidores;
- desconexión de equipos;
- instalación fallida de actualizaciones.

Cortes de energía eléctrica

Una interrupción del suministro eléctrico puede dejar fuera de servicio toda la infraestructura informática.

Por este motivo, las organizaciones críticas utilizan:

- sistemas de alimentación ininterrumpida (UPS);
- grupos electrógenos;
- centros de datos con alimentación redundante.

Desastres naturales

Entre ellos:

- incendios;
- inundaciones;
- terremotos;
- tormentas severas.

Estos eventos pueden afectar tanto los equipos como las instalaciones donde se encuentran.

Ataques informáticos

Algunos ataques tienen como objetivo impedir el funcionamiento normal de los sistemas.

Ejemplos:

- ransomware;
- ataques de denegación de servicio (DoS);
- ataques distribuidos de denegación de servicio (DDoS);
- sabotaje interno.

Fallas en proveedores externos

Muchas organizaciones dependen de servicios brindados por terceros.

Por ejemplo:

- proveedores de Internet;
- servicios de computación en la nube;
- suministro eléctrico;
- servicios DNS;
- plataformas de autenticación.

Una falla en cualquiera de estos servicios puede afectar la disponibilidad de la organización.

Mecanismos para garantizar la Disponibilidad

La disponibilidad requiere la implementación de controles preventivos y correctivos.

Redundancia

Consiste en disponer de recursos alternativos que puedan asumir el funcionamiento cuando un componente falla.

Ejemplos:

- servidores redundantes;
- enlaces de Internet duplicados;
- fuentes de alimentación redundantes;
- discos configurados en RAID.

Copias de seguridad

Las copias de seguridad permiten recuperar información cuando se produce una pérdida de datos.

No evitan la interrupción del servicio, pero facilitan su recuperación.

Monitoreo

El monitoreo continuo permite detectar fallas antes de que provoquen una interrupción importante.

Ejemplos:

- uso excesivo de CPU;
- poco espacio en disco;
- caídas de servicios;
- sobrecarga de la red.

Mantenimiento preventivo

Incluye actividades programadas como:

- actualización de software;
- reemplazo de componentes;
- limpieza de equipos;
- verificación del estado de los sistemas.

Planes de contingencia

Definen las acciones que deben ejecutarse cuando ocurre un incidente que afecta la disponibilidad.

Incluyen:

- responsables;

- procedimientos;
- recursos alternativos;
- tiempos de recuperación.

Recuperación ante desastres

La recuperación ante desastres (**Disaster Recovery**) comprende las actividades necesarias para restaurar la infraestructura tecnológica después de un evento grave.

Ejemplo

Una universidad almacena toda su información académica en un único servidor. Un desperfecto eléctrico daña el disco duro.

Como no existían:

- copias de seguridad;
- servidores redundantes;
- procedimientos documentados;

la institución permanece varios días sin poder acceder al sistema académico.

Consecuencias:

- suspensión de inscripciones;
- retraso en la emisión de certificados;
- imposibilidad de cargar calificaciones;
- pérdida de confianza por parte de estudiantes y docentes.

En este caso, el principio comprometido fue la **Disponibilidad**.

Diferencias entre Integridad y Disponibilidad

Integridad	**Disponibilidad**
Protege el contenido de la información	Protege el acceso oportuno a la información
Evita modificaciones indebidas	Evita interrupciones del servicio
Responde a la pregunta: "¿La información sigue siendo correcta?"	Responde a la pregunta: "¿La información puede utilizarse cuando se necesita?"
Se apoya en hash, firmas digitales, validaciones y auditorías	Se apoya en redundancia, respaldo, monitoreo y planes de contingencia

1.6.7. Autenticidad

Introducción

Los tres principios clásicos de la seguridad son:

- Confidencialidad.
- Integridad.
- Disponibilidad.

Sin embargo, en muchos sistemas surge una pregunta adicional:

¿Cómo se puede asegurar que una persona, un dispositivo o un sistema es realmente quien dice ser?

Responder esta pregunta es fundamental.

Por ejemplo:

- ¿Cómo sabe un banco que quien intenta acceder a una cuenta es realmente su titular?
- ¿Cómo puede una universidad verificar que un docente es quien carga las calificaciones?
- ¿Cómo sabe un navegador web que el sitio al que se conecta pertenece realmente al banco y no a un atacante?
- ¿Cómo puede un sistema garantizar que un documento fue emitido por el organismo correspondiente?

En todos estos casos interviene el principio de **Autenticidad**.

Definición de Autenticidad

La **autenticidad** es la propiedad que garantiza que una entidad, un dato o un recurso es genuino y corresponde realmente a quien afirma ser.

En otras palabras:

La autenticidad permite verificar la identidad y el origen de la información o de las entidades que participan en una comunicación.

La norma **ISO/IEC 27000** define la autenticidad como:

La propiedad de que una entidad es quien afirma ser.

Esta entidad puede ser:

- una persona;
- un usuario;
- un servidor;
- un dispositivo;
- una aplicación;
- un documento;
- un mensaje electrónico.

¿Por qué es importante la autenticidad?

Sin mecanismos que permitan verificar identidades, cualquier persona podría hacerse pasar por otra. Las consecuencias pueden ser muy graves.

Ejemplo 1

Un atacante obtiene acceso al correo electrónico de un director financiero y envía instrucciones falsas para realizar una transferencia bancaria. Si la organización no verifica la autenticidad del remitente, la transferencia podría ejecutarse.

Ejemplo 2

Un estudiante logra ingresar al sistema académico utilizando las credenciales de un docente. El sistema interpreta que todas las acciones realizadas corresponden al profesor.

Ejemplo 3

Un usuario accede a un sitio web falso que imita la apariencia del banco. Introduce sus credenciales creyendo que el sitio es auténtico. En realidad, está entregando sus datos a un atacante.

Amenazas que afectan la autenticidad

Diversas técnicas buscan suplantar la identidad de personas, sistemas o dispositivos.

Suplantación de identidad (*Spoofing*)

Consiste en hacerse pasar por otra entidad.

Puede afectar:

- usuarios;
- direcciones IP;
- direcciones MAC;
- servidores;
- sitios web;
- correos electrónicos.

Phishing

Ataques que buscan engañar al usuario para obtener credenciales o información confidencial simulando provenir de una fuente legítima.

Robo de credenciales

Las contraseñas pueden obtenerse mediante:

- malware;
- ingeniería social;
- fuerza bruta;
- reutilización de contraseñas comprometidas.

Certificados falsificados

Si un atacante consigue utilizar un certificado digital fraudulento, puede engañar a los usuarios haciéndoles creer que se comunican con un sitio legítimo.

Mecanismos para garantizar la autenticidad

La autenticidad se logra mediante una combinación de controles técnicos y organizacionales.

Usuarios y contraseñas

Es el mecanismo más difundido. Aunque sencillo, presenta limitaciones cuando se utilizan contraseñas débiles o reutilizadas.

Autenticación multifactor (MFA)

Requiere dos o más factores independientes.

Ejemplos:

- contraseña;
- código temporal generado por una aplicación;
- huella digital;
- reconocimiento facial;
- llave de seguridad física.

La MFA reduce significativamente el riesgo de accesos no autorizados.

Certificados digitales

Permiten verificar la identidad de servidores, organizaciones y personas mediante criptografía de clave pública. Son fundamentales para protocolos como HTTPS y para la firma digital.

Firmas digitales

Una firma digital no solo protege la integridad de un documento, sino que también permite verificar quién lo firmó.

Ejemplo

Un usuario accede al sitio de su banco. Antes de ingresar sus credenciales, el navegador verifica el certificado digital del servidor.

Si el certificado es válido:

- confirma la identidad del servidor;
- establece una conexión segura.

Si el certificado es inválido o pertenece a otra organización:

- el navegador muestra una advertencia.

Este mecanismo protege la autenticidad del servidor y ayuda a prevenir ataques de suplantación.

Diferencias entre Autenticidad e Integridad

Aunque suelen relacionarse, representan propiedades distintas.

Autenticidad	**Integridad**
Verifica la identidad o el origen	Verifica que el contenido no haya sido alterado
Responde a la pregunta: "¿Quién es?"	Responde a la pregunta: "¿La información sigue siendo correcta?"
Se implementa mediante autenticación, certificados y MFA	Se implementa mediante hash, firmas digitales y controles de validación

Es importante destacar que **las firmas digitales contribuyen tanto a la autenticidad como a la integridad**, por lo que constituyen uno de los mecanismos criptográficos más relevantes.

1.6.8. No Repudio

Introducción

Imaginemos la siguiente situación:

Una empresa recibe una orden de transferencia bancaria firmada electrónicamente por su director financiero. Horas después, cuando el dinero ya fue transferido, el director afirma:

"Yo nunca autoricé esa operación."

Surge entonces una pregunta fundamental:

¿Cómo puede demostrarse quién realizó realmente esa acción?

Otro ejemplo:

Un estudiante envía por correo electrónico su trabajo práctico minutos antes del cierre de la entrega. Al día siguiente afirma:

"Nunca envié ese archivo."

O bien:

Una empresa firma electrónicamente un contrato y, meses después, intenta desconocer la firma alegando que nunca aceptó el acuerdo.

En todos estos casos aparece un problema común:

Una de las partes intenta negar haber realizado una acción.

El principio de **No Repudio** busca precisamente impedir este tipo de situaciones.

Definición de No Repudio

El **No Repudio** es el principio que garantiza que una entidad no pueda negar posteriormente haber realizado una determinada acción.

En otras palabras:

Una vez realizada una acción y registrada mediante mecanismos adecuados, su autor no puede negar legítimamente haberla efectuado.

La norma **ISO/IEC 27000** considera el no repudio como una propiedad que proporciona evidencia de la ocurrencia de un evento o de una acción realizada por una entidad determinada.

Este principio resulta especialmente importante cuando las acciones producen efectos legales, económicos o administrativos.

¿Por qué es importante el No Repudio?

En muchas actividades resulta indispensable poder demostrar quién realizó una determinada acción.

Algunos ejemplos son:

- aprobación de una transferencia bancaria;
- firma de un contrato;
- emisión de una factura electrónica;
- presentación de una declaración impositiva;
- emisión de una receta médica electrónica;
- autorización de un pago;
- aceptación de condiciones contractuales.

Si cualquiera de las partes pudiera negar posteriormente su participación, la confianza en los sistemas electrónicos desaparecería.

Ejemplo cotidiano

Cuando una persona firma un documento en papel delante de un escribano, posteriormente resulta muy difícil negar que participó del acto. En el mundo digital ocurre algo similar.

La diferencia es que la evidencia ya no se basa únicamente en una firma manuscrita, sino en mecanismos criptográficos que permiten demostrar matemáticamente quién realizó la operación.

¿Qué acciones requieren No Repudio?

El no repudio resulta especialmente importante cuando existen consecuencias legales o económicas.

Ejemplos:

- firmar contratos;
- aprobar pagos;
- emitir órdenes de compra;
- autorizar préstamos;
- enviar declaraciones juradas;
- aprobar calificaciones;
- emitir certificados académicos;
- autorizar recetas médicas;
- firmar documentos oficiales.

En estos casos es necesario poder demostrar posteriormente quién realizó la acción.

El principio de no repudio se basa en la generación y conservación de evidencias que permiten demostrar la autoría de una acción.

Amenazas al No Repudio

Diversas situaciones pueden impedir demostrar quién realizó una acción.

Credenciales compartidas

Si varios empleados utilizan la misma cuenta de usuario, resulta imposible determinar cuál de ellos efectuó una operación.

Contraseñas robadas

Cuando un atacante obtiene las credenciales de un usuario, posteriormente puede surgir una controversia sobre quién realizó realmente las acciones registradas.

Ausencia de registros

Si un sistema no conserva evidencia suficiente, será imposible reconstruir los hechos.

Falta de mecanismos criptográficos

Un simple documento electrónico puede copiarse o modificarse. Sin mecanismos criptográficos adecuados, resulta difícil demostrar su autoría.

Manipulación de evidencias

Si los registros pueden modificarse libremente, dejan de constituir pruebas confiables.

Mecanismos para garantizar el No Repudio

El no repudio requiere la combinación de varios controles.

Firma digital

Es el mecanismo más importante para garantizar el no repudio.

Una firma digital permite:

- identificar al firmante;
- verificar la integridad del documento;
- demostrar que el documento fue firmado por quien posee la clave privada correspondiente.

A diferencia de una firma escaneada, una firma digital posee respaldo criptográfico.

Certificados digitales

Los certificados digitales vinculan una identidad con una clave pública.

Gracias a ellos puede verificarse quién firmó un documento.

Sellado de tiempo (Timestamp)

Permite demostrar el momento exacto en que una acción fue realizada. Esto resulta importante cuando existen plazos legales.

Registros de auditoría

Los sistemas deben conservar evidencia sobre:

- usuario;
- fecha;
- hora;
- dirección IP (cuando corresponda);
- acción realizada;
- resultado de la operación.

Estos registros complementan los mecanismos criptográficos.

Políticas de gestión de credenciales

Cada usuario debe poseer una identidad única. Nunca deben compartirse cuentas.

Ejemplo

Una empresa firma electrónicamente un contrato con un proveedor. Meses después surge un conflicto. El proveedor afirma:

"Nunca firmamos ese documento."

La empresa presenta:

- el documento firmado digitalmente;
- el certificado digital utilizado;
- el sello de tiempo;
- los registros del sistema.

La verificación demuestra que la firma fue realizada utilizando la clave privada del representante legal del proveedor y que el documento no fue modificado. Como consecuencia, el proveedor no puede negar válidamente la autoría de la firma.

Este es un ejemplo clásico del principio de **No Repudio**.

Diferencias entre Autenticidad y No Repudio

Autenticidad	No Repudio
Verifica quién es una entidad	Impide que una entidad niegue posteriormente una acción realizada
Se centra en la identidad	Se centra en la responsabilidad sobre una acción
Responde a la pregunta: "¿Quién es?"	Responde a la pregunta: "¿Quién realizó esta acción?"
Se implementa mediante autenticación y certificados	Se implementa mediante firmas digitales, certificados, sellos de tiempo y evidencias

1.6.9. Trazabilidad

Introducción

Supongamos que una organización detecta que un archivo confidencial fue eliminado. La primera pregunta que surge es:

¿Quién eliminó el archivo?

Luego aparecen otras preguntas igualmente importantes:

- ¿Cuándo ocurrió?
- ¿Desde qué equipo?
- ¿Qué usuario inició sesión?
- ¿Qué otros archivos modificaron?
- ¿Qué ocurrió antes y después del incidente?

Si el sistema no registró esa información, será prácticamente imposible reconstruir los hechos. En cambio, si existen registros completos y confiables, será posible analizar el incidente y determinar responsabilidades. Esta capacidad constituye el principio de **Trazabilidad**.

Definición de Trazabilidad

La **trazabilidad** es la capacidad de registrar y reconstruir las acciones realizadas sobre la información, los sistemas y los recursos tecnológicos, permitiendo identificar quién realizó una acción, cuándo la realizó, sobre qué recurso actuó y cuál fue su resultado.

En términos simples:

La trazabilidad permite reconstruir la historia de un evento.

Aunque la familia ISO/IEC 27000 no define la trazabilidad como un principio independiente con el mismo nivel de formalidad que la confidencialidad o la integridad, sí reconoce la importancia del **registro de eventos**, la **auditoría** y la **responsabilidad**

(accountability) como controles esenciales para la gestión de la seguridad de la información.

¿Por qué es importante la trazabilidad?

Sin registros adecuados:

- no pueden investigarse incidentes;
- no es posible demostrar responsabilidades;
- resulta difícil detectar accesos indebidos;
- las auditorías pierden eficacia;
- se dificulta el cumplimiento de requisitos legales y normativos.

La trazabilidad proporciona evidencia objetiva sobre el funcionamiento de un sistema.

Ejemplo cotidiano

En una empresa desaparece un archivo con información financiera.

Gracias a los registros del sistema se determina que:

- el usuario **jperez** inició sesión;
- accedió al archivo;
- lo modificó;
- posteriormente lo eliminó;
- realizó estas acciones desde una computadora específica;
- todo ocurrió entre las 10:14 y las 10:19 horas.

Sin estos registros sería imposible reconstruir la secuencia de los hechos.

¿Qué información debe registrarse?

Para garantizar una adecuada trazabilidad, los sistemas deben registrar información suficiente para reconstruir los eventos. Entre los datos más importantes se encuentran:

Identificación del usuario

Debe registrarse quién realizó la acción.

Ejemplo:

- nombre de usuario;
- identificador único;
- cuenta utilizada.

Fecha y hora

Toda acción debe asociarse a una fecha y hora precisas.

Recurso afectado

Debe identificarse claramente el recurso involucrado.

Ejemplos:

- archivo;
- base de datos;
- aplicación;
- servidor;
- dispositivo.

Acción realizada

Ejemplos:

- creación;
- modificación;
- eliminación;
- consulta;
- impresión;
- exportación;
- inicio de sesión;
- cierre de sesión.

Resultado de la acción

Es importante conocer si la operación:

- fue exitosa;
- fue rechazada;
- produjo un error.

Origen de la conexión

Cuando corresponda, puede registrarse:

- dirección IP;
- nombre del equipo;
- ubicación lógica;
- dispositivo utilizado.

Amenazas a la trazabilidad

Borrado de logs

Un atacante borra las bitácoras tras entrar a un sistema.

Modificación de datos

Se cambian los registros para ocultar acciones ilegales.

Inyección de comandos

Se alteran archivos de texto o bases de datos de auditoría.

Inyección de eventos

Se crean rastros falsos para desviar la culpa.

Ataques DoS a logs

Se llena el disco duro para que el sistema deje de registrar.

Mecanismos para garantizar la trazabilidad

La trazabilidad requiere la implementación de distintos controles.

Registros de auditoría (Logs)

Constituyen el principal mecanismo para registrar eventos.

Los logs pueden almacenar información sobre:

- accesos;
- modificaciones;
- errores;
- intentos fallidos de autenticación;
- cambios de configuración;
- actividades administrativas.

Sistemas de monitoreo

Permiten supervisar continuamente la actividad de los sistemas. Además de registrar eventos, facilitan la detección temprana de comportamientos anómalos.

Gestión centralizada de registros

En organizaciones grandes es habitual concentrar los registros provenientes de múltiples sistemas en un repositorio central.

Esto facilita:

- la correlación de eventos;
- las investigaciones;
- las auditorías.

Protección de los registros

Los registros deben protegerse contra:

- modificación;
- eliminación;
- acceso no autorizado.

Si un atacante pudiera alterar los logs, perderían su valor como evidencia.

Sincronización horaria

Todos los sistemas deben utilizar una referencia temporal común. De lo contrario, sería muy difícil reconstruir correctamente la secuencia de los eventos.

Ejemplo

Una universidad detecta que fueron modificadas varias calificaciones.

Los registros muestran que:

- el usuario **docente23** inició sesión a las 18:42;
- accedió al módulo de carga de notas;
- modificó cinco registros;
- cerró la sesión a las 18:48;
- la conexión se realizó desde una computadora del laboratorio.

Gracias a esta información, la institución puede reconstruir el incidente y determinar qué ocurrió.

Diferencias entre No Repudio y Trazabilidad

No Repudio	**Trazabilidad**
Impide que una entidad niegue una acción realizada	Permite reconstruir todas las acciones realizadas
Se centra en demostrar la autoría	Se centra en registrar la secuencia completa de eventos
Utiliza principalmente firmas digitales y certificados	Utiliza registros de auditoría, monitoreo y control de eventos
Responde a la pregunta: "¿Quién realizó esta acción?"	Responde a las preguntas: "¿Qué ocurrió?, ¿cuándo?, ¿dónde y cómo?"

1.6.10. Integración de los Principios Fundamentales de la Seguridad

Síntesis para visualizar cómo se relacionan todos los principios estudiados

Principio	Pregunta fundamental que responde	Objetivo principal	Ejemplo
Confidencialidad	¿Quién puede acceder a la información?	Evitar accesos no autorizados.	Solo el docente puede consultar las calificaciones de sus alumnos.
Integridad	¿La información permanece correcta y completa?	Evitar modificaciones no autorizadas o accidentales.	Nadie puede alterar una nota sin autorización.
Disponibilidad	¿La información está accesible cuando se necesita?	Garantizar el acceso oportuno a los recursos.	El sistema académico funciona durante el período de inscripciones.
Autenticidad	¿Quién es realmente la entidad con la que interactúo?	Verificar identidades y el origen de la información.	El sistema confirma la identidad del docente antes de permitir el acceso.
No Repudio	¿Cómo demostrar quién realizó una acción?	Impedir que una entidad niegue una acción realizada.	Un docente firma digitalmente el acta de examen y no puede negar posteriormente su emisión.
Trazabilidad	¿Qué ocurrió, cuándo, dónde y cómo?	Registrar y reconstruir las acciones realizadas.	Los registros permiten conocer quién modificó una calificación, desde qué equipo y en qué momento.

1.7. Clasificación de medidas de seguridad
1.7.1. Introducción

Las organizaciones implementan numerosas medidas para proteger sus activos de información. Estas medidas pueden clasificarse según distintos criterios, como su naturaleza, su ámbito de aplicación o la función que cumplen. Una de las clasificaciones más utilizadas distingue entre medidas de seguridad activa y medidas de seguridad pasiva, según su finalidad dentro de la estrategia de protección.

Seguridad activa

Es el conjunto de medidas de protección destinadas a prevenir y evitar daños que puedan afectar a los sistemas informáticos y a la información.

La seguridad activa comprende todos aquellos mecanismos que actúan de forma preventiva, dificultando que se produzcan accesos no autorizados, modificaciones indebidas o cualquier otra acción que comprometa la seguridad de la información. Estas medidas constituyen la primera línea de defensa de una organización y buscan evitar que los daños lleguen a producirse.

Ejemplos de seguridad activa

Medida	¿Por qué es seguridad activa?
Firewall	Filtra el tráfico de red para impedir accesos no autorizados.
Antivirus	Detecta y bloquea software malicioso.
Autenticación multifactor	Reduce el riesgo de accesos indebidos.
Control de acceso físico	Impide el ingreso de personas no autorizadas.
CCTV con monitoreo	Permite detectar actividades sospechosas.
IDS/IPS	Detectan o bloquean intentos de intrusión.
Cifrado	Protege la información frente a accesos no autorizados.

Seguridad pasiva

Es el conjunto de medidas de protección destinadas a reducir las consecuencias de los daños producidos y facilitar la recuperación de los sistemas informáticos y de la información.

La seguridad pasiva reúne aquellos mecanismos que no evitan necesariamente que ocurra un daño, pero permiten minimizar sus efectos y recuperar el funcionamiento normal de los sistemas en el menor tiempo posible. Estas medidas contribuyen a garantizar la continuidad de las operaciones cuando las medidas preventivas no han sido suficientes.

Ejemplos de seguridad pasiva

Medida	¿Por qué es seguridad pasiva?
Copias de seguridad	Permiten recuperar la información perdida.
UPS	Mantiene el suministro eléctrico durante cortes breves.
Generador eléctrico	Garantiza el suministro ante interrupciones prolongadas.
RAID	Reduce la pérdida de información por fallas de discos.
Puertas cortafuego	Limitan la propagación del incendio.
Materiales ignífugos	Disminuyen los daños provocados por el fuego.
Planes de recuperación	Facilitan el restablecimiento de los servicios.

Comparación entre seguridad activa y seguridad pasiva

Seguridad activa	Seguridad pasiva
Previene daños.	Reduce las consecuencias de los daños.
Actúa antes de que ocurra el daño.	Actúa cuando el daño ya se produjo o para facilitar la recuperación.

Seguridad activa	Seguridad pasiva
Busca evitar interrupciones.	Busca restablecer el funcionamiento normal.
Ejemplos: firewall, antivirus, MFA.	Ejemplos: backup, UPS, RAID.

Complementariedad

Ningún tipo de medida es suficiente por sí sola.

Una organización que solo implementa medidas de seguridad activa puede reducir significativamente la probabilidad de sufrir daños, pero no estará preparada para recuperarse si estos llegan a producirse. Del mismo modo, una organización que únicamente dispone de medidas de seguridad pasiva podrá recuperarse, pero seguirá siendo vulnerable a nuevos daños. Por ello, una estrategia de seguridad eficaz combina ambos tipos de medidas de forma complementaria.

Ejemplo de ambas medidas: seguridad en una universidad

La Facultad de Ingeniería dispone de un centro de datos donde funcionan el sistema de gestión académica, el correo institucional y las plataformas de educación virtual.

Para proteger esta infraestructura se han implementado las siguientes medidas:

- acceso al centro de cómputos mediante tarjetas de proximidad y reconocimiento biométrico;
- firewall perimetral para controlar el tráfico de red;
- autenticación multifactor para administradores;
- antivirus administrado centralmente;
- copias de seguridad automáticas diarias;
- UPS para mantener operativos los servidores durante cortes de energía;
- grupo electrógeno para interrupciones prolongadas del suministro eléctrico.

Analizando estas medidas puede observarse que algunas buscan impedir que ocurran daños, mientras que otras permiten mantener la continuidad del servicio y recuperar la información cuando los daños no pudieron evitarse.

En este caso:

Medida implementada	Tipo de seguridad
Firewall	Activa
Autenticación multifactor	Activa
Control biométrico	Activa
Antivirus	Activa
Copias de seguridad	Pasiva
UPS	Pasiva
Generador eléctrico	Pasiva

Este ejemplo muestra que una organización necesita combinar medidas de ambos tipos para lograr una protección adecuada.

Ejemplo de seguridad activa y pasiva con amenazas

Amenaza	Medidas de seguridad activa	Medidas de seguridad pasiva
Acceso no autorizado	Autenticación, MFA, control de acceso, biometría	Registros de auditoría, copias de seguridad, planes de recuperación
Malware	Antivirus, antimalware, firewall, actualización del software	Copias de seguridad, restauración del sistema
Falla del suministro eléctrico	Mantenimiento de la instalación eléctrica, monitoreo del suministro	UPS, generadores eléctricos, líneas redundantes
Incendio	Detectores de humo, alarmas	Puertas cortafuego, sistemas automáticos de extinción, copias de seguridad externas
Robo de equipos	CCTV, control de acceso, guardias, cerraduras	Cifrado de discos, copias de seguridad, equipos de reemplazo
Error humano	Capacitación, procedimientos, validación de datos	Copias de seguridad, control de versiones, recuperación de información
Falla de hardware	Monitoreo preventivo, mantenimiento	RAID, servidores redundantes, equipos de reserva
Desastres naturales	Selección adecuada de la ubicación, diseño resistente	Centro alternativo, copias externas, plan de recuperación ante desastres

Una misma medida de seguridad puede contribuir tanto a la seguridad activa como a la seguridad pasiva, dependiendo de la finalidad con la que sea implementada. La clasificación presentada en la tabla corresponde a la función predominante de cada medida.

Bibliografía

- Bishop, M. (2019). *Computer Security: Art and Science* (2nd ed.). Addison-Wesley.
- Easttom, C. (2022). *Computer Security Fundamentals* (4th ed.). Pearson.
- ISO/IEC. (2018). ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary.
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF 2.0).*
-
- NIST. (2013). FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems.
-
- Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in Computing* (5th ed.). Pearson.

- Stallings, W., & Brown, L. (2021). *Computer Security: Principles and Practice* (5th ed.). Pearson.
- Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7th ed.). Cengage Learning.