Facultad de Ingeniería

Unidad 3. Seguridad Lógica

Apunte de cátedra

Contenido

3. Seguridad lógica y gestión de usuarios
3.1. Seguridad Lógica
3.1.1. Concepto de Seguridad Lógica

La **Seguridad Lógica** es el conjunto de políticas, procedimientos, mecanismos y controles destinados a proteger los sistemas informáticos y la información frente a accesos no autorizados, modificaciones indebidas, pérdidas de datos o cualquier otra acción que pueda comprometer su seguridad.

Su finalidad es garantizar que únicamente las personas autorizadas puedan acceder a los recursos informáticos y realizar las operaciones permitidas según las funciones que desempeñan dentro de una organización.

En la actualidad, gran parte de los incidentes de seguridad se producen debido a problemas relacionados con el acceso lógico, como el uso de contraseñas débiles, cuentas compartidas, privilegios excesivos o configuraciones incorrectas de permisos. Por ello, la correcta administración de usuarios y privilegios constituye una de las tareas más importantes dentro de la gestión de la seguridad de una organización.

La Seguridad Lógica no depende únicamente de la tecnología. También requiere procedimientos adecuados, políticas organizacionales y usuarios capacitados que utilicen correctamente los recursos informáticos.

3.1.2. Objetivos de la Seguridad Lógica

La Seguridad Lógica tiene como propósito proteger los activos de información mediante mecanismos que controlen el acceso y el uso de los sistemas informáticos.

Sus principales objetivos son los siguientes:

- **Impedir el acceso no autorizado a los sistemas informáticos.** Solo los usuarios debidamente autorizados deben poder ingresar a los recursos de la organización.
- **Proteger la información almacenada y procesada por los sistemas.** Se busca evitar la lectura, modificación o eliminación no autorizada de los datos.
- **Garantizar la confidencialidad de la información.** La información debe estar disponible únicamente para quienes poseen autorización para conocerla.
- **Preservar la integridad de los datos.** La información debe mantenerse completa, correcta y libre de modificaciones no autorizadas.
- **Contribuir a la disponibilidad de los sistemas.** Los usuarios autorizados deben poder acceder a los recursos cuando los necesiten, salvo situaciones excepcionales.
- **Registrar las actividades realizadas por los usuarios.** El registro de eventos permite reconstruir las acciones realizadas sobre un sistema y facilita las tareas de auditoría e investigación.
- **Reducir el riesgo de incidentes de seguridad.** La aplicación de controles adecuados disminuye la probabilidad de accesos indebidos, errores humanos y acciones maliciosas.

Estos objetivos se alcanzan mediante la aplicación coordinada de distintos mecanismos de protección, como el control de acceso, la gestión de usuarios, la administración de privilegios, las políticas de contraseñas y la auditoría de los sistemas.

3.1.3. Relación entre la Seguridad Física y la Seguridad Lógica

La Seguridad Física y la Seguridad Lógica son dos componentes complementarios de la Seguridad Informática. Aunque protegen recursos diferentes, ambas persiguen un objetivo común: **garantizar que los activos de información de una organización permanezcan protegidos frente a amenazas internas y externas**.

La diferencia principal radica en el tipo de recurso que protege cada una.

La **Seguridad Física** se ocupa de proteger las instalaciones, los equipos, los centros de datos y demás recursos materiales frente a amenazas como robos, incendios, inundaciones o accesos físicos no autorizados.

La **Seguridad Lógica**, en cambio, protege los sistemas informáticos, las aplicaciones y la información mediante mecanismos que controlan quién puede acceder a ellos y qué operaciones puede realizar.

Un ejemplo permite comprender fácilmente esta diferencia.

Supongamos que un empleado desea consultar información almacenada en el servidor de una empresa. Antes de acceder al sistema deberá ingresar al edificio utilizando una credencial o un sistema biométrico. Este proceso pertenece a la **Seguridad Física**.

Una vez frente al equipo, deberá ingresar un nombre de usuario y una contraseña para acceder al sistema. Posteriormente, el sistema verificará qué información está autorizado a consultar. Este proceso corresponde a la **Seguridad Lógica**.

En consecuencia, ambos tipos de seguridad trabajan de manera complementaria. De poco serviría proteger adecuadamente una sala de servidores si cualquier persona pudiera acceder libremente a los sistemas informáticos. Del mismo modo, una excelente política de autenticación pierde efectividad si un atacante puede ingresar físicamente al centro de datos y manipular los equipos.

La siguiente tabla resume las principales diferencias entre ambos enfoques.

Seguridad Física	**Seguridad Lógica**
Protege instalaciones, equipos e infraestructura.	Protege sistemas, aplicaciones e información.
Controla el acceso a espacios físicos.	Controla el acceso a recursos informáticos.
Utiliza cerraduras, credenciales, biometría, CCTV y otros mecanismos físicos.	Utiliza usuarios, contraseñas, permisos, autenticación multifactor y auditoría.
Evita accesos físicos no autorizados.	Evita accesos lógicos no autorizados.

Seguridad Física	Seguridad Lógica
Su objetivo es proteger los recursos materiales de la organización.	Su objetivo es proteger los recursos informáticos y la información.

La Seguridad Física y la Seguridad Lógica no deben considerarse mecanismos independientes, sino partes de una estrategia integral de Seguridad Informática.

3.1.4. Principales mecanismos de Seguridad Lógica

La Seguridad Lógica se implementa mediante diversos mecanismos que actúan de forma coordinada para proteger los sistemas informáticos y la información.

Los principales mecanismos que se estudiarán en esta unidad son:

- **Control de acceso lógico.** Permite verificar la identidad de los usuarios y determinar qué recursos pueden utilizar.
- **Gestión de usuarios y grupos.** Comprende la creación, modificación y eliminación de cuentas, así como la organización de los usuarios según sus funciones dentro de la organización.
- **Gestión de privilegios.** Consiste en asignar permisos adecuados a cada usuario aplicando principios como el mínimo privilegio y la separación de funciones.
- **Modelos de control de acceso.** Definen la forma en que los permisos son administrados dentro de un sistema. Entre los más utilizados se encuentran DAC, MAC, RBAC y ABAC.
- **Políticas de contraseñas.** Establecen los requisitos que deben cumplir las credenciales de acceso para reducir el riesgo de accesos no autorizados.
- **Autenticación multifactor (MFA).** Incrementa la seguridad del proceso de autenticación mediante la combinación de dos o más factores de verificación.
- **Registro y auditoría.** Permiten registrar las acciones realizadas por los usuarios y detectar actividades sospechosas o incidentes de seguridad.

Todos estos mecanismos forman parte de una estrategia integral de Seguridad Lógica y serán desarrollados en los apartados siguientes de esta unidad.

3.2. Control de Acceso Lógico

3.2.1. Concepto

El **control de acceso lógico** es el conjunto de mecanismos, procedimientos y políticas que regulan el acceso de los usuarios a los recursos informáticos de una organización. Su finalidad es garantizar que únicamente las personas autorizadas puedan utilizar los sistemas, acceder a la información y ejecutar las operaciones permitidas según las funciones que desempeñan.

Los recursos protegidos por el control de acceso lógico pueden ser muy variados, entre ellos:

- Sistemas operativos.
- Aplicaciones.

- Bases de datos.
- Archivos y carpetas.
- Servicios de red.
- Sistemas en la nube.
- Equipos y dispositivos informáticos.

El control de acceso lógico constituye uno de los mecanismos más importantes de la Seguridad Informática, ya que la mayoría de los incidentes de seguridad se originan por accesos indebidos o por una asignación incorrecta de permisos.

Su implementación permite reducir el riesgo de accesos no autorizados, limitar las acciones que cada usuario puede realizar y mantener un adecuado nivel de protección sobre la información.

3.2.2. Componentes del Control de Acceso

Todo sistema de control de acceso, ya sea físico o lógico, se basa en tres componentes fundamentales:

- **Identificación.**
- **Autenticación.**
- **Autorización.**

Estos conceptos fueron desarrollados en la **Unidad 2 (Seguridad Física)**, donde se analizaron como parte del proceso de ingreso a instalaciones y áreas restringidas. En la Seguridad Lógica se aplican exactamente los mismos principios, pero orientados al acceso a sistemas informáticos.

3.2.2.1. Identificación

La **identificación** consiste en informar al sistema quién solicita el acceso. Para ello el usuario proporciona un identificador único, por ejemplo:

- Nombre de usuario;
- Dirección de correo electrónico;
- Número de empleado;
- Identificador asignado por el sistema.

La identificación únicamente indica la identidad declarada por el usuario; todavía no demuestra que dicha identidad sea verdadera.

3.2.2.2. Autenticación

La **autenticación** es el proceso mediante el cual el sistema verifica que el usuario es realmente quien dice ser. Para ello puede utilizar uno o más mecanismos de verificación, como:

- Contraseña;
- Código de un solo uso (otp);

- Aplicación autenticadora;
- Token físico;
- Certificado digital;
- Huella dactilar;
- Reconocimiento facial.

La autenticación constituye la segunda etapa del proceso de control de acceso y permite impedir que personas no autorizadas utilicen cuentas ajenas.

3.2.2.3. Autorización

Una vez autenticado el usuario, el sistema determina qué recursos puede utilizar y qué operaciones tiene permitido realizar.

Este proceso recibe el nombre de **autorización**.

Por ejemplo, un sistema de gestión universitaria puede establecer que:

- Un estudiante únicamente pueda consultar sus calificaciones;
- Un docente pueda cargar y modificar notas de las asignaturas que dicta;
- Un director de carrera pueda acceder a información académica de todas las asignaturas;
- Un administrador pueda gestionar usuarios y configurar el sistema.

La autorización se implementa mediante permisos, privilegios o roles, temas que se desarrollarán en el apartado **Gestión de Privilegios y Modelos de Control de Acceso**.

Comparación entre Seguridad Física y Seguridad Lógica

Aunque los conceptos son los mismos, los recursos protegidos y los mecanismos utilizados son diferentes.

Etapa	Seguridad Física	Seguridad Lógica
Identificación	Credencial, documento o identificación personal.	Nombre de usuario, correo electrónico o identificador del sistema.
Autenticación	PIN, tarjeta, biometría o credencial.	Contraseña, OTP, token, certificado digital o biometría.
Autorización	Permiso para ingresar a un edificio o área restringida.	Permiso para acceder a aplicaciones, archivos, bases de datos o funciones del sistema.

Como puede observarse, la diferencia no radica en el proceso, sino en el recurso que se protege. En ambos casos se busca garantizar que únicamente las personas autorizadas puedan acceder a un determinado recurso.

3.2.3. Flujo del Control de Acceso

El funcionamiento del control de acceso lógico puede representarse como una secuencia ordenada de etapas.

Este modelo se aplica en prácticamente todos los sistemas informáticos modernos, independientemente de su tamaño o complejidad.

3.2.4. Ejemplo Integrador

Supóngase que una universidad dispone de un sistema académico utilizado por estudiantes, docentes y personal administrativo.

Cuando un docente desea ingresar al sistema para cargar las calificaciones de sus alumnos, el proceso se desarrolla de la siguiente manera:

1. Introduce su **nombre de usuario**, permitiendo que el sistema identifique la cuenta con la que desea acceder.
2. Ingresa su **contraseña** y, si la institución utiliza autenticación multifactor, confirma su identidad mediante un código generado por una aplicación autenticadora.
3. El sistema verifica que la autenticación sea correcta.
4. A continuación, consulta los permisos asociados a la cuenta del docente.
5. Finalmente, el sistema permite acceder únicamente a las asignaturas que tiene asignadas y habilita las funciones correspondientes, como cargar o modificar calificaciones. No podrá acceder a funciones reservadas para administradores ni consultar información de otras áreas para las cuales no posee autorización.

Este ejemplo muestra cómo la identificación, la autenticación y la autorización actúan de manera coordinada para proteger los sistemas y la información de una organización.

3.3. Gestión de Usuarios

A partir de este apartado comenzamos con uno de los temas más importantes de la Seguridad Lógica. Mientras que el apartado anterior explicó **cómo un usuario accede al sistema**, ahora estudiaremos **cómo se administran las cuentas de usuario durante todo su ciclo de vida**. Este tema constituye la base para comprender posteriormente la gestión de privilegios, los modelos de control de acceso y la auditoría.

3.3.1. Concepto

La **gestión de usuarios** es el conjunto de procedimientos y actividades destinadas a administrar las cuentas de usuario que permiten el acceso a los sistemas informáticos de una organización.

Su objetivo es garantizar que cada persona disponga únicamente de las cuentas necesarias para realizar sus funciones y que dichas cuentas sean administradas de forma segura durante todo su ciclo de vida.

Una adecuada gestión de usuarios permite:

- controlar quién puede acceder a los sistemas;
- asignar correctamente permisos y privilegios;
- reducir el riesgo de accesos no autorizados;
- facilitar las tareas de auditoría;
- cumplir las políticas de seguridad de la organización.

La administración de usuarios no consiste únicamente en crear cuentas. También implica modificarlas cuando cambian las funciones del usuario, suspenderlas temporalmente cuando corresponde y eliminarlas cuando dejan de ser necesarias.

En organizaciones medianas y grandes, esta administración suele estar a cargo del área de Tecnología de la Información (TI) o de los administradores de sistemas, quienes deben seguir procedimientos establecidos para evitar errores que puedan comprometer la seguridad.

3.3.2. Importancia de la Gestión de Usuarios

Una gestión inadecuada de las cuentas de usuario constituye una de las causas más frecuentes de incidentes de seguridad.

Por ejemplo, si un empleado deja de trabajar en una empresa y su cuenta continúa activa, otra persona podría utilizarla para acceder a información confidencial. Del mismo modo, asignar permisos excesivos a un usuario aumenta el riesgo de modificaciones accidentales o acciones maliciosas.

Una correcta administración de usuarios permite:

- garantizar que cada cuenta pertenezca a una persona identificable;
- evitar la existencia de cuentas innecesarias o duplicadas;
- reducir el riesgo de accesos indebidos;
- facilitar la asignación de permisos según las funciones de cada usuario;
- mantener actualizada la información de las cuentas;
- mejorar la trazabilidad de las acciones realizadas en los sistemas.

La gestión de usuarios forma parte de las políticas de seguridad de cualquier organización y constituye un requisito fundamental en normas y estándares como la familia ISO/IEC 27000.

3.3.3. Ciclo de Vida de una Cuenta de Usuario

Toda cuenta de usuario atraviesa distintas etapas desde su creación hasta su eliminación. Este conjunto de etapas se conoce como **ciclo de vida de la cuenta**.

Administrar correctamente este ciclo permite reducir riesgos y mantener actualizado el control sobre quién puede acceder a los sistemas.

Las etapas principales son:

3.3.3.1. Alta de la cuenta

El **alta** consiste en crear una nueva cuenta cuando una persona necesita acceder a uno o más sistemas de la organización.

Durante esta etapa normalmente se realiza:

- creación del identificador de usuario;
- asignación de una contraseña inicial o mecanismo de autenticación;
- incorporación a los grupos correspondientes;
- asignación de permisos mínimos necesarios;
- registro de la creación de la cuenta.

Es recomendable que el usuario cambie su contraseña en el primer inicio de sesión.

3.3.3.2. Modificación de la cuenta

Durante la vida laboral o académica de un usuario pueden producirse cambios que requieran modificar su cuenta.

Algunos ejemplos son:

- cambio de puesto de trabajo;
- incorporación a un nuevo proyecto;
- cambio de departamento;
- modificación de responsabilidades.

En estos casos deben revisarse los permisos existentes y actualizarse únicamente aquellos que sean necesarios para las nuevas funciones.

3.3.3.3. Suspensión de la cuenta

La **suspensión** consiste en deshabilitar temporalmente una cuenta sin eliminarla.

Puede aplicarse en situaciones como:

- licencias prolongadas;
- vacaciones extensas;
- suspensión laboral;
- investigaciones internas;
- inactividad prolongada.

Una cuenta suspendida conserva su información, pero no permite iniciar sesión hasta ser reactivada.

3.3.3.4. Baja de la cuenta

La **baja** representa la etapa final del ciclo de vida. Se realiza cuando el usuario deja definitivamente de necesitar acceso al sistema.

Las causas más habituales son:

- finalización de la relación laboral;
- egreso de un estudiante;
- finalización de un contrato;
- eliminación de un servicio.

Al dar de baja una cuenta deben eliminarse o revocarse todos los permisos asociados y conservar únicamente la información necesaria para fines administrativos o de auditoría, de acuerdo con las políticas de la organización.

Mantener cuentas inactivas constituye una práctica insegura, ya que pueden convertirse en un punto de acceso para personas no autorizadas.

3.3.4. Tipos de Cuentas

No todas las cuentas de usuario poseen la misma finalidad. Dependiendo de las funciones que desempeñan, es posible distinguir distintos tipos.

3.3.4.1. Cuenta de Administrador

Las cuentas de administrador poseen privilegios elevados que permiten instalar software, modificar configuraciones del sistema, crear usuarios y administrar permisos.

Debido a su alto nivel de privilegios, estas cuentas deben utilizarse únicamente para tareas administrativas y no para el trabajo cotidiano.

3.3.4.2. Cuenta de Usuario Estándar

Es la cuenta utilizada por la mayoría de los usuarios. Permite ejecutar las tareas habituales necesarias para desarrollar el trabajo diario, pero limita las operaciones que podrían afectar la seguridad o el funcionamiento del sistema.

Siempre que sea posible, los usuarios deberían trabajar con este tipo de cuentas.

3.3.4.3. Cuenta de Invitado

Las cuentas de invitado ofrecen acceso muy limitado y generalmente se utilizan para usuarios temporales o visitantes.

Actualmente muchas organizaciones prefieren no habilitar este tipo de cuentas debido a los riesgos de seguridad que pueden representar.

3.3.4.4. Cuenta de Servicio

Las cuentas de servicio no pertenecen a personas físicas, sino que son utilizadas por aplicaciones, procesos automáticos o servicios del sistema para comunicarse entre sí.

Por ejemplo:

- servicios de bases de datos;
- servidores web;
- servicios de respaldo;
- aplicaciones corporativas.

Estas cuentas deben administrarse cuidadosamente, ya que suelen ejecutarse de forma permanente y, en muchos casos, poseen privilegios elevados.

3.3.5. Gestión de Grupos

Administrar permisos individualmente para cientos o miles de usuarios resulta una tarea compleja y propensa a errores. Para simplificar esta administración, los sistemas permiten organizar a los usuarios en **grupos**.

Un grupo reúne usuarios que comparten funciones similares dentro de la organización y facilita la asignación de permisos comunes.

Por ejemplo, una universidad podría definir los siguientes grupos:

- Estudiantes.
- Docentes.
- Personal Administrativo.

- Directores de Carrera.
- Administradores del Sistema.

En lugar de asignar permisos uno por uno, estos se asignan al grupo correspondiente y cada usuario hereda automáticamente los permisos del grupo al que pertenece.

Las principales ventajas de utilizar grupos son:

- simplifican la administración de usuarios;
- reducen errores en la asignación de permisos;
- facilitan los cambios de funciones;
- mejoran la organización de los sistemas;
- favorecen el cumplimiento del principio del mínimo privilegio.

La gestión mediante grupos constituye una práctica ampliamente utilizada en sistemas operativos, directorios corporativos y aplicaciones empresariales, ya que permite administrar de manera eficiente grandes cantidades de usuarios.

3.4. Gestión de Privilegios y Modelos de Control de Acceso

Una vez que un usuario ha sido identificado, autenticado y autorizado para ingresar a un sistema, surge una pregunta fundamental:

¿Qué acciones puede realizar dentro del sistema?

La respuesta depende de los **privilegios** y **permisos** que tenga asignados. Una correcta gestión de privilegios permite proteger la información y evitar que los usuarios realicen acciones para las cuales no están autorizados.

3.4.1. Concepto de Permiso, Privilegio y Rol

Aunque suelen utilizarse como sinónimos, los términos **permiso**, **privilegio** y **rol** poseen significados diferentes.

3.4.1.1. Permiso

Un **permiso** es la autorización para realizar una acción específica sobre un recurso.

Algunos ejemplos son:

- leer un archivo;
- modificar un documento;
- eliminar un registro de una base de datos;
- imprimir un informe;
- ejecutar una aplicación.

Los permisos constituyen la unidad básica del control de acceso.

3.4.1.2. Privilegio

Un **privilegio** es un conjunto de permisos que permite realizar tareas de mayor importancia o impacto sobre un sistema.

Por ejemplo, un administrador puede tener privilegios para:

- crear usuarios;
- modificar permisos;
- instalar programas;
- configurar servicios;
- administrar dispositivos.

Cuanto mayores son los privilegios asignados a un usuario, mayor es el impacto que podrían tener sus acciones sobre el sistema.

3.4.1.3. Rol

Un **rol** representa una función o responsabilidad dentro de una organización y agrupa los permisos necesarios para desempeñar dicha función.

Por ejemplo, en una universidad podrían existir los siguientes roles:

Rol	Permisos principales
Estudiante	Consultar materias, inscribirse a exámenes y visualizar calificaciones.
Docente	Cargar notas, administrar cursos y consultar información académica de sus asignaturas.
Secretario Académico	Gestionar planes de estudio y administrar inscripciones.
Administrador del Sistema	Configurar el sistema, crear usuarios y administrar permisos.

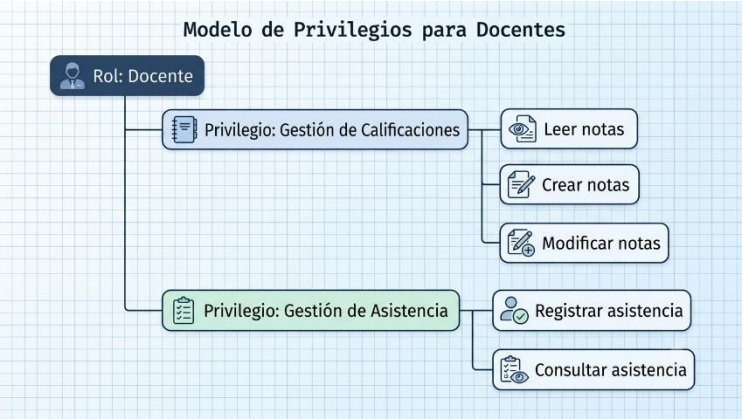
Asignar permisos mediante roles simplifica considerablemente la administración de grandes cantidades de usuarios.

3.4.1.4. Relación entre permiso, privilegio y rol

Los tres conceptos están estrechamente relacionados.

Un **rol** agrupa uno o más **privilegios**, y cada privilegio está formado por uno o varios **permisos**.

Por ejemplo:



Esta organización facilita la administración de permisos y reduce la probabilidad de errores.

3.4.2. Principio del Mínimo Privilegio

Uno de los principios fundamentales de la Seguridad Informática es el **Principio del Mínimo Privilegio**.

Este principio establece que:

Cada usuario debe disponer únicamente de los permisos estrictamente necesarios para realizar sus tareas y nada más.

El objetivo es reducir el riesgo de errores, accesos indebidos y daños ocasionados por acciones accidentales o maliciosas.

Por ejemplo:

- un estudiante no necesita permisos para modificar las calificaciones de otros alumnos;
- un docente no requiere acceso a la configuración del servidor;
- un empleado del área administrativa no debería tener permisos para instalar software en todos los equipos de la organización.

Aplicar este principio ofrece numerosas ventajas:

- reduce la superficie de ataque;
- limita el impacto de un incidente de seguridad;
- disminuye los errores de configuración;
- facilita las tareas de auditoría;
- mejora el cumplimiento de las políticas de seguridad.

El principio del mínimo privilegio constituye una buena práctica recomendada por normas internacionales como la **ISO/IEC 27002** y el **NIST**.

3.4.3. Separación de Funciones

La **separación de funciones** consiste en distribuir tareas críticas entre diferentes personas para evitar que un único usuario tenga el control absoluto de un proceso. Este principio busca reducir el riesgo de fraude, errores y abuso de privilegios.

Por ejemplo, en una empresa:

- un empleado registra una orden de compra;
- otro empleado la aprueba;
- un tercero realiza el pago.

De esta forma, ninguna persona puede controlar completamente todo el proceso.

En un sistema informático también pueden separarse responsabilidades.

Por ejemplo:

Usuario	Función
Administrador de Usuarios	Crea cuentas y asigna roles.
Administrador de Bases de Datos	Gestiona la base de datos.
Auditor	Revisa los registros de actividad.
Operador	Ejecuta tareas operativas del sistema.

La separación de funciones reduce el riesgo de que un error o una acción maliciosa comprometa la seguridad de la organización.

3.4.4. Modelos de Control de Acceso

Existen diferentes formas de administrar permisos dentro de un sistema informático. Estas formas reciben el nombre de **modelos de control de acceso**.

Los modelos de control de acceso establecen la forma en que un sistema administra los permisos de los usuarios sobre los recursos informáticos.

Cada modelo define **quién puede asignar permisos**, **cómo se administran** y **qué nivel de flexibilidad o seguridad ofrece**.

No existe un modelo universalmente mejor que otro. La elección depende de las necesidades de cada organización, del tipo de información que se protege y del nivel de seguridad requerido.

Los modelos más utilizados son:

- DAC (Discretionary Access Control).
- MAC (Mandatory Access Control).
- RBAC (Role-Based Access Control).
- ABAC (Attribute-Based Access Control).

3.4.4.1. DAC (Discretionary Access Control)

El **Control de Acceso Discrecional (DAC)** es uno de los modelos más antiguos y ampliamente utilizados. En este modelo, el **propietario de un recurso** decide quién puede acceder a él y qué acciones puede realizar.

Por ejemplo, si un usuario crea un documento, normalmente podrá decidir:

- quién puede leerlo;
- quién puede modificarlo;
- quién puede eliminarlo;
- quién puede compartirlo.

El sistema simplemente proporciona los mecanismos para administrar esos permisos.

Características

- El propietario controla los permisos.
- Los permisos pueden modificarse fácilmente.
- Es un modelo flexible.
- Su administración resulta sencilla en sistemas pequeños.

Ventajas

- Fácil de utilizar.
- Gran flexibilidad.
- Los usuarios pueden administrar sus propios recursos.

Desventajas

- Difícil de controlar en organizaciones grandes.
- Puede producir asignaciones incorrectas de permisos.
- Existe mayor riesgo de propagación de accesos no autorizados.

Ejemplo

Supóngase que un profesor crea un archivo con las notas de sus alumnos.

Como propietario del archivo puede decidir:

- compartirlo con otro profesor;
- permitir únicamente la lectura;
- autorizar también su modificación.

En este caso, el propietario administra directamente los permisos.

3.4.4.2. MAC (Mandatory Access Control)

El **Control de Acceso Obligatorio (MAC)** se utiliza en organizaciones donde la seguridad tiene prioridad sobre la flexibilidad.

En este modelo, **los usuarios no pueden modificar los permisos**.

Las reglas de acceso son establecidas por la organización mediante una política centralizada y son aplicadas automáticamente por el sistema.

Los recursos y los usuarios reciben **niveles de clasificación**, y el sistema determina qué accesos están permitidos.

Ejemplo de clasificaciones

- Público.
- Uso interno.
- Confidencial.
- Secreto.
- Alto secreto.

Un usuario únicamente podrá acceder a la información compatible con el nivel de autorización que posea.

Características

- Administración completamente centralizada.
- Los usuarios no modifican permisos.
- Alto nivel de seguridad.
- Poco flexible.

Ventajas

- Excelente protección de la información.
- Reduce errores humanos.
- Muy adecuado para información sensible.

Desventajas

- Administración más compleja.
- Menor flexibilidad.
- Mayor costo de implementación.

Ejemplo

Un organismo gubernamental almacena documentos clasificados.

Un empleado con autorización **Confidencial** podrá acceder únicamente a documentos clasificados como **Confidencial** o inferiores, pero nunca a documentos **Secretos**.

Aunque el propietario del documento quisiera compartirlo, el sistema no lo permitiría porque las reglas son obligatorias.

3.4.4.3. RBAC (Role-Based Access Control)

El **Control de Acceso Basado en Roles (RBAC)** es actualmente el modelo más utilizado en empresas, universidades y organismos públicos.

En lugar de asignar permisos directamente a cada usuario, los permisos se asignan a **roles**.

Posteriormente, cada usuario recibe uno o más roles según las funciones que desempeña. Este enfoque simplifica enormemente la administración cuando existen muchos usuarios.

Funcionamiento

Por ejemplo:

Rol	Permisos
Estudiante	Consultar materias y notas.
Docente	Cargar notas y administrar cursos.
Director	Consultar información académica completa.
Administrador	Configurar el sistema y administrar usuarios.

Cuando un docente deja de ser director, basta con quitarle el rol correspondiente; automáticamente perderá todos los permisos asociados.

Características

- Los permisos se asignan a roles.
- Los usuarios heredan los permisos de sus roles.
- Fácil administración.
- Escalable.

Ventajas

- Simplifica la administración.
- Reduce errores.
- Facilita auditorías.
- Muy adecuado para organizaciones grandes.

Desventajas

- Requiere una buena definición de roles.
- Puede aumentar la complejidad si existen demasiados roles.

Ejemplo

En una universidad:

- todos los docentes pertenecen al rol **Docente**;
- todos los estudiantes pertenecen al rol **Estudiante**;
- todos los administradores pertenecen al rol **Administrador**.

Cada usuario recibe automáticamente los permisos correspondientes a su rol.

3.4.4.4. ABAC (Attribute-Based Access Control)

El **Control de Acceso Basado en Atributos (ABAC)** es un modelo más moderno y flexible. En lugar de tomar decisiones únicamente según el usuario o el rol, el sistema evalúa un conjunto de **atributos** antes de autorizar el acceso.

Estos atributos pueden pertenecer a:

- el usuario;
- el recurso;
- la acción solicitada;
- el entorno donde se realiza el acceso.

Ejemplos de atributos

Del usuario

- departamento;

- cargo;
- edad;
- ubicación.

Del recurso

- clasificación del documento;
- propietario;
- tipo de archivo.

Del entorno

- horario;
- dirección IP;
- ubicación geográfica;
- dispositivo utilizado.

Ejemplo

Un sistema podría establecer la siguiente regla:

Un médico podrá acceder a las historias clínicas únicamente si pertenece al servicio correspondiente, se encuentra dentro del hospital y realiza el acceso durante su horario laboral.

Como puede observarse, la decisión no depende únicamente del usuario, sino de múltiples condiciones evaluadas simultáneamente.

Características

- Gran flexibilidad.
- Decisiones dinámicas.
- Basado en políticas.

Ventajas

- Muy adaptable.
- Permite reglas complejas.
- Adecuado para servicios en la nube.

Desventajas

- Diseño más complejo.
- Requiere una adecuada definición de atributos y políticas.

Actualmente muchos proveedores de servicios en la nube utilizan variantes del modelo ABAC para administrar permisos de manera dinámica.

3.4.5. Comparación entre los Modelos de Control de Acceso

Cada modelo presenta características particulares que lo hacen más adecuado para determinados escenarios.

Característica	DAC	MAC	RBAC	ABAC
¿Quién administra los permisos?	Propietario del recurso	Organización	Organización mediante roles	Políticas basadas en atributos
Flexibilidad	Alta	Baja	Media-Alta	Muy alta
Facilidad de administración	Media	Baja	Alta	Media
Nivel de seguridad	Medio	Muy alto	Alto	Muy alto
Escalabilidad	Baja	Media	Alta	Muy alta
Uso habitual	Equipos personales y pequeños entornos	Organismos gubernamentales y militares	Empresas, universidades y organismos públicos	Plataformas en la nube y sistemas modernos

Puede observarse que la evolución de estos modelos busca equilibrar dos aspectos fundamentales: la facilidad de administración y el nivel de seguridad. Mientras DAC ofrece mayor flexibilidad, MAC prioriza la protección de la información. RBAC simplifica la administración mediante roles y ABAC incorpora reglas dinámicas basadas en atributos, adaptándose mejor a los entornos tecnológicos actuales.

3.4.6. Casos de Aplicación

Cada modelo resulta más apropiado para determinados contextos.

Modelo	Ejemplo de aplicación
DAC	Computadoras personales y compartición de archivos entre usuarios.
MAC	Organismos militares, fuerzas de seguridad y organismos gubernamentales con información clasificada.
RBAC	Universidades, hospitales, bancos, empresas y organismos públicos.
ABAC	Plataformas de computación en la nube, servicios web y aplicaciones empresariales con políticas de acceso dinámicas.

En la práctica, muchas organizaciones combinan varios modelos de control de acceso para satisfacer diferentes necesidades de seguridad. Por ejemplo, una empresa puede utilizar **RBAC** para administrar los permisos generales de sus empleados y aplicar reglas **ABAC** para restringir el acceso a determinados recursos según el horario, la ubicación o el dispositivo desde el cual se realiza la conexión.

3.5. Políticas de Contraseñas

Las contraseñas constituyen uno de los mecanismos de autenticación más utilizados para proteger el acceso a sistemas informáticos. A pesar del crecimiento de tecnologías como la autenticación multifactor y la biometría, la mayoría de las aplicaciones, sistemas operativos y servicios en línea continúan utilizando contraseñas como primer mecanismo para verificar la identidad de los usuarios.

Sin embargo, una contraseña débil puede comprometer la seguridad de toda una organización. Por esta razón, las empresas establecen **políticas de contraseñas**, es decir, un conjunto de normas que regulan su creación, uso, almacenamiento y renovación.

El objetivo principal de estas políticas es reducir el riesgo de accesos no autorizados y proteger la información frente a ataques dirigidos a las credenciales de los usuarios.

3.5.1. Concepto

Una **política de contraseñas** es el conjunto de reglas definidas por una organización para garantizar que las credenciales utilizadas por los usuarios posean un nivel adecuado de seguridad.

Estas políticas buscan establecer criterios uniformes respecto a:

- creación de contraseñas;
- longitud mínima;
- complejidad;
- almacenamiento;
- renovación;
- reutilización;
- protección frente a intentos de acceso no autorizados.

Las políticas deben aplicarse a todos los usuarios de la organización, independientemente de su cargo o nivel jerárquico.

3.5.2. Características de una Contraseña Segura

Una contraseña segura debe resultar difícil de adivinar tanto para una persona como para un programa diseñado para descubrirla mediante ataques automáticos.

Entre las principales características de una contraseña segura se encuentran las siguientes.

3.5.2.1. Longitud suficiente

Actualmente se recomienda utilizar contraseñas de **al menos 12 caracteres**, ya que una mayor longitud incrementa significativamente la cantidad de combinaciones posibles.

En sistemas que protegen información especialmente sensible pueden exigirse contraseñas aún más largas.

3.5.2.2. Combinación de distintos tipos de caracteres

Siempre que el sistema lo permita, es conveniente combinar:

- letras mayúsculas;
- letras minúsculas;
- números;
- caracteres especiales.

Esta combinación aumenta la dificultad para adivinar la contraseña mediante ataques automatizados.

3.5.2.3. Evitar información personal

No deben utilizarse datos fáciles de obtener, tales como:

- nombre o apellido;
- fecha de nacimiento;
- número de documento;
- nombre de familiares;
- nombre de mascotas;
- teléfono;
- dirección.

Esta información suele encontrarse fácilmente en redes sociales u otras fuentes públicas.

3.5.2.4. Evitar palabras comunes

Las palabras presentes en diccionarios, nombres de ciudades, deportes, equipos de fútbol o secuencias simples son las primeras utilizadas en los ataques de diccionario.

Ejemplos poco seguros:

- `password`
- `admin`
- `123456`
- `abcdef`
- `qwerty`
- `argentina`

3.5.2.5. Utilizar una contraseña diferente para cada servicio

Reutilizar la misma contraseña en varios sistemas representa uno de los mayores riesgos actuales. Si un servicio sufre una filtración de credenciales, un atacante podría intentar utilizar la misma contraseña para acceder a otros sistemas donde el usuario tenga una cuenta.

3.5.2.6. Preferir frases de paso (Passphrase)

En lugar de una contraseña corta y compleja, muchas organizaciones recomiendan utilizar una **frase de paso** (*passphrase*).

Por ejemplo:

```
MiPerroCorrePorElParqueTodosLosDias2026
```

Este tipo de contraseña resulta más sencilla de recordar y, al mismo tiempo, ofrece una elevada resistencia frente a ataques de fuerza bruta debido a su longitud.

3.5.3. Políticas de Complejidad

Las políticas de complejidad establecen los requisitos mínimos que deben cumplir las contraseñas utilizadas dentro de una organización.

Aunque pueden variar según el tipo de sistema, es habitual que incluyan reglas como las siguientes:

- longitud mínima de 12 caracteres;
- combinación de mayúsculas y minúsculas;
- inclusión de números;
- inclusión de caracteres especiales;
- prohibición de utilizar el nombre del usuario;
- prohibición de reutilizar las últimas contraseñas utilizadas;
- verificación contra listas de contraseñas comprometidas.

Además de definir estas reglas, muchas organizaciones implementan controles automáticos que impiden aceptar contraseñas que no cumplan con los requisitos establecidos.

Es importante señalar que las recomendaciones actuales priorizan **la longitud y la unicidad** de la contraseña por encima de reglas excesivamente complejas que dificulten su memorización.

3.5.4. Bloqueo de Cuentas

Una medida complementaria para proteger las credenciales consiste en limitar la cantidad de intentos fallidos de autenticación.

Cuando un usuario introduce repetidamente una contraseña incorrecta, el sistema puede:

- bloquear temporalmente la cuenta;
- aumentar progresivamente el tiempo de espera entre intentos;
- solicitar mecanismos adicionales de autenticación;
- notificar el evento al administrador.

Estas medidas reducen significativamente la eficacia de los ataques de fuerza bruta, en los cuales un atacante intenta probar una gran cantidad de contraseñas hasta encontrar la correcta. El tiempo de bloqueo y la cantidad máxima de intentos permitidos dependen de la política de seguridad definida por cada organización.

3.5.5. Gestores de Contraseñas

A medida que aumenta la cantidad de servicios utilizados por una persona, resulta cada vez más difícil recordar una contraseña diferente para cada uno de ellos. Para resolver este problema existen los **gestores de contraseñas**, aplicaciones diseñadas para almacenar de forma segura las credenciales de acceso.

Estos programas permiten:

- generar contraseñas aleatorias;
- almacenar las credenciales cifradas;
- completar automáticamente formularios de inicio de sesión;
- sincronizar contraseñas entre distintos dispositivos;
- facilitar el uso de contraseñas únicas para cada servicio.

El usuario únicamente necesita recordar una **contraseña maestra**, que protege el acceso al gestor. No obstante, dicha contraseña debe ser especialmente robusta, ya que constituye la llave de acceso a todas las demás credenciales almacenadas. El uso de gestores de contraseñas es actualmente una de las prácticas recomendadas por organismos internacionales dedicados a la ciberseguridad.

3.5.6. Recomendaciones para el uso seguro de contraseñas

Como complemento a las políticas de seguridad, es conveniente que los usuarios adopten las siguientes buenas prácticas:

- utilizar una contraseña distinta para cada servicio;
- emplear frases de paso cuando sea posible;
- activar la autenticación multifactor en los servicios que la soporten;
- utilizar gestores de contraseñas confiables;
- no compartir las contraseñas con otras personas;
- no anotarlas en lugares visibles;
- evitar enviarlas por correo electrónico o aplicaciones de mensajería;
- modificar inmediatamente una contraseña cuando exista sospecha de que ha sido comprometida.

La seguridad de un sistema no depende únicamente de la fortaleza de las contraseñas, sino también del comportamiento responsable de los usuarios y del cumplimiento de las políticas de seguridad establecidas por la organización.

3.6. Autenticación Multifactor

La autenticación basada únicamente en una contraseña presenta una limitación importante: si un atacante logra obtener esa contraseña, podrá acceder al sistema haciéndose pasar por el usuario legítimo.

Para reducir este riesgo surgió la **Autenticación Multifactor** (*Multi-Factor Authentication*, **MFA**), un mecanismo que exige la utilización de **dos o más factores de autenticación independientes** para verificar la identidad de un usuario.

De esta manera, aunque uno de los factores sea comprometido, el atacante todavía deberá superar los demás mecanismos de verificación para obtener acceso al sistema.

Actualmente, la autenticación multifactor es considerada una de las medidas más eficaces para proteger cuentas de correo electrónico, servicios bancarios, plataformas en la nube y sistemas corporativos.

3.6.1. Concepto

La **Autenticación Multifactor (MFA)** es un mecanismo de seguridad que requiere que el usuario demuestre su identidad utilizando **dos o más factores de autenticación pertenecientes a categorías diferentes**.

El objetivo es aumentar el nivel de seguridad durante el proceso de inicio de sesión y reducir el riesgo de accesos no autorizados.

Por ejemplo, además de ingresar una contraseña, el sistema puede solicitar un código temporal generado por una aplicación móvil o una huella dactilar.

La utilización de múltiples factores dificulta considerablemente los ataques basados en el robo o filtración de contraseñas.

Es importante distinguir entre:

- **Autenticación de un solo factor (Single-Factor Authentication - SFA):** utiliza únicamente un mecanismo de autenticación, como una contraseña.
- **Autenticación de dos factores (Two-Factor Authentication - 2FA):** utiliza exactamente dos factores diferentes.
- **Autenticación multifactor (MFA):** utiliza dos o más factores pertenecientes a distintas categorías.

En la práctica, el término **MFA** engloba también a la autenticación de dos factores.

3.6.2. Factores de Autenticación

Los factores de autenticación se clasifican según el tipo de evidencia utilizada para demostrar la identidad del usuario.

3.6.2.1. Algo que sé (Factor de conocimiento)

Corresponde a información que únicamente debería conocer el usuario.

Ejemplos:

- contraseña;
- PIN;
- frase secreta;
- respuesta a una pregunta de seguridad.

Es el mecanismo más utilizado, aunque también el más vulnerable cuando se emplean contraseñas débiles o reutilizadas.

3.6.2.2. Algo que tengo (Factor de posesión)

Corresponde a un objeto físico que posee el usuario.

Ejemplos:

- teléfono móvil;
- token físico;
- tarjeta inteligente (Smart Card);
- llave de seguridad USB;
- aplicación autenticadora instalada en un dispositivo móvil.

Este factor incrementa considerablemente la seguridad, ya que un atacante necesitaría disponer físicamente del dispositivo.

3.6.2.3. Algo que soy (Factor biométrico)

Se basa en características físicas o biológicas del usuario.

Ejemplos:

- huella dactilar;
- reconocimiento facial;
- reconocimiento del iris;
- reconocimiento de voz;
- geometría de la mano.

La biometría resulta muy cómoda para el usuario, aunque debe utilizarse respetando las políticas de privacidad y protección de datos personales.

3.6.3. Métodos de Autenticación Multifactor

Existen diferentes mecanismos para implementar la autenticación multifactor.

Los más utilizados son los siguientes.

3.6.3.1. Aplicaciones Autenticadoras

Son aplicaciones instaladas en teléfonos móviles que generan códigos temporales de un solo uso (OTP), válidos durante un breve período de tiempo. Al iniciar sesión, el usuario ingresa su contraseña y posteriormente introduce el código generado por la aplicación.

Este método ofrece un buen equilibrio entre seguridad y facilidad de uso, por lo que es ampliamente utilizado en servicios en línea y sistemas empresariales.

3.6.3.2. Tokens Físicos

Un **token** es un dispositivo electrónico diseñado específicamente para generar códigos temporales o realizar procesos criptográficos de autenticación. Algunos modelos muestran un código que cambia periódicamente, mientras que otros requieren ser conectados al equipo para validar la identidad del usuario.

Los tokens físicos suelen emplearse en entidades financieras, organismos gubernamentales y organizaciones con altos requerimientos de seguridad.

3.6.3.3. Llaves de Seguridad

Las **llaves de seguridad** son dispositivos físicos que se conectan al equipo mediante USB, NFC o Bluetooth. Cuando el usuario intenta iniciar sesión, el sistema solicita la presencia de la llave para completar el proceso de autenticación.

Una de sus principales ventajas es que ofrecen una elevada protección frente a ataques de phishing, ya que verifican que el usuario se encuentre accediendo al sitio legítimo.

3.6.3.4. Biometría

La biometría también puede utilizarse como segundo factor de autenticación. En este caso, después de ingresar la contraseña, el usuario debe verificar su identidad mediante un rasgo biométrico, como su huella dactilar o reconocimiento facial.

Este método es ampliamente utilizado en teléfonos inteligentes y dispositivos modernos.

3.6.4. Ventajas y Limitaciones del MFA

La autenticación multifactor ofrece numerosas ventajas, aunque también presenta algunos desafíos que deben considerarse durante su implementación.

3.6.4.1. Ventajas

- Incrementa significativamente la seguridad de las cuentas.
- Reduce el impacto del robo o filtración de contraseñas.

- Dificulta los ataques de fuerza bruta y de phishing.
- Protege mejor el acceso a información crítica.
- Constituye una práctica recomendada por organismos internacionales como NIST e ISO.

3.6.4.2. Limitaciones

- Requiere un proceso de autenticación más complejo.
- Puede generar inconvenientes si el usuario pierde el dispositivo utilizado como segundo factor.
- Su implementación implica mayores costos de administración y soporte.
- Algunos usuarios pueden mostrar resistencia inicial debido al cambio en el proceso de inicio de sesión.

A pesar de estas limitaciones, los beneficios de la autenticación multifactor superan ampliamente sus inconvenientes, especialmente en sistemas que manejan información sensible o crítica.

3.6.5. Ejemplo de Autenticación Multifactor

Supóngase que un empleado desea acceder al sistema de gestión de una empresa.

El proceso de autenticación podría desarrollarse de la siguiente manera:

1. El usuario ingresa su nombre de usuario.
2. Introduce su contraseña.
3. El sistema verifica las credenciales.
4. Se solicita un código temporal generado por una aplicación autenticadora instalada en el teléfono móvil del usuario.
5. El usuario introduce el código recibido.
6. Si ambos factores son correctos, el sistema concede el acceso.

En este ejemplo se utilizan dos factores de autenticación diferentes:

- **Algo que sé:** la contraseña.
- **Algo que tengo:** el teléfono móvil con la aplicación autenticadora.

Aunque un atacante lograra obtener la contraseña, no podría acceder al sistema sin disponer también del segundo factor de autenticación.

3.7. Registro y Auditoría

Todo acceso a un sistema informático y muchas de las acciones realizadas por los usuarios generan información que puede ser almacenada para su posterior consulta. Estos registros permiten conocer qué ocurrió dentro de un sistema, quién realizó una determinada acción y en qué momento se produjo.

El registro de eventos constituye uno de los mecanismos más importantes de la Seguridad Lógica, ya que facilita la detección de actividades sospechosas, la investigación de incidentes y la realización de auditorías.

Sin un adecuado sistema de registros sería muy difícil determinar el origen de un problema de seguridad o reconstruir la secuencia de hechos ocurridos durante un incidente.

3.7.1. Concepto

El **registro y auditoría** comprende el conjunto de mecanismos destinados a **registrar, almacenar, supervisar y analizar las actividades realizadas dentro de un sistema informático**.

Cada vez que un usuario inicia sesión, modifica información, ejecuta una aplicación o realiza una operación importante, el sistema puede generar automáticamente un registro del evento.

Estos registros permiten:

- conocer las actividades realizadas por los usuarios;
- detectar comportamientos anómalos;
- investigar incidentes de seguridad;
- verificar el cumplimiento de las políticas de seguridad;
- facilitar auditorías internas y externas.

Es importante destacar que registrar información no es suficiente. Los registros deben revisarse periódicamente para identificar situaciones que puedan representar un riesgo para la organización.

3.7.2. Registros de Eventos (Logs)

Los **logs** son archivos o bases de datos donde el sistema almacena información acerca de los eventos que ocurren durante su funcionamiento. Cada registro suele contener diversos datos relacionados con el evento ocurrido.

Entre los datos más habituales se encuentran:

- fecha y hora;
- usuario involucrado;
- equipo o dirección IP de origen;
- recurso utilizado;
- operación realizada;
- resultado de la operación (éxito o error).

Por ejemplo, un registro podría indicar:

Fecha y hora	Usuario	Evento	Resultado
12/09/2026 08:15	jgarcia	Inicio de sesión	Correcto
12/09/2026 08:17	jgarcia	Consulta de expediente	Correcto
12/09/2026 08:35	jgarcia	Modificación de calificación	Correcto
12/09/2026 08:40	usuario123	Inicio de sesión	Contraseña incorrecta

Este tipo de información permite reconstruir posteriormente las actividades realizadas por los usuarios.

3.7.3. Tipos de registros

Dependiendo del sistema, pueden existir distintos tipos de registros.

3.7.3.1. Registros de autenticación

Almacenan información relacionada con:

- inicios de sesión;
- cierres de sesión;
- intentos fallidos de autenticación;
- bloqueos de cuentas.

3.7.3.2. Registros de acceso

Indican qué recursos fueron utilizados por cada usuario.

Por ejemplo:

- acceso a archivos;
- acceso a bases de datos;
- utilización de aplicaciones;
- acceso a servicios de red.

3.7.3.3. Registros administrativos

Registran actividades realizadas por administradores del sistema.

Algunos ejemplos son:

- creación de usuarios;
- modificación de permisos;
- instalación de software;
- cambios de configuración.

Debido a su importancia, estos registros suelen conservarse durante períodos más prolongados.

3.7.3.4. Registros de errores

Almacenan información sobre fallos producidos durante el funcionamiento del sistema. Estos registros resultan especialmente útiles para tareas de mantenimiento y resolución de problemas.

3.7.4. Eventos de Seguridad

No todos los eventos registrados poseen la misma importancia.

Los **eventos de seguridad** son aquellos que pueden afectar la confidencialidad, integridad o disponibilidad de los sistemas y de la información.

Algunos ejemplos son:

- múltiples intentos fallidos de inicio de sesión;
- creación de nuevas cuentas de administrador;
- modificación de permisos críticos;
- eliminación de registros;
- acceso fuera del horario habitual;
- acceso desde ubicaciones inusuales;
- desactivación de mecanismos de seguridad.

Estos eventos suelen generar alertas para que el personal responsable pueda analizarlos rápidamente. La detección temprana de eventos de seguridad permite actuar antes de que un incidente produzca daños mayores.

3.7.5. Trazabilidad

La **trazabilidad** es la capacidad de reconstruir las acciones realizadas dentro de un sistema a partir de los registros almacenados.

Gracias a la trazabilidad es posible responder preguntas como:

- ¿Quién realizó una determinada acción?
- ¿Cuándo ocurrió?
- ¿Desde qué equipo o dirección IP?
- ¿Qué información fue consultada o modificada?
- ¿Qué cambios se realizaron?

La trazabilidad constituye un requisito fundamental en sistemas que administran información crítica, como:

- bancos;
- hospitales;
- universidades;

- organismos gubernamentales;
- empresas de servicios.

Sin registros adecuados resulta prácticamente imposible investigar incidentes o determinar responsabilidades.

3.7.6. Importancia de la Auditoría

La **auditoría informática** consiste en revisar y evaluar los registros, procedimientos y controles de seguridad con el fin de verificar que los sistemas funcionen de acuerdo con las políticas establecidas por la organización.

Entre sus principales objetivos se encuentran:

- comprobar el cumplimiento de las políticas de seguridad;
- detectar configuraciones incorrectas;
- identificar actividades sospechosas;
- verificar la correcta administración de usuarios y privilegios;
- proponer mejoras para fortalecer la seguridad.

La auditoría puede realizarse de forma periódica o cuando ocurre un incidente de seguridad que requiere una investigación detallada.

Para que una auditoría sea efectiva, los registros deben cumplir ciertas características.

3.7.7. Características de un buen sistema de registros

- registrar los eventos importantes;
- almacenar información suficiente para identificar cada acción;
- proteger los registros contra modificaciones no autorizadas;
- conservar los registros durante el tiempo establecido por la organización;
- facilitar la búsqueda y el análisis de la información.

Si los registros pudieran modificarse fácilmente, perderían su valor como evidencia durante una investigación.

3.7.8. Ejemplo Integrador

Supóngase que una universidad detecta que las calificaciones de varios estudiantes fueron modificadas fuera del período habilitado.

El auditor consulta los registros del sistema y obtiene la siguiente información:

- usuario que realizó la modificación;
- fecha y hora del acceso;
- dirección IP desde la cual se efectuó la conexión;
- asignatura afectada;
- calificaciones modificadas;
- equipo utilizado para acceder al sistema.

Con esta información es posible reconstruir la secuencia de hechos, determinar si la modificación fue autorizada e identificar al responsable de la acción.

Este ejemplo muestra cómo los registros y la auditoría permiten investigar incidentes y fortalecer la seguridad de los sistemas informáticos.

3.8. Buenas Prácticas de Seguridad Lógica

La implementación de mecanismos de seguridad lógica no garantiza por sí sola la protección de los sistemas informáticos. Su eficacia depende también de que los usuarios y administradores adopten buenas prácticas en el uso y administración de los recursos tecnológicos.

Las buenas prácticas constituyen recomendaciones ampliamente aceptadas que contribuyen a reducir los riesgos de seguridad, minimizar errores humanos y mejorar la protección de la información.

A continuación, se presentan algunas de las prácticas más importantes que deberían aplicarse en cualquier organización.

3.8.1. Aplicar el Principio del Mínimo Privilegio

Cada usuario debe disponer únicamente de los permisos necesarios para realizar sus tareas habituales. No es recomendable otorgar privilegios administrativos a usuarios que no los necesitan, ya que esto incrementa el riesgo de modificaciones accidentales, instalación de software no autorizado o acceso indebido a información sensible.

Asimismo, los privilegios asignados deben revisarse periódicamente para verificar que continúen siendo necesarios.

3.8.2. Utilizar Cuentas Individuales

Cada usuario debe utilizar una cuenta personal e intransferible. El uso de cuentas compartidas dificulta identificar quién realizó una determinada acción y limita la posibilidad de efectuar auditorías confiables.

Cuando varias personas utilizan la misma cuenta resulta imposible determinar responsabilidades ante un incidente de seguridad. Siempre que sea posible, cada usuario debe contar con un identificador único dentro del sistema.

3.8.3. Utilizar Contraseñas Robustas

Las contraseñas constituyen la primera barrera de protección frente a accesos no autorizados.

Por ello se recomienda:

- utilizar contraseñas largas y difíciles de adivinar;

- evitar información personal;
- utilizar una contraseña diferente para cada servicio;
- no compartir las credenciales con otras personas;
- utilizar gestores de contraseñas cuando sea necesario.

Una contraseña robusta reduce significativamente el riesgo de ataques de fuerza bruta y de diccionario.

3.8.4. Implementar Autenticación Multifactor

Siempre que un sistema lo permita, resulta recomendable habilitar la autenticación multifactor (MFA).

La combinación de dos o más factores de autenticación proporciona una capa adicional de seguridad frente al robo o filtración de contraseñas. Actualmente, numerosos servicios de correo electrónico, plataformas en la nube y aplicaciones empresariales ofrecen soporte para este mecanismo.

3.8.5. Administrar Correctamente las Cuentas de Usuario

La administración de usuarios debe realizarse siguiendo procedimientos claramente definidos.

Entre las principales recomendaciones se encuentran:

- crear únicamente las cuentas necesarias;
- eliminar o deshabilitar cuentas que ya no se utilizan;
- revisar periódicamente los permisos asignados;
- mantener actualizada la información de los usuarios;
- evitar cuentas genéricas o anónimas.

Una adecuada gestión del ciclo de vida de las cuentas reduce considerablemente los riesgos de acceso no autorizado.

3.8.6. Revisar Periódicamente los Permisos

Las funciones de un usuario pueden cambiar con el tiempo. Como consecuencia, también deben revisarse los permisos que posee.

Es recomendable realizar auditorías periódicas para detectar:

- permisos innecesarios;
- privilegios excesivos;
- cuentas inactivas;
- usuarios duplicados;
- configuraciones incorrectas.

Esta práctica contribuye a mantener el principio del mínimo privilegio.

3.8.7. Supervisar los Registros de Eventos

Los registros de eventos constituyen una importante fuente de información para detectar incidentes de seguridad.

No basta con almacenar los registros; es necesario analizarlos periódicamente para identificar:

- intentos reiterados de autenticación fallida;
- accesos fuera del horario habitual;
- modificaciones de permisos;
- creación de nuevas cuentas administrativas;
- actividades inusuales.

Una supervisión continua permite detectar tempranamente posibles incidentes y adoptar medidas correctivas.

3.8.8. Capacitar a los Usuarios

La tecnología por sí sola no garantiza la seguridad de un sistema. Los usuarios deben conocer las políticas de seguridad de la organización y comprender los riesgos asociados al uso inadecuado de los recursos informáticos.

La capacitación debería incluir, entre otros temas:

- creación de contraseñas seguras;
- reconocimiento de correos electrónicos fraudulentos;
- protección de la información confidencial;
- uso adecuado de dispositivos corporativos;
- importancia de informar incidentes de seguridad.

La formación continua contribuye a reducir los errores humanos, una de las principales causas de los incidentes de seguridad.

3.8.9. Mantener Actualizados los Sistemas

Los fabricantes de sistemas operativos y aplicaciones publican periódicamente actualizaciones destinadas a corregir errores y vulnerabilidades de seguridad.

Por ello es recomendable:

- instalar actualizaciones de seguridad;
- mantener actualizado el software utilizado;
- eliminar aplicaciones que ya no sean necesarias;
- utilizar versiones soportadas por el fabricante.

Un sistema desactualizado puede contener vulnerabilidades conocidas que podrían ser aprovechadas por un atacante.

3.8.10. Cumplir las Políticas de Seguridad de la Organización

Todas las medidas técnicas estudiadas a lo largo de esta unidad deben complementarse con el cumplimiento de las políticas de seguridad establecidas por la organización. Estas políticas definen las normas que regulan el uso de los recursos informáticos y establecen las responsabilidades de usuarios, administradores y directivos.

Su cumplimiento favorece una administración uniforme de la seguridad y reduce la posibilidad de errores o incumplimientos.

3.9. Fraudes y Delitos Informáticos

Las tecnologías de la información han transformado la forma en que las organizaciones almacenan, procesan y transmiten información. Sin embargo, estas mismas tecnologías también han generado nuevas modalidades de fraude y nuevos tipos de delitos que aprovechan las vulnerabilidades de los sistemas informáticos.

Los mecanismos de **Seguridad Lógica** estudiados en esta unidad —como la autenticación, el control de acceso, la gestión de usuarios y la auditoría— constituyen herramientas fundamentales para prevenir estas conductas ilícitas.

Es importante diferenciar los conceptos de **fraude informático** y **delito informático**, ya que, aunque suelen utilizarse como sinónimos, poseen significados diferentes.

3.9.1. Concepto de Fraude Informático

El **fraude informático** consiste en la utilización indebida de sistemas informáticos, aplicaciones, redes o información digital con el objetivo de obtener un beneficio económico, comercial o personal mediante el engaño, la manipulación o el uso no autorizado de los recursos informáticos.

Su finalidad principal es obtener una ventaja indebida perjudicando a otra persona, empresa u organismo.

El fraude puede ser cometido por:

- usuarios externos;
- empleados de la organización;
- proveedores;
- administradores de sistemas;
- cualquier persona con acceso a los recursos informáticos.

No todos los fraudes informáticos constituyen automáticamente un delito penal. En algunos casos pueden tratarse de incumplimientos contractuales, faltas administrativas o conductas sancionadas únicamente dentro de una organización.

Ejemplos de fraude informático

- Un empleado modifica el sistema de liquidación de comisiones para incrementar ilegalmente su salario.
- Un usuario utiliza la cuenta informática de un compañero para realizar operaciones que le generan un beneficio personal.
- Una persona modifica datos de facturación para reducir el importe que debe pagar un cliente.
- Un proveedor altera registros electrónicos para simular la entrega de productos que nunca fueron enviados.

En todos estos casos existe una utilización indebida de los sistemas informáticos con el propósito de obtener un beneficio.

3.9.2. Concepto de Delito Informático

Un **delito informático** es una conducta ilícita realizada mediante sistemas informáticos o dirigida contra ellos, que se encuentra expresamente tipificada y sancionada por la legislación penal.

A diferencia del fraude informático, el delito informático posee una definición jurídica. Para que una conducta sea considerada delito debe estar prevista por una ley penal. En Argentina, la **Ley N.º 26.388**, sancionada en el año 2008, incorporó diversos delitos informáticos al Código Penal, adaptando la legislación a las nuevas tecnologías.

Esta ley protege distintos bienes jurídicos, entre ellos:

- la privacidad de las comunicaciones;
- la confidencialidad de la información;
- la integridad de los datos;
- los sistemas informáticos;
- las bases de datos personales;
- la integridad sexual cuando se utilizan medios informáticos para cometer determinados delitos.

Por lo tanto, mientras el fraude informático describe una conducta orientada a obtener un beneficio indebido, el delito informático hace referencia a aquellas conductas que la ley considera punibles.

3.9.3. Diferencias entre Fraude Informático y Delito Informático

Aunque ambos conceptos están relacionados, no representan exactamente la misma situación.

El fraude informático describe una conducta cuyo objetivo consiste en obtener una ventaja indebida mediante el uso de tecnologías de la información.

El delito informático, en cambio, hace referencia a una conducta prohibida por la ley penal.

En otras palabras, **el fraude informático pertenece principalmente al ámbito de la seguridad y de la gestión de riesgos**, mientras que **el delito informático pertenece al ámbito jurídico y penal**.

En determinadas circunstancias un mismo hecho puede constituir simultáneamente un fraude y un delito.

Por ejemplo, un atacante que obtiene las credenciales de acceso a una cuenta bancaria mediante phishing y realiza una transferencia de dinero sin autorización está cometiendo un fraude informático y, además, varios delitos tipificados por la legislación penal.

Sin embargo, no todo fraude constituye necesariamente un delito.

La siguiente tabla muestra la diferencia entre fraude y delito informático

Aspecto	Fraude Informático	Delito Informático
Definición	Uso indebido de sistemas informáticos para obtener un beneficio o ventaja indebida.	Conducta ilícita tipificada por la legislación penal.
Naturaleza	Técnica, organizacional o económica.	Jurídica y penal.
Objetivo principal	Obtener un beneficio económico o personal.	La conducta puede perseguir diversos fines (económicos, personales, ideológicos, etc.).
¿Siempre está previsto por la ley penal?	No necesariamente.	Sí.
Consecuencia	Puede generar sanciones administrativas, civiles o penales, según el caso.	Puede dar lugar a una investigación penal y a las sanciones previstas por la ley.

Ejemplos comparativos

Situación	¿Fraude?	¿Delito?
Un empleado modifica el sistema para incrementar ilegalmente sus comisiones.	Si	Puede serlo, según el caso y el perjuicio ocasionado.
Un usuario utiliza la contraseña de otro empleado para acceder a información confidencial.	Si	Si
Un atacante instala un ransomware que cifra la información de una empresa y exige un rescate.	Si	Si

Situación	¿Fraude?	¿Delito?
Un administrador consulta información confidencial sin autorización, pero sin obtener beneficio económico.	No	Si
Un cliente registra información falsa para obtener un descuento no autorizado en una plataforma de ventas.	Si	Puede serlo, dependiendo de la legislación aplicable.

Puede observarse que el concepto de fraude está asociado al **beneficio indebido**, mientras que el concepto de delito depende de la existencia de una conducta sancionada por la legislación penal.

3.9.4. Principales Delitos Informáticos incorporados por la Ley N.º 26.388

La **Ley N.º 26.388**, sancionada en el año 2008, modificó diversos artículos del Código Penal Argentino para incorporar delitos relacionados con el uso de las tecnologías de la información. Antes de esta ley, muchas conductas realizadas mediante computadoras o redes informáticas no se encontraban expresamente contempladas por la legislación penal.

La norma incorporó figuras destinadas a proteger bienes jurídicos como:

- la privacidad de las comunicaciones;
- la confidencialidad de la información;
- la integridad de los datos;
- el correcto funcionamiento de los sistemas informáticos;
- las bases de datos personales;
- la integridad sexual cuando intervienen medios informáticos.

A continuación, se presentan los delitos más relevantes para el profesional informático.

3.9.4.1. Violación de secretos y de la privacidad

Uno de los principios fundamentales de la Seguridad Informática es la **confidencialidad**. La Ley 26.388 protege este principio sancionando a quienes acceden, interceptan o divulgan comunicaciones privadas sin autorización.

Entre las principales conductas sancionadas se encuentran:

- acceder indebidamente a correos electrónicos ajenos;
- interceptar comunicaciones electrónicas privadas;
- desviar comunicaciones destinadas a otra persona;
- divulgar información obtenida ilícitamente mediante el acceso a comunicaciones privadas.

No es necesario modificar la información para cometer el delito; basta con acceder o conocer comunicaciones privadas sin autorización.

Ejemplo

Un administrador de sistemas utiliza sus privilegios para leer los correos electrónicos personales de un empleado sin autorización. Aunque no modifique ningún mensaje ni obtenga dinero mediante esa acción, está vulnerando la privacidad del usuario.

Relación con la Seguridad Lógica

Este delito puede prevenirse mediante:

- políticas de control de acceso;
- gestión adecuada de privilegios;
- registros de auditoría;
- autenticación robusta.

3.9.4.2. Acceso ilegítimo a sistemas y bases de datos

La ley también sanciona el acceso no autorizado a sistemas informáticos o bases de datos protegidas. El objetivo consiste en proteger la información almacenada por organizaciones públicas y privadas.

Entre las conductas sancionadas pueden encontrarse:

- ingresar a un sistema utilizando credenciales robadas;
- acceder a una base de datos sin autorización;
- consultar información protegida aprovechando vulnerabilidades del sistema.

En el caso de bases de datos personales, la legislación brinda una protección especial debido al carácter sensible de la información almacenada.

Ejemplo

Un atacante obtiene la contraseña de un empleado mediante phishing e ingresa al sistema de gestión de clientes para consultar información personal. Aunque no modifique ningún dato, el simple acceso no autorizado constituye una conducta sancionada por la legislación.

Relación con la Seguridad Lógica

Este delito puede prevenirse mediante:

- autenticación multifactor;
- políticas de contraseñas;
- gestión de usuarios;
- principio del mínimo privilegio;
- monitoreo de accesos.

3.9.4.3. Daño Informático

El daño informático consiste en destruir, alterar, inutilizar o deteriorar datos, programas o sistemas informáticos.

Este delito afecta directamente el principio de **integridad** y, en muchos casos, también la **disponibilidad** de la información.

Algunas conductas comprendidas son:

- eliminar archivos de forma intencional;
- modificar información crítica;
- destruir bases de datos;
- inutilizar aplicaciones;
- alterar el funcionamiento de servidores.

El daño puede producirse tanto por personas externas como por empleados con acceso legítimo a los sistemas.

Ejemplo

Un empleado despedido elimina deliberadamente la base de datos de clientes antes de abandonar la empresa. La organización pierde información crítica y debe restaurarla utilizando las copias de seguridad.

Relación con la Seguridad Lógica

Los principales mecanismos de prevención son:

- control de privilegios;
- auditoría de operaciones;
- separación de funciones;
- copias de seguridad periódicas;
- registro de actividades.

3.9.4.4. Fraude Informático

La Ley 26.388 también contempla diversas conductas relacionadas con la utilización de medios informáticos para obtener beneficios económicos ilícitos.

Estas conductas incluyen, entre otras:

- manipulación de registros electrónicos;
- modificación de datos financieros;
- alteración de sistemas de facturación;
- utilización indebida de credenciales para realizar operaciones económicas.

En este tipo de delitos el objetivo principal consiste en obtener un beneficio económico mediante el uso fraudulento de sistemas informáticos.

Ejemplo

Un atacante modifica el número de cuenta bancaria registrado en el sistema de pagos de una empresa. Cuando se realiza la transferencia correspondiente al proveedor, el dinero es enviado a la cuenta del atacante.

Relación con la Seguridad Lógica

Los controles que ayudan a prevenir este tipo de fraude son:

- segregación de funciones;
- auditoría permanente;
- autorización de operaciones críticas;
- autenticación multifactor;
- revisión periódica de permisos.

3.9.4.5. Delitos contra la Integridad Sexual

La Ley 26.388 también incorporó modificaciones destinadas a sancionar delitos contra la integridad sexual cuando intervienen tecnologías de la información. Entre las principales conductas contempladas se encuentran aquellas relacionadas con la utilización de medios informáticos para producir, distribuir o difundir material de abuso sexual infantil.

La legislación protege especialmente a los menores de edad frente a la utilización de Internet como medio para cometer este tipo de delitos.

No corresponde a esta asignatura estudiar los aspectos jurídicos de estas figuras penales, pero resulta importante que el futuro profesional informático conozca que estos hechos constituyen delitos graves y que las tecnologías pueden ser utilizadas como medio para cometerlos.

Ejemplo

Una organización detecta que uno de sus servidores está siendo utilizado para almacenar o distribuir material ilegal. Además de eliminar el contenido y preservar la evidencia digital, deberá informar inmediatamente a las autoridades competentes.

Relación con la Seguridad Lógica

Los mecanismos que ayudan a prevenir estas situaciones incluyen:

- monitoreo de servidores;
- registros de auditoría;
- control de acceso;
- políticas de uso aceptable de los recursos informáticos;

- sistemas de detección de actividades sospechosas.

Importancia para el profesional informático

El ingeniero o profesional de informática no tiene como función determinar si una persona es culpable de un delito, ya que esa tarea corresponde a la Justicia.

Sin embargo, sí debe ser capaz de:

- identificar conductas sospechosas;
- proteger adecuadamente los sistemas de información;
- preservar la evidencia digital;
- colaborar con las investigaciones cuando sea requerido por las autoridades competentes.

Por este motivo, conocer las principales figuras contempladas por la Ley N.º 26.388 constituye un complemento importante para la formación en Seguridad Lógica.

3.9.5. Relación entre los Delitos Informáticos y la Seguridad Lógica

Los delitos informáticos aprovechan, en la mayoría de los casos, fallas en los mecanismos de seguridad lógica implementados por una organización. Por este motivo, los controles estudiados en esta unidad constituyen la primera línea de defensa para prevenir este tipo de incidentes.

La siguiente tabla resume la relación entre algunos delitos informáticos y los mecanismos de seguridad lógica que contribuyen a evitarlos.

Delito informático	Controles de Seguridad Lógica que ayudan a prevenirlo
Acceso ilegítimo a sistemas	Autenticación, control de acceso, MFA
Violación de la privacidad	Gestión de privilegios, control de acceso, auditoría
Robo de credenciales	Políticas de contraseñas, MFA, capacitación de usuarios
Phishing	Capacitación de usuarios, MFA, filtros de correo
Modificación no autorizada de datos	Gestión de privilegios, segregación de funciones, auditoría
Daño informático	Control de acceso, backups, auditoría
Fraude informático	Auditoría, segregación de funciones, doble autorización
Ransomware	Gestión de privilegios, backups, actualización de sistemas
Sabotaje informático	Auditoría, monitoreo, control de acceso

Puede observarse que un mismo mecanismo de seguridad puede contribuir a prevenir distintos delitos.

Por ejemplo, la **autenticación multifactor (MFA)** no sólo dificulta el acceso ilegítimo a los sistemas, sino que también reduce significativamente el impacto del robo de credenciales y de los ataques de phishing. De igual manera, los **registros de auditoría** permiten detectar modificaciones no autorizadas, reconstruir los hechos ocurridos durante un incidente y aportar evidencia para una investigación posterior.

En consecuencia, la implementación adecuada de controles de seguridad lógica constituye una de las medidas más eficaces para disminuir la probabilidad de sufrir fraudes y delitos informáticos.

3.9.6. Denuncia de Delitos Informáticos en Argentina

Cuando una persona o una organización es víctima de un presunto delito informático, resulta fundamental actuar rápidamente y preservar toda la evidencia disponible. Una actuación incorrecta puede dificultar o incluso impedir la investigación posterior.

Preservación de la evidencia digital

Antes de intentar solucionar el problema, se recomienda:

- no eliminar archivos relacionados con el incidente;
- no formatear computadoras ni dispositivos afectados;
- conservar correos electrónicos, mensajes y registros del sistema;
- registrar fechas, horarios y direcciones IP cuando sea posible;
- documentar todas las acciones realizadas desde el descubrimiento del incidente.

La evidencia digital constituye un elemento fundamental durante una investigación judicial.

3.9.7. ¿Dónde denunciar un delito informático?

En Argentina, la denuncia puede realizarse ante cualquiera de los siguientes organismos:

- la comisaría más cercana;
- la fiscalía correspondiente a la jurisdicción donde ocurrió el hecho;
- las fiscalías especializadas en ciberdelincuencia cuando existan en la jurisdicción.

Además, existen organismos especializados que colaboran en la investigación y asistencia técnica.

3.9.7.1. Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)

La **UFECI**, dependiente del Ministerio Público Fiscal de la Nación, coordina investigaciones relacionadas con delitos informáticos y brinda asistencia técnica a fiscales de todo el país.

Entre sus funciones se encuentran:

- colaborar en investigaciones penales;
- asesorar técnicamente a fiscales;
- intervenir en casos complejos relacionados con tecnologías de la información.

3.9.7.2. División Delitos Tecnológicos de la Policía Federal Argentina

La Policía Federal Argentina posee áreas especializadas dedicadas a la investigación de delitos informáticos.

Estas unidades colaboran en:

- secuestro de evidencia digital;
- análisis forense de dispositivos;
- investigación de ataques informáticos;
- identificación de responsables.

3.9.7.3. CERT.ar

El **Centro Nacional de Respuesta a Incidentes Informáticos (CERT.ar)** brinda asistencia frente a incidentes de ciberseguridad. Es importante destacar que **CERT.ar no reemplaza la denuncia penal**.

Su función principal consiste en:

- recibir reportes sobre incidentes;
- brindar asistencia técnica;
- emitir alertas de seguridad;
- coordinar respuestas ante incidentes de gran impacto.

Organismos relacionados con delitos informáticos en Argentina

Organismo	Función principal
Policía o Fiscalía	Recepción de denuncias penales
UFECI	Investigación especializada en ciberdelitos
Policía Federal Argentina	Investigación policial y análisis forense
CERT.ar	Asistencia técnica y respuesta a incidentes

3.9.8. Buenas Prácticas para prevenir Fraudes y Delitos Informáticos

La prevención constituye la estrategia más efectiva para reducir la probabilidad de sufrir fraudes y delitos informáticos. Las organizaciones deben combinar controles tecnológicos con procedimientos administrativos y capacitación permanente del personal.

Entre las principales recomendaciones se destacan:

- utilizar contraseñas robustas y únicas para cada sistema;
- implementar autenticación multifactor;
- aplicar el principio del mínimo privilegio;
- mantener actualizados los sistemas operativos y aplicaciones;
- instalar únicamente software proveniente de fuentes confiables;
- realizar copias de seguridad periódicas;
- registrar y auditar las actividades críticas;
- capacitar periódicamente a los usuarios sobre phishing e ingeniería social;
- verificar cuidadosamente la identidad de las personas antes de compartir información sensible;
- revisar periódicamente los permisos de acceso otorgados a cada usuario.

La seguridad informática no depende únicamente de la tecnología. La participación responsable de los usuarios constituye uno de los factores más importantes para prevenir incidentes.

3.10. Bibliografía

3.10.1. Bibliografía básica

- Gómez Vieites, Á. *Enciclopedia de la Seguridad Informática*. Alfaomega.
- Stallings, W. *Seguridad Informática: Principios y Práctica*. Pearson.
- De la Torre, A. *Seguridad Informática*. Ra-Ma Editorial.
- Nombela, J. J. *Seguridad Informática*. Paraninfo.
- Gómez Vieites, Á. *Auditoría de Seguridad Informática*. Ra-Ma Editorial.

3.10.2. Bibliografía complementaria

- ISO/IEC 27001. *Sistemas de Gestión de Seguridad de la Información*.
- ISO/IEC 27002. *Código de buenas prácticas para los controles de seguridad de la información*.
- NIST SP 800-63B. *Digital Identity Guidelines: Authentication and Lifecycle Management*.
- NIST Cybersecurity Framework (CSF).
- INCIBE (Instituto Nacional de Ciberseguridad de España). Guías de buenas prácticas en ciberseguridad.

3.10.3. Bibliografía del apartado 3.9

- Argentina. **Ley N.º 26.388**. Modificación del Código Penal de la Nación Argentina. Delitos Informáticos.
- **Código Penal de la Nación Argentina** (texto actualizado).
- **Ministerio Público Fiscal de la Nación.** Unidad Fiscal Especializada en Ciberdelincuencia (UFECI). Material informativo y guías sobre ciberdelitos.
- **CERT.ar.** Centro Nacional de Respuesta a Incidentes Informáticos. Guías y recomendaciones de seguridad informática.

- **Instituto Nacional de Ciberseguridad (INCIBE).** Guías sobre phishing, ingeniería social, ransomware y fraudes informáticos.
- Whitman, Michael E.; Mattord, Herbert J. **Principles of Information Security.** Cengage Learning.
- Stallings, William. **Effective Cybersecurity: A Guide to Using Best Practices and Standards.** Addison-Wesley.
- ISO/IEC 27002:2022. **Information security, cybersecurity and privacy protection — Information security controls.**