FACULTAD DE INGENIERÍA

**Universidad Nacional de Jujuy**

Unidad 3

# Seguridad Lógica y Gestión de Usuarios

Apunte de Cátedra · Seguridad y Auditoría Informática

# Contenidos de la Unidad 3

01 **Seguridad Lógica**
Concepto, objetivos y relación con la Seguridad Física

02 **Control de Acceso Lógico**
Identificación, autenticación y autorización

03 **Gestión de Usuarios**
Ciclo de vida de cuentas, tipos y grupos

04 **Privilegios y Modelos de Control**
Mínimo privilegio, DAC, MAC, RBAC, ABAC

05 **Políticas de Contraseñas y MFA**
Complejidad, bloqueo y autenticación multifactor

06 **Registro, Auditoría y Buenas Prácticas**
Logs, trazabilidad y recomendaciones

07 **Fraudes y Delitos Informáticos**
Ley 26.388, diferencias y prevención

# 3.1.1 Concepto de Seguridad Lógica

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 acción que comprometa su seguridad.

## Finalidad principal

Garantizar que únicamente las personas autorizadas puedan acceder a los recursos informáticos y realizar las operaciones permitidas según las funciones que desempeñan.

Gran parte de los incidentes se deben a contraseñas débiles, cuentas compartidas, privilegios excesivos o configuraciones incorrectas de permisos.

# 3.1.2 Objetivos de la Seguridad Lógica

### Impedir acceso no autorizado

Solo usuarios autorizados ingresan a los recursos

### Proteger la información

Evitar lectura, modificación o eliminación indebida

### Garantizar confidencialidad

Información solo para quienes tienen autorización

### Preservar integridad

Datos completos, correctos y sin cambios no autorizados

### Contribuir a la disponibilidad

Usuarios autorizados acceden cuando lo necesitan

### Registrar actividades

Facilitar auditoría e investigación de incidentes

# 3.1.3 Seguridad Física vs Seguridad Lógica

| Aspecto | Seguridad Física | Seguridad Lógica |
|---|---|---|
| Qué protege | Instalaciones, equipos, infraestructura | Sistemas, aplicaciones, información |
| Qué controla | Acceso a espacios físicos | Acceso a recursos informáticos |
| Mecanismos | Cerraduras, biometría, CCTV | Usuarios, contraseñas, permisos, MFA |
| Objetivo | Proteger recursos materiales | Proteger recursos informáticos e información |

Son complementarias: proteger la sala de servidores no sirve si cualquiera puede acceder a los sistemas; una buena autenticación pierde valor si alguien manipula los equipos físicamente.

# 3.1.4 Principales mecanismos de Seguridad Lógica

| | |
|---|---|
| **Control de acceso lógico** | Verificar identidad y determinar qué recursos puede usar cada usuario |
| **Gestión de usuarios y grupos** | Crear, modificar y eliminar cuentas; organizar según funciones |
| **Gestión de privilegios** | Asignar permisos con mínimo privilegio y separación de funciones |
| **Modelos de control de acceso** | DAC, MAC, RBAC, ABAC: definen cómo se administran los permisos |
| **Políticas de contraseñas** | Requisitos de complejidad y rotación para reducir riesgos |
| **Autenticación multifactor** | Combinar dos o más factores de verificación |
| **Registro y auditoría** | Registrar acciones y detectar actividades sospechosas |

# 3.2 Control de Acceso Lógico

Conjunto de mecanismos, procedimientos y políticas que regulan el acceso de los usuarios a los recursos informáticos. Garantiza que únicamente las personas autorizadas utilicen los sistemas y ejecuten las operaciones permitidas.

## Recursos protegidos

| | | |
|---|---|---|
| Sistemas operativos | Aplicaciones | Bases de datos |
| Archivos y carpetas | Servicios de red | Sistemas en la nube |

# 3.2.2 Componentes del Control de Acceso

1

## Identificación

El usuario informa quién es (nombre de usuario, correo, ID). Solo declara la identidad; aún no la prueba.

2

## Autenticación

El sistema verifica que es quien dice ser (contraseña, token, biometría, certificado digital).

3

## Autorización

Una vez autenticado, el sistema determina qué recursos puede usar y qué operaciones puede realizar.

# 3.2.4 Ejemplo: sistema académico universitario

Un docente desea cargar calificaciones. El proceso es:

| | | |
|---|---|---|
| 1 | **Identificación** | Introduce su nombre de usuario |
| 2 | **Autenticación** | Contraseña + código MFA (si aplica) |
| 3 | **Verificación** | El sistema confirma que la autenticación es correcta |
| 4 | **Consulta de permisos** | Revisa los permisos asociados a la cuenta |
| 5 | **Autorización** | Permite solo las asignaturas asignadas y las funciones permitidas |

# 3.3 Gestión de Usuarios

Conjunto de procedimientos y actividades destinadas a administrar las cuentas de usuario que permiten el acceso a los sistemas informáticos. Garantiza que cada persona disponga únicamente de las cuentas necesarias y que se administren de forma segura durante todo su ciclo de vida.

## Importancia

- Controlar quién puede acceder a los sistemas
- Asignar correctamente permisos y privilegios
- Reducir el riesgo de accesos no autorizados
- Facilitar las tareas de auditoría
- Evitar cuentas huérfanas o con privilegios excesivos
- Cumplir políticas y normas (ISO 27000, etc.)

# 3.3.3 Ciclo de vida de una cuenta de usuario

| | |
|---|---|
| **Alta** | Creación del identificador, contraseña inicial, grupos y permisos mínimos. Cambio de contraseña en el primer acceso. |
| **Modificación** | Cambio de puesto, departamento o responsabilidades. Revisar y actualizar permisos. |
| **Suspensión** | Deshabilitar temporalmente (licencias, vacaciones, investigaciones). La cuenta no permite inicio de sesión. |
| **Baja** | Eliminación definitiva. Revocar todos los permisos y conservar solo lo necesario para auditoría. |

# 3.3.4 – 3.3.5 Tipos de cuentas y gestión de grupos

## Tipos de cuentas

**Usuario estándar**
Acceso normal a recursos asignados

**Administrador**
Privilegios elevados; uso restringido

**Servicio / sistema**
Cuentas de aplicaciones o procesos

**Invitado / temporal**
Acceso limitado y por tiempo definido

## Gestión de grupos

Los grupos permiten asignar permisos de forma colectiva según roles o funciones.

Ventajas:
- Simplifican la administración
- Reducen errores de asignación
- Facilitan el mínimo privilegio
- Mejoran la trazabilidad

Ejemplo: grupo “Docentes” con permisos para cargar notas; grupo “Alumnos” solo para consultar.

# 3.4.1 Permiso, Privilegio y Rol

## Permiso

Autorización específica para realizar una acción sobre un recurso (leer un archivo, modificar un registro, ejecutar un programa).

## Privilegio

Conjunto de permisos o derechos especiales, a menudo asociados a funciones administrativas o críticas.

## Rol

Representa una función o responsabilidad dentro de una organización y agrupa los permisos necesarios para desempeñar dicha función(docente, contador, administrador de sistemas).

# 3.4.2 – 3.4.3 Principios clave

## Principio del mínimo privilegio

Cada usuario debe disponer únicamente de los permisos estrictamente necesarios para cumplir sus funciones.

Beneficios:
- Reduce el impacto de un compromiso de cuenta
- Limita errores accidentales
- Facilita la auditoría
- Disminuye la superficie de ataque

Ejemplo: un docente solo puede modificar notas de sus materias, no de toda la universidad.

## Separación de funciones

Consiste en distribuir tareas críticas entre diferentes personas para evitar que un único usuario tenga el control absoluto de un proceso

Objetivo:
- Evitar fraudes y errores
- Requerir al menos dos personas para operaciones sensibles

Ejemplo: quien carga una factura no puede autorizar el pago; quien solicita un acceso no puede aprobarlo solo.

# 3.4.4 Modelos de Control de Acceso

Son las diferentes formas de administrar permisos dentro de un sistema informático.
Cada modelo define quién puede asignar permisos, cómo se administran y qué nivel de flexibilidad o seguridad ofrece.

**DAC** Discretionary Access Control

El propietario del recurso decide quién puede acceder. Flexible pero riesgoso si se asignan permisos de forma informal.

**MAC** Mandatory Access Control

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.

**RBAC** Role-Based Access Control

Los permisos se asignan a roles y los usuarios a roles. Facilita la administración y el mínimo privilegio.

**ABAC** Attribute-Based Access Control

El acceso se determina dinámicamente evaluando atributos del usuario, recurso, acción y entorno. Muy flexible y granular. Ej. permitir acceso al archivo ‘proyecto_alpha.docx’ si: El usuario tiene el atributo ‘departamento=I+D’, la hora es entre 8:00 y 18:00, el dispositivo está en la red corporativa, El archivo no tiene etiqueta ‘top_secret’”

# 3.4.5 Comparación entre modelos

| Modelo | Quién decide | Flexibilidad | Uso típico |
|---|---|---|---|
| DAC | Propietario del recurso | Alta | Sistemas de archivos, entornos pequeños |
| MAC | Política central del sistema | Baja | Gobierno, defensa, alta seguridad |
| RBAC | Administración de roles | Media-Alta | Empresas, universidades, la mayoría de organizaciones |
| ABAC | Reglas basadas en atributos | Muy alta | Nube, entornos dinámicos y complejos |

# 3.5 Políticas de Contraseñas

Conjunto de reglas que definen cómo deben crearse, usarse y administrarse las contraseñas para reducir el riesgo de accesos no autorizados.

## Características de una contraseña segura

### Longitud

Al menos 12 caracteres (idealmente más)

### Complejidad

Mayúsculas, minúsculas, números y símbolos

### Unicidad

No reutilizar entre sistemas ni cuentas

### Impredecible

Evitar datos personales, diccionarios o patrones

### Rotación

Cambio periódico según política organizacional

### Secreta

Nunca compartir ni escribir en lugares visibles

# 3.5.4 – 3.5.5 Bloqueo de cuentas y gestores

## Bloqueo de cuentas

Tras un número definido de intentos fallidos de autenticación, la cuenta se bloquea temporal o permanentemente.

- Reduce ataques de fuerza bruta
- Debe combinarse con notificaciones al usuario
- Evitar bloqueos demasiado agresivos que generen denegación de servicio
- Definir tiempo de espera o desbloqueo por administrador

## Gestores de contraseñas

Herramientas que almacenan de forma cifrada las contraseñas y permiten generar credenciales fuertes y únicas.

Ventajas:
- Contraseñas largas y aleatorias
- Una sola contraseña maestra
- Autocompletado seguro
- Menor reutilización

Recomendación: usar gestores de confianza y proteger la contraseña maestra con MFA.

# 3.6 Autenticación Multifactor (MFA)

Proceso que exige dos o más factores de verificación independientes para confirmar la identidad del usuario, aumentando significativamente la seguridad del acceso.

## Factores de autenticación

1

**Algo que se sabe**

Contraseña, PIN, respuesta a pregunta secreta

2

**Algo que se tiene**

Token, tarjeta, teléfono, llave de seguridad

3

**Algo que se es**

Huella, iris, rostro, voz (biometría)

4

**Algo que se hace**

Patrón de comportamiento, firma dinámica

# 3.6.3 – 3.6.4 Métodos, ventajas y limitaciones

## Métodos comunes

| | | |
|---|---|---|
| OTP por SMS o correo | App autenticadora (TOTP) | Llaves de seguridad (FIDO2) |
| Notificaciones push | Biometría + PIN | Certificados / tokens de hardware |

### Ventajas

- Reduce el impacto del robo de contraseñas
- Dificulta phishing y fuerza bruta
- Aumenta la confianza en el acceso
- Requerido en muchas normativas

### Limitaciones

- SMS puede ser interceptado (SIM swap)
- Usuarios pueden resistirse por fricción
- Pérdida del segundo factor
- Costos de implementación y soporte

# 3.7 Registro y Auditoría

El registro (logging) consiste en almacenar de forma ordenada los eventos relevantes del sistema. La auditoría es el análisis de esos registros para detectar anomalías, investigar incidentes y demostrar cumplimiento.

## ¿Qué debe registrarse?

### Autenticación

Éxitos y fallos de inicio de sesión

### Cambios de permisos

Altas, bajas y modificaciones de privilegios

### Accesos a datos críticos

Consultas o modificaciones de información sensible

### Acciones administrativas

Creación de cuentas, cambios de configuración

### Errores del sistema

Fallos, excepciones y condiciones anómalas

### Actividad de red relevante

Conexiones sospechosas o no autorizadas

# 3.7.5 – 3.7.7 Trazabilidad y características de un buen log

Trazabilidad: capacidad de reconstruir quién hizo qué, cuándo, desde dónde y con qué resultado. Es esencial para investigación de incidentes y cumplimiento normativo.

## Características de un buen sistema de registros

### Completo

Incluye usuario, fecha/hora, recurso, acción y resultado

### Inmutable

Protegido contra modificación o borrado no autorizado

### Centralizado

Facilita correlación y análisis

### Sincronizado

Relojes alineados (NTP) para secuencia correcta

### Retención definida

Política clara de tiempo de conservación

### Monitoreado

Alertas ante eventos críticos o anómalos

# 3.8 Buenas prácticas de Seguridad Lógica

1. Aplicar el principio del mínimo privilegio
2. Utilizar cuentas individuales (no compartidas)
3. Implementar contraseñas robustas y únicas
4. Activar autenticación multifactor (MFA)
5. Administrar correctamente el ciclo de vida de cuentas
6. Revisar periódicamente los permisos asignados
7. Supervisar y analizar los registros de eventos
8. Capacitar permanentemente a los usuarios
9. Mantener sistemas y aplicaciones actualizados
10. Cumplir las políticas de seguridad de la organización

# 3.9 Fraudes y Delitos Informáticos

## Fraude Informático

Uso indebido de sistemas, aplicaciones o información digital para obtener un beneficio económico, comercial o personal mediante engaño o manipulación.

- Ámbito: técnico / organizacional
- No siempre es delito penal
- Objetivo: beneficio indebido

Ejemplo: modificar el sistema de comisiones para aumentar el propio salario.

## Delito Informático

Conducta ilícita realizada mediante sistemas informáticos o dirigida contra ellos, tipificada y sancionada por la legislación penal.

- Ámbito: jurídico / penal
- Siempre previsto por la ley
- En Argentina: Ley N.º 26.388

Ejemplo: acceder sin autorización a una base de datos de clientes (aunque no se modifique nada).

# 3.9.4 Principales delitos (Ley N.º 26.388)

### Violación de secretos y privacidad

Acceder, interceptar o divulgar comunicaciones privadas sin autorización.

### Acceso ilegítimo a sistemas

Ingresar a sistemas o bases de datos protegidas sin autorización.

### Daño informático

Destruir, alterar, inutilizar o deteriorar datos, programas o sistemas.

### Fraude informático

Manipular registros o sistemas para obtener beneficio económico ilícito.

### Delitos contra la integridad sexual

Uso de medios informáticos para producir o difundir material de abuso sexual infantil (delitos graves).

# 3.9.5 Relación con la Seguridad Lógica

| Delito / amenaza | Controles de Seguridad Lógica |
|---|---|
| Acceso ilegítimo | Autenticación, control de acceso, MFA |
| Violación de privacidad | Gestión de privilegios, auditoría |
| Robo de credenciales / phishing | Políticas de contraseñas, MFA, capacitación |
| Modificación no autorizada | Mínimo privilegio, segregación, auditoría |
| Daño informático | Control de acceso, backups, logs |
| Fraude informático | Segregación de funciones, doble autorización |
| Ransomware / sabotaje | Privilegios, backups, actualización, monitoreo |

# 3.9.6 – 3.9.7 Denuncia de delitos informáticos en Argentina

Preservar evidencia: no eliminar archivos, no formatear, conservar correos, logs, fechas, IPs y documentar todas las acciones desde el descubrimiento.

### Comisaría / Fiscalía

Recepción de la denuncia penal. Primer paso formal.

### UFECI

Unidad Fiscal Especializada en Ciberdelincuencia. Asistencia técnica y coordinación.

### Policía Federal

División Delitos Tecnológicos. Análisis forense e investigación.

### CERT.ar

Asistencia técnica y respuesta a incidentes. No reemplaza la denuncia penal.

# 3.9.8 Buenas prácticas para prevenir fraudes y delitos

- Contraseñas robustas y únicas + MFA
- Principio del mínimo privilegio
- Sistemas y aplicaciones actualizados
- Software solo de fuentes confiables
- Copias de seguridad periódicas
- Registro y auditoría de actividades críticas
- Capacitación sobre phishing e ingeniería social
- Verificar identidad antes de compartir información sensible
- Revisión periódica de permisos
- Políticas de uso aceptable y denuncia de incidentes

# Síntesis de la Unidad 3

### Seguridad Lógica

Protege sistemas e información mediante controles de acceso, usuarios y privilegios.

### Control de acceso

Identificación → Autenticación → Autorización. Base de toda protección lógica.

### Gestión de usuarios

Ciclo de vida completo: alta, modificación, suspensión y baja.

### Modelos y privilegios

Mínimo privilegio, separación de funciones y modelos DAC/MAC/RBAC/ABAC.

### Contraseñas y MFA

Políticas robustas + autenticación multifactor reducen riesgos de compromiso.

### Auditoría y prevención

Logs, trazabilidad y buenas prácticas previenen fraudes y delitos (Ley 26.388).

Unidad 3 completada

# Seguridad Lógica y Gestión de Usuarios

¿Preguntas?

Facultad de Ingeniería · Universidad Nacional de Jujuy