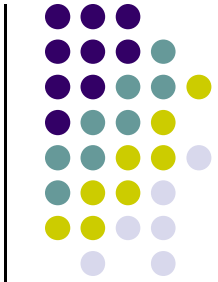
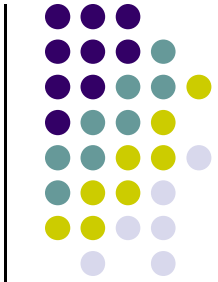


Seminario CISSP
Control de Acceso

Roberto Woo Borrego
CISSP, CISA, ITIL, ISO27001



CÁPSULA:

Conceptos generales de Control de Acceso

Instructor

- Nombre: Roberto Woo Borrego

- Experiencia en SI:

Proyectos de SI, Seguridad en Redes, Auditoria,

- Certificaciones: CCDA, CCNA, CISA, CISSP, ITIL, ISO27001

- E mail: rwooborr@alestra.com.mx

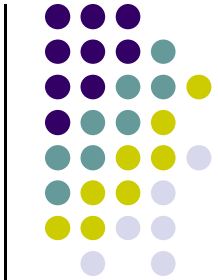
Introducción

- El proceso de administración de identidades y de privilegios de los usuarios en los sistemas de información nos permite reducir el riesgo de acceso o modificación no autorizada de la información.

- El mantener el acceso a los sistemas a los usuarios válidos con los privilegios correctos requiere la definición de políticas de control de acceso, así como una administración de los mismos.

Necesidad de Control de Acceso

Control de Acceso



- El control de acceso son los mecanismos para limitar el **acceso** a la información y recursos de procesamiento de datos sólo a los usuarios o aplicaciones autorizadas, así como las tareas que pueden realizar en los mismos.

- Tradicionalmente los controles se agrupan en físicos, técnicos (o lógicos) y administrativos.

- Este capítulo está concentrado en los sistemas de información y por lo tanto en el acceso lógico

Metas de la Integridad

- Evitar la modificación por usuarios **no autorizados.**
- Evitar la modificación no autorizada o no intencional por parte de **usuarios autorizados**
- Preservación de la consistencia **interna y externa**
  - Interna: Por ejemplo, la suma de cada una de las partes resulta en el todo.
  - Externa: La información es consistente con la realidad.

Temas de Control de Acceso

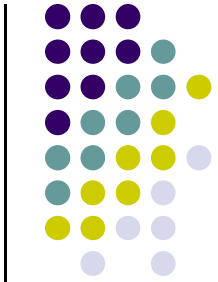
- **El control de acceso abarca temas diversos como**
  - Seguridad Física
  - Administración de la identidad (alta, baja y cambios de usuarios)
  - Administración de roles
  - Administración de privilegios
    - Red
    - Sistemas operativos
    - Aplicaciones
  - Administración de autenticación (contraseñas)
  - Auditoría de acceso y autorizaciones
  - Cumplimiento con Regulaciones

Control de Acceso

Identity Management

Comercialmente

Metas de control de acceso

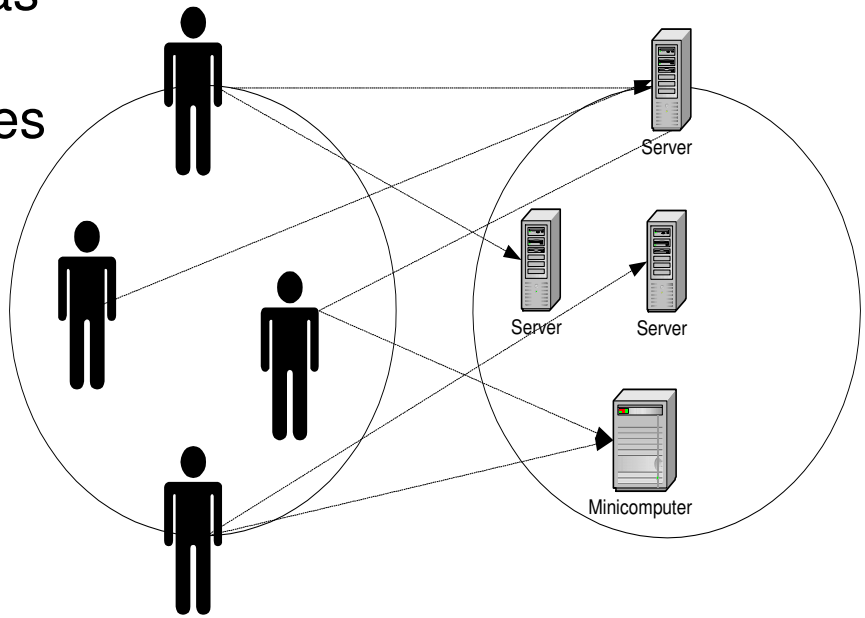


- Necesidad de conocer (*Need to Know)*
  - Acceso a la información que es pertinente para realizar su trabajo o función.

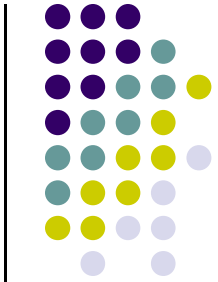
- Menor Privilegio (*Least privilege)*
  - El menor permiso o acción sobre la información a la que se tiene acceso.

Retos del Control de Acceso

- Número de plataformas o sistemas
- Usuarios con diferentes identidades y contraseñas por sistema
- Múltiples administradores con diferentes criterios de seguridad.
- Procesos para autorización y otorgamiento de privilegios en el ciclo de vida de un empleado.
- Múltiples puntos de entrada a los sistemas (p.ej. aplicación, base de datos, red local, acceso remoto, consola local)



Necesidades de Control de Acceso lógico / Administration de Identidades



SEGURIDAD

- Política de control de acceso : “necesidad de conocer” y “menor privilegio”:
- Acceso basado en roles
- Integración de identidad
- Revocación de acceso
- Registro y auditoría de accesos integrado
- Obligar contraseñas fuertes
- Controles de seguridad en una sola plataforma (p. ej. criptografía)

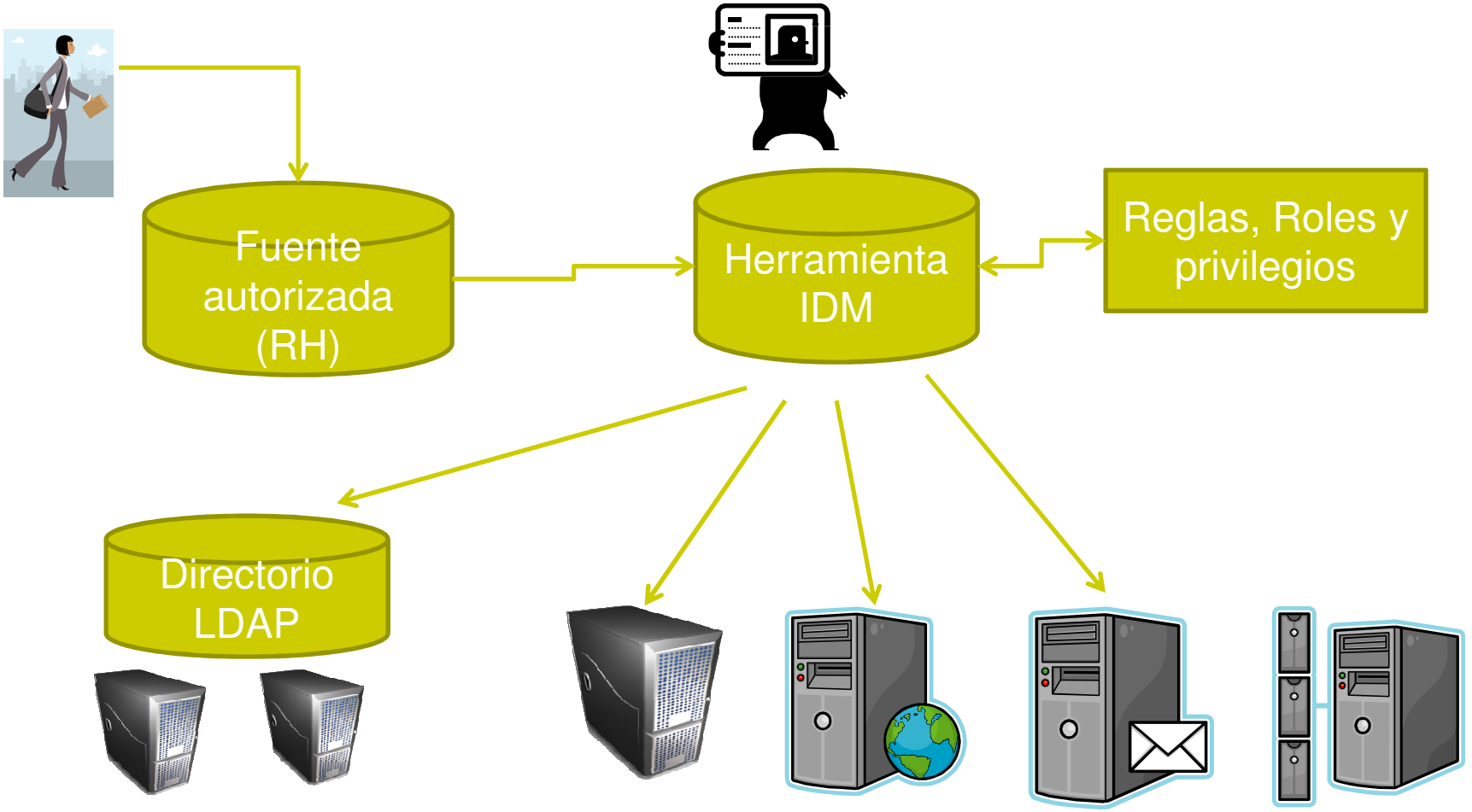
ADMINISTRACION

- Simplificación de procesos de alta, baja y modificación de privilegios
- Disminución en el tiempo de creación de cuentas de acceso
- Integración de identidad para varios activos de información
- Centralización de privilegios
- Reducción en el número de llamadas relacionadas con contraseñas

REGULATORIO

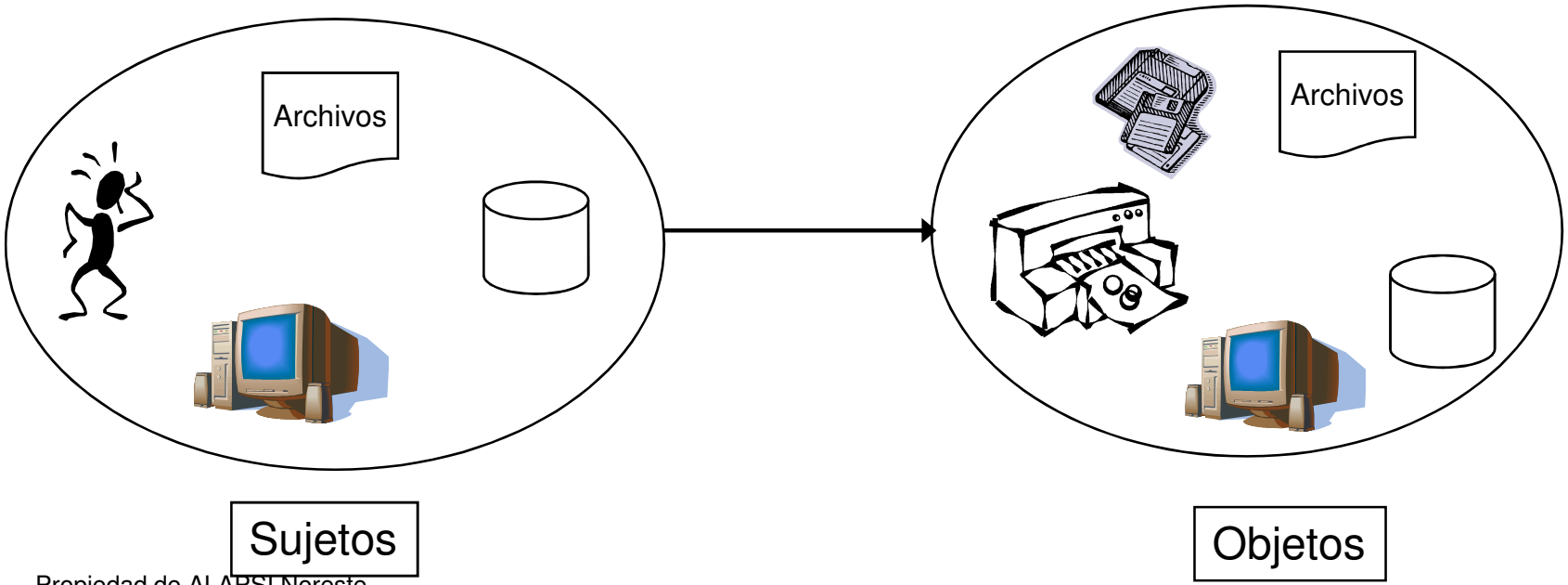
- Cumplimiento con regulaciones gubernamentales relacionadas con auditoría de acceso
- Apoyo al cumplimiento del estándares como ISO 27001
- *Sarbanes Oxley*

Ejemplo de Manejo de Control de acceso (alta)

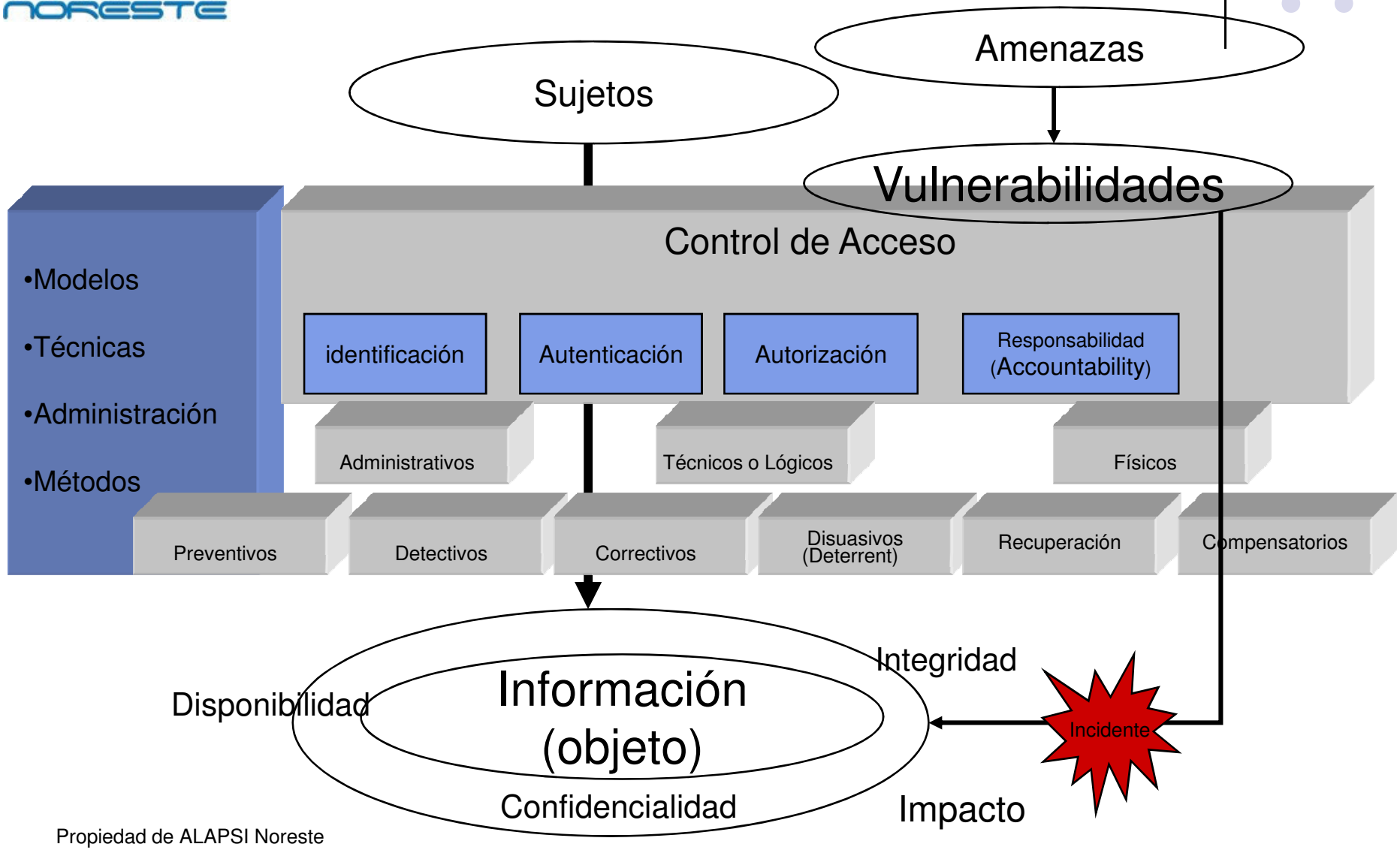


Conceptos de Control de Acceso

- Acceso: Es un flujo de información entre en sujeto y un objeto.
- Sujeto: Es una entidad activa que solicita acceso a un objeto o a los datos de un objeto.
- Objeto: Es una entidad pasiva que contiene información.

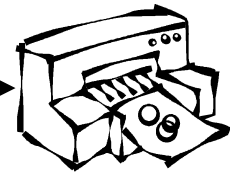


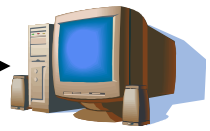
Control de acceso



Proceso de Identificación, Autenticación y Autorización

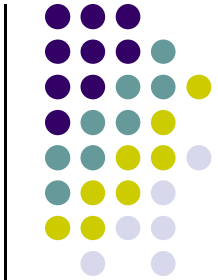
1. Identificación
2. Autenticación
3. Autorización





Control de acceso (AAA)

- **Identificación / Autenticación**
  - Establecer la identidad del usuario o sistema
  - Password / PIN / Tarjeta / Biométrico
- **Autorización**
  - Asignación de privilegio sobre información.
  - Leer, borrar, modificar, agregar, etc.
- **Registro *Accounting /Accountability***
  - Evitar repudiación
  - Detección de violación de políticas
  - Cadena de custodia (manejo de evidencia)



Control de acceso: Tipos

Ejemplos de controles de acceso por tipo

Administrativos

- Políticas y procedimientos
- Concientización
- Supervisión de empleados
- Separación de funciones
- Rotación de funciones
- Vacaciones mandatorias

Lógicos o Técnicos

- Separación de redes
- Firewall
- Antivirus
- Smartcard/Biométricos
- Listas de acceso
- Encripción
- Detección de Intrusos
- Contraseñas

Físicos

- Guardias
- Candados
- Credencial
- Tarjetas de acceso
- Seguridad Perimetral

Preventivos	Detectivos	Correctivos	Disuasivos (Deterrent)	Recuperación	Compensatorios

Tipos de Controles de Acceso

Type of Control	Preventive	Detective	Corrective	Deterrent	Recovery	Compensation
	Controls used to deter and avoid undesirable events from taking place	Controls used to identify undesirable events that have occurred	Controls used to correct undesirable events that have occurred	Controls used to discourage security violations	Controls used to restore resources and capabilities	Controls used to provide alternatives to other controls
Category of Control						
Physical						
Fences	x			x		
Locks	x			x		
Badge system	x			x		
Security guard	x	x		x		
Biometric system	x					
Mantrap doors	x			x		
Lighting	x					
Motion detectors		x				
Closed-circuit TVs		x		x		
Alarms	x	x		x		
Backups					x	
Administrative						
Security policy	x					
Monitoring and supervising	x	x		x		x
Separation of duties	x			x		
Job rotation	x	x				
Information classification	x					
Personnel procedures	x			x		x
Investigations		x				

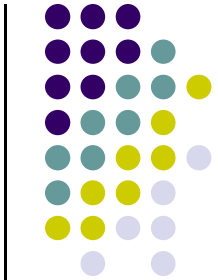
Tipos de Controles de Acceso

Type of Control	Preventive	Detective	Corrective	Deterrent	Recovery	Compensation
	Controls used to deter and avoid undesirable events from taking place	Controls used to identify undesirable events that have occurred	Controls used to correct undesirable events that have occurred	Controls used to discourage security violations	Controls used to restore resources and capabilities	Controls used to provide alternati to other control
Category of Control						
Administrative						
Testing	x					
Security awareness training	x			x		
Technical						
ACLs	x					
Routers	x					
Encryption	x			x		
Audit logs		x				
IDS		x	x			
Antivirus software	x	x	x		x	
Firewalls	x	x		x		
Smart cards	x					
Dial-up call-back systems	x					
Alarms and alerts		x				

Ejemplos de amenazas y vulnerabilidades de control de acceso relacionadas a ISO 27001

Amenazas	Ejemplos de vulnerabilidades	Controles sugeridos en el ISO 27001 de control de acceso
Acceso no autorizado a información por exceso de privilegios	▪No existe una política de control de acceso ▪No existen roles ▪Se tienen usuarios desactualizados	A.11.1.1 Política de control de acceso A.11.2.2 Administración de privilegios
Acceso no autorizado a información por selección de contraseña o administración de contraseña	▪Uso de contraseñas simples. ▪Falta de responsivas de usuarios ▪Contraseñas que no expiran	A.11.2.3 Administración de contraseñas de usuario A.11.5.3 Sistema de administración contraseñas
Acceso no autorizado a la información por falta de una identificación y autorización única	▪Proceso de verificación de identidad para cambio de contraseña ▪Aplicaciones con su propio repositorio de identidad	A.11.2.1 Registro de usuarios A.11.5.2 Identificación y autenticación de usuarios
Incapacidad de proveer evidencia (Repudiación)	▪Usuarios de *Help desk* conocen los códigos de los usuarios	A.11.5.2 Identificación y autenticación de usuarios A.10.10.2 Monitoreo de uso de sistema A.10.10.1 Registro eventos

11. Control de acceso > 11.2 Administración de acceso de usuarios (ISO/IEC 17799)



- **A.11.2.2 Administración de privilegios**
  - La asignación y uso de privilegios debe ser restringido y controlado (ISO/IEC 27001:2005).

  - Lineamientos (ISO/IEC 17799):
    - Se deben identificar los privilegios de accesos para todos los sistemas de información (bases de datos, sistemas operativos, etc.)
    - Los privilegios de deben asignar considerando las políticas de control de accesos y la necesidad de conocer del usuario
    - Debe existir un proceso de requisición, autorización, alta, baja y cambios de privilegios
    - Debe existir una bitácora o registro de todas las autorizaciones y movimientos en privilegios
    - Las aplicaciones y sistemas de información deben contar con el nivel de privilegios necesarios y acorde a los requerimientos del negocio

11. Control de acceso > 11.2 Administración de acceso de usuarios (ISO/IEC 17799)

- **A.11.2.3 Administración de contraseñas de usuarios**
  - La asignación de contraseñas debe ser controlada y administrada a través de un proceso formal (ISO/IEC 27001).

  - Lineamientos (ISO/IEC 17799): :
    - Los usuarios deben firmar políticas de manejo adecuado de contraseñas (que no se compartan, que se cambien regularmente, etc.)
    - Asignación de contraseñas temporales y cambios de la misma al primer acceso
    - Procedimientos para verificar la identidad de los usuarios antes de realizar algún movimiento en sus contraseñas
    - Mantener confirmaciones de recepción de contraseñas por parte de los usuarios
    - Las contraseñas deben mantenerse resguardadas
    - Las contraseñas default de los sistemas de información deben ser cambiadas

Separación de Redes (A.11.4.5) e Identificación de equipos (A.11.4.3)

Amenaza	Controles que se pueden implementar al dividir redes y colocar elementos de protección
Acceso no autorizado a la información	•Restringir el acceso por dirección IP origen a una red o servidor •Restringir el acceso a sólo ciertos servicios de red
Acceso no autorizado a facilidades de procesamiento	•Restringir el acceso por dirección IP origen •Restringir el acceso a sólo ciertos servicios de red •Limitar el número de conexiones a una red o servidor
Acceso no autorizado a servicios de red	•Restringir el acceso por dirección IP origen •Restringir el acceso a sólo ciertos servicios de red
Denegación de Servicio	•Detectar condiciones de ataque a la red •Limitar el número de conexiones a una red o servidor
Código Malicioso	•Detectar condiciones de ataque a la red •Contener un ataque mediante la implementación de filtros por puerto o dirección IP

Preguntas

Preguntas

Identification is:

a. A user being authenticated by the system
b. A user providing a password to the system
c. A user providing a shared secret to the system
d. A user professing an identity to the system.

The correct answer is “d”. A user presents an ID to the system as identification. Answer a is incorrect because presenting an ID is not an authentication act. Answer b is incorrect because a password is an authentication mechanism. Answer c is incorrect because it refers to cryptography or authentication.

Preguntas

32. A database View operation implements the principle of:
    a. Least privilege
    b. Separation of duties
    c. Entity integrity
    d. Referential integrity.

The correct answer is “a”. Least privilege, in the database context, requires that subjects be granted the most restricted set of access privileges to the data in the database that are consistent with the performance of their tasks. Answer b, separation of duties, assign parts of security-sensitive tasks to several individuals. Entity integrity, answer c, requires that each row in the relation table must have a non-NULL attribute. Referential integrity, answer d, refers to the requirement that for any foreign key attribute, the referenced relation must have the same value for its primary key.

Conclusiones

- El contar con un proceso de manejo de identidades permite cumplir requerimientos regulatorios, mejorar la experiencia del usuario y fortalecer la seguridad de información

- La identificación, autenticación y autorización son elementos claves para otorgar el acceso

- Las vulnerabilidades en el proceso de control de acceso pueden ser explotadas y ciertas amenazas se materializan en incidentes.

GRACIAS