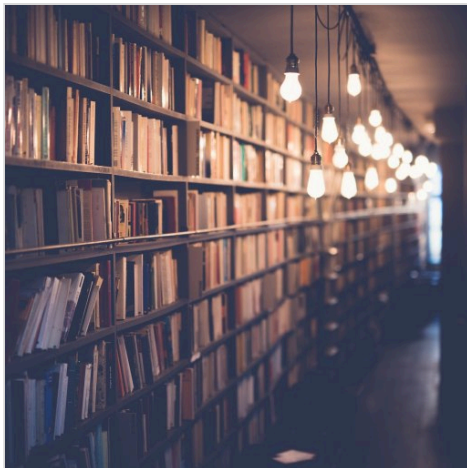


L U M B R E



Seguridad básica y control de acceso

Materia: Privacidad y Seguridad de Datos · Responsabilidad Profesional

11/10/2026

Antes de empezar

La privacidad no se logra solo en el dato sino en su entorno. Cifrar, limitar quién accede y registrar lo que se hace forman la base defensiva que impide accesos y fugas indebidas.

QUÉ APRENDERÁS

- Aplicar los fundamentos de seguridad de datos —cifrado, control de acceso y mínimo privilegio— para proteger la información.

Seguridad básica y control de acceso

Bloquear por defecto

Cifrado en reposo y en tránsito, autenticación fuerte y acceso limitado a lo justo: son las cerraduras básicas. La mayoría de fugas exitosas explotan accesos excesivos y datos sin cifrar.

VIDEO

Minimizar privilegios

Por qué conviene dar a cada usuario y servicio solo el acceso imprescindible y cómo eso reduce el daño de una credencial robada.



Escanea para verlo en Lumbre

<https://www.youtube.com/watch?v=NjGkMz-kWfE>

Cifrado en tránsito y reposo

- En tránsito: protege los datos que viajan (TLS).
- En reposo: protege los almacenados en discos o bases.
- Ambos cierran ventanas típicas de interceptación.

Autenticación

Verificar la identidad de quien accede. Credenciales robustas, multifactor y gestión de sesiones reducen el riesgo de suplantación.

Autorización y control de acceso

No basta saber quién eres: hay que decidir qué puedes ver. La autorización asigna permisos según el rol y la necesidad.

Principio de mínimo privilegio

- Cada usuario o servicio recibe solo el acceso necesario.
- Nada de permisos amplios «por comodidad».
- Reduce la superficie expuesta ante una credencial robada.

Modelos de control de acceso

Basado en roles (RBAC), discrecional, o obligatorio (ABAC según atributos). El patrón elegido modela quién accede a qué, y conviene que sea auditable.

Gestión de identidades y ciclo de vida

- Dar de alta, modificar y retirar accesos sin demora.
- Revisar periódicamente quién tiene qué permisos.
- Las cuentas zombis son puerta trasera.



La defensa se construye por capas: cifrado, control de acceso con mínimo privilegio y registro de lo que ocurre.

Registros y auditoría

Guardar quién accedió a qué y cuándo permite detectar y reconstruir un incidente. Sin trazas, el abuso pasa invisible.

Gestión segura de secretos

- No incrustar contraseñas en el código.
- Usar almacenes cifrados de secretos.
- Rotar credenciales periódicamente.

Defensa en capas

Ningún control basta solo. Cifrado más control de acceso más monitorización más formación: varias capas que un atacante debe superar.

Respaldo y recuperación

- Copias cifradas y probadas de restauración.
- Proteger también contra borrado o secuestro.

- La seguridad incluye poder volver atrás.

Seguridad como proceso continuo

No es un casillero que se marca una vez: exige revisiones, parches y vigilancia constantes. La defensa caduca si se deja de atender.

Errores frecuentes

- Dar permisos amplios «por comodidad» y no retirarlos nunca.
- Cifrar solo en tránsito y dejar los datos desnudos en el disco.
- Incrustar contraseñas en el código en lugar de usar un almacén de secretos.

Ejemplo resuelto: un acceso que debía ser temporal

Un analista pide acceso permanente a la base de nómina por si acaso. El equipo aplica mínimo privilegio: concede lectura de solo los campos necesarios, durante un plazo acotado y con registro de cada consulta; al terminar, revoca el permiso automáticamente.

1. cifrar los datos en reposo y en tránsito
2. verificar la identidad con autenticación robusta
3. autorizar solo el acceso imprescindible por rol
4. registrar quién accedió a qué y cuándo
5. retirar permisos y secretos sin demora

¿Para qué sirve en la realidad?

La mayoría de fugas explotan accesos excesivos y datos sin cifrar: el control de acceso con mínimo privilegio, el cifrado y la auditoría cierran esas puertas y son exigencia de cualquier marco de seguridad y de la continuidad del negocio.

1. El principio de mínimo privilegio sostiene que:

- ☐ todos deben poder acceder a todo para colaborar
- ☐ cada agente recibe solo el acceso necesario para su tarea
- ☐ las contraseñas se comparten para agilidad
- ☐ el cifrado sustituye al control de acceso

2. Cifrar los datos en tránsito protege también los datos almacenados en el disco del servidor.

- ☐ Verdadero
- ☐ Falso

ACTIVIDAD INTERACTIVA DISPONIBLE EN LUMBRE

3. Seguridad**4. Ordena una política defensiva para un almacén de datos:****Elementos:**

- proteger los datos en reposo y tránsito
- verificar la identidad del que accede
- limitar el acceso por mínimo privilegio
- registrar accesos para revisar

Cifrar	. . .
Autenticar	. . .
Autorizar	. . .
Auditar	. . .

Principio de mínimo privilegio https://en.wikipedia.org/wiki/Principle_of_least_privilege
 Conceder solo los permisos necesarios para la función.

5. Une cada control de seguridad con su función:

5.	autenticación	-----
5.	autorización	-----
5.	mínimo privilegio	-----
5.	auditoría	-----

Opciones: verificar quién accede · decidir qué puede ver · conceder solo lo imprescindible · registrar los accesos realizados

Seguridad

Seguridad y control de acceso

Cifrado

en tránsito

en reposo

gestión de claves

Identidad

autenticación

multifactor
 ciclo de vida
 Acceso
 roles
 mínimo privilegio
 atributos
 Verificación
 auditoría
 registros
 defensa en capas

El mapa mental interactivo es interactivo en la versión online.



Control de acceso https://en.wikipedia.org/wiki/Access_control Restringir el acceso a un entorno u objeto según identidad y permisos.

6. Un analista necesita una vez ciertos datos y te pide acceso permanente «por si acaso». ¿Cómo aplicas mínimo privilegio y qué tipo de acceso propondrías?

Referencia curricular

Materia:	Privacidad y Seguridad de Datos · Responsabilidad Profesional
-----------------	---

Versión interactiva completa (con actividades, videos y autoevaluación):



<https://univ.lumbre.lat/object/cdia-priv-003-seguridad-basica-y-control-de-acceso>

Material educativo generado desde Lumbre · lumbre.lat