

# SUPUESTO PRÁCTICO: Gestión de la Seguridad de Datos en GlobalTech Solutions

---

## ¿Quiénes son?

---

GlobalTech Solutions es una empresa española de desarrollo de software.

Maneja datos personales de empleados, clientes y usuarios.

Opera también a nivel europeo.

Ha sufrido un incidente de seguridad: un ex empleado accedió sin permiso a la base de datos de clientes.

## 1. Análisis Legal y Normativo

---

 ¿Qué leyes aplican? A nivel europeo:


RGPD (Reglamento General de Protección de Datos)

Obligatorio en toda la UE.

Protege datos personales y establece derechos.

En España:

LOPDGDD (Ley Orgánica 3/2018)

Adapta el RGPD al marco legal español.  Ambos obligan a empresas como GlobalTech a manejar los datos de forma segura y responsable.

## Principios clave del RGPD

---

Licitud y transparencia

Finalidad específica

Minimización de datos

Exactitud

Conservación limitada

Seguridad (confidencialidad e integridad)

Responsabilidad proactiva

## ¿Qué pasa si se confirma el incidente?

---





Deben notificarlo a la AEPD en 72h.

Si hay alto riesgo, también deben avisar a los afectados.

Posibles sanciones:

Hasta 20 millones € o el 4% del volumen de negocio.

## 2. Seguridad en la Base de Datos

- ¿Qué medidas debe implementar GlobalTech?  Autenticación y autorización MFA (doble verificación)
- Gestión por roles (RBAC)
- Integración con LDAP / Active Directory
-  Integridad y transacciones ACID Validaciones en tablas (FOREIGN KEY, NOT NULL)
- Transacciones seguras y consistentes
-  Encriptación En reposo: AES-256
- En tránsito: TLS 1.3
-  Backups Copias diarias y semanales
- Simulacros de recuperación (disaster recovery)

## ¿Cómo habría ayudado DCL (Data Control Language)?

```
REVOKE ALL PRIVILEGES ON clientes FROM 'usuario_expleado';
```

## Anonimización vs. Pseudonimización


	Anonimización	Pseudonimización
Definición	Irreversible	Reversible con clave
Uso	Estadísticas	Entornos de prueba
Aplicación	Sin identificar a nadie	Datos protegidos pero recuperables


## 3. Seguimiento y Auditoría

-  Monitoreo en tiempo real Uso de herramientas SIEM como Splunk o Elastic Stack

Triggers SQL para registrar accesos

```
CREATE TRIGGER log_acceso ...
```

 Análisis forense Herramientas como Wireshark o Autopsy


Logs de actividad para saber qué hizo el empleado  ¿Se puede monitorear legalmente? Sí, pero:

Debe ser informado en el contrato o políticas internas.

Solo si es proporcional y justificado.

No se puede invadir la privacidad del empleado.

## 4. Criptografía

 Clave pública vs clave privada

Tipo	Uso principal	Aplicación en GlobalTech
Clave pública	Envío de datos cifrados	Comunicaciones seguras
Clave privada	Descifrar y firmar datos	Protección de bases de datos

## ¿Qué aporta la criptografía?

Función	Qué logra
Autenticación	Verificar la identidad del usuario
Confidencialidad	Proteger la información privada
Integridad	Detectar cambios o alteraciones
No repudio	Asegurar que el autor no niegue su acción

## Conclusiones

GlobalTech debe actuar rápido y aplicar medidas correctivas.

Las leyes europeas y españolas protegen los datos con rigor.

Las bases de datos deben tener control de accesos, cifrado, y respaldo.

Es fundamental auditar, monitorear y aplicar criptografía correctamente.

## Recomendaciones Finales

Revisión de accesos y permisos periódicamente.

Formación al personal en ciberseguridad.

Políticas internas claras y actualizadas.

Registro y reporte inmediato de incidentes.