

PROTECCIÓN DE DATOS



Ignacio Fernández Mira
Hugo González Febles
Darío Racero Morales

¿QUÉ ES LA PROTECCIÓN DE DATOS?



LOS DATOS PERSONALES SON CUALQUIER INFORMACIÓN QUE PUEDA IDENTIFICAR A UNA PERSONA, COMO NOMBRE, DNI, DIRECCIÓN, CORREO ELECTRÓNICO, DATOS BANCARIOS O INCLUSO ASPECTOS MÁS SENSIBLES COMO SALUD, ORIENTACIÓN SEXUAL O CREENCIAS. LA PROTECCIÓN DE DATOS BUSCA EVITAR QUE ESTOS DATOS SEAN USADOS SIN CONSENTIMIENTO O DE MANERA INDEBIDA.

¿CÓMO SE CONSIGUE ESTO?



MEDIANTE UN CONJUNTO DE MEDIDAS TÉCNICAS Y LEGALES QUE
GARANTIZAN:

INTEGRIDAD
CONFIDENCIALIDAD
DISPONIBILIDAD

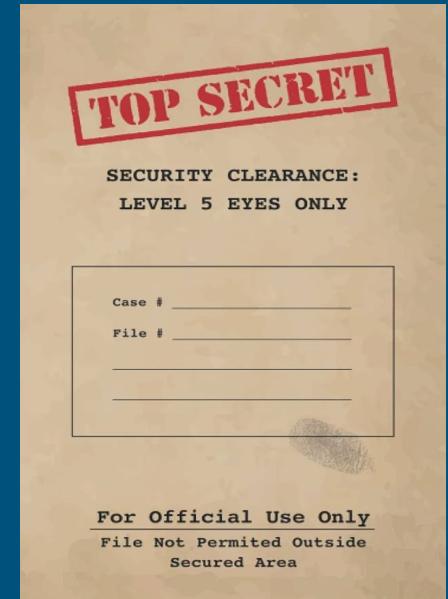
INTEGRIDAD

LA INTEGRIDAD ASEGURA QUE LOS DATOS SEAN EXACTOS, COMPLETOS Y NO SE HAYAN ALTERADO DE FORMA NO AUTORIZADA. EN PROTECCIÓN DE DATOS SIGNIFICA QUE LA INFORMACIÓN SE MANTIENE FIEL A SU ESTADO ORIGINAL, SIN MANIPULACIONES, PÉRDIDAS O MODIFICACIONES INDEBIDAS.



CONFIDENCIALIDAD

LA CONFIDENCIALIDAD SE ENCARGA DE QUE LA INFORMACIÓN SÓLO PUEDA SER CONOCIDA Y UTILIZADA POR LAS PERSONAS AUTORIZADAS. EN PROTECCIÓN DE DATOS IMPLICA GARANTIZAR QUE LOS DATOS PERSONALES NO SE REVELEN A TERCEROS NO AUTORIZADOS, PROTEGIÉNDOLOS CONTRA ACCESOS INDEBIDOS, FILTRACIONES O USOS INDEBIDOS.



DISPONIBILIDAD

LA DISPONIBILIDAD GARANTIZA QUE LOS DATOS Y SISTEMAS ESTÉN ACCESIBLES Y UTILIZABLES CUANDO SE NECESITEN POR LAS PERSONAS AUTORIZADAS, EVITANDO INTERRUPCIONES O PÉRDIDAS DE ACCESO DEBIDAS A FALLOS, ATAQUES O DESASTRES.



MÉTODOS DE SEGURIDAD



- CIFRADO DE BASES DE DATOS Y ARCHIVOS
- COPIAS DE SEGURIDAD PERIÓDICAS
- CONTROL DE ACCESOS Y CONTRASEÑAS SEGURAS
- AUDITORÍAS Y MONITORIZACIÓN

CIFRADO DE BASES DE DATOS Y ARCHIVOS

EL CIFRADO SE ENCARGA DE TRANSFORMAR EL TEXTO PLANO A TEXTO CIFRADO USANDO ALGORITMOS MATEMÁTICOS (RSA,AES,CHACHA20,SHA) Y UNA CLAVE, Y SOLO LOS QUE TENGAN ESA CLAVE PODRÁN DESCIFRAR LA INFORMACIÓN.



COPIAS DE SEGURIDAD PERIÓDICAS

LOS BACKUP SON RESPALDOS PROGRAMADOS DE LA INFORMACIÓN ALMACENADA EN LA BASE DE DATOS QUE SIRVEN POR SI HAY UN PROBLEMA Y TIENES QUE VOLVER A UN PUNTO INICIAL



TIPOS DE COPIAS EN BASES DE DATOS

EXISTEN MUCHOS TIPOS DE BACKUP PERO LOS PRINCIPALES SON:

COMPLETO:COPIA TODA LA BASE DE DATOS

INCREMENTAL:COPIA SOLO LO QUE CAMBIÓ DESDE EL ÚLTIMO
BACKUP

DIFERENCIAL:COPIA LO QUE CAMBIÓ DESDE EL ÚLTIMO BACKUP
COMPLETO

CONTROL DE ACCESO Y CONTRASEÑAS SEGURAS

EL OBJETIVO ES LIMITAR QUIÉN TIENE ACCESO Y QUE PUEDE HACER, SE PUEDE HACER DANDO PRIVILEGIOS DIFERENTES A CADA USUARIO, HACIENDO QUE EL USUARIO TENGA QUE PONER UNA CUENTA PARA ENTRAR



AUDITORÍAS Y MONITORIZACIÓN

CONSISTE EN REGISTRAR Y ANALIZAR ACTIVIDADES QUE SE HAN HECHO EN LA BASE DE DATOS O POR SI HAY ALGÚN ACCESO INDEBIDO



OBJETIVOS PRINCIPALES EN LA MONITORIZACIÓN

LOS OBJETIVOS PRINCIPALES SON:

SABER QUIEN ACCEDIÓ Y QUE DATOS CONSULTÓ

DETECTOR COMPORTAMIENTOS SOSPECHOSOS

VIGILAR EL ESTADO DEL SERVIDOR

DETECTOR ANOMALÍAS DE TRÁFICO

LEGISLACIÓN EN ESPAÑA - LOPD



LA LOPD (LEY ORGÁNICA DE PROTECCIÓN DE DATOS) FUE LA PRIMERA LEY EN ESPAÑA QUE REGULABA EL USO Y PROTECCIÓN DE LOS DATOS PERSONALES.

FUE APROBADA EN 1999, Y TRAS ESTO, LA LOPD CREÓ LA AEPD (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS) PARA PROTEGER NUESTROS DERECHOS SOBRE LOS DATOS PERSONALES, PERMITIÉndonos SABER, CORREGIR O ELIMINAR LA INFORMACIÓN QUE TIENEN SOBRE NOSOTROS.

LEGISLACIÓN EN ESPAÑA - LOPD

LAS EMPRESAS TENÍAN LA OBLIGACIÓN DE PROTEGER NUESTROS DATOS Y OBTENER NUESTRO CONSENTIMIENTO PARA USARLOS, AUNQUE LAS SANCIONES ERAN LEVES COMPARADAS CON EL GDPR.

LIMITACIÓN: LA LEY NO SE ADAPTABA A LOS CAMBIOS TECNOLÓGICOS. POR EJEMPLO, NO CONTEMPLABA CÓMO MANEJAR LOS DATOS QUE UNA EMPRESA TENÍA EN LA NUBE O CÓMO GESTIONAR LA ENORME CANTIDAD DE DATOS QUE LAS REDES SOCIALES RECOPILABAN.

LEGISLACIÓN EN EUROPA - GDPR



EL GDPR (REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS) ES LA NUEVA LEY DE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA QUE REEMPLAZÓ A LA LOPD EN 2018.

A DIFERENCIA DE LA LOPD, NO SOLO AFECTA A ESPAÑA, SINO A TODA EUROPA Y A CUALQUIER EMPRESA DEL MUNDO QUE TRATE LOS DATOS DE CIUDADANOS EUROPEOS.

LEGISLACIÓN EN EUROPA - GDPR

CON EL GDPR, SI UNA EMPRESA PIERDE O FILTRA TUS DATOS, DEBE NOTIFICARLO EN UN PLAZO DE 72 HORAS A LAS AUTORIDADES Y A LAS PERSONAS AFECTADAS.

ADEMÁS, TE DA EL DERECHO AL OLVIDO, O SEA, QUE PUEDES PEDIR QUE ELIMINEN TUS DATOS SI YA NO SON NECESARIOS.

SI LAS EMPRESAS NO CUMPLEN CON EL GDPR, PUEDEN RECIBIR MULTAS DE HASTA EL 4% DE SUS INGRESOS ANUALES.

COMPARACIÓN LOPD VS GDPR

LA LOPD SÓLO APLICABA EN ESPAÑA, MIENTRAS QUE EL GDPR AFECTA A TODA LA UNIÓN EUROPEA Y A CUALQUIER EMPRESA QUE TRATE DATOS DE CIUDADANOS EUROPEOS.

LA LOPD TE DABA DERECHOS BÁSICOS SOBRE TUS DATOS, PERO EL GDPR INCLUYE NUEVOS DERECHOS COMO EL DERECHO AL OLVIDO Y LA PORTABILIDAD DE LOS DATOS.

COMPARACIÓN LOPD VS GDPR

CON LA LOPD, EL CONSENTIMIENTO NO SIEMPRE ERA CLARO, PERO CON EL GDPR, LAS EMPRESAS DEBEN PEDIRTE UN CONSENTIMIENTO EXPLÍCITO PARA USAR TUS DATOS.

LAS MULTAS BAJO LA LOPD ERAN MÁS SUAVES, MIENTRAS QUE EL GDPR PUEDE LLEGAR A SER DEL 4% DE LA FACTURACIÓN GLOBAL DE LA EMPRESA.

EL GDPR OBLIGA A LAS EMPRESAS A INFORMAR EN 72 HORAS SI HAY UNA BRECHA DE SEGURIDAD Y LA LOPD NO.

FIN

DATABASE PROTECTION

