

GENERAL

Afecta a todas aquellas organizaciones que manejen información personal de ciudadanos de la UE, incluso a aquellas que estén ubicadas fuera de la unión.

DATOS

Los datos corporativos están expuestos y son sensibles. Los almacenamos, los enviamos por email, guardamos en la Nube o los manejamos desde móviles y tabletas.

PROTECCIÓN

La nueva normativa añade al derecho de acceso, rectificación, cancelación y oposición, la protección de los datos a un nivel superior. Deben cifrarlos y garantizar su integridad.

REGULACIÓN

La Unión Europea para garantizar el cumplimiento ha regulado las sanciones aplicables, que llegan hasta 20 millones de euros o el correspondiente al 4% de la facturación mundial anual de la organización sancionada.

DECÁLOGO DE LA GDPR

- 1.** Informarse sobre GDPR. Buscar información y pasos a seguir para aplicarla. Esta guía es un buen comienzo.
- 2.** Asegurarse de que los empleados entiendan cuáles son los pasos que la empresa está siguiendo para proteger su información.
- 3.** Crear conciencia de la importancia de la protección de datos. Los empleados deben entender que proteger los datos de la empresa y de sus clientes es vital.
- 4.** Segmentar la información a la que acceden los empleados. En el nuevo reglamento incluso la lectura de información confidencial se considera como fuga de datos.
- 5.** Ante la duda tratar toda la información como confidencial. Es recomendable no recopilar datos innecesarios. Los ladrones robarán lo que encuentren.
- 6.** Señalar de manera clara qué información se utilizará y cuánto tiempo se va a conservar. Los clientes confían en las marcas claras y honestas.
- 7.** Usar contraseñas robustas y únicas. Asegúrese de que las contraseñas nunca se comparten y que son robustas y únicas.
- 8.** Cifrar los datos. Es recomendable cifrar los datos para proteger la información de los ladrones y de las miradas indiscretas. El cifrado imprescindible.
- 9.** Tener copias de seguridad. La normativa obliga a mantener la integridad de los datos. Por ello es obligatorio tener copias de seguridad de los mismos.
- 10.** Asesorarse por un profesional de la ciberseguridad. La complejidad técnica requerida para satisfacer estos requisitos precisa de personal experto.

GDPR

Reglamento Europeo de Protección de Datos

¿Qué es y cómo me afecta?



LA GDPR OBLIGA



NOTIFICAR BRECHAS Y FUGAS DE INFORMACIÓN

Si una empresa sufre una brecha de seguridad y los datos no estaban debidamente cifrados debe notificarlo a los usuarios afectados así como a la Agencia de Protección de Datos.

DESIGNAR UN DPO

Obligatorio para empresa de más de 250 empleados. Será la persona responsable del tratamiento de los datos. En las empresas más pequeñas será obligatorio el DPO cuando necesiten un seguimiento sistemático y periódico de los datos personales tratados.

DERECHO AL OLVIDO y PORTABILIDAD DE DATOS

Los usuarios ganan estos derechos que les hacen más dueños de sus datos personales pero a la vez hacen más difícil la tarea de las empresas.

MANTENER LA INTEGRIDAD DE LOS DATOS

Este punto es probablemente el más sensible pues es el núcleo de la GDPR. La custodia y protección de los datos personales. Las copias de seguridad y el cifrado serán nuestros aliados.

GENERAMOS DATOS

La relación empresa-cliente genera datos



Los datos se almacenan y emplean según la actividad de la empresa



Acceso a ellos desde PCs, Servidores o la Nube.



SON DATOS PERSONALES:

Nombres, datos de contacto, emails, fechas de nacimiento, dirección IP, información bancaria, perfiles en redes sociales...

QUE ESTÁN AMENAZADOS



Secuestro del PC y los datos



Robo de los datos



Pérdida y destrucción de datos

Y MANTENER SU INTEGRIDAD ES OBLIGATORIO

COPIAS DE SEGURIDAD

La obligatoriedad de mantener la integridad de los datos requiere que llevemos a cabo copias de seguridad, y según la norma, una segunda copia de la copia.

CIFRADO DE ARCHIVOS

Tanto los archivos que use en el día a día como las copias de seguridad han de estar cifradas, de modo que si caen en manos ajenas los datos sean ilegibles y no le comprometan.

PROTECCIÓN DE EQUIPOS y REDES

La integridad de sus equipos y de su red local ante ataques informáticos es vital para mantener la integridad y confidencialidad de su información. Protéjase del malware, ransomware y del spam del correo electrónico; pero no olvide una solución Firewall para su red.

Y DEBEMOS HACERLO

Según la GDPR (Regulation (EU) 2016/679)
Antes del 25 de mayo de 2018

