Inycom
innovation technologies

SOLUCIONES TECNOLÓGICAS QUE PERMITEN CUMPLIR CON EL NUEVO GDPR

www.inycom.es
info@inycom.es
+34 902 995 820

EL NUEVO GDPR

Texto complejo y minucioso. Con aplicación en Mayo de 2018

Abundantes conceptos jurídicos indeterminados que dificultan su interpretación en ocasiones.

Lleno de letra pequeña que te ayudamos a interpretar y gestionar

El GDPR obliga a realizar cambios de gestión de la información en la organización y la consecuente necesidadde una adecuación tecnológica.

Obligación para las organizaciones:

- Evaluaciones de impacto
- Información de brechas de seguridad
- Nombramiento de un Delegado de Protección de Datos
- Notificación de rectificación, cancelación o restricción en el tratamiento

NUEVOS RESPONSABILIDADES RECOGIDAS EN EL REGLAMENTO

Uno de los aspectos esenciales del Reglamento es que se basa en la prevención por parte de las organizaciones que tratan datos. Es lo que se conoce como responsabilidad activa. Las empresas deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece. El Reglamento entiende que actuar sólo cuando ya se ha producido una infracción es insuficiente como estrategia, dado que esa infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar.

Para ello, el Reglamento prevé una batería completa de medidas:

- Protección de datos desde el diseño
- Protección de datos por defecto
- Medidas de seguridad
- Mantenimiento de un registro de tratamientos
- Realización de evaluaciones de impacto sobre la protección de datos
- Nombramiento de un delegado de protección de datos
- Notificación de violaciones de la seguridad de los datos
- Promoción de códigos de conducta y esquemas de certificación

1

CONCIENCIACIÓN DE SEGURIDAD

Las personas, son el eslabón más débil de la cadena, por tanto, es fundamental hacerles plenamente conscientes de la repercusión y consecuencia de sus acciones en lo que en materia de seguridad de la información se refiere.

Para ello, es necesario realizar formaciones adaptadas a los diferentes perfiles que comprenden las compañías, así como también al sector en el que se encuentra la organización. Tomando en cuenta los requisitos de seguridad, como valor intrínseco de la compañía.

Las organizaciones con un programa de concienciación en seguridad fueron un 50% menos propensas a tener brechas de seguridad y gastaron un 76% menos en incidentes de seguridad

2

CIFRADO

Tecnologías como el **cifrado,** es con seguridad una de las que se necesitan para proteger los datos sensibles.

Diseñando una política de cifrado que equilibre adecuadamente la privacidad de datos en diferentes capas:

- Desarrollo SW
- Discos
- Tráfico de Ross
- Tráfico de Internet

La tecnología de gestión de tráfico cifrado está disponible para que las empresas puedan descifrar fragmentos seleccionados de tráfico cifrado y enviar el contenido para su procesamiento, mediante controles de seguridad antes de volverlo a cifrar y mandarlo a su destino.

3

PREVENCIÓN DE FUGA DE INFORMACIÓN

Las soluciones de prevención de pérdida de datos cobran una especial relevancia cuando se manejan en la organización datos de carácter confidencial, siendo necesaria la supervisión y protección de los datos en movimiento.

A través de soluciones tecnológicas conocidas como DLP (Data Loss Prevention) es posible supervisar los datos confidenciales que se están descargando, copiando o transmitiendo desde y hacia equipos portátiles y de escritorio mediante diversos medios como correo electrónico, almacenamiento en la nube, etc.

Fuga de información, la mayor amenaza para la reputación corporativa que puede forjarse, o destruirse, a la velocidad de un click. Según estudios recientes, el software de prevención de fuga de datos resuelve eficazmente el 80% de las fugas debidas a accidentes y negligencias

4

SISTEMAS DE AUDITORIA PARA NOTIFICACIONES DE FUGA

El RGPD exige que, en menos de **72 horas**, las organizaciones que han sufrido una fuga de datos tengan que notificarlo a la autoridad supervisora de la UE.

Las organizaciones deben evaluar su capacidad de respuesta inmediata para asegurarse que pueden ofrecer una imagen completa de **lo que ha sucedido y cómo.**

Según estudios recientes la fuga de datos puede tardar de promedio **más de 250 días en ser detectada y otros 80 días adicionales en ser resuelta**

Soluciones como el sistema de gestión de la información y de los eventos de seguridad **(SIEM)** y el **análisis forense de redes** permiten a las empresas capturar automáticamente toda la información de la red en un único lugar, **identificar cómo** se produjo la brecha, **qué recursos** fueron afectados y **que datos** se perdieron.

5

CONTROL DE DATOS EN LA NUBE

Para todas aquellas aplicaciones presentes en nube, es necesario:

- Que la organización tenga **visibilidad de su uso.**
- Que la organización tenga **control sobre los datos** que viajan en esas aplicaciones.
- Que la organización tenga control de **quiénes usan** esas aplicaciones.
- Qué la organización sea conocedora de **qué tipo de datos** y qué aplicaciones intercambian datos privados.

Otra tecnología que ayudará a las organizaciones en lo relativo a la ubicación de los datos es la **tokenización.**

Permite el uso de aplicaciones en la nube de modo seguro, **sustituyendo los datos privados por tokens seguros** a medida que el tráfico abandona la red corporativa y se dirigen hacia la nube.

De esta manera, **los datos privados nunca salen de la sede de la empresa**, cumpliendo así con las obligaciones del GDPR sobre ubicación de la información y sobre la debida protección de datos

6

CONTINUIDAD DE LOS SERVICIOS Y DISPONIBILIDAD

Los servicios que soportan la información sensible han de estar respaldados mediante una copia de seguridad que permita su restauración con garantía, por ello, sistemas como backups en la nube aportan ventajas frente a los sistemas convencionales.

- Disponibilidad 24x7.
- Reducción de costes.
- Acceso desde múltiples ubicaciones y dispositivos.

La importancia de los datos es incuestionable y esto hace que hoy en día, la correcta gestión y protección de la información de una organización sea un asunto de máxima relevancia dado que perder un solo día de trabajo en los datos, puede ocasionar no sólo un grave coste económico sino también un coste de imagen en cuanto a clientes y proveedores.