Adecuación Tecnológica

Respaldo de la información

Se debe **proteger** la información con medidas de respaldo que garanticen su recuperación en caso de necesidad.

Catálogo de la información y control de acceso

Es importante implementar los controles necesarios para garantizar la confidencialidad de los datos, **restringiendo el acceso** a la información estrictamente necesaria para prestar el servicio al personal autorizado, así como validar la identidad de las personas que acceden a los mismos. Para ello es necesario disponer de un **inventario de la información** utilizada en la compañía.

Protección frente a amenazas

Es preciso dotar a los sistemas informáticos de la compañía de medidas de protección contra las amenazas de **ciberseguridad** existentes, para evitar posibles incidencias de seguridad.

Registros y controles

Una parte fundamental es disponer de la **trazabilidad** sobre el uso de la información de carácter personal, estableciendo los registros y controles necesarios que recojan información sobre a qué datos se ha accedido, quién ha accedido, cuándo, qué se ha hecho con ese dato, y cualquier otra información que permita conocer en todo momento el tratamiento que ha sido realizado. También es importante conocer los intentos de acceso fallidos a los datos.

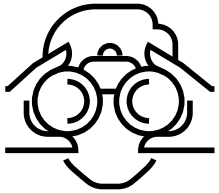
Auditorías y revisiones

La revisión de los registros de los sistemas informáticos es vital para detectar comportamientos anómalos o peligrosos que puedan ocasionar incidentes de seguridad. Es importante **auditar** de manera periódica la correcta aplicación de las medidas de seguridad mediante auditorías que permitan evaluar el nivel de seguridad y detectar posibles vulnerabilidades para corregir, así como puntos de mejoras aplicables.

Concienciación del personal

"Una cadena es tan fuerte como su eslabón mas débil". Es vital concienciar al personal sobre la importancia de la seguridad de la información y formarles adecuadamente en materia de seguridad informática para que sepan cómo actuar.

Plan de Acción

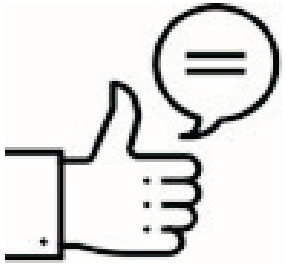


Diagnosis

Determinar el GAP regulatorio, las acciones precisas para su cumplimiento y cuantificar los recursos necesarios

Control

Herramientas y procesos para **asegurar** la realización del plan y el cumplimiento continuo a lo largo del tiempo

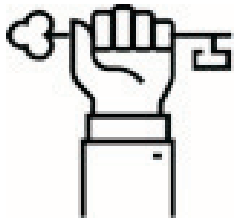


Privacidad

Identificar los datos personales que se utilizan y asegurar su uso adecuado de acuerdo a los derechos del interesado

Ciberseguridad

Asegurar el nivel óptimo de **seguridad** de acuerdo al riesgo, notificando las violaciones de la seguridad de los datos



Reglamento General de Protección de Datos

KEY IBERBOARD
Consultoría & Outsourcing

KEY IBERLEX
Abogados

PrimeGlobal
An Association of Independent Accounting Firms

Novedades destacadas

Consentimiento expreso

No son validos los **consentimientos tácitos**, por lo que deben revisarse las fórmulas utilizadas en las empresas y adaptarse de acuerdo a las nuevas exigencias. Es necesario una declaración o acción afirmativa para que el consentimiento sea **explícito**, mediante una acción proactiva del titular del dato.

Responsabilidad proactiva

Las empresas, como responsables del tratamiento, tienen que aplicar medidas técnicas y organizativas activas y eficaces para garantizar el cumplimiento de las obligaciones legales en la materia. Ya no sirve el mero cumplimiento formal y documental.

Derecho de información

El nuevo Reglamento introduce nuevos elementos de control a favor de los titulares de los datos, potenciando **el derecho a la información** e incorporando nuevos derechos como **el de portabilidad, el de suspensión o el derecho al olvido.**

Registro de actividades

Cada empresa tiene que llevar un registro interno de las **actividades de tratamiento** efectuadas, debiendo contener una determinada información acerca de los datos tratados.

Evaluación de impacto

Es obligatoria en aquellos casos en los que se genere un alto riesgo para los derechos y libertades de los interesados al tratarse datos sensibles a gran escala o que supongan evaluación sistemática y exhaustiva de aspectos personales de personas físicas. En otros supuestos será recomendable para conocer el grado de cumplimiento en el tratamiento y facilitar la gestión de los riesgos.

Delegado de protección de datos (DPO)

Para una gestión y coordinación adecuada de los datos personales, en determinados supuestos se exige la designación de la figura del **Delegado de Protección de Datos (DPO).** Podrá ser interno o externo, aunque sólo es obligatorio en determinadas situaciones.

Obligaciones

Principio de accountability

Una de las principales novedades del RGPD es el principio por el que se exige a las empresas que cumplan con el conjunto de obligaciones y que, además, estén en disposición de **demostrar** dicho cumplimiento. Para ello, el responsable del tratamiento debe aplicar las medidas técnicas y organizativas apropiadas para garantizar y acreditar que el tratamiento que se realiza es conforme al RGPD, teniendo en cuenta el ámbito, el contexto y los fines del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas.

El RGPD obliga a llevar internamente un **Registro de actividades de tratamiento** y exige la aplicación de medidas concretas de seguridad sobre los datos, debiendo justificar su pertinencia y probar su aplicación efectiva para cumplir con los objetivos obligatorios de **integridad y confidencialidad** de la información personal.

Adaptación al RGPD
(Ogligatoria desde el 25/05/2018)

Todas las empresas que traten datos personales deben verificar el grado de cumplimiento con respecto a las nuevas exigencias del RGPD. Cada organización debe acometer sus propios cambios, pero con carácter general, se pueden identificar las siguientes actuaciones:

1. Verificar si procede el nombramiento de un **Delegado de Protección de Datos (DPO)** o identificar a la persona/s responsables de coordinar la adecuación.

2. Revisión y análisis de los procesos de tratamiento de datos y de las medidas de seguridad existentes.

3. Crear un **registro de actividades de tratamiento** conforme a la finalidad y a la base jurídica.

4. Establecer **mecanismos** y un procedimiento de notificación de quiebra de seguridad.

5. Realizar un **análisis de riesgos** según las circunstancia de cada empresa, identificando las amenazas y diseñando un sistema de gestión de dichos riesgos que garantice la seguridad del tratamiento.

6. A partir del análisis de riesgos, se deberá valorar si existe la obligación de efectuar una **evaluación de impacto** en la protección de datos.

7. Adaptación de la documentación existente, revisando los formularios de recogida de datos, las cláusulas contractuales informativas, los contratos con los responsables y encargados, la política de privacidad, etc.

8. Documentar el cumplimiento para acreditar su conformidad con el RGPD. Se debe elaborar un expediente documental que recoja las acciones y actuaciones llevadas a cabo, el cual deberá ser revisado y actualizado regularmente para verificar su alineación con el RGPD.

KEY IBERBOARD
Consultoría & Outsourcing

Paseo de la Castellana 163, 9º derecha
28046 Madrid
+34 91 561 14 22
RGPD@keyiberboard.com
www.keyiberboard.com