Guía de anticipación al Nuevo Reglamento General de Protección de Datos Europeo

panda

La normativa GDPR responde a un aumento de los ciberataques y una búsqueda de colaboración entre las entidades públicas y privadas para remediarlo.

La creación de un marco digital común supone **una barrera extra de seguridad del principal activo corporativo: los datos.**

1. Introducción

¿Qué es la GDPR?

El nuevo Reglamento General de Protección de Datos Europeo (GDPR, General Data Protection Regulation) fue aprobada por el Parlamento Europeo y el Consejo el 27 de abril de 2016, entrando en vigor el 25 de mayo de 2016 y aplicable a partir del **25 de mayo de 2018**.

El periodo de dos años hasta la aplicación del Reglamento tiene como objetivo permitir que los Estados de la Unión Europea, las Instituciones Europeas y también las organizaciones que tratan datos vayan preparándose y adaptándose para el momento en que el Reglamento sea aplicable.

El Reglamento europeo busca proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, tanto si son procesados por entidades privadas como por Administraciones públicas.

Se reconocen los derechos de acceso, rectificación, cancelación, oposición, y dos nuevos derechos: el denominado “derecho al olvido”, como efectivo derecho de supresión, y la portabilidad de los datos.

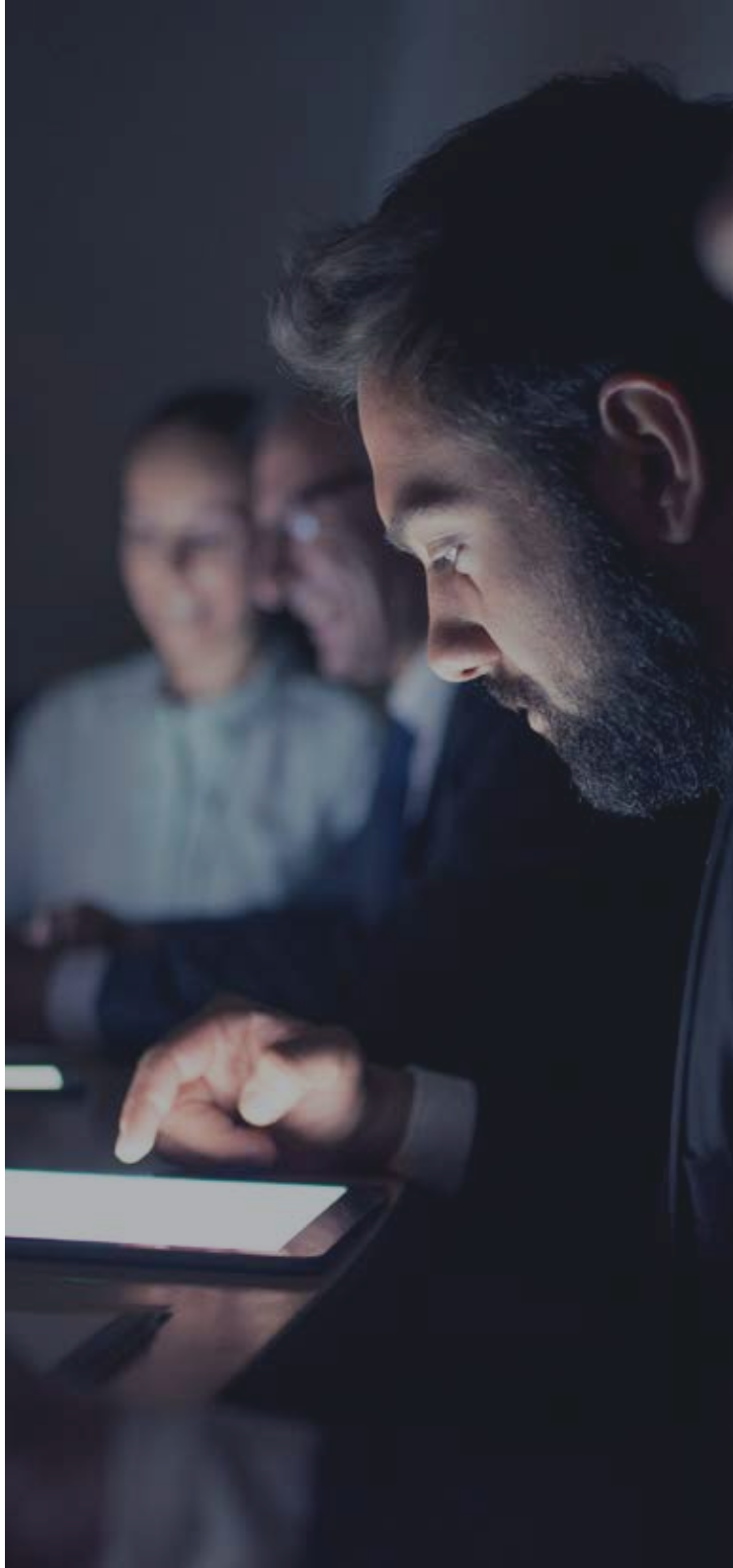
También se detallan las especificaciones del deber de información y de transparencia y la limitación del tratamiento de datos personales con fines de archivo en interés público, de investigación científica e histórica o fines estadísticos.

Otra novedad es la referencia al procesamiento de datos de europeos por entidades establecidas en Europa y fuera de la Unión Europea que realicen actividades dentro de la UE y que impliquen el tratamiento de datos personales, incluso aunque no tengan presencia física en el territorio de la Unión.

A esta novedad se suma la obligación para las entidades públicas de designar en ciertos casos a un «delegado de protección de datos» (DPO, Data Protection Officer) para garantizar el cumplimiento de la normativa. La diferencia principal con el Responsable de Seguridad es que el DPO deberá tener conocimientos normativos debidamente acreditados.

El nuevo reglamento establece la obligación de notificar a la Agencia de Protección de Datos (DPA), y este organismo podrá obligar incluso a hacer públicos, los detalles de los incidentes de seguridad que la empresa haya sufrido, en un plazo máximo de 72 horas después de conocerse.

Panda Security ha elaborado este documento que facilita la comprensión del nuevo marco normativo para ayudar a las organizaciones a adaptarse a los cambios que incorpora y cumplir así con sus obligaciones.



2. La aplicación del Reglamento en las empresas

¿Cómo afecta a tu negocio?

La prevención por parte de las organizaciones que tratan datos es el aspecto base del Reglamento. Esto es la denominada responsabilidad proactiva de las empresas, que juega aquí un papel diferencial. **Actuar sólo cuando ya se ha producido una infracción es insuficiente como estrategia**, ya que esa falta puede causar daños irreversibles a los interesados que pueden ser muy difíciles de compensar. Hablamos de una protección de datos desde el diseño del plan.

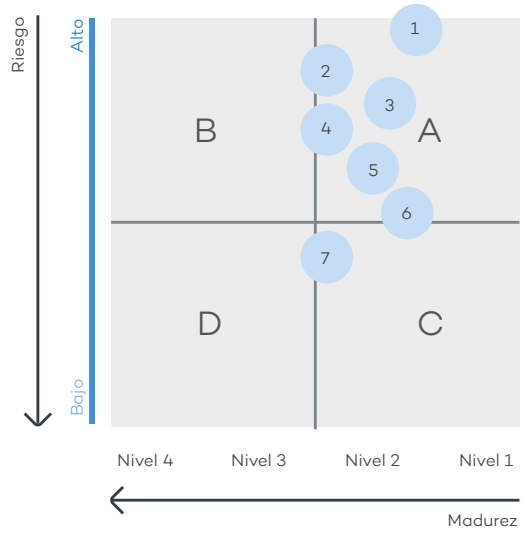
A pesar de que las empresas no tienen que aplicar de manera obligatoria todavía las nuevas medidas, una vez más resaltar la **importancia de trabajar con visión y antelación como ventaja competitiva**. Puede ser útil para las organizaciones empezar ya a valorar la implantación de algunas medidas previstas, como:

- Realizar análisis de riesgo de sus tratamientos, comenzando por identificar el tipo de tratamientos que realizan.
- Establecer el registro de tratamientos de datos.
- Implantar las evaluaciones de impacto o cualquiera otra de las medidas previstas.
- Diseñar e implantar los procedimientos para notificar adecuadamente a las Autoridades o a los interesados los incidentes de seguridad que pudieran producirse.

Hay que preparar un plan de acción para prepararse para la GDPR. Las empresas deben comenzar por entender su actual posición en la conformidad del reglamento. Un primer paso importante será que las organizaciones tengan bajo control los procesos de tratamiento de datos personales, incluyendo:

- Qué datos personales se tratan, incluyendo la recogida, tránsito, almacenamiento y procesamiento.
- Donde está esta información y quien tiene acceso a ella, través de su organización, incluyendo terceras empresas y colaboradores.
- Cuando se transfiera desde y hacia, incluido a terceros y transfronterizos.
- Cuáles son las medidas de seguridad a lo largo de su ciclo de vida.
- Cómo se almacena la información que permite la identificación del resto de la información.
- Cómo se permite la identificación, modificación, borrado o transferencia de los datos personales de un interesado si así lo solicitara.
- Cómo se comunica la política de privacidad, cómo se guarda y hace uso en el tratamiento de los datos, las respuestas.

Con la comprensión de las lagunas en el cumplimiento con el reglamento, las empresas estarán en una buena posición para evaluar el riesgo en su tratamiento de datos personales y desarrollar planes de remediación priorizados.



LEYENDA

Círculos

1. Gestión de terceros
2. Formación y concienciación
3. Gestión de riesgos
4. Política
5. Filtración de datos
6. Tratando equitativamente al cliente
7. Gestión de incidencias

Sectores

A. Mayor riesgo; menor madurez

B. Mayor riesgo; mayor madurez

C. Menor riesgo; menor madurez

D. Menor riesgo; mayor madurez

Figura 1. Las empresas se enfrentan a muchos retos para prepararse para. El primer paso es entender su estado actual y establecer los siguientes.

3. Obligaciones y ventajas

El Reglamento supone un mayor compromiso de las organizaciones, públicas o privadas, con la protección de datos. Esto no significa que deba suponer una mayor carga, sino que en muchos casos será sólo una forma de gestionar la protección de datos de manera distinta que hasta ahora.

La ventaja de una pronta aplicación es que permitirá detectar dificultades, insuficiencias o errores en una etapa en que estas medidas no son obligatorias y su corrección o eficacia no estarían sometidas a supervisión.

Esto permitiría corregir errores para el momento en que el Reglamento sea de aplicación obligatoria y entren en juego **sanciones y otros problemas derivados del incumplimiento del Reglamento.**

Si las empresas no cumplen con el Reglamento a partir de la fecha de aplicación, el 25 de mayo de 2018, se enfrentan a:

- **Daños económicos directos o indirectos.** ocasionados por incidentes de seguridad provenientes del exterior o por los propios empleados y colaboradores.
- **Daños reputacionales.** derivados de que el incidente de seguridad debe notificarse públicamente.
- **Pérdida de clientes actuales y potenciales** cuando la empresa no puede demostrar que se encuentra en conformidad con la regulación.
- Riesgo de **limitación o prohibición de procesamiento de datos** que las DPAs pueden imponer, afectando la actividad normal de la empresa.
- **Posible suspensión de los servicios** a los clientes, con el consecuente **abandono de estos** o incluso posibles **acciones legales** de los clientes, por la **limitación para procesar los datos**.
- **Indemnizaciones** que en virtud del nuevo Reglamento ya que los **interesados** tienen derecho a **reclamar en caso de infracción**.
- Así como las **costosas multas de administración** que pueden alcanzar hasta 20.000.000€ o el 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Con el cumplimiento del Reglamento las empresas evitarán los problemas anteriores y ganará la confianza de los consumidores.

Ventajas de un cumplimiento anticipado: Mecanismo de certificación aprobado

Otro punto a favor de la prevención y pronta implementación de la GDPR según los legisladores es que, para muchas empresas, ser capaces de demostrar que se adhieren al GDPR será una ventaja. Para ello se empieza a hablar de introducir los mecanismos de certificación de protección de datos y los sellos y marcas de protección de datos.

La GDPR habla incluso de la posibilidad de llegar a un sello europeo común de protección de datos, y aunque por ahora la GDPR proporciona escasos detalles es de esperar que este mecanismo para mostrar la adhesión, se desarrollará en los próximos meses.

Afectará a las empresas con **datos personales de personas físicas miembros de la UE**

Se aplicará al tratamiento de datos personales de **personas físicas dentro de la UE**

Datos que son considerados sensibles y que precisan **una especial protección**

Multas de hasta **20.000.000€** o el **4% del volumen de negocio** total anual global

4. Panda Adaptive Defense te ayuda en el cumplimiento de la nueva ley

¿Quieres conseguir la certificación?

Las organizaciones se enfrentan a dos grandes retos de cara al 25 de mayo de 2018: s**olventar la necesidad de adaptar las prácticas de seguridad de datos** y las tecnologías que lo sustentan a las exigencias del nuevo Reglamento y **paliar el desconocimiento de las organizaciones y los riesgos económicos**, reputaciones e incluso de la propia actividad empresarial.

La actitud proactiva por parte de las empresas es muy importante en este sentido. Estar preparadas para la prevención de cualquier incidente de seguridad para neutralizarla lo antes posible o el bloqueo del atacante si logra entrar en los sistemas, ahora es fundamental. Lo mismo en lo referido a disponibilidad de realizar investigaciones forenses detalladas en cada momento.

Las empresas que confían en Adaptive Defense tiene ya un camino recorrido en el cumplimiento de la GDPR, aportando:

- **Prevención:** Adaptive Defense permite realizar auditorías internas para verificar el estado de seguridad del parque en cualquier momento, incluido antes del despliegue de la solución, en la puesta en marcha del plan de acción para el cumplimiento de la GDPR o periódicamente.
- **Protección** de los datos personales procesado en los sistemas de la empresa, evitando por ejemplo la ejecución de cualquier proceso no confiables en los servidores corporativos.
- **Reducción del riesgo** de ser objeto de ataques de seguridad e **indicadores claves de la actividad y estado de los endpoints** que ayudan a establecer las medidas de seguridad: equipos vulnerables, actividad de red anómala entre dispositivos o entre dispositivos de dentro de la empresa hacia el exterior, etc.
- **Herramientas** para satisfacer la obligatoriedad de **notificar los incidentes de seguridad en las primeras 72 horas**. Gracias a las herramientas de análisis forense, alertas, visibilidad y control de Adaptive Defense/ Adaptive Defense 360, la empresa estará en condiciones de notificar tanto el detalle del incidente como del plan de acción para solventar y evitar el incidente en el futuro.
- **Mecanismos de control y gobierno del dato al DPO**, que será notificado en tiempo real, no solo de los incidentes de seguridad y si en estos están involucrados los ficheros con datos personales.

Y tu negocio, ¿todavía no se ha sumado a la inteligencia contextual?

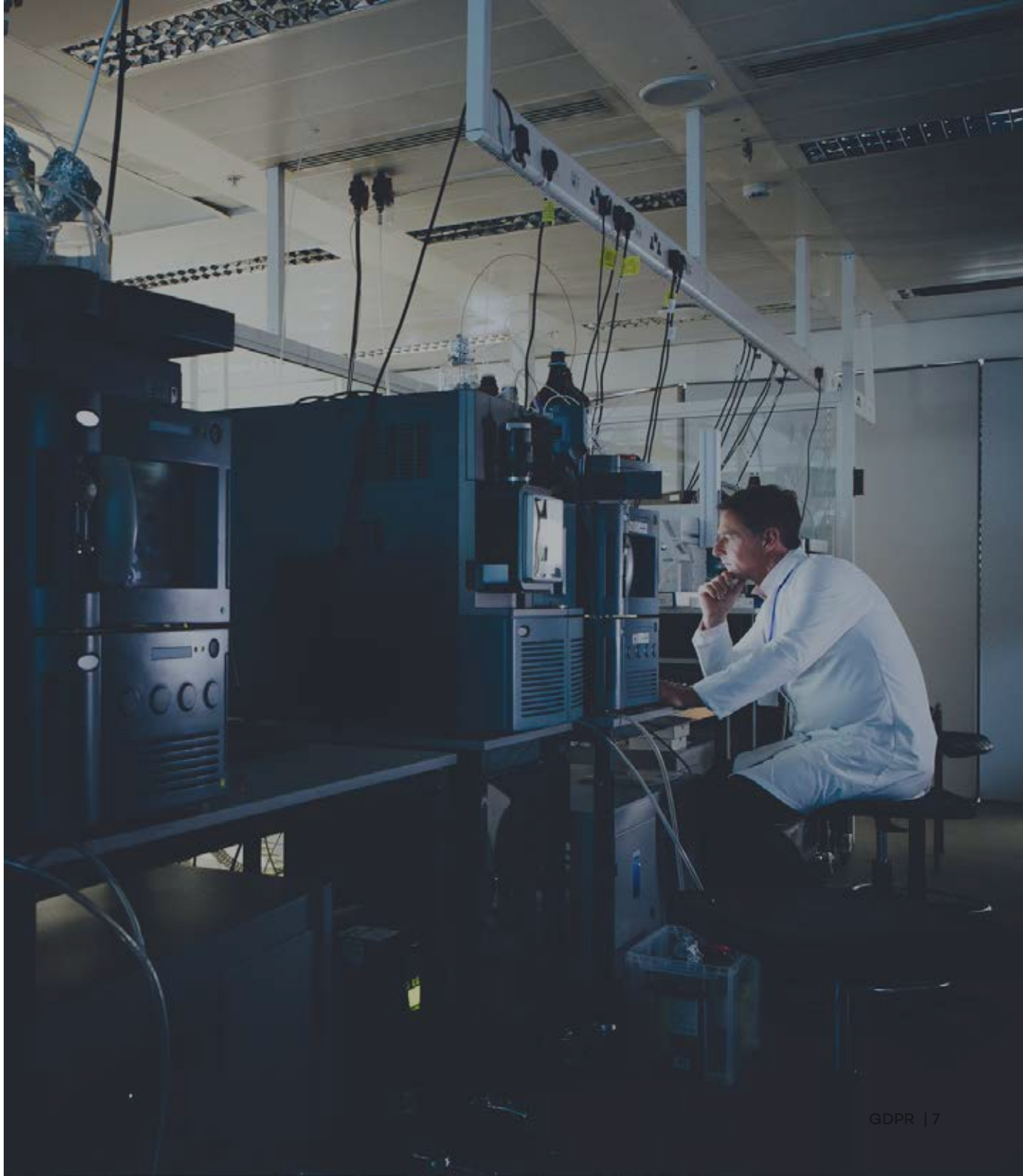
panda

Adaptive Defense 360

5. Sobre Panda Security

Panda Security es la **multinacional española líder en soluciones de ciberseguridad avanzada** y en herramientas para la gestión y control de equipos y sistemas. Desde su fundación en 1990, y manteniendo consistentemente su espíritu innovador, la compañía **ha firmado numerosos hitos históricos** en el sector.

Actualmente, el desarrollo de estrategias y tecnologías avanzadas de ciberseguridad se ha convertido en el núcleo de su modelo. Panda Security cuenta con **presencia en más de 80 países**, productos traducidos a más de 23 idiomas y más de 30 millones de clientes en todo el mundo.



Contacta con nosotros para más información

ARGENTINA
+54 11 6632 6632
argentina@pandasecurity.com

BOLIVIA
+59 12 21 20 300
bolivia@pandasecurity.com

BRASIL
+55 11 3054-1722
brazil@pandasecurity.com

CHILE
+56 2 6394774
chile@pandasecurity.com

COLOMBIA
+57 1 2560344
colombia@pandasecurity.com

COSTA RICA
+506 2523-4300
ventas@cr.pandasecurity.com

ECUADOR
+593 02 6012384
ecuador@pandasecurity.com

EL SALVADOR
+503 22087435
ventas.elsalvador@pandasecurity.com

GUATEMALA
+502 66400100
ventas.guatemala@pandasecurity.com

MÉXICO
+52 55 8000 2381
mexico@pandasecurity.com

PANAMÁ
+507 833 7263
ventas.panama@pandasecurity.com

PARAGUAY
+595 21 6075 94
paraguay@pandasecurity.com

PERÚ
+51 1 204 55 00
peru@pandasecurity.com

URUGUAY
+598 2 402 0673
ventas@uy.pandasecurity.com

VENEZUELA
+58 212-7612535
venezuela@pandasecurity.com

Más información en:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

o llamando al:

900 90 70 80

panda

Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

pandasecurity.com

panda