¿Está tu empresa preparada para la GDPR de UE?

¡El reloj ya ha empezado a correr!

pandasecurity.com

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

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.**

La GDPR establece las normas para garantizar un nivel uniforme de protección en el tratamiento de datos personales de las personas físicas dentro de la Unión y a la libre circulación de estos datos dentro de los Estados miembros.

Desde Panda Security, hemos elaborado este documento simplificado, para facilitar la comprensión de las líneas más relevantes del nuevo marco normativo y ayudar así a las organizaciones a obtener una vista de nivel superior de los cambios que incorpora y cumplir así con sus obligaciones.

Te invitamos a la lectura completa del Reglamento GDPR en el que se detallan todas las obligaciones y sus implicaciones.

2. Principales conclusiones

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.

Las empresas deberán hacer públicas las violaciones de seguridad que sufran y a comunicárselo a los usuarios afectados en un plazo de 72 horas, lo que hará crecer el presupuesto destinado a la seguridad de redes en las corporaciones ante la obligatoriedad de informar sobre estos incidentes, como ya sucede en Estados Unidos.

El foco de la seguridad corporativa se traslada del eje de las infraestructuras al eje de las personas (gestión de identidad y accesos), que no ha sido siempre atendido debidamente. Este cambio de paradigma deriva de la doble necesidad que supone la aplicación del GDPR: realizar una gestión preventiva de la privacidad y la seguridad de los datos y acreditar el cumplimiento y la gestión de responsabilidades.

Surgen nuevos roles, como la figura del DPO (Data Protection Officer). Este se encargará de informar y asesorar sobre obligaciones, supervisar el cumplimiento, cooperar con la autoridad de control y actuar como interlocutor con los titulares de los datos.

Desarrollo e implementación de un plan de acción para adaptar las prácticas empresariales a la GDPR, así como subsanar el desconocimiento de las empresas sobre sus obligaciones. Para ello, **las soluciones de ciberseguridad en la empresa deberán ser avanzadas** y acordes al nuevo paradigma, ofreciendo una seguridad más proactiva que reactiva.

3. ¿Qué es el Reglamento General de Protección de Datos Europeos (GDPR)?

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.

Esta medida también afecta a casi todas las empresas privadas, ya que, aunque en principio depende de la cantidad de datos tratados y de lo susceptible que sea de recibir ataques, el Reglamento es algo ambiguo en este aspecto.

Asimismo, el 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.

4. Datos básicos sobre la GDPR

1. ¿A quién afecta?

El reglamento afecta a todas las empresas que dispongan de datos personales de personas físicas miembros de la UE, aunque no tengan presencia física en su territorio.

Como personas físicas, debemos englobar no solo a sus clientes, sino también a candidatos, ex-clientes y usuarios de los productos y servicios que pueden haber sido adquiridos por un tercero, así como a los empleados y colaboradores de las empresas.

2. ¿De qué tiempo disponen las empresas para adecuarse?

Aunque fue aprobada por el Parlamento Europeo y del Consejo el 27 de abril de 2016 y haya entrado en vigor el 25 de mayo de 2016, se aplicará a partir del 25 de mayo de 2018.

3. ¿Qué son considerados Datos Personales y objeto de la GDPR?

Es considerado dato personal, la información sobre personas cuya identidad pueda determinarse, directa o indirectamente, mediante un nombre, un número de identificación, datos de localización, un identificador on-line e información relativa a la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

La GDPR se aplica al tratamiento de datos personales de personas físicas que se encuentran en la UE. Como dato curioso; la regulación sólo es aplicable a las personas vivas.

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

Entrará en vigor a partir del **25 de mayo de 2018.**

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

4. ¿Qué son considerados Datos Personales Sensibles?

El Reglamento establece categorías especiales de datos que son considerados sensibles y que precisan una especial protección, ya sea por su naturaleza o por la relación que puedan tener con los derechos y las libertades fundamentales de las personas.

El reglamento dispone expresamente la prohibición de tratar con estos datos personales sensible y que puedan revelar: Origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, biométricos que permitan la identificación unívoca de una persona y datos relativos a la salud a la vida y orientación sexuales.

Como excepción a la prohibición, el reglamento permite tratar categorías especiales de datos cuando el interesado haya dado su consentimiento, sea necesario para proteger sus intereses vitales o haya hecho manifiestamente públicos sus datos o cuando el tratamiento lo realiza legítimamente una organización sin ánimo de lucro.

5. ¿Cuáles son las consecuencias de la violación del Reglamento?

El Reglamento autoriza a los reguladores a imponer multas notablemente elevadas en cantidades 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. Sin embargo, tal y como veremos más adelante, las sanciones no son las únicas consecuencias del incumpliendo del Reglamento a partir de su entrada en vigor en el 2018.

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.

5.Obligaciones y Derechos más relevantes de la GDPR

El objetivo de la GDPR es reforzar la protección de los datos de los ciudadanos de la UE, para ello las empresas deberán de cumplir con unas obligaciones que permitirán a las personas físicas, cuyos datos personales son recogidos, almacenados y procesados por estas, disfrutar de una serie de derechos.

Recogemos en este apartado, algunas obligaciones claves por parte de la empresa y los derechos más relevantes de las personas físicas, que marca el nuevo Reglamento. Su comprensión ayudará a dimensionar mejor las adaptaciones operaciones a abordar para cumplir con la GDPR.

1. Obligación de notificar un incidente de seguridad sobre los datos

Los incidentes de seguridad sobre los datos personales deben ser notificados a la autoridad de control que corresponda en las 72 horas después de que se haya tenido constancia de ella.

La notificación incluirá:

- Descripción de la naturaleza del incidente e impacto.
- Número de interesados afectados y el número de registros.
- Nombre y datos de contacto del delegado de protección de datos.
- Descripción de las posibles consecuencias del incidente sobre los datos.
- Descripción de las medidas adoptadas o propuestas.

2. Obligación de la figura de delegado de protección de datos (DPO)

Las empresas están obligadas a designar un delegado de protección de datos cuando esta sea un organismo público o la actividad principal sea el tratamiento habitual y sistemática a gran escala de datos entre los que se incluyen los personales, o se traten datos relativos a condenas y delitos penales.

En el Reglamento, no se define en profundidad de lo que realmente es gran escala y es un término relativo y ambiguo, que obliga a asignar un DPO a casi todas las empresas.
Las funciones de un delegado de protección de datos son:

- Informar y asesorar a los empleados, que se ocupen del tratamiento de datos, de sus obligaciones.
- Supervisar el cumplimiento del Reglamento, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control y actuar como punto de contacto de esta.

3. Principio de transparencia y consentimiento

El principio de transparencia exige que toda información y comunicación relativa al tratamiento de datos personales sea explícitos y legítimos, fácilmente accesible y fácil de entender por las personas físicas afectadas.

En esta comunicación debe quedar totalmente claro:

- Que se están recogiendo, utilizando, consultando y tratando datos personales, en particular, los fines, plazo de tratamiento, destinatarios, la lógica implícita en todo tratamiento automático y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento.
- Los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales.
- El modo de hacer valer sus derechos en relación con el tratamiento de datos personales.

4. Incentivo para la seudonimización

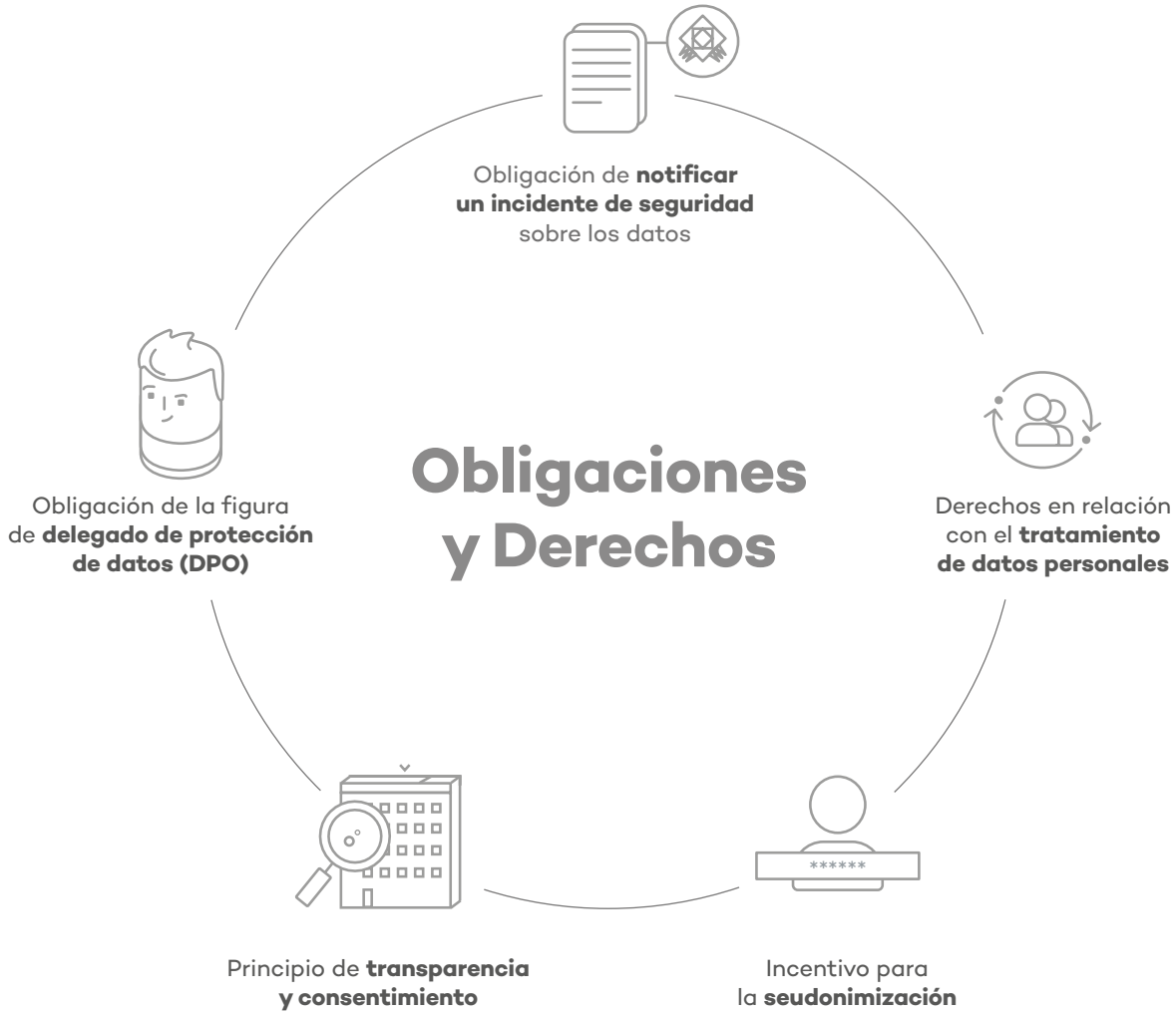
El foco de la GDPR son los datos relativos a una persona física identificable. Por consiguiente, el Reglamento no afecta a los datos de personas físicas no identificadas o identificables.

Por este motivo la GDPR crea incentivos para que las empresas seudonimicen los datos que recopilan. La seudinimización es la separación de los datos de los identificadores que permiten identificar directamente las personas físicas.
La seudonimización, por lo tanto, puede reducir significativamente los riesgos asociados con el procesamiento de datos, al tiempo que mantiene la utilidad de estos. Aunque los datos seudónimos no están exentos del Reglamento en su totalidad, la GDPR relaja varios requisitos en los controladores que utilizan esta técnica.

5. Derechos en relación con el tratamiento de datos personales

Las empresas deben facilitar al interesado mecanismos para el ejercicio de sus derechos, entre los que se incluye:

1. Derecho a solicitar y obtener de forma gratuita el acceso a sus datos personales.
2. Derecho a rectificar y borrar los datos personales que le conciernen.
3. Derecho al olvido, es decir, derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados o si el interesado ha retirado su consentimiento para el tratamiento.
4. Derecho a no ser objeto de Perfilado. El interesado tiene derecho a no ser objeto de una decisión basada únicamente en un perfilado automatizado.
5. El Perfilado es el tratamiento de los datos que ayudan a analizar, comparar y predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado.
6. Derecho a la portabilidad de los datos personales, que exige a las empresas proporcionar los datos personales de los interesados en un formato comúnmente utilizado y de transferir estos datos a otra empresa si así lo solicitan.



6.La aplicación del Reglamento en las empresas

La obligatoriedad de adaptar las prácticas de protección de datos de prácticamente todas las empresas que trabajan en los mercados de la UE, a la GDPR, es un hecho.

Las empresas que no lo hagan, se enfrentarán a sanciones y otros problemas, tan graves como los primeros. Afrontarlo cuanto antes debe verse como una prioridad y a la vez como una oportunidad, que ayudará a tener una mayor visibilidad y control de los datos, un mayor nivel de protección e incluso un nuevo factor diferencial con la competencia.

1. 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 directo o indirectos ocasionados por incidentes de seguridad provenientes del exterior o por los propios empleados y colaboradores.
- Daños de reputación producto de la notificación pública del incidente de seguridad.
- 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 ganarán la confianza de los consumidores y como tal una ventaja competitiva.

Mecanismo de certificación aprobado

Los legisladores han reconocido que para muchas empresas ser capaces de demostrar que se adhieren al GDPR será una ventaja. Para ello se está empezando a introducir los mecanismos de certificación de protección de datos y los sellos y marcas de protección de datos.

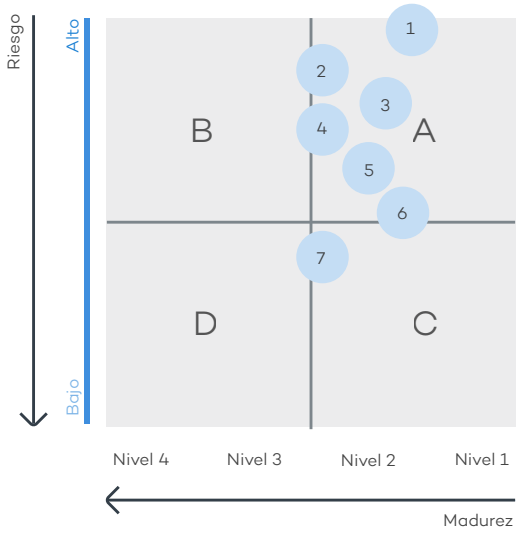
La GDPR habla incluso de la posibilidad de llegar a un sello europeo común de protección de datos, y aunque por ahora la GDPR proporciona escasos detalles es de esperar que este mecanismo para mostrar la adhesión, se desarrollará en los próximos meses.

2. Plan de acción para prepararse para la GDPR

Para adaptar las prácticas empresariales a 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.
- Dónde está esta información y quién tiene acceso a ella a través de su organización, incluyendo terceras empresas y colaboradores.
- Cuándo 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 y 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 la GDPR de la UE en los próximos meses. El primer paso es entender su estado actual y establecer los siguientes para avanzar hacia su conformidad.

7. La realidad de la adopción del Reglamento en las empresas

Una encuesta realizada por Dell en septiembre del 2016 , a un total de 821 empleados que, entre otras asignaciones, son responsables de la privacidad de datos de empresas con más del 10% de clientes en Europa, revela que tanto las pymes como las grandes empresas tienen un desconocimiento común acerca del nuevo Reglamento General de Protección de Datos de la Unión.

En resumen, las empresas no tienen un plan, ni saben cómo prepararse para su llegada y desconocen las repercusiones que podría tener su incumplimiento tanto para la seguridad de los datos, como para los resultados de negocio.

Así, el 82% de los profesionales de las áreas comerciales y de IT encargados de la seguridad de los datos se muestran preocupados por la entrada y el cumplimiento del nuevo reglamento, la preocupación es mayor en Europa, especialmente en Alemania y Suecia, sobre todo en las grandes empresas.

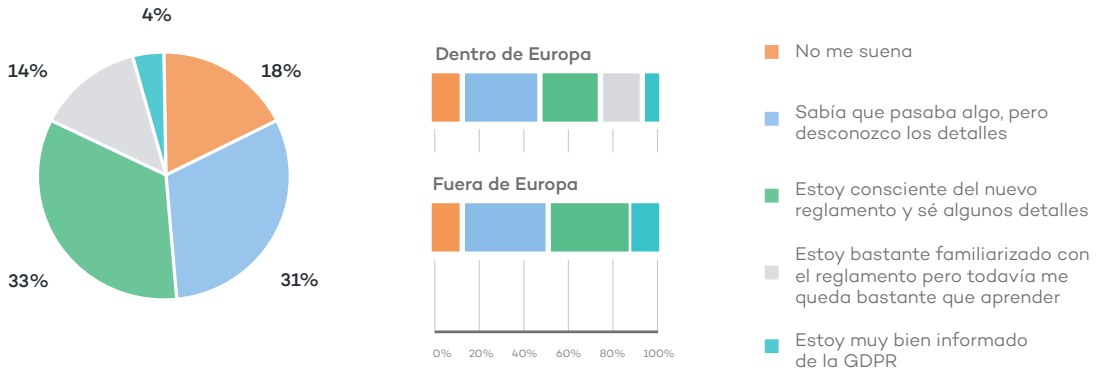


Figura 2. ¿Cómo describiría su conocimiento de GDPR?

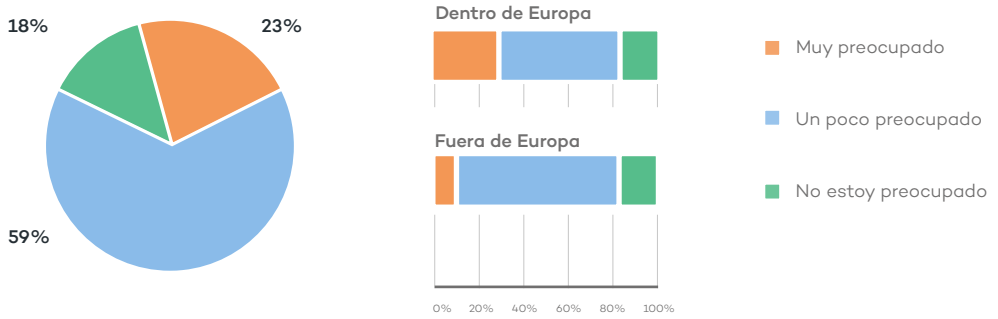


Figura 3. ¿Cuánto preocupa el cumplimiento de GDPR en su organización?

Y esto está alineado con el hecho de que los alemanes son los que se sienten más preparados para aplicar la GDPR (4%), mientras que los encuestados en Benelux (Bélgica, Holanda y Luxemburgo) son los que afirman estar menos preparados.

De hecho, más del 80% aseguran saber poco o nada acerca de las connotaciones que acarreará y tan solo un 3% de los profesionales del área IT están listos para ello.

Los resultados de la encuesta también reflejan que, aunque las empresas se dan cuenta de que el incumplimiento de la GDPR puede tener un impacto tanto en la seguridad de los datos como en sus resultados, no tienen claro ni el alcance de los cambios que deberían implantar, ni la severidad de las sanciones por incumplimiento o como estos cambios legislativos pueden afectar a su negocio.

De este modo, solo el 23% esperan cambios importantes en sus prácticas de seguridad de datos y en su tecnología.

Más del 80% de los encuestados conocen muy pocos o ningún detalle sobre el nuevo reglamento, no disponen de ningún plan para aplicar el nuevo Reglamento, no están preparados y tan sólo un 3% cuentan con un plan para su implementación.

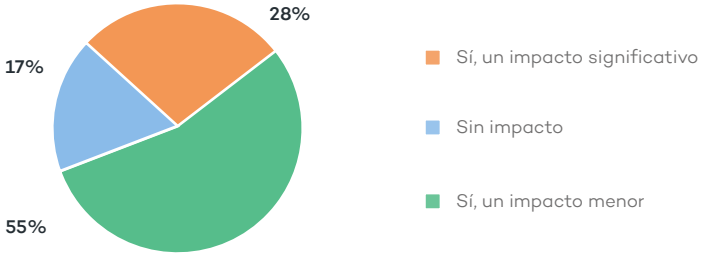


Figura 4. En tu opinión, ¿tendrá la GDPR un impacto en su enfoque de la SEGURIDAD DE DATOS?

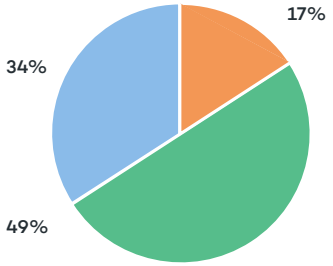


Figura 5. En tu opinión, ¿tendrá la GDPR un impacto en sus RESULTADOS DE NEGOCIOS?

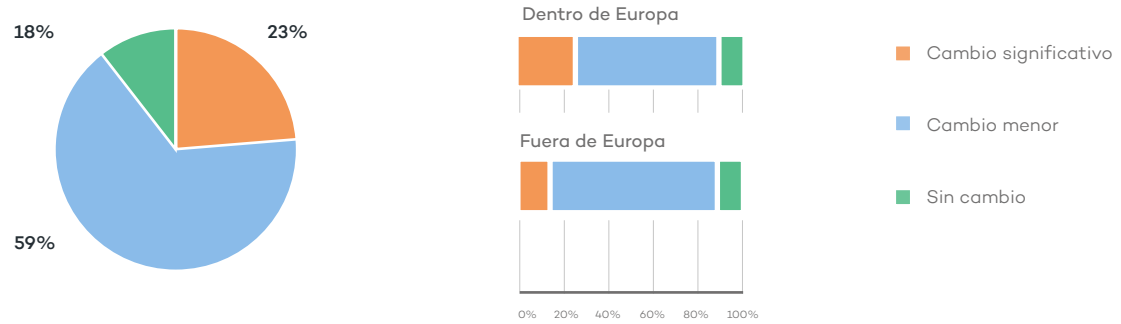


Figura 6. ¿Cuánto crees que las prácticas y tecnologías actuales de seguridad de datos tendrán que cambiar como resultado de GDPR?

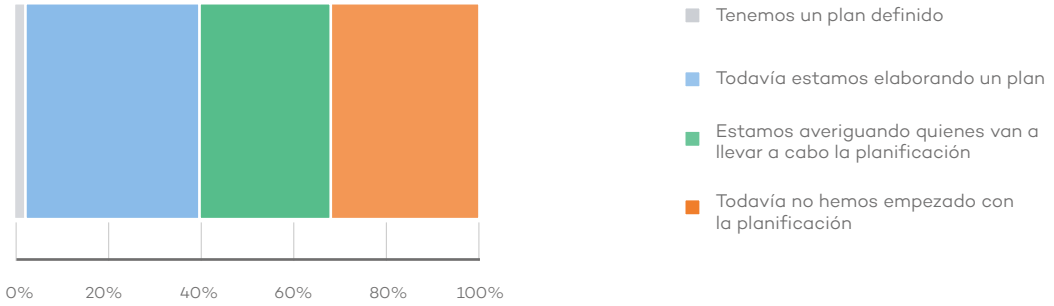


Figura 7. ¿Tiene tu empresa un plan para prepararse para la GDPR?

8. Panda Adaptive Defense te ayuda a cumplir con la GDPR

Como acabamos de ver, existe, por un lado, **una necesidad de adaptar las prácticas de seguridad de datos y las tecnologías** que lo sustentan a las exigencias del nuevo Reglamento que comienza a aplicarse en mayo de 2018 y, por otro lado, **el desconocimiento de las empresas sobre las obligaciones,** el impacto en sus organizaciones y los riesgos económicos, reputaciones e incluso de la propia actividad empresarial.

Una vez las empresas sean conscientes, el proceso de adecuación requiere de un gran esfuerzo de concienciación, formación y análisis e implantación de nuevas prácticas y tecnología. Todo este esfuerzo corre el riesgo de acabar por no servir de nada si, la elección no es la acertada y por un fallo de seguridad en los sistemas, los datos que están siendo gestionados por la empresa se pierden o un atacante logra acceder a ellos.

E incluso peores aún son las consecuencias: sanciones económicas directas e indirectas, daños reputaciones, pérdida de clientes, limitaciones en el ejercicio, demandas de clientes e indemnizaciones.

Panda Adaptive Defense reduce al mínimo estos riesgos y ayuda al cumplimiento de la GDPR asentándose en dos pilares fundamentales: Seguridad y Gobernanza de la Información.

Y es que estas son las dos claves, **un buen control** de los datos que se recogen, almacenan y tratan en los diferentes departamentos de la empresa (RRHH, marketing, etc.) tanto en los equipos como en los servidores, y la **adopción de las medidas de seguridad** necesarias para protegerlos de atacantes, adversarios o fallos de seguridad.

Una vez las empresas sean conscientes, el proceso de adecuación requiere de un gran esfuerzo de concienciación, formación y análisis e implantación de nuevas prácticas y tecnología.

A partir de estas bases, se marcan tres líneas de acción que permiten garantizar la seguridad de los datos:

1. Preparación

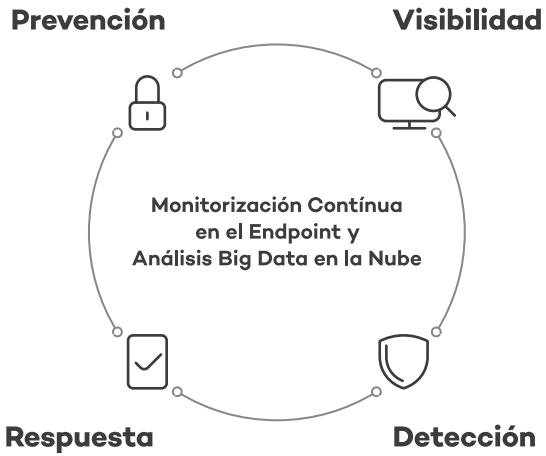
La actitud proactiva por parte de las empresas es muy importante en este sentido. Así, lo más importante es estar preparadas para la prevención de cualquier incidente de seguridad con el fin de neutralizarla lo antes posible o el bloqueo del atacante en el caso de que logre entrar en los sistemas, y lo mismo en lo referido a disponibilidad de realizar investigaciones forenses detalladas en cada momento.

Además, 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.

2. Protección

Las verdaderas soluciones de seguridad deben combinar tecnología avanzadas e inteligencia humana y computacional, machine learning en manos de expertos en seguridad. Para que una solución de seguridad sea tomada en serio, debe ofrecer el tipo de prevención, detección, visibilidad e inteligencia que pueda detener y prevenir ciber-atacantes de cualquier tipo una y otra vez.

Las exigencias de protección de una empresa, incluida las exigencias de la GDPR, que obliga a notificar en las primeras 72 horas del incidente el detalle de lo sucedió, impacto y acciones tomadas hasta el momento, obliga a que las soluciones de seguridad cubran los siguientes aspectos calves, que Adaptive Defense y Adaptive Defense 360 proporcionan:



- **Monitorización continua,** mediante el registro y supervisión de toda la actividad de los procesos en los puestos para detener el software no confiable en el momento de la ejecución, detectar amenazas avanzadas en tiempo real, responder en segundos y recuperarse de forma instantánea.
- **Detección de la ejecución de archivos no confiables,** que permite a tu empresa reducir la superficie de ataque en sus puestos. Debes buscar soluciones que clasifiquen todas las aplicaciones en confiables o maliciosas.
- **Automatización de la detección de amenazas.** La amenaza funciona más rápido que cualquier equipo. No permitas que deleguen en ti la supervisión de la respuesta. Las soluciones de seguridad eficaces deben poder funcionar de forma autónoma, automatizada y adaptarse al entorno operativo único de su organización.
- **Respuesta rápida y automatizada.** Las organizaciones están saturadas con el volumen de eventos y alertas generados por los sistemas, pero una vez el cibercriminal se infiltra con éxito, gran cantidad de información puede ser robada en segundos.

Las soluciones de seguridad deben identificar rápidamente un ataque en curso, tomar medidas para evitar daños y aliviar la carga del equipo, generando reducción de costes, automatizando totalmente lo que les ocupaba el tiempo durante días.

3. Visibilidad y Control

Los datos están vivos: crecen, cambian e incluso se mueven. Organizar la gestión de los mismos para adecuarse a la nueva norma es solo el principio. Una vez que todo esté como debe, es imprescindible mantener un control constante sobre los mismos, con el fin de comprobar si se

produce algún movimiento anómalo sobre ellos. **Advanced Reporting Tool (ART),** el módulo opcional de Adaptive Defense y Adaptive Defense 360, es una herramienta de Informes Avanzados que genera automáticamente inteligencia de seguridad y de actividad a nivel de endpoints.

Esta Inteligencia permite a las empresas identificar ataques y comportamientos inusuales, así como mal uso interno, basados en los eventos continuamente monitorizados en los endpoints, enviados y enriquecidos en la Plataforma de Adaptive Defense. ART permite a las organizaciones:

- **Supervisar y controlar** el uso indebido de recursos corporativos.
- **Recibir alertas** sobre Indicadores de seguridad y uso de recursos corporativos, como los ficheros con los datos personales.
- **Realizar análisis** de aspectos claves de incidentes de seguridad y anomalías en el acceso a ficheros con datos personales.
- **Realizar cálculos y visualización gráfica** sobre la actividad en los endpoints.

En el caso en el que el **departamento de seguridad** de la empresa opere un **SIEM** (Security Information Event Management) corporativo, el carácter abierto de la Plataforma de **Adaptive Defense**, facilita la integración en tiempo real de la información de la **actividad monitorizada en los endpoints** en el conjunto de logs gestionados en el SIEM.

Esto permite a los equipos de seguridad de las Organizaciones o al Centro de Operaciones de Seguridad (SoC) externo:

- **Ampliar el enfoque de seguridad Integral** abarcado no solo la red perimetral, sino los endpoints.
- **Obtener una vista única de los ataques y todo su impacto,** permitiendo un análisis forense en profundidad.
- **Explotar en profundidad** la información recogida para conocer mejor la **situación del parque** y facilitar la **elaboración de planes de mejora.**
- **Enriquecer la información del SIEM** con datos de otros orígenes más operativos, como puede ser los endpoints, y correlacionarlos con datos de negocio u otra naturaleza, aportando un grado superior de Inteligencia empresarial.

Figura 8. Ejemplos de visibilidad y control sobre los accesos a dato en ART.

Figura 9. Geolocalización del tráfico de salida de la empresa.

Panda Adaptive Defense vela por la seguridad de la empresa y sus datos y ayuda en la gobernanza de la información. Las empresas que confían en Adaptive defense tiene ya un camino recorrido en el cumplimiento de la GDPR, aportando:

- **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, detallando los incidentes de seguridad y si en estos están involucrados los ficheros con datos personales. Tanto ART, a través de alertas en tiempo real, paneles de control e informes, como el sistema de notificación del SIEM corporativo alertarán al DPO en tiempo real de accesos anómalos a los ficheros con datos personales.

9. Preguntas frecuentes sobre la GDPR

1. ¿Quiénes son los principales organismos y actores afectados por la GDPR?

Comité Europeo de Protección de Datos. El Comité está compuesta por una autoridad de control de cada Estado miembro (28) y del Supervisor Europeo de Protección de Datos. La función del Comité será revisar lo que está funcionando y lo que no está funcionando y también dar asesoramiento y orientación.

Autoridad de Control de Protección de Datos (DPA). Autoridad pública independiente que se establece por un Estado miembro para hacer cumplir la legislación local.

Encargado del tratamiento. Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales en nombre del responsable del tratamiento. El encargado no determina el propósito y el o los medios del tratamiento. Ellos sólo procesan los datos conforme a lo solicitado por el controlador.

Ejemplo: Empresa de gestión nóminas subcontratada o proveedor en la nube como Microsoft Azure donde se recogen, almacenan y procesan los datos.

Si un proveedor está actuando en conformidad con los requisitos de un responsable de datos, este es un encargado de datos. Bajo la antigua directiva, sólo se impondría una multa en caso de incumplimiento al responsable del tratamiento. Según el nuevo Reglamento, el encargado también es responsable de cumplir sus propias obligaciones, como tener las medidas de seguridad adecuadas.

Responsable del tratamiento. La persona o el departamento de la empresa responsable de define qué datos personales necesita y con qué propósito. Entonces, la empresa solicita los datos de las personas (empleados, clientes, etc. público). Un ejemplo sencillo podría ser una página web que solicita su nombre y dirección para enviarle un paquete. La compañía que define el hecho de que hay que pedir esa información y que fin tiene dicha solicitud, es el responsable de los datos.

El responsable del tratamiento no sólo debe cumplir con el reglamento, debe también demostrar el cumplimiento. Esta es una de las principales diferencias entre este Reglamento y otros. El responsable tendrá que ser capaz de demostrar el cumplimiento en un momento dado, ajustándose a las peticiones de la Autoridad de control o del interesado.

2. ¿Qué pasará con las Leyes de Protección de Datos de los Estados miembros?

El Reglamento no las deroga ni puede derogarlas, pues dicha atribución corresponde a cada Estado miembro. El Reglamento provoca el "desplazamiento normativo" de las Leyes de los Estados en todo lo que se oponga a la regulación europea. Pero estas Leyes quedarán vigentes hasta que se logre su completa derogación o bien su modificación para adecuarlas al RGPD.

En consecuencia, en los Estados miembros será necesario tener en cuenta tanto la GDPR como la Ley del cada Estado. Cuando haya conflicto entre una y otra, entonces, aquello dictado por la GDPR aplicará por encima de la Ley del Estado miembro.

3. ¿Deben las empresas revisar sus avisos de privacidad?

Con carácter general, sí. El Reglamento prevé que se incluyan en la información que se proporciona a los interesados una serie de cuestiones que con la Directiva y muchas leyes nacionales de trasposición no eran necesariamente obligatorias. Por ejemplo, habrá que explicar la base legal para el tratamiento de los datos, los períodos de retención de los mismos y que los interesados pueden dirigir sus reclamaciones a las Autoridades de protección de datos, si creen que hay un problema con la forma en que están manejando sus datos.
Es importante recordar que el Reglamento exige de forma expresa que la información que se proporcione sea fácil de entender y presentarse en un lenguaje claro y conciso.

4. ¿Cambia la forma en la que hay que obtener el consentimiento?

Una de las bases fundamentales para tratar datos personales es el consentimiento. El Reglamento pide que el consentimiento, con carácter general, sea libre, informado, específico e inequívoco. Para poder considerar que el consentimiento es inequívoco, el Reglamento requiere que haya una declaración de los interesados o una acción positiva que indique el acuerdo del interesado. El consentimiento no puede deducirse del silencio o de la inacción de los clientes u otras personas físicas.

Las empresas deberían revisar la forma en la que obtienen y registran el consentimiento.

Hay que tener en cuenta que el consentimiento tiene que ser verificable y que quienes recopilen datos personales deben ser capaces de demostrar que el afectado les otorgó su consentimiento. Por ello, es importante revisar los sistemas de registro del consentimiento para que sea posible verificarlo ante una auditoría.

5. ¿Puedo subcontratar o compartir las tareas del DPO?

Las empresas de presupuesto limitado pueden subcontratar o compartir las tareas del DPO. En Alemania, en virtud de la Ley Federal de Protección de Datos, las empresas con más de 9 empleados deben nombrar un DPO, pero es una práctica común subcontratar el papel a empresas especializadas de datos o firmas de abogados.

La Regulación establece que un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

Si se sigue la ruta de subcontratar su DPO sería necesario establecer un acuerdo de nivel de servicio (SLA) que garantice que puede cumplir con la GDPR, no sólo marcando la casilla de verificación del DPO, sino que el DPO pueda responder a la solicitud de los datos por parte de interesados y el resto de derechos establecidos en el Reglamento.

6. ¿Cuándo, cómo y qué tengo que notificar ante un incidente de seguridad?

¿Cuándo?: Un incidente de seguridad debe ser notificado siempre que afecte a datos personales de personas físicas, tanto si el acceso es pérdida o robo como si es un simple acceso a esos datos.

Si no se notifica el incidente cuando se requiera hacerlo, puede resultar en multas de hasta 10 millones de euros o el 2% de su facturación global.

¿A quién?: Es importante tener en cuenta es que hay dos umbrales diferentes, uno para notificar a los clientes o público en general y otro para alertar a la DPA.

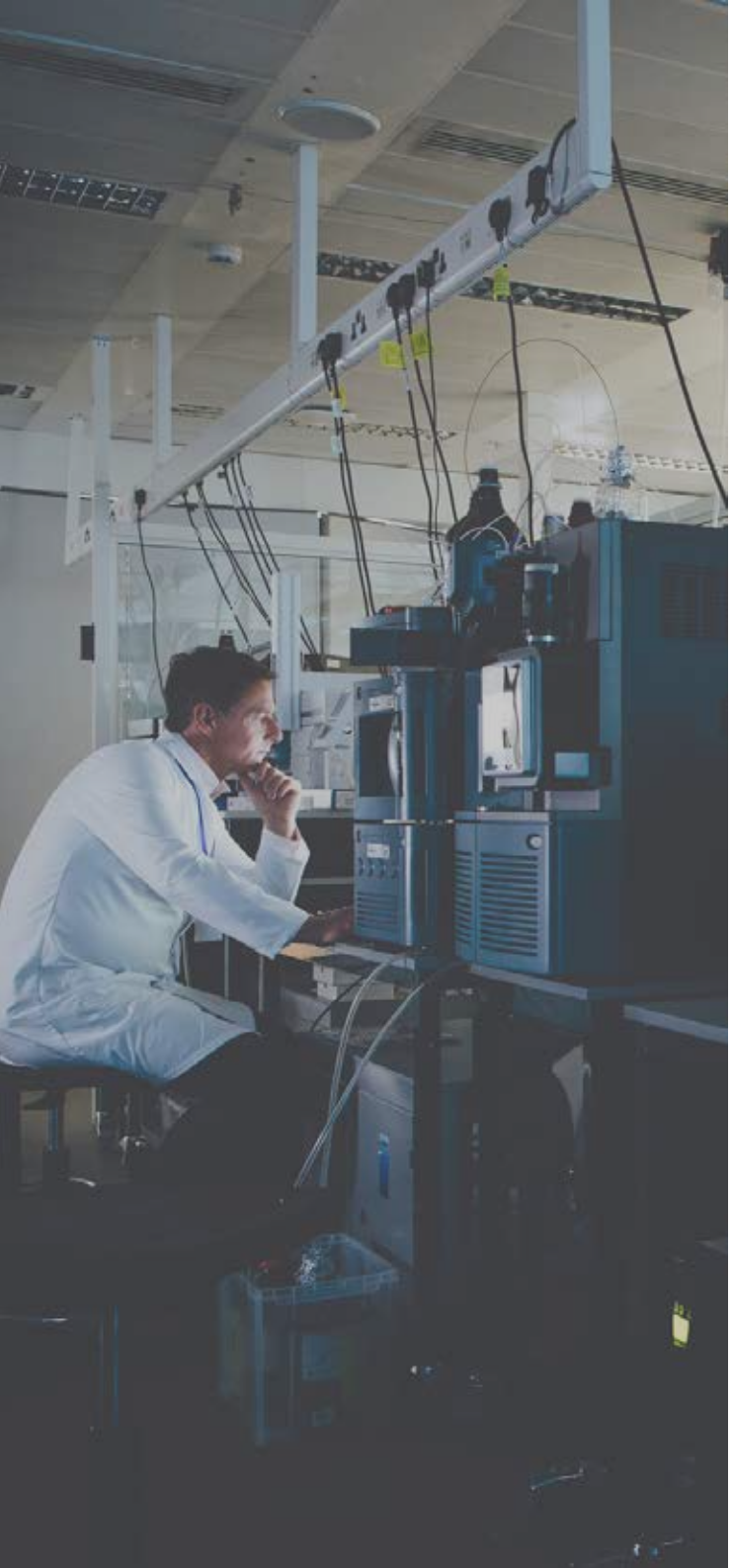
- Si los datos personales accedidos incluyen cualquier identificador, por ejemplo, direcciones de correo electrónico, ID. de cuenta online o IP, será necesario notificarlo a las personas físicas afectadas.
- Si los datos contienen información monetaria - números de cuenta bancaria u otros identificadores financieros - entonces el incidente es “probable que dañe” al individuo y se debe notificar a la DPA.

¿Cómo?: Además, de describir la naturaleza del incidente, la notificación debe mencionar los tipos de datos, el número de individuos y el número de registros expuestos. La empresa debe describir las posibles consecuencias del incumplimiento, así como cualquier esfuerzo de mitigación que se deba realizar.

¿En qué plazo?: La notificación a la DPA debe realizarse dentro de las 72 hora para informar sobre el incidente.

¿Cómo puedes estar preparado para ello?: Debes asegurarte que tienes un procedimiento interno de notificación de incidentes y que dispone de todo lujo de detalles sobre el incidente, sobre todo si se ha producido un acceso a datos personales. Recuerda que debes presentar un dossier de las medidas correctivas que se han llevado a cabo, para ellos necesitarás información de las vías de entrada del atacante, de la situación de los puestos para ser atacados y su estado de vulnerabilidad, los equipos afectados, etc. Esto facilitará la toma de decisiones sobre si es necesario notificar al público y a la DPA.

.



A la luz de los escasos plazos de notificación de A la luz de los escasos plazos de notificación de un incidente, es importante contar con sólidos procedimientos de detección de ataques, investigación forense, alertas en tiempo real e informes detallados a ser analizadas y presentados al público y a la DPA.

Panda Adaptive Defense es el mejor aliado de las empresas en el proceso de adaptación a la GDPR, ofreciendo:

- Protección de los datos personales procesado en los sistemas de la empresa.
- Reducción del riesgo de ser objeto de ataques de seguridad.
- Herramientas para satisfacer la obligatoriedad de notificar los incidentes de seguridad en las primeras 72 horas.
- 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.

7. ¿Tienen las empresas que empezar a aplicar ya las medidas contempladas en el Reglamento?

No. El Reglamento está en vigor, pero no será aplicable hasta el 25 de mayo de 2018.

Sin embargo, puede ser útil para las empresas empezar ya a valorar la implantación de algunas de las medidas previstas:

- 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.

Panda Adaptive Defense vela por la seguridad de la empresa y sus datos y ayuda en la gobernanza de la información. Las empresas que confían en Adaptive Defense tiene ya un camino recorrido en el cumplimiento de la GDPR.

10. Sobre Panda Security

Este informe utiliza los datos recogidos por el equipo multidisciplinar de Panda Security, una red de expertos fundada en 1990 cuya misión es simplificar la complejidad creando nuevas y mejores soluciones para salvaguardar la vida digital de sus usuarios.

Compartimos **el conocimiento de nuestros técnicos de Pandalabs,** el laboratorio que procesa y neutraliza en tiempo real las amenazas contra los usuarios de Panda, desarrolladores especializados en ciberseguridad avanzada y expertos de producto y marketing.

Reiventamos la ciberseguridad y la hacemos extensible a nivel global.

panda

Más información en:

www.pandasecurity.com/intelligence-platform

Contacta:

900 90 70 80

panda

Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

pandasecurity.com

panda