La guía esencial para el cumplimiento del GDPR

Brought to you by

Contents

Introducción

Ha llegado el momento de adoptar la privacidad por diseño

El 25 de mayo de 2018, entra en vigor el Reglamento general de protección de datos de la UE. Sustituirá a todos los reglamentos de protección de datos nacionales de la UE y todo aquel que haga negocios en el mercado único tendrá que cumplir con él. Esto incluye empresas que no sean de la UE pero que traten con clientes de la UE.

Según el GDPR, cualquier vulneración de datos personales se debe notificar en un plazo de 72 horas tras conocerse. Si no se hace, o si se desmiente la negligencia, se pueden imponer multas de hasta 20 millones de euros o el 4 % de la facturación global, lo que sea mayor.

Afortunadamente, las medidas necesarias para proteger los datos de la empresa en su conjunto también servirán para mantener los datos de los clientes seguros. El mismo enfoque de seguridad en terminales de múltiples capas que recomendamos en HP ayudará a garantizar el cumplimiento del GDPR.

En esta guía electrónica examinaremos los componentes clave del GDPR que los profesionales de TI tendrán que conocer, y veremos cómo un programa de seguridad en terminales centrado en los dispositivos puede ayudar con el cumplimiento.

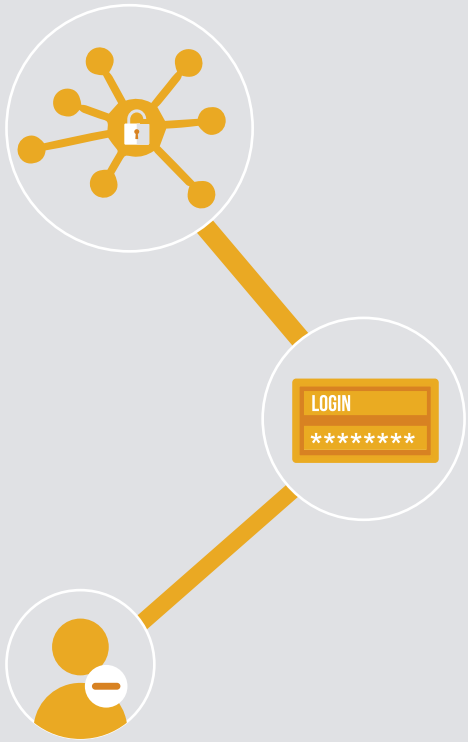
Explicación del GDPR de la UE

Puntos clave para TI

Esencialmente hay dos aspectos en el GDPR: protección de los derechos de los interesados de la UE y protección de la privacidad de los interesados de la UE. Ambos tienen implicaciones tecnológicas.

Para conocer los detalles, lea el texto completo. Sin embargo, para los encargados de las decisiones informáticas, estos son los puntos que tienen que saber:

1. **Las vulneraciones se deben notificar en un plazo de 72 horas**
   Si se produce una vulneración de datos, se debe notificar en un plazo de 72 horas tras conocerse. Las sanciones por no hacerlo son muy elevadas (consulte "¿Cuáles son las sanciones por incumplimiento?")
2. **Derecho al olvido**
   Todos los interesados de la UE tienen el derecho al olvido. Si lo solicitan, se deben borrar sus datos, incluidas todas las copias
3. **Derecho de portabilidad de datos**
   Los residentes de la UE tienen el derecho de controlar sus propios datos. Si lo solicitan, se les debe proporcionar sus datos en un formato accesible, que puedan ser transferidos a un tercero
4. **Transferencias internacionales**
   Solo se pueden transferir los datos personales a otra jurisdicción de datos (es decir, fuera de la UE) con el consentimiento explícito y solo a reguladores considerados "adecuados" o con salvaguardias adicionales implantadas[1]
5. **Privacidad por diseño**
   Las organizaciones deben adoptar un enfoque de privacidad por diseño que integre la seguridad de los datos en los productos, procesos y servicios de forma predeterminada[2,3]



¿A quién se aplica el GDPR?

El GDPR se aplica a cualquier empresa que recopile o procese datos personales de residentes de la UE. Esto incluye organizaciones con sede fuera de la UE que operen en ella.

[1]https://iapp.org/news/a/top-10-operational impacts-of-the-gdpr-part-4-cross-border-data-transfers/ [2]Allen & Overy – The EU General Data Protection Regulation 2016
[3]http://www.computerweekly.com/news/450296306/10-key-facts-businesses-need-to-note-about-the-GDPR

Explicación del GDPR de la UE

¿Qué se considera “datos personales”?

Según el GDPR, los “datos personales” son “cualquier dato que se pueda utilizar para identificar a un individuo”.

Esto incluye información genética, mental, cultural, económica o social, junto con la información tradicionalmente considerada de identificación.

Esto puede incluir a organizaciones que anteriormente se encontraban fuera del alcance de la legislación referente a la protección de datos, bajo la competencia del GDPR.

¿Cuáles son las sanciones por incumplimiento?

La multa máxima es de 20 millones de euros o el 4 % de la facturación global, lo que sea mayor. Esto se aplica a las infracciones más graves según la normativa, como no notificar una vulneración en la seguridad en un plazo de 72 horas tras conocerse.

Las infracciones menos graves conllevan un máximo de 10 millones de euros o el 2 % de la facturación global. No hace falta decir que los costes del incumplimiento son considerables.

Lista de comprobación del procedimiento del GDPR

Dentro de su marco de administración de datos, necesitará procedimientos explícitos para:

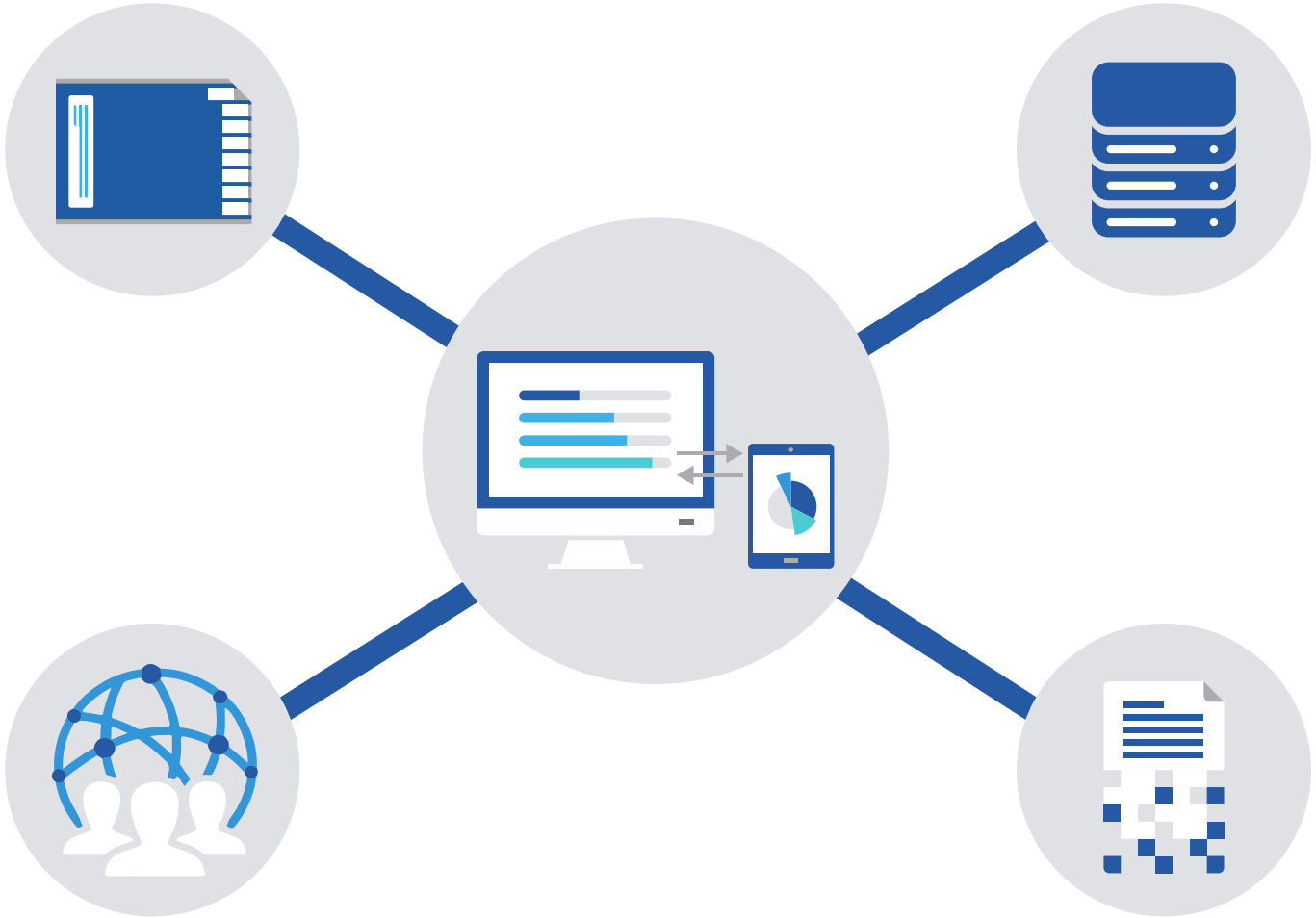
- Informar a los interesados de cómo se recopilarán, almacenarán y procesarán sus datos
- Obtener el consentimiento explícito de los interesados para hacerlo
- Proporcionar la información de los interesados en un formato accesible para ellos
- Borrar todos los datos personales de un interesado, incluidas las copias
- Transferir datos a otro controlador o procesador de datos
- Transferir datos fuera de la UE, incluso dentro de la organización

Desafíos tecnológicos para el cumplimiento

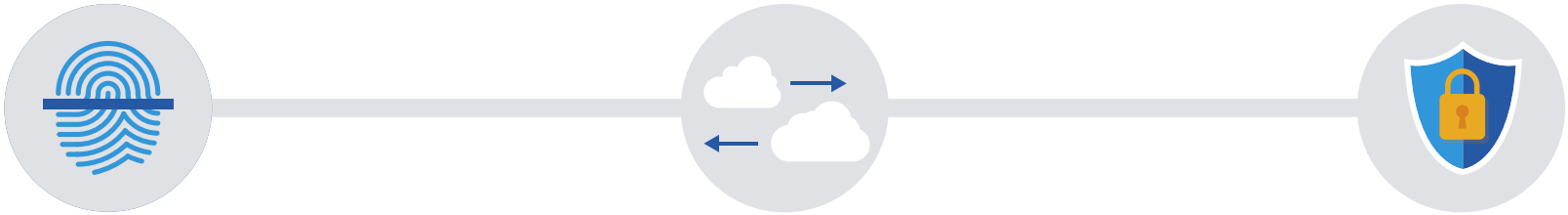
Los mayores desafíos del GDPR son técnicos.

Permitir la portabilidad segura de los datos, la protección de estos y el derecho al olvido con el que cuentan los individuos requiere de un mapa global de localización de datos así como accesibilidad desde distintos dispositivos.

A medida que aumenta la amenaza de los delitos cibernéticos, el mantenimiento de la seguridad absoluta es un desafío creciente.



Desafíos tecnológicos para el cumplimiento



Seguimiento de los dispositivos

El cumplimiento de la portabilidad de datos y el derecho al olvido requieren una cuenta detallada de todos los datos personales de los que dispone la organización.

Tiene que conocer:

- Cada dispositivo que contiene datos personales
- Cada dispositivo que tiene acceso a datos personales

Esta es la única forma de garantizar que pueda recuperar o borrar datos personales que tenga la empresa.

Seguimiento de la nube

La empresa media europea utiliza 608 aplicaciones, una cifra aproximada ya que no se informa del 90 % de ellas. Los empleados a menudo utilizan aplicaciones de nube comerciales sin el conocimiento del departamento de TI.[4]

Para el cumplimiento del GDPR, el uso de la nube se debe reducir a servicios que estén:

- En la UE y, por lo tanto, conformes al GDPR
- Bajo la jurisdicción de un regulador de protección de datos considerado “adecuado” por la UE

Todo lo demás puede infringir la norma de transferencia internacional. Y tiene que saber qué servicios de nube utilizan los empleados, en caso de invocarse el derecho al olvido.

Defensa de los datos

La amenaza de delitos cibernéticos está aumentando, sobre todo debido a que el uso de redes y dispositivos personales no seguros también está creciendo.

Es prácticamente imposible evitar las vulneraciones de seguridad, y la UE lo sabe. Para evitar una costosa multa, debe:

- Implantar una herramienta de control de eventos de incidentes de sistemas (Systems Incident Event Monitoring, SIEM) para notificar una infracción en un plazo de 72 horas
- Implantar seguridad de terminales de múltiples capas para demostrar la debida diligencia en cuanto a la prevención de una infracción

También se debe concienciar a los usuarios de sus responsabilidades por utilizar dispositivos y redes no autorizadas.

[4]https://www.cloudindustryforum.org/content/cloud-and-eu-gdpr-six-steps-compliance

La amenaza del delito cibernético

El delito cibernético es real y representa una amenaza creciente

El 82 %

de las empresas han sufrido alguna amenaza/ vulneración en los últimos 12 meses[5]

El 80 %

de los profesionales de TI piensa que la amenaza del delito cibernético aumentará en los próximos tres años[6]

El 78 %

de las empresas ha informado de un aumento en los ataques de malware en los últimos cinco años[7]

El 60 %

de los líderes de TI creen que la delincuencia cibernética está superando las defensas[8]

El 81 %

de las empresas clasifica la negligencia interna como la mayor amenaza para la ciberseguridad[9]

El 81 %

de los líderes de TI afirma que los dispositivos móviles de sus redes han sido objetivo de ataques de malware[9]

El 72 %

corrobora que el uso por parte de los empleados de software de nube comercial es un riesgo[9]

El 69 %

afirma que BYOD es un riesgo de seguridad

[5]HPI Printer Security Research 2016 (Spiceworks) [6]HP Printer Security Report 2015 [7] Ponemon 2016 State of the Endpoint Report [8]IBM CISO Assessment 2014 [9]Ponemon 2016 State of the Endpoint Report

Implementación de seguridad de terminales

Enfoque de múltiples capas de HP sobre la seguridad de terminales

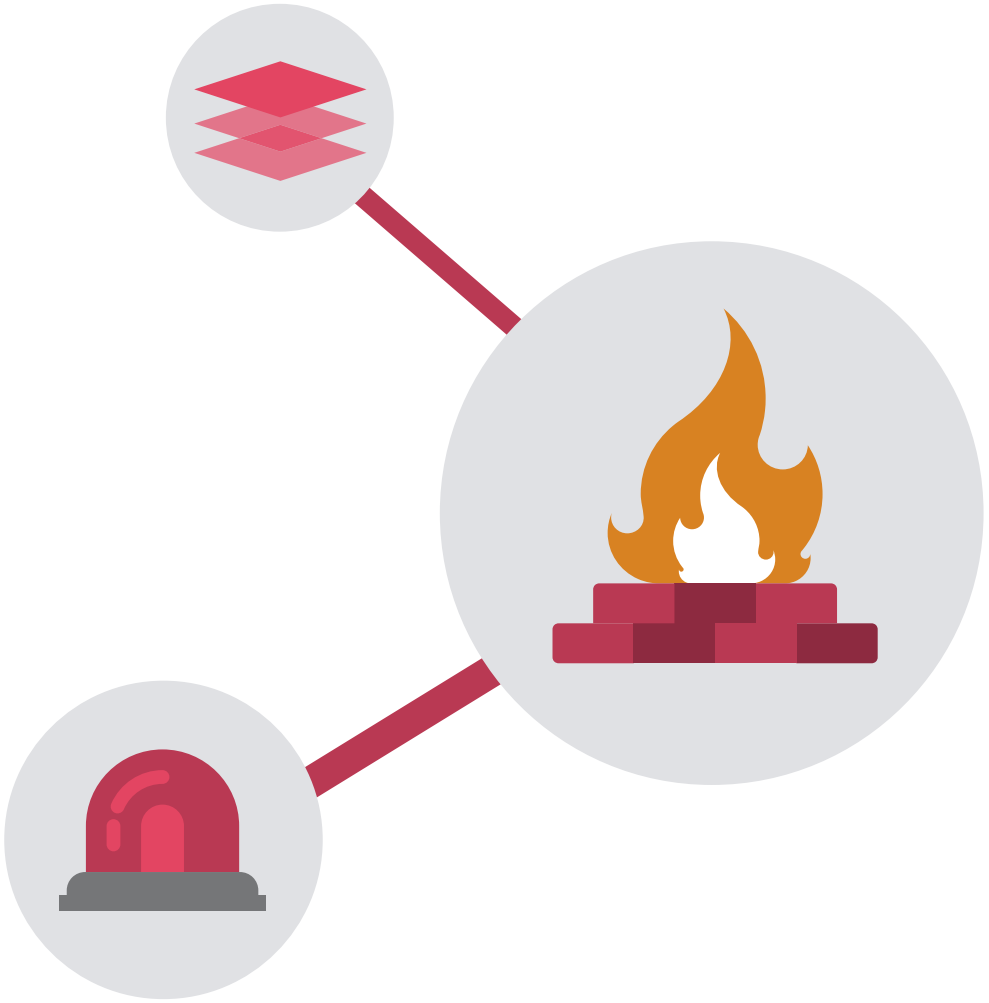
El enfoque de prevención y protección para la ciberseguridad (cortafuegos y antivirus) no basta. Nunca ha bastado. En un estudio de Damballa, el software antivirus tardó seis meses en identificar y eliminar el 100 % de los archivos maliciosos que se le lanzaron.[10]

La opinión de HP es que la ciberseguridad debe ser de múltiples capas, que opere a nivel de red, de dispositivo y de usuario, con varias defensas en cada uno. La detección y la respuesta deben favorecerse sobre la protección y la defensa. Las terminales son el punto de partida, tanto del dispositivo como del usuario.

Controles de seguridad críticos (CSC)

El Centro para la Seguridad de Internet (Center for Internet Security, CIS) ha definido 20 controles de seguridad críticos (Critical Security Controls, CSC) reconocidos internacionalmente, desarrollados, ajustados y validados por relevantes expertos en seguridad de TI de todo el mundo. Se contemplan como importantes acciones de mantenimiento cibernéticos para todas las organizaciones.

Hemos hecho referencia a los CSC clave para el cumplimiento del GDPR ya que son instrucciones útiles, el texto completo está disponible en línea. Descárguelo gratuitamente en la biblioteca de CIS.



[10]https://www.damballa.com/time-to-fix-malware-strategies-2/

Seguridad en la red

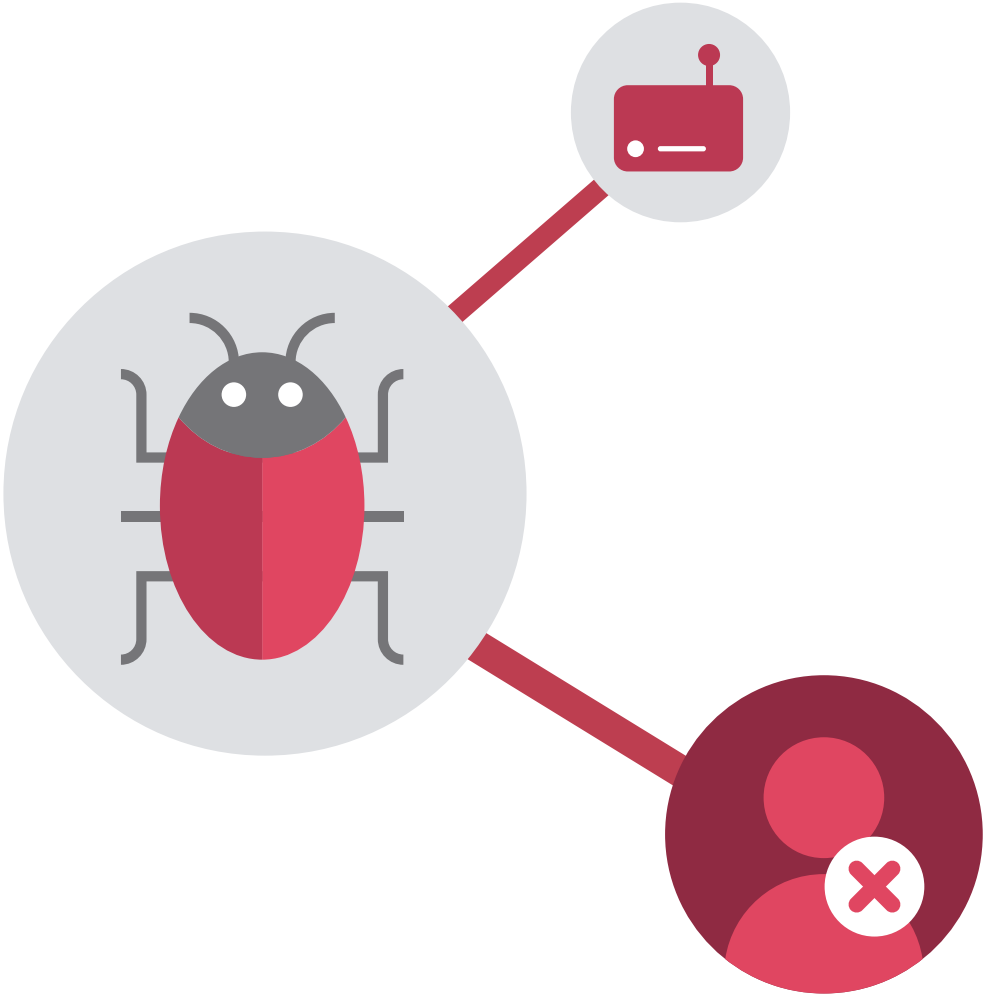
Los accesos ilegales importantes tienden a explotar un único punto de entrada para obtener acceso a toda la red. Por lo tanto, la seguridad a nivel de red se debe basar en evitar eso.

- **Privilegios administrativos de control (CSC 5)**
  Restringir la capacidad para cambiar los ajustes de la red y las contraseñas al número mínimo de personas posible
- **Controlar el acceso según la necesidad de saber (CSC 14)**
  Clasificar el acceso a información confidencial según el usuario, dispositivo y ubicación. Sopesar el riesgo de seguridad con respecto a la confidencialidad de los datos
- **Limitación y control de puertos, protocolos y servicios de red (CSC 9)**
  Desactivar cualquier punto de acceso innecesario, virtual o físico, incluidos FTP, Telnet y servicios de impresión
- **Mantenimiento, vigilancia y análisis de registros de auditoría (CSC 6)**
  Revisar periódicamente los registros de auditoría para analizar el comportamiento del sistema y detectar cualquier actividad sospechosa
- **Evaluación continua de la vulnerabilidad y resolución (CSC 4)**
  Evaluar continuamente el entorno en busca de vulnerabilidades y emprender acciones según los resultados, minimizando la oportunidad de infracciones

El objetivo es una red subdividida según la confidencialidad de la información. Se evalúan los riesgos de seguridad de las solicitudes de acceso, y se bloquea el acceso de los dispositivos, usuarios y solicitudes no reconocidos de redes no seguras a la información más confidencial. La política BeyondCorp de Google es un buen modelo.[11]

[11] https://research.google.com/pubs/pub43231.html

Seguridad en la red



Cada dispositivo es una vulnerabilidad potencial, tanto a nivel de empresa como personal. Tiene que conocer cada teléfono, tablet, ordenador portátil y ordenador de sobremesa que tenga acceso a los datos de la empresa.

- **Inventario de dispositivos autorizados y no autorizados (CSC 1)**
  Auditar cada dispositivo que tenga acceso a datos
- **Inventario de software autorizado y no autorizado (CSC 2)**
  Auditar cada aplicación utilizada en la red, para acceder o no directamente a datos
- **Defensas antimalware (CSC 8)**
  Asegurarse de que todos los dispositivos tienen un antivirus y antimalware actualizados. Asegurarse de que se realizan exploraciones y actualizaciones periódicas

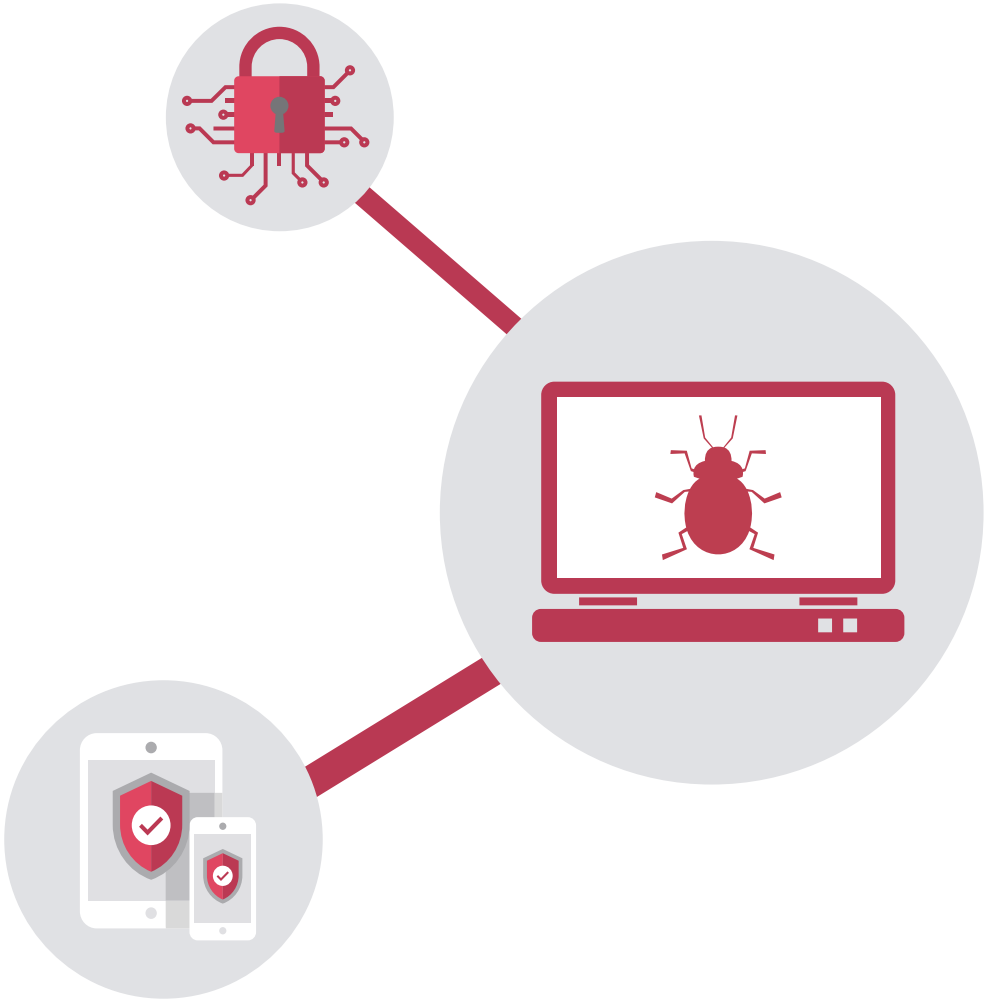
Device Security

Además, los departamentos de TI deben plantearse las siguientes comprobaciones adicionales:

- **Autenticación por multifactor**
  Garantizar que todos los dispositivos de trabajo son seguros. Utilizar idealmente la autenticación biométrica junto con contraseñas (consulte la página 14: “Dispositivos de privacidad por diseño”)
- **Acceso remoto**
  Garantizar el acceso de dispositivos remotos para recuperar y borrar datos personales, realizar procesos de cuarentena y rescisión, y apagar y bloquear el dispositivo en caso de pérdida o robo (consulte la página 14: “Detección y respuesta”)
- **Informar a todos los empleados de los protocolos y procedimientos de seguridad**
  Asegurarse de que todos los empleados son conscientes y conocen sus responsabilidades con respecto a la ciberseguridad, como el alertar de actividad sospechosa
- **Realizar una formación sobre ciberseguridad activa**
  Organizar talleres, seminarios, simulacros de phishing: asegúrese de que todos saben cómo evitar errores básicos y cómo seguir siendo conformes al GDPR
- **Minimizar el uso de dispositivos/aplicaciones personales**
  Disuadir del uso de dispositivos y aplicaciones personales para fines profesionales. Una política CYOD integral y flexible debería ayudar

La implementación de un marco de seguridad como este debería ayudarle a mantener el control de los dispositivos de la empresa para proteger los datos y facilitar la ejecución de la portabilidad de datos y el derecho al olvido.

Para obtener más información sobre el enfoque de HP sobre la seguridad de múltiples capas, lea nuestro Informe blanco, La seguridad comienza en los terminales.



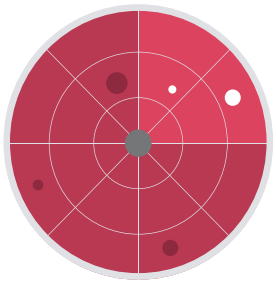
Por qué todos los empleados deben ser conscientes de las amenazas cibernéticas

El 58 % de las amenazas cibernéticas proceden de los empleados, exempleados y socios fiables. Proteger cada uno de los dispositivos significa proteger también a sus usuarios.

- El Comité Nacional Demócrata (DNC) de EE. UU. sufrió un ataque de piratas informáticos en 2016 cuando John Podesta hizo clic en un enlace de phishing considerado seguro por error por un asistente[13]
- Las fotos de famosas desnudas inundaron Internet en 2014 después de que Ryan Collins, de 36 años, obtuviera acceso al iCloud de Jennifer Lawrence y otras mujeres con correos electrónicos de phishing básicos que se hicieron pasar por Apple[14]
- Se filtraron 68 millones de contraseñas de Dropbox en 2012 gracias a un empleado que utilizaba la misma contraseña para sistema internos que para su LinkedIn[15]
- El presidente Donald Trump sigue utilizando un teléfono Samsung Galaxy estándar. Los expertos no se preguntan si ya ha sido hackeado, sino cuántas agencias de inteligencia extranjeras ya han sufrido estos ataques[16]

[12]http://www.clearswift.com/sites/default/files/images/blog/enemy-within.pdf [13]https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds [14]http://www.forbes.com/sites/thomasbrewster/2016/03/16/icloud-hacking-jennifer-lawrence-fappening-apple-nude-photo-leaks/#45fed5d77b88 [15]https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach [16]https://www.theguardian.com/commentisfree/2017/feb/19/if-trump-hates-leaks-needs-to-give-up-phone

Detección y respuesta

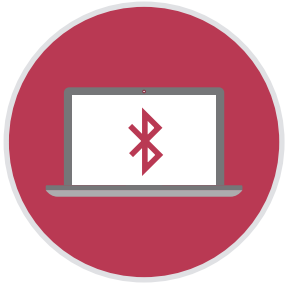


La detección y la respuesta son un marco de ciberseguridad que reconoce que la prevención total es casi imposible.

Lo que importa es conocer la infracción (detectar) y realizar una acción inmediata (respuesta).

Hay productos de software disponibles que convierten cada dispositivo en un sensor en tiempo real, y que permiten al administrador responder, por ejemplo, apagando los dispositivos, poniendo en cuarentena archivos y borrando datos.

Dispositivos de privacidad por diseño



Los dispositivos de HP personifican la privacidad por diseño.

Las funciones de seguridad incluyen la primera BIOS autorreparadora del mundo, cierre automático de Bluetooth (que bloquea el dispositivo cuando está lejos) y pantallas de privacidad integradas.

Estas funciones no garantizarán el cumplimiento del GDPR por sí solas, pero sin duda ayudarán.

Preparación para el GDPR

Pasos prácticos que realizar ahora

El GDPR entra en vigor el 25 de mayo de 2018. Aún queda tiempo para prepararse, pero hay que ser consciente de que hay mucho por hacer.

El primer paso es **auditar la situación actual de sus datos**. Evalúe dónde están almacenados, dónde se copian y quién tiene acceso a ellos. Si utiliza cualquier solución de nube, averigüe dónde tienen la sede sus servicios y si serán conformes al GDPR. Lo mismo para cualquier SaaS u otras organizaciones aliadas con las que trabaja y comparte sus datos. Esto le dará una idea clara de cuánto tiene que cambiar para cumplir con la reglamentación

Diseñe su política de datos. Incluya procedimientos y protocolos detallados sobre dónde se almacenan los datos, quién tiene acceso y la realización de copias fuera de la empresa, o a través de las fronteras en una multinacional. Incluya procedimientos para recuperar y borrar datos personales. Comunique esto a todo el personal de la empresa. Realice sesiones de formación. Resalte su importancia.

Diseñe su política de seguridad. Cree un nuevo marco de ciberseguridad que funcione según la base de detección y respuesta a terminales. Revise su política de dispositivos e invierta en nuevas tecnologías si es necesario. Invierta en nuevas tecnologías si es necesario. Solo el 36 % de los directores de TI creen que tienen presupuesto suficiente para la seguridad de terminales.[17] Las sanciones del GDPR pueden suponer finalmente el punto de inflexión para que los mandos superiores se interesen.

[17]Ponemon 2016 State of the Endpoint Report

Preparación para el GDPR

GDPR checklist

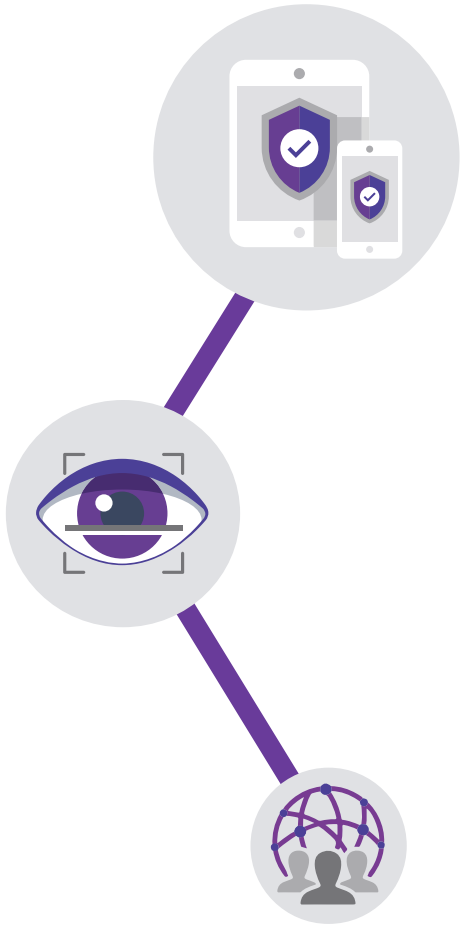
5 pasos clave hacia el cumplimiento del GDPR

1. Nombrar a alguien para que se ocupe de los datos, un oficial de protección de datos (DPO) si es necesario
2. Realizar una auditoría de datos completa, incluida la idoneidad de proveedores de nube y SaaS con referencia al GDPR
3. Crear un nuevo marco de gobierno de los datos que incluya procedimientos para portabilidad de datos y derecho al olvido
4. Crear un nuevo marco de ciberseguridad, implementando la seguridad de terminales de múltiples capas
5. Comunicar las políticas y protocolos a todo el personal de la empresa

Device Security Checklist

6 pasos clave para proteger los terminales

1. Auditar todos los dispositivos autorizados y no autorizados con acceso a datos personales
2. Invertir en dispositivos nuevos y más seguros, si fuera necesario
3. Implementar el acceso remoto y los derechos de cancelación de los datos de la empresa en los dispositivos
4. Implementar un análisis regular y una política de actualización del software de seguridad
5. Implementar software de detección y respuesta en tiempo real
6. Formar a los empleados en ciberseguridad



Calendario de seguridad de terminales

Cronología básica para la implementación de la seguridad de terminales por el GDPR

2017

Mayo

Nombrar a un director de proyectos a cargo de la implementación de la seguridad de terminales

Junio

Realizar una auditoría de las políticas de seguridad, prácticas y dispositivos actuales

Julio

Considerar los requisitos de dispositivos y la política para la seguridad de terminales (CYOD/BYOD, etc.)

Agosto

Considerar soluciones de software para detectar y responder a la seguridad

Septiembre

Diseñar un sistema de acceso por niveles de múltiples capas para los datos de la empresa

Octubre

Diseñar una nube pública/privada para permitir el acceso adecuado a los datos en instalaciones externas

Noviembre

Diseñar un programa de formación de usuarios, que incluya simulacros de phishing habituales

Diciembre

Comunicar las nuevas políticas de seguridad al resto de la empresa

2018

Enero

Implementar una nueva arquitectura de datos en la nube pública/privada

Febrero

Implementar una nueva política de dispositivos

Marzo

Implementar la solución de software de detección y respuesta

Abril

Realizar una formación de seguridad de usuarios, que incluya políticas relacionadas con el GDPR

Mayo

El GDPR entra en vigor

Resumen

El GDPR no está muy lejos

Si tiene suerte, su organización ya estará poniendo en práctica mucho de lo que se incluye en las normativas: en gran parte, estas encapsulan simplemente lo que constituyen las mejores prácticas.

Y, si opera en varios países de la UE, puede que ya se haya encontrado con varias de las medidas más severas incluidas.

Las medidas de seguridad que recomendamos implementar para cumplir con el GDPR ayudan a prevenir cualquier infracción, las cuales podrían ser terriblemente costosas para una organización. En el último recuento, el gobierno del Reino Unido calcula que las empresas británicas perdieron 21 mil millones de libras en un solo año, una cifra que se espera que crezca.[18]

Además, muchas de las medidas requeridas para una seguridad realmente sólida también ayudarán a cumplir con otros aspectos del GDPR. Restringir el acceso a los datos a usuarios, dispositivos y redes concretos no solo minimiza el riesgo de los datos, sino que facilita el seguimiento de los datos personales y, por lo tanto, el cumplimiento con la portabilidad de datos y el derecho al olvido, por no mencionar las transferencias internacionales.

Esta guía electrónica es solo el principio. La seguridad siempre ha sido una prioridad en HP. La privacidad por diseño ha sido nuestra política durante años. Ahora que es necesaria, más que deseada, estamos bien posicionados para ayudarle a adoptar el mismo enfoque.

Para averiguar más sobre cómo HP y nuestros productos pueden ayudarle a cumplir con el GDPR, visite **nuestra página "Privacidad por diseño".**

[18]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the cost-of-cyber-crime-full-report.pdf