Kensington The Professionals' Choice™

Por qué una Política de Seguridad Física es integral para **el Cumplimiento del GDPR**

Aviso legal: *Nada de lo aquí contenido debe ser interpretado como consejo legal. Las organizaciones deben consultar a un asesor jurídico con respecto al cumplimiento del Reglamento General de Protección de Datos o cualquier otra ley o normativa.*

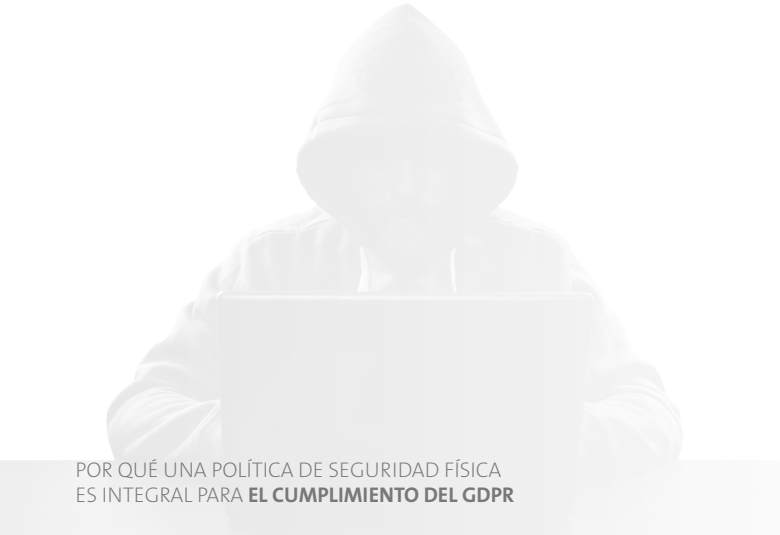
DATOS PROTEGIDOS

Índice

POR QUÉ UNA POLÍTICA DE SEGURIDAD FÍSICA
ES INTEGRAL PARA **EL CUMPLIMIENTO DEL GDPR**

Acerca de **este documento**

Este documento aporta una visión general de lo que pretende lograr el ***GDPR y los problemas que puede representar para las organizaciones****.*



POR QUÉ UNA POLÍTICA DE SEGURIDAD FÍSICA ES INTEGRAL PARA **EL CUMPLIMIENTO DEL GDPR**

El objetivo de este documento es presentar una introducción al Reglamento General de Protección de Datos (GDPR) de la UE y cómo afectará a las diferentes empresas, para que puedan desarrollar un marco para una política de seguridad del hardware para su propia empresa, antes de que el reglamento entre en vigor en mayo de 2018.

Pero, ¿qué es el GDPR? Requiere que las organizaciones apliquen buenas prácticas de seguridad a los datos electrónicos y en papel y, en caso de violación de los datos, notifiquen a las personas afectadas o potencialmente afectadas. El alcance del GDPR se extiende globalmente a todas las organizaciones que controlan o procesan datos de identificación personal sobre personas en la UE, independientemente de la presencia geográfica de dichas organizaciones. Los requisitos del GDPR se aplican tanto a los datos personales electrónicos como en papel e implican que todas las organizaciones deben cumplir los requisitos del GDPR si manejan datos de identificación personal originados en la UE.

Proteger los datos contra la piratería informática y el malware es prioritario para muchas organizaciones, aunque muchas de ellas no abordan adecuadamente la seguridad física del hardware informático. Más de la mitad no logra aplicar un bloqueo físico a los equipos informáticos[1]. Esto pone a las organizaciones en riesgo de incumplimiento del GDPR y a los propietarios de los datos en riesgo de fraude y robo de identidad. Teniendo esto en cuenta, Kensington anima a las organizaciones a revisar sus políticas y prácticas de seguridad relacionadas con los datos electrónicos.

Visión general

Si bien el principal objetivo del GDPR es reforzar los derechos de privacidad online, la seguridad del hardware físico tiene un importante papel que desempeñar.

El GDPR se centra en abordar los retos cada vez mayores que se plantean a la protección de datos y la privacidad, la exposición a las violaciones de la seguridad, la piratería informática y otros procesamientos ilegales.

*Estos puntos **identifican las áreas específicas dentro del GDPR** que son nuevos derechos o potenciados para las personas.*

POR QUÉ UNA POLÍTICA DE SEGURIDAD FÍSICA
ES INTEGRAL PARA **EL CUMPLIMIENTO DEL GDPR**

1

La portabilidad de los datos y el derecho a ser olvidados

- Las personas tienen ahora el derecho a transferir sus datos personales de una organización a otra.
- Los datos personales deben ser facilitados en un formato estructurado y legible mecánicamente.
- Una persona puede solicitar la eliminación o borrado de los datos personales.

2

Inventario

- Las autoridades locales ya no tendrán que ser informadas de que se están procesando esos datos personales.
- Las organizaciones deben mantener un registro de las actividades de procesamiento bajo su responsabilidad.

3

Seguridad y evaluaciones del impacto de la protección de datos (DPIA)

- Las DPIA son un medio para identificar los elevados riesgos para los derechos de privacidad de las personas.
- Los requisitos y las recomendaciones de seguridad deberían basarse en una evaluación de riesgos.

4

Notificación de violación de datos

- Cualquier violación debe notificarse a la autoridad supervisora.
- Las personas afectadas por la violación también deben ser informadas.

5

Gobernanza y responsabilidad de los datos

- Las organizaciones deben poder demostrar el cumplimiento del GDPR.

¿A quién se **le aplica?**

Cualquier organización que mantenga datos sobre ciudadanos de la UE (independientemente de que tengan su sede fuera de la UE) está sujeta al GDPR y afecta a todos los que se ocupan de esa información.

El GDPR se aplica a las organizaciones dentro de la UE así como a las organizaciones fuera de la UE que procesan o controlan datos relativos a residentes o nacionales que viven en la UE.

El GDPR afecta principalmente a:

Controladores de datos - dicen cómo y por qué se procesan datos personales

Procesadores de datos - personas que actúan en nombre de los controladores

Es responsabilidad de estas dos figuras garantizar que sus clientes cumplan plenamente con todos los aspectos del GDPR, para evitar incurrir en multas.

El cumplimiento efectivo y demostrable del GDPR debe involucrar a todos los miembros de una organización que se ocupen de información personal y sensible. Por ejemplo, el portátil de un comercial contendrá información sensible sobre sus clientes y deberá estar físicamente protegido cuando trabaje a distancia.

Es posible que un Procesador de datos o un Controlador de datos necesite **designar a un Responsable de protección de datos** y mantener registros de todas las actividades de procesamiento que realizan en nombre de los clientes.

El GDPR cubre los **datos personales** y **datos personales sensibles** en formato físico y electrónico

POR QUÉ UNA POLÍTICA DE SEGURIDAD FÍSICA ES INTEGRAL PARA **EL CUMPLIMIENTO DEL GDPR**

Es importante considerar en qué tipo de datos se aplicará el GDPR antes de elaborar una política de cumplimiento para su organización.

Los datos dentro del alcance del GDPR incluyen cualquier información acerca de una persona identificable y se dividen en dos categorías:

Datos personales incluyen datos como la dirección de correo electrónico o física, así como cualquier información que pueda utilizarse como identificador online, por ej. una dirección IP.

Datos personales sensibles abarcan cualquier información privada entre la que se incluyen datos de origen étnico, opiniones políticas, religión y salud. En general, las organizaciones requieren fundamentos más sólidos para procesar esta información que los datos personales 'normales'.

El GDPR tiene que ver con datos personales gestionados por las organizaciones tanto en **formato electrónico como físico.**

Un marco empresarial para el **Cumplimiento del GDPR**

Mediante el examen de las personas, los procesos y la tecnología, las organizaciones podrán construir marcos claros de una política de seguridad de los datos, lo que contribuirá a apoyar el cumplimiento en todas las áreas del GDPR.

POR QUÉ UNA POLÍTICA DE SEGURIDAD FÍSICA ES INTEGRAL PARA **EL CUMPLIMIENTO DEL GDPR**

Las organizaciones tienen tres áreas principales que deben ser examinadas con el fin de lograr el cumplimiento del GDPR:

Personal - la responsabilidad del personal de cualquier dato procesado por el mismo dentro de la organización es crítica. Una organización debe establecer normas claras para cada uno de los empleados para la adecuada gestión de todos los datos electrónicos mantenidos dentro de la empresa. Este reglamento pone en práctica los requisitos del GDPR con respecto a la gestión de todos los datos. Por ejemplo, quizás usted desee introducir normas claras acerca del uso de los datos sensibles albergados en los portátiles de los empleados y el proceso para borrar datos.

Procesos - esto está relacionado con los procesos dentro de la organización. Por ejemplo, para gestionar el uso de datos como el tratamiento o el almacenamiento de datos sobre los clientes. Es crucial que las empresas revisen todos sus procesos actuales relacionados con los datos. Una vez que se hayan identificado las lagunas y debilidades dentro de los procedimientos existentes, la empresa debe elaborar un plan marco en el que se verán reforzadas o sustituidas estas áreas, donde sea necesario, para cumplir con el GDPR.

Tecnología - las capacidades y requisitos actuales informáticos deben revisarse y ajustarse en consecuencia antes de mayo de 2018. Corresponde a cada empresa garantizar que cualquier sistema existente que no cumpla plenamente el reglamento sea mejorado o sustituido, para evitar incurrir en potenciales multas tras la entrada en vigor del GDPR.

¿Por qué **importa** la seguridad física?

Si bien las amenazas online y basadas en software ocupan un lugar prioritario en la agenda de una organización, sería un error suponer que los ***riesgos de la seguridad física*** *han desaparecido.*

Una vez debatido lo que el GDPR exige a las empresas, ahora es pertinente abordar el problema de la seguridad física del hardware dentro de las organizaciones y por qué es una preocupación clave para las empresas mientras se preparan para cumplir los requisitos del GDPR.

Después de las amenazas online y la divulgación no intencionada de datos, los **dispositivos portátiles** y **la pérdida física** son las mayores fuentes de violación de datos[2]:

Cada día, una media de más de **5 millones de registros de datos se pierden o se roban**[3], donde más de un **tercio de las empresas no tienen una política de seguridad física implementada** para proteger los portátiles, los dispositivos móviles y otros activos electrónicos.[4]

Dado el nivel de potenciales multas que señala el GDPR, las plantillas cada vez más móviles y el crecimiento del *hot desking*, la seguridad física de portátiles y dispositivos móviles es una precaución razonable, tanto dentro como fuera del lugar de trabajo. Bloquear un dispositivo es una forma rápida y sencilla de evitar el robo y también muy eficaz.

Kensington ofrece una gama completa de **soluciones de bloqueo** para una gran variedad de portátiles, incluidos dispositivos sin ranura de seguridad. La gama de maletines SecureTrek™ se puede anclar físicamente a entornos de objetos fijos como aeropuertos, hoteles y ferias comerciales.

POR QUÉ UNA POLÍTICA DE SEGURIDAD FÍSICA ES INTEGRAL PARA **EL CUMPLIMIENTO DEL GDPR**

La seguridad física sigue siendo la causa de **muchas violaciones comunes de la seguridad**

POR QUÉ UNA POLÍTICA DE SEGURIDAD FÍSICA ES INTEGRAL PARA **EL CUMPLIMIENTO DEL GDPR**

De los 697 incidentes de seguridad relacionados con datos registrados entre abril y junio de 2017 por el regulador de protección de datos del Reino Unido (Oficina del Comisionado de Información o ICO), el 6 % se debieron al robo de un dispositivo no cifrado, habiendo dejado los datos en un lugar no seguro y el robo de la única copia de datos cifrados representa un 3,5 % adicional.[5]

En el **sector financiero**, el 25 % de las violaciones se deben a dispositivos perdidos o robados y son la causa más frecuente de filtración de datos, ya que son objetivos especialmente tentadores debido al volumen de datos confidenciales almacenados y utilizados.[6]

En el sector de la **asistencia sanitaria**, el robo o pérdida física es la mayor causa de incidentes de seguridad, ya que representa el 32 % de los más de 100 000 incidentes estudiados en 82 países.[7]

Las capacidades y requisitos actuales en materia informática también deberían revisarse y ajustarse en consecuencia antes de mayo de 2018. Corresponde a cada empresa garantizar que cualquier sistema existente que no cumpla plenamente el reglamento sea mejorado o sustituido, para evitar incurrir en potenciales multas tras la entrada en vigor del GDPR.

La cooperación de los usuarios es fundamental para el Cumplimiento del GDPR

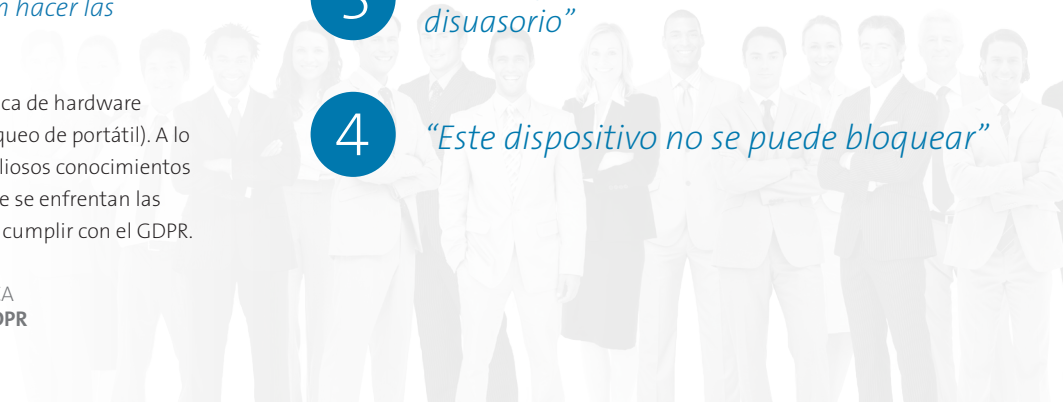
Si podemos concluir que la seguridad física sigue siendo esencial para la seguridad de la información, entonces la pregunta es: ¿qué pueden hacer las organizaciones al respecto?

Kensington es líder mundial en seguridad física de hardware informático, y el creador del Laptop Lock (bloqueo de portátil). A lo largo de 35 años, Kensington ha adquirido valiosos conocimientos sobre las necesidades, deseos y retos a los que se enfrentan las organizaciones que buscan autoprotegerse y cumplir con el GDPR.

POR QUÉ UNA POLÍTICA DE SEGURIDAD FÍSICA ES INTEGRAL PARA **EL CUMPLIMIENTO DEL GDPR**

Estas percepciones nos han llevado a creer que hay cuatro principales objeciones y barreras en la seguridad física efectiva en las organizaciones:

1. *"Operamos en un entorno seguro"*
2. *"Usamos el cifrado y el almacenamiento en la nube"*
3. *"Los bloqueos son solo un elemento disuasorio"*
4. *"Este dispositivo no se puede bloquear"*



Superando barreras para el Cumplimiento del GDPR

POR QUÉ UNA POLÍTICA DE SEGURIDAD FÍSICA
ES INTEGRAL PARA **EL CUMPLIMIENTO DEL GDPR**

"Operamos en un entorno seguro"

Los CCTV, los pases de empleados y el personal de seguridad pueden crear una mayor sensación de seguridad y un menor riesgo percibido. El 58 % de los portátiles se roban en las oficinas y los directores de TI sospechan que el 85 % son robos internos.[8] Los datos están en riesgo en cuanto desaparece un portátil, especialmente porque solo se recupera el 3 % de ellos[9]. Los bloqueos de portátil evitan el robo oportunista y la inversión en tiempo y costes asociados al seguimiento del infractor y la sustitución del portátil, por no hablar de las sanciones potenciales en virtud del GDPR.

"Usamos el cifrado y el almacenamiento en la nube"

El cifrado no es una solución cuando nos enfrentamos a un dispositivo robado que contiene datos que no se han guardado en copias de seguridad. Incluso aunque los usuarios no guarden los datos en sus discos duros, vale la pena protegerse frente a la pérdida de productividad experimentada por un empleado sin su dispositivo informático primario. Dé un paseo por su edificio. ¿Hasta qué punto sería fácil para un mensajero robar un dispositivo? El 49 % de las Pymes tardan entre 2 y 4 días en sustituir un portátil robado o perdido.[8]

"Los bloqueos son solo un elemento disuasorio"

Los bloqueos de portátiles están diseñados principalmente para proteger contra el robo oportunista. Pero también son muy eficaces para prevenir el robo en sí mismo. IDC informó que, de los directores de TI que han sufrido el robo de un portátil, el 52 % informó que los robos se habrían podido prevenir mediante un bloqueo.[8]

Superando barreras para el Cumplimiento del GDPR

"Este dispositivo no se puede bloquear"

Con el paso a factores de forma más finos, es posible que los dispositivos informáticos actuales no incorporen la Kensington Security Slot™ estándar del sector. Sin embargo, es un error creer que esos dispositivos no se pueden proteger físicamente. Incluso los dispositivos sin una ranura de seguridad se pueden bloquear para prevenir el robo oportunista. Kensington ofrece una gama completa de soluciones para una gran variedad de dispositivos:

MicroSaver® 2.0 y ClickSafe® 2.0

Para dispositivos que integran la Kensington Security Slot™ (ranura de seguridad) estándar usada en el 90 % de los dispositivos comerciales.

Kensington Security Slot™ en portátiles y equipos de escritorio

El bloqueo MicroSaver® 2.0 se fija directamente a la ranura de seguridad

El bloqueo ClickSafe® 2.0 se fija a través del anclaje ClickSafe

N17 para dispositivos Dell de 2017

Para dispositivos que integran la ranura de seguridad en cuña habitual en los modelos Dell Latitude de 2017 (posteriores) y otros dispositivos seleccionados.

Ranura de seguridad en cuña

Portátil anclado a un objeto fijo

Bloqueo de portátil por llave NanoSaver™

Para dispositivos que integran la Kensington Nano Security Slot™, habitual en los dispositivos ultrafinos

Kensington Nano Security Slot™

Bloqueo de portátil por llave NanoSaver™

Soluciones de bloqueo Microsoft Surface™

Bloqueos específicos para equipos como el Surface™ Pro, Surface™ Book y Surface™ Studio

Bloqueo por llave para Surface™ Pro

Kit de bloqueo para Surface™ Studio

Soporte de bloqueo para Surface™ Book de 13,5”

Estación de bloqueo de portátil 2.0

Para dispositivos sin ranura de seguridad como el portátil Surface™ y el MacBook Pro®

Estación de bloqueo para portátil MacBook Pro®

Encuentre la solución de bloqueo ideal para su portátil o dispositivo en:
kensington.com/securityselector.com

6 Puntos clave del GDPR a tener en cuenta

1. Considerar designar a un Responsable de protección de datos

Este responsable debe ser totalmente proporcionado con las responsabilidades de la organización en lo relativo al GDPR y tener un conocimiento profundo de qué datos dentro de su organización se consideran "personales", dónde se guardan, quién tiene acceso a ellos, cómo detectar las violaciones cuando se producen y a quién informar al respecto. **El Responsable de protección de datos no tiene por qué ser un empleado, esta función puede externalizarse.**

2. Evaluar sus sistemas

Revisar todos los contratos, soporte tecnológico, procedimientos y herramientas relacionados con el procesamiento, gestión, almacenamiento y borrado de datos para permitirle identificar cualquier deficiencia o laguna que requiera aplicar cambios.

3. Desarrollar una estrategia

Construir una nueva estrategia que garantice el pleno cumplimiento del GDPR. Esta estrategia puede incluir nuevas inversiones en tecnología, revisar los procedimientos del personal y la responsabilidad del procesamiento de los datos y crear nuevas funciones dentro de la organización.

POR QUÉ UNA POLÍTICA DE SEGURIDAD FÍSICA ES INTEGRAL PARA **EL CUMPLIMIENTO DEL GDPR**

6 Puntos clave del GDPR a tener en cuenta

4. Implementar una nueva Política de la organización

El siguiente paso para el cumplimiento del GDPR es poner su plan en acción en todos los niveles de la organización. Invertir e introducir las nuevas tecnologías y sistemas que sean necesarios en el lugar de trabajo y publicar una guía informativa relativa al tratamiento y gestión de los datos.

5. Compromiso de los empleados

Poner en marcha su nueva política de cumplimiento de la normativa de datos para todo el personal; facilitar formación, información y guías a los empleados para que estén bien formados al respecto y se mantengan al tanto de los cambios que se están produciendo y su responsabilidad en asegurar que la empresa cumpla con los requisitos del GDPR.

6. Revisar y mejorar

Tras la puesta en marcha de su plan de cumplimiento del GDPR, es el momento de revisar y mejorar con antelación a la entrada en vigor del reglamento. Identificar las mejoras necesarias con bastante antelación a la fecha límite del GDPR, para que cuando llegue el mes de mayo de 2018, su organización se haya adaptado con éxito y eficiencia a los cambios y cumpla con todos los requisitos.

Soluciones

Los bloqueos de portátiles y dispositivos son una respuesta directa a la necesidad de las organizaciones de fomentar el cumplimiento por parte de los empleados de una política de seguridad del hardware físico y reducir los riesgos de posibles violaciones de la seguridad. Otras soluciones adicionales pueden ayudar a reducir aún más este riesgo dentro y fuera del entorno de oficina.

Equipaje SecureTrek™
La gama de maletas, maletines y mochilas SecureTrek™ puede anclarse en lugares donde el robo es una preocupación, como aeropuertos, hoteles y ferias comerciales.

Pantallas de privacidad
El 'hacking visual' es fácil, se produce rápidamente y a menudo pasa desapercibido.[10] Una pantalla de privacidad reduce el ángulo de visión y, con ello, este riesgo.

Bloqueadores de puertos USB
Los administradores de sistemas pueden impedir físicamente que los usuarios conecten dispositivos USB, reduciendo el riesgo del copiado no autorizado de datos, o a la inversa, la carga de malware en un sistema.

Armarios
Una forma rápida y sencilla de cargar, sincronizar y asegurar múltiples tabletas y portátiles ultrafinos.

Llave con huella digital VeriMark™
Proporciona un inicio de sesión Windows Hello™ biométrico sencillo, rápido y seguro y funciona con servicios que requieren autenticación de doble factor, protegiendo así contra el acceso no autorizado y mejorando la seguridad online.

Fuentes

1. Kensington IT Security & Laptop Theft Survey, Agosto 2016
2. 2016 Data Breaches - Privacy Rights Clearinghouse
3. Breach Level Index, Septiembre 2017
4. Kensington IT Security & Laptop Theft Survey, Agosto 2016
5. Information Commisioner's Office - https://ico.org.uk/action-weve-taken/data-security-incident-trends
6. Financial Services Breach Report, Bitglass, 2016
7. Verizon Data Breach Investigations Report 2016
8. IDC Executive Brief 2010 - Laptop Theft: The Internal and External Threat
9. IDC White Paper 2007 - The Threat of Theft and Loss of Laptops for the SME
10. Ponemon Institute Visual Hacking Experiment, 2015

Kensington®

kensington.com

PARA MÁS INFORMACIÓN CONTACTAR:

Ricardo Hernández
Regional Manager Southern Europe
ricardo.hernandez@kensington.com
+34 600 53 11 32

Helena Gonzalez
Key Account Manager
helena.gonzalez@kensington.com
+34 663 11 25 77

The Professionals' Choice™