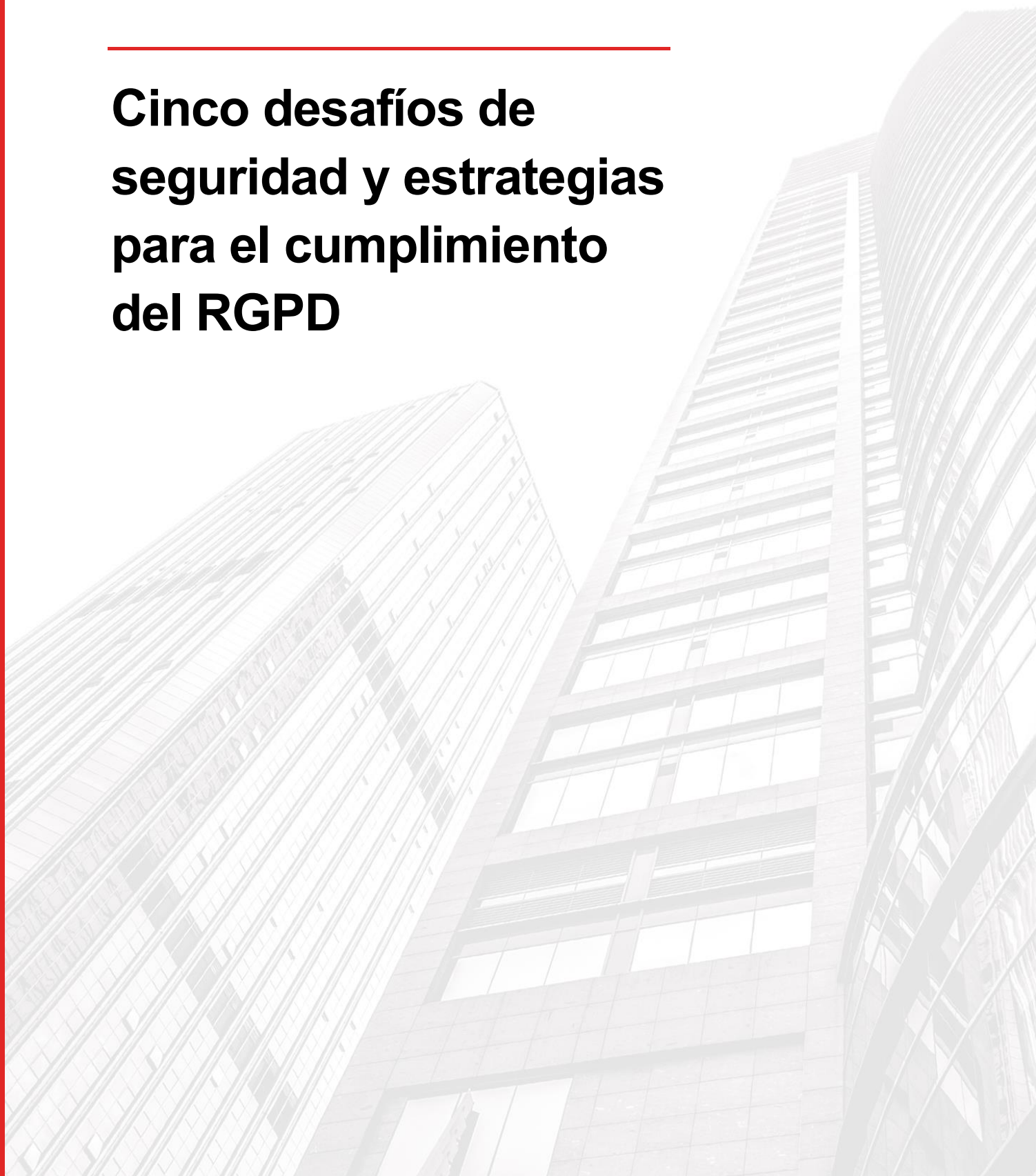
ivanti

Cinco desafíos de seguridad y estrategias para el cumplimiento del RGPD



Contenidos

Introducción

2017 fue el año de las brechas de datos. Esto, junto con la mayor demanda de seguridad de datos personales, está obligando a los gobiernos a crear legislaciones estrictas para proteger los datos de los ciudadanos: legislaciones como il nuevo Reglamento General de Protección de Datos (RGDP). Sin embargo, estas legislaciones de protección también colocan una gran carga en los departamentos de TI de las empresas para descubrir nuevas formas de proporcionar una mayor seguridad y garantizar que los trabajadores pueden hacer su trabajo. Esta guía ofrece recomendaciones prácticas y clave al departamento de TI para navegar el cumplimiento del RGPD y la seguridad de los datos personales (PII).

El impacto del RGPD

Tras los ataques a empresas como Equifax y Uber, que fueron víctimas de ataques cibernéticos, pero no divulgaron la exposición de los datos personales a tiempo, la Unión Europea exige una reforma completa con la nueva legislación del RGPD. Para muchas organizaciones, esto significa una nueva reforma en la forma en que adquieren, gestionan, protegen y supervisan la información de clientes y empleados. Además, las organizaciones ya no pueden esconder las brechas en los datos personales del público. La legislación normaliza y refuerza las leyes que gobiernan los datos personales, para cualquier empresa que de servicios o emplee ciudadanos de la UE. Los costes del incumplimiento incluyen multas, sanciones y daños compensatorios por las infracciones.[i] Las multas administrativas por el incumplimiento con ciertas disposiciones del RGPD pueden alcanzar los 20 millones de euros o un cuatro por ciento de los ingresos totales mundiales anuales de la empresa.

Entonces, ¿cuándo deben cumplir estas regulaciones las empresas? La fecha límite es el 25 de mayo de 2018. Este posible enorme impacto financiero hace que a muchos financieros de la UE se les haga la boca agua. Los aseguradores corporativos ven el cumplimiento del RGPD como una fuente de considerable riesgo al calcular las primas de seguros de la empresa, y los bufetes legales seguro que se aprovecharán de las organizaciones que no cumplan el RGPD y expongan los datos de sus clientes. Hay mucho en juego. Y queda poco tiempo.

El RGPD introduce:

- Procesos detallados de cumplimiento para la remediación de amenazas, incluyendo la regla de las 72 horas, que requiere un informe oportuno sobre la brecha de datos personales a una autoridad supervisora tras el descubrimiento
- Grandes multas para organizaciones que no cumplan las regulaciones del RGPD
- Estrictos requisitos que otorgan un mayor control a los ciudadanos de la UE sobre sus datos personales
- La necesidad de que las organizaciones contraten a "oficiales de protección de datos" centrados en proteger los datos del consumidor

Preparándose para el RGPD: Cinco estrategias de seguridad clave

El RGPD es clara sobre la necesidad de los requisitos de seguridad para proteger los datos de los ciudadanos de la UE, pero es menos específica sobre qué hacer para proteger la información personal. Aunque el cumplimiento puede ser distinto en todas las organizaciones, la mayoría podrá minimizar amenazas a los datos personales y el riesgo de estas considerables multas abordando estos cinco aspectos de la seguridad:

1. Proteger los datos personales contra amenazas de trabajadores móviles
2. Gestionar derechos de administrador en sistemas y aplicaciones
3. Mitigar el impacto del ransomware y otros malware
4. Mitigar los riegos del onboarding y offboarding del empleado
5. Supervisar e informar sobre el acceso de datos personales

Afortunadamente, para cada uno de estos aspectos existe una estrategia de seguridad potente y fácil de implementar que puede utilizar para prepararse para el cumplimiento del RGPD y proteger los datos personales.

Estrategia 1: Disminuya la exposición de seguridad de los trabajadores móviles.

Se estima que, en 2020, un 72 % de los trabajadores de EE. UU. utilizará un dispositivo móvil para realizar su trabajo.[ii] Sin embargo, cada dispositivo móvil y punto de acceso aumenta la oportunidad de los atacantes de infiltrarse en su red. Durante años, las TI han desarrollado tremendas tecnologías de seguridad estáticas basadas en el perímetro, pero estas pueden ser evitadas por un trabajador pulsando un botón en su teléfono mientras trabaja en una cafetería.

Disminuir el riesgo y garantizar el cumplimiento del RGPD no es fácil. Para proteger a las organizaciones de estos nuevos riesgos y garantizar el cumplimiento del RGPD, necesita nuevos controles de seguridad y políticas basados en contexto. Los controles basados en contexto adaptan cada espacio de trabajo digital del trabajador al nivel de riego de seguridad que suponen en un momento determinado, en función de varios criterios:

- ¿Trabajan con un dispositivo conocido o desconocido?
- ¿Se conectan mediante una red fiable o no?
- ¿Utilizan dispositivos o periféricos USB no reconocidos o no autorizados por la empresa?
- ¿Intentan acceder a información confidencial durante horas de oficina o a una hora extraña?

Estrategia 2: Recupere el control de los accesos de usuarios privilegiados.

Los privilegios administrativos proporcionan acceso a los usuarios que, en caso de utilizarse incorrectamente, pueden resultar en un coste de soporte alto y una experiencia de usuario comprometida. En muchos casos, la seguridad también se ve comprometida al manejar datos incorrectamente, instalar hardware software no aprobado, la pérdida de datos o ataques de software malicioso. Todos los usuarios privilegiados con un enfoque de los actores maliciosos, aumentando así la vulnerabilidad porque sus mayores derechos de acceso permiten a los atacantes navegar las redes, sistemas y aplicaciones corporativas más fácilmente.

Sin embargo, existen escenarios en los que los usuarios requieren derechos de administrador locales para trabajar de forma efectiva. Muchas aplicaciones, incluyendo algunas nuevas, permiten realizar cambios a ajustes de hardware o adaptadores de red, y todos requieren privilegios de administrador. Se incluyen las actualizaciones de aplicaciones web, la instalación de componentes Active-X, actualizaciones de Adobe/Flash/Java o la instalación de controladores de la impresora.

Para acelerar la eficiencia, algunas organizaciones otorgan derechos de acceso elevados a casi cualquier persona en la empresa simplemente porque no tienen los recursos y la capacidad de

gobernarlos con más cuidado. En muchas organizaciones, las políticas de acceso de los "usuarios con menos privilegios" a menudo se combinan con normas demasiado liberales. Además, cuando no se les permite acceder a aplicaciones que necesitan para realizar su trabajo, pueden introducir alternativas no autorizadas que presentan un riesgo a su entorno y su cumplimiento.

Las organizaciones deben poder otorgar y eliminar derechos de administrador cuando sea necesario para proteger la empresa y mantenerla productiva. Con los controles dinámicos, los derechos de usuarios privilegiados se pueden reducir inmediatamente cuando los usuarios salen de una aplicación o indican que la tarea está finalizada. Estas reducciones de los privilegios de usuario reducen el riesgo de brechas de seguridad. Establecer controles dinámicos puede tener un impacto tremendo para gestionar derechos de administrador a escala y lograr el cumplimiento del RGPD.

Estrategia 3: Contenga los ataques de ransomware y otros malware.

El ransomware y otros malware no afectarán su organización si no pueden entrar. El medio de acceso más probable son los ataques de phishing por correo electrónico y software vulnerable que no se parchee. Los atacantes también usan unidades y periféricos externos para transferir códigos maliciosos y obtener acceso a sus datos personales. Cuando los trabajadores hacen clic en el enlace en un correo, visitan páginas web comprometidas o se conectan a unidades USB no seguras, el dispositivo u ordenador en el que trabajan se puede infectar. Este malware intentará esparcirse en su entorno e incluso robar credenciales para iniciar sesión en páginas web de terceros como la banca y tiendas. Al parchear los sistemas operativos y aplicaciones de terceros de forma uniforme y completa, evitar que se ejecuten códigos no autorizados con las listas blancas de aplicaciones y bloqueando el acceso a páginas web y archivos, las organizaciones pueden reducir en gran medida la exposición a los ataques.

La mayoría de las organizaciones ya han establecido una lista blanca, pero a menudo tiene problemas. El descubrimiento puede ser un proceso exhaustivo. Una vez implementado, la lista blanca debe mantenerse y actualizarse. Los usuarios de hoy en día deben realizar su trabajo rápida y eficazmente, y se introducen nuevas aplicaciones y versiones cada día a nuestros entornos, aumentando el coste de propiedad de los métodos de listas blancas tradicionales. Algunas soluciones causan un gran impacto en el rendimiento del sistema, dado que cada aplicación accedida debe evaluarse para garantizar que concuerda con la buena aplicación conocida y que no es un archivo renombrado que intenta hacerse pasar por el archivo en la lista blanca.

Considere soluciones de listas blancas que eliminan gran cantidad de la carga para maximizar el valor que aportan. Además, añadir controles granulares a nivel de código, que empleen firmas para abrir archivos o ejecutar aplicaciones ayudará en gran medida a evitar que los usuarios lancen un ataque accidentalmente al hacer clic en un enlace o adjunto de correo. Las organizaciones pueden establecer controles para bloquear a los usuarios al acceder a páginas web o archivos específicos, evitar que los usuarios guarden archivos maliciosos en discos locales o bloquear dispositivos externos para que solo puedan abrirse o guardarse archivos protegidos o codificados. Además de evitar que se ejecuten aplicaciones no autorizadas o no deseadas, es importante garantizar que los nodos finales no han sido comprometidos por aplicaciones de confianza modificadas mientras estaban cargadas en la memoria. Los controles proactivos ayudan a las organizaciones a garantizar la protección de los datos personales y demostrar el cumplimiento de los requisitos de seguridad del RGPD.

Estrategia 4: Implemente onboarding y offboarding seguros.

Muchas organizaciones todavía dependen de procesos manuales para los procesos de onboarding y offboarding de los trabajadores, que a

menudo producen inexactitudes y retrasos de días o semanas. Un estudio reciente del Ponemon Institute determinó que más de un 24 % de las personas que se marchan de la organización siguen teniendo acceso a sus datos corporativos varias semanas después.[iii] Los procesos de TI pueden aprovisionar automáticamente los trabajadores con acceso basado en la función a las aplicaciones y servicios que necesitan para realizar su trabajo. Esta misma tecnología se puede usar para desaprovisionar a los trabajadores inmediatamente en el momento en que se marchan de la empresa o cambian su función. Automatizar las políticas de aplicación del aprovisionamiento y desaprovisionamiento simplifica la seguridad sin la preocupación de que se nos olvide algo, y también simplifica la preparación para una auditoría de TI. Los procesos de aprovisionamiento y desaprovisionamiento deben integrarse en las aplicaciones existentes de RR. HH., sistemas de gestión de proyectos u otras tiendas de identidad de la empresa, para que los cambios de acceso se puedan activar automáticamente cuando el estado de identidad del trabajador cambie en dichos sistemas. Con este enfoque más completo para identificar la gestión del ciclo de vida, las organizaciones pueden mejorar considerablemente la productividad y la seguridad a la vez que cumplen los requisitos del RGPD.

Estrategia 5: Mejorar la visibilidad de los datos personales y los informes

Para demostrar el cumplimiento del RGPD, las organizaciones necesitan una mayor visibilidad sobre los datos que pasan por sus entornos de TI. Debe supervisarse quién accede a qué datos, y debe poder demostrarse que se han implementado controles adecuados para proteger datos personales. Para descubrir y remediar amenazas antes de que se conviertan en los titulares de la próxima brecha de seguridad, los administradores de TI deben poder consolidar y descomponer la gran cantidad de información supervisada, extrayendo la información crítica en tiempo real.

Las organizaciones deben poder producir informes fácilmente sobre espacios de trabajo desplegados, incluidos los cambios, uso, dispositivos, aplicaciones y configuraciones. La supervisión de registros e informes permite a las organizaciones demostrar el cumplimiento del RGPD y preparar rápidamente la información necesaria para informar sobre brechas a las autoridades supervisoras y los individuos. Con esta visibilidad a grandes cantidades de datos, no solo podrá demostrar su cumplimiento más eficientemente, sino que podrá compartir información sobre datos con el personal adecuado para acelerar su negocio e introducir nuevas fuentes de ingresos.

Cómo Ivanti puede apoyar su estrategia de RGPD

Ayudamos a las organizaciones más fiables del mundo a gestionar y proteger sus entornos de TI con soluciones de tecnología que unifican la seguridad, la gestión de servicios y las operaciones de TI para automatizar y proteger el espacio de trabajo digital.

Evalúe

Las organizaciones deben prepararse para el RGPD al evaluar su nivel de riego de incumplimiento. Necesitan transparencia y acceso a datos de aprovisionamiento de clientes, servidores y usuarios para realizar esta evaluación. Ivanti le puede ayudar a evaluar su nivel rápidamente con paneles de control y herramientas de informes. Puede ver amenazas a la seguridad de la información personal en tiempo real y ver información sobre qué flujos de trabajo deben establecerse para lograr el cumplimiento.

Automatice

A continuación, las empresas deben aplicar políticas para garantizar una gestión uniforme de datos personales y privacidad. Dado que más de un 50 % de los exempleados retiene acceso a aplicaciones del empleador y un 20 % de las brechas de datos aparece a causa de no desaprovisionar los derechos de acceso,[iv] las

organizaciones necesitan poder actuar rápidamente para proteger los datos personales.

Ivanti puede ayudarle a transformar procesos y políticas manuales y propensos a errores, en flujos de trabajo automatizados basados en funciones de los usuarios en su organización. Ahora puede aprovisionar y desaprovisionar empleados rápidamente en su entorno de TI.

Proteger

Las soluciones de Ivanti descubren y proporcionan información sobre áreas vulnerables en su entorno de TI y toman medidas y protegen datos personales confidenciales de los ataques. Con las soluciones de Ivanti puede:

- Descubrir el hardware y software en su entorno. No puede proteger o defender aquello que no conoce.
- Recuperar y supervisar datos, informar y analizar.
- Parchear las aplicaciones que puede parchear y controlar el acceso de aquellas que no puede.
- Implementar controles de aplicaciones para evitar el ransomware y proteger datos personales.
- Controlar el uso de dispositivos extraíbles y forzar la codificación en dispositivos extraíbles y discos duros.
- Limitar los derechos de administrador sin afectar la productividad o consumir el valioso tiempo de su departamento de TI.
- Otorgue a los usuarios los niveles adecuados de acceso en base a su identidad, lo cual les permite mantenerse productivos y la empresa permanece segura.

Responder y cumplir

Finalmente, Ivanti puede ayudarle a demostrar que se están aplicando las políticas necesarias, consolidando datos en todo su ecosistema de TI para proporcionar informes contextuales en tiempo real y acelerar las solicitudes de auditoría. Con conectores prefabricados a más de 50 soluciones de TI de terceros líderes en la industria, Ivanti se lo pone fácil. Ahora puede automatizar flujos de trabajo para identificar datos solicitados en cuestión de minutos, en vez de horas, y obtener información procesable sobre sus sistemas y nodos finales para mantener el cumplimiento del RGPD

Póngase en contacto con Ivanti hoy

Con la fecha límite a la vuelta de la esquina y más riesgos de seguridad que nunca, no puede permitirse retrasar su estrategia de cumplimiento del RGPD. Lleva tiempo preparar los procesos y políticas y tecnologías correctas. Si quiere saber más sobre cómo Ivanti puede prepararle una solución personalizada, póngase en contacto con **contact@ivanti.es**.

www.ivanti.es/GDPR

1 +33 (0)1 49 03 77 80

contact@ivanti.es

[i] **http://eur-lex.europa.eu/eli/reg/2016/679/oj** , Artículos 83 y 84
[ii] **http://www.channelfutures.com/mobile-computing/idc-mobile-workers-us-exceed-105-million-2020**
[iii] **http://media.techtarget.com/Syndication/NATIONALS/Data_Loss_Risks_During_Downsizing_Feb_23_2009.pdf**
[iv] **https://www.onelogin.com/press-center/press-releases/new-research-from-onelogin-finds-over-50-of-ex-employees-still-have-access-to-corporate-applications**