¿LAS EMPRESAS LATINOAMERICANAS ESTÁN PREPARADAS PARA LA **REGULACIÓN GENERAL DE PROTECCIÓN DE DATOS**?

Licencias OnLine

PARTICIPAN EN ESTE INFORME:

Índice

La Unión Europea lanzó el ***Reglamento General de Datos Personales*** *con el objetivo de que los ciudadanos de la comunidad europea tengan un mayor control sobre la gestión que se hace de sus datos personales.*

GDPR: Marco Referencial

GDPR, como se conoce a esta nueva legislación, **entrará en vigor el 25 de mayo de 2018** y ampliará las obligaciones de implantación de medidas de seguridad para todas las empresas europeas, los autónomos y la administración pública, entre otros sectores. Las medidas incluyen la obligación de implementar cifrados y sistemas de autenticación de dos factores, incluso sobre datos considerados de nivel básico, cuando el riesgo lo exige. **Otros sujetos también obligados son los ubicados fuera de la Unión Europea que dirijan sus servicios a usuarios de países miembros o que reciban datos personales desde Europa.**

La GDPR busca proteger los datos personales y la forma en la que las organizaciones los procesan, almacenan y, finalmente, destruyen, cuando esos datos ya no son requeridos.

La ley provee control individual en relación con la manera en la que las compañías pueden usar la información que está directa y personalmente relacionada con los individuos, y otorga ocho derechos específicos:

- *El derecho* ***a ser informado***
- *El derecho* ***al acceso***
- *El derecho* ***de la rectificación***
- *El derecho* ***al borrado de datos***
- *El derecho* ***a restringir el procesamiento***
- *El derecho* ***de portabilidad de los datos***
- *El derecho* ***de objeción***
- *El derecho* ***en relación con la creación de perfiles y toma de decisiones automatizadas***

A su vez, establece normas muy estrictas si se viola el acceso a datos personales y las consecuencias (multas) que las organizaciones pueden sufrir en tal caso.

Aunque este reglamento es de cumplimiento obligatorio únicamente en Europa, va a cambiar la forma de trabajar de todas las empresas en el mundo que manejen, almacenen o utilicen datos personales, sin importar si es de empleados, clientes, posibles clientes o proveedores, debido a que deberán tener en cuenta el manejo de la privacidad como base fundamental del manejo de los datos personales.

El **Principio de Transferencias Internacionales** recoge que únicamente podrá realizarse una transferencia de datos personales a un tercer país u organización internacional, cuando la Comisión haya considerado que éstos cuentan con un adecuado nivel de protección; ofrecen garantías adecuadas sobre la protección que los datos recibirán en su destino; se dan circunstancias previstas como excepciones; y se cumplen los demás requisitos del Reglamento.

Es decir, las empresas de América Latina que cuentan con filiales y/o almacenan y procesan información personal sobre ciudadanos de la UE deben prepararse también para su cumplimiento y deberán proteger los datos personales de sus clientes, estén donde estén, incluso en la nube. *"Es por ello - comentan desde **Symantec** - que nuestros clientes de Latinoamérica han comenzado a realizar preguntas e interiorizarse sobre GDPR, para saber de qué se trata y qué deben hacer para poder cumplir".*

Para **Forcepoint**, la implementación de esta regulación impactará el modo en que las empresas abordan la seguridad de la información, el control y la privacidad de los datos. ***"La nueva legislación se centra en la protección de la información desde la identificación y protección inicial de la Información Personalmente Identificable (PII), hasta la exigencia de notificar oportunamente los incidentes de acceso no autorizado a la información directamente a la autoridad supervisora competente".***

Como consecuencia, desde **Trend Micro** explican que el GDPR exigirá que las organizaciones de cualquier parte del mundo que procesen datos ciudadanos de la UE, incluidas grandes empresas, pequeñas y medianas empresas, gobiernos e incluso propietarios únicos, reevalúen sus controles de procesamiento de datos y establezcan un plan para proteger mejor los datos ciudadanos de la UE.

Desde el punto de vista de **Imperva**, el nuevo reglamento es una oportunidad para empresas de todo tipo a mejorar su postura de seguridad en cuanto al manejo de datos, y convertirse en referentes en su industria.

> *"Nuestra marca está perfectamente posicionada para apoyar la implementación de controles en cumplimiento del GDPR. El foco está en brindar protección a los datos y procesamiento de estos, así como la creación de controles efectivos tanto para su acceso como para su proliferación. Esta es exactamente la misión que Imperva ha tenido desde que se fundó",* ***Imperva.***

La economía mundial de Internet está borrando rápidamente las barreras para hacer negocios entre países o continentes, y no es raro que las empresas en cualquier parte del mundo hagan negocios con cualquier otra región. En este sentido, según **Sophos**:

"Si una empresa latinoamericana tiene la intención de hacer negocios con clientes europeos de cualquier forma, es muy probable que se vean afectados y deberán cumplir con las regulaciones especificadas en el GDPR. Las organizaciones en América Latina están gobernadas por el GDPR si ofrecen bienes o servicios a individuos de la UE, ya sean gratuitos o pagados, o si almacenan datos o monitorean el comportamiento de estas personas", ***Sophos.***

Respecto al tipo de empresas que serán alcanzada por esta legislación, desde **Veeam** aclaran: *"no hay una tipificación de industria afectada a GDPR, aunque hay algunos segmentos que tal vez se vean más impactados que otros, por ejemplo, sector financiero, salud y gobierno entre otras, en tanto el tipo de dato que procesen sea sensible hacia las personas que consuman sus servicios o productos. GDPR aplica para TODAS las compañías que procesen datos considerados sensibles de ciudadanos de la UE, por lo que prácticamente cualquier compañía en el mundo es alcanzable".*

Seguridad, nube y protección de datos

No hay dudas de que **la nube permite traspasar fronteras tecnológicas, geográficas y administrativas, asegurando la disponibilidad, accesibilidad y compartición de los datos.**

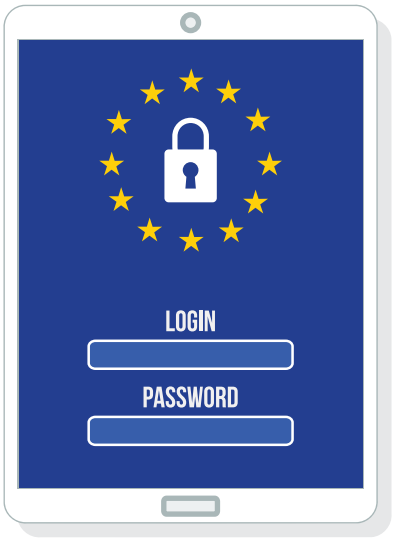
Sin embargo, también impulsa un importante abanico de amenazas.

Uno de los mayores problemas que surge en torno a esta infraestructura es que los datos personales se procesan en la nube, por lo que los equipos de seguridad y de TI no tienen percepción ni control sobre lo que sucede con ellos.

Al no poder las empresas limitar el uso de servicios cloud por parte de sus empleados, puede significar que los datos sensibles acaben en manos equivocadas, exponiendo en consecuencia todo el ecosistema empresarial.

Con el GPRD a la vuelta de la esquina obtener una visibilidad completa del uso y actividades de los servicios y aplicaciones cloud nunca había sido tan importante. A partir de ahora, todas las empresas, cualquiera que sea su localización o ubicación, deberán responsabilizarse de la protección de los datos de sus clientes. **En el caso de las empresas que contratan servicios en la nube, serán los responsables últimos de la seguridad de los datos de carácter personal, y no el prestador del servicio.**

Forcepoint propone algunos aspectos clave para realizar una evaluación básica de una estrategia de protección de datos actual. Por un lado, las organizaciones deben contar con una empresa que brinde el soporte necesario para realizar un inventario de los datos personales almacenados dentro de la organización. A su vez, realizar un mapeo, manejo y control del flujo de datos personales. Por último, es necesario contar con un servicio que permita responder a incidentes que involucren datos con la madurez en su tecnología y la fuerza visionaria. "***Forcepoint es experto en la regulación GDPR y cuenta con las herramientas para asistir al respecto***", aseguran.



Desde **A10 Networks** postulan que dentro de los componentes más importantes para cumplir con esta legislación estarán los sistemas de prevención de perdida de información (DLP) y los mecanismos de control de acceso de usuarios (Federación de autenticación).

Con respecto a DLP, una preocupación muy importante que deben tener las empresas que deben cumplir con GDPR es la visibilidad del tráfico.

> *"Si la empresa no tiene visibilidad del tráfico no puede saber si le han extraído información relevante", **A10 Networks**.*

El vendor ofrece soluciones que trabajan en conjunto con otros líderes del mercado de seguridad informática. Por ejemplo, **A10 Networks** Thunder SSLi ofrece la solución de visibilidad de SSL más escalable del mercado, la cual permite a las empresas optimizar el uso de sus plataformas de DPI, NGFW, y análisis forense, entre otras.

Por su parte, las soluciones de **Imperva** permiten gestionar el ciclo completo de vida de los datos de seguridad con visibilidad y control para bases de datos empresariales, aplicaciones y usuarios.

En el caso de **Veritas**, la marca asegura estar lista para ayudar al gran número de empresas e instituciones que se verán obligadas al cumplimiento de la normativa GDPR a través de sus soluciones de Information Management.

> *"Esta regulación es una gran tendencia a nivel mundial y demuestra la preocupación de los clientes por tener una administración responsable de los datos. En este sentido, representa una gran oportunidad para el ecosistema de partners de Veritas. Nuestras soluciones de Data manegment 360 permiten entender qué información estamos guardando y administrarla correctamente. Veritas puede reforzar las conductas necesarias para que los usuarios se apeguen a la norma a través de sus soluciones como Enteprise Vault, Net BackUp, Information Map y Data Insight".* ***Veritas***

Sophos también tiene una amplia gama de herramientas de seguridad y protección de datos que pueden ayudar a resolver uno de los mayores desafíos en torno al GDPR: mitigar los riesgos relacionados con la pérdida de datos. *"Como primer paso, sugerimos a los clientes que implementen soluciones fáciles de administrar de Sophos Central para ayudar a detener las principales causas de pérdida de datos: protección contra malware, ransomware y piratería con Sophos Intercept X y Sophos Endpoint Protection; soluciones de red sólidas para detener a los malos en la puerta con Sophos XG Firewall; y todos los discos duros que están cifrados y los dispositivos móviles se administran con Sophos Central Device Encryption y Sophos Mobile"*, detallan.

El GDPR es un marco legal masivo que cubre muchos desafíos individuales con respecto a la seguridad y gobernabilidad de los datos. Es importante entender que no existe una solución fácil o una "solución mágica" para resolver todos los requisitos y cumplir con la regulación.

Una de las soluciones de seguridad que **RSA** ofrece es Archer Suite, líder en los temas de Gobierno, Riesgo y Cumplimiento (GRC), diseñada para apoyar en la gestión de múltiples dimensiones del riesgo, con base en estándares de la industria y buenas prácticas sobre una plataforma integrada y configurable. Esta solución provee varios casos de uso ya configurados que juegan un papel clave en ayudar a las empresas a establecer y mantener su estrategia de cumplimiento frente a GDPR.
"RSA ofrece, dentro de su portafolio, soluciones de seguridad orientada al negocio que pueden apoyar a las organizaciones a establecer el marco de trabajo necesario para prepararse para dar cumplimiento con los requerimientos de la normativa".

Por su parte, la visión de **Symantec** se enfoca en ayudar a las organizaciones a mantener una protección sólida y fluida de los datos a través de su ciclo de vida. Para esto, *"nos enfocamos en cuatro etapas o pilares fundamentales: En la preparación, para obtener un mejor manejo de los datos personales y el riesgo asociado; en la protección, para prevenir mejor los ataques o el uso indebido de datos personales; en ayudar a detectar rápidamente cuándo ha ocurrido una violación de datos y entender su impacto; y en responder eficazmente y mitigar el impacto"*, detallan. Y agregan: *"como punto de partida, es importante poder descubrir todos los datos personales que puedan encontrarse en su organización. Symantec puede agilizar esta tarea".*

La difícil labor de preparar a una organización para cumplir las nuevas normas

De acuerdo con un informe de Gartner, muchas empresas no estarán listas para cumplir con los requisitos exigidos para la fecha prevista. **Symantec** coincide.

> *"Muchos clientes no están preparados para el GDPR. No es inusual preguntarse qué se debe hacer. GDPR está haciendo que muchas organizaciones revisen completamente, y en algunos casos, examinen sus procesos. Con tan poco tiempo, es más importante que nunca elaborar una estrategia coherente. La estrategia debe estar centrada en la seguridad alrededor de la información. Básicamente, el uso y combinación de tecnologías de protección de la información implementadas con el objetivo de proteger los datos confidenciales, donde sea que vayan o quien sea que la esté accediendo. Las organizaciones se pueden apoyar en Symantec para desarrollar e implementar esa estrategia", **Symantec.***

Para que las empresas puedan permanecer dentro del cumplimiento normativo, deberán aplicar importantes cambios en su cultura organizacional, frente a este nuevo panorama, **Veeam** detalla: *"las organizaciones deberán hacer modificaciones en varios aspectos, el principal está relacionado al cumplimiento de procesos en el manejo, transferencia y disposición de los datos. Ya no es suficiente con la protección de los mismos en el sentido del resguardo, sino que se incorporan exigencias como encripción de punta a punta, descarte segurizado y 'derecho al olvido' entre otras cosas desde lo funcional, y desde lo organizacional, por ejemplo, la existencia de un responsable de protección de datos (Data Protection Officer) que deberá velar por el cumplimiento de estas normas y procedimientos".*

Por su parte, **Veritas** también apunta a la gran cantidad de modificaciones que deberán hacer los clientes, *"estamos lista para ayudar al gran número de empresas e instituciones que se verán obligadas al cumplimiento de la normativa GDPR a través de nuestras soluciones de Information Management. A su vez, ayudamos a reforzar las conductas necesarias para que los usuarios se apeguen a la norma a través de sus soluciones como Enteprise Vault, Net BackUp, Information Map y Data Insight".*

Para **Trend Micro**, si bien algunas organizaciones consideran que el GDPR es una oportunidad para aumentar la asociación de su marca con la protección de los datos de los usuarios y para el crecimiento general del negocio, también existen posibles impactos negativos derivados del incumplimiento.

> *"El GDPR es una regulación multifacética que incluye directrices sobre personas, procesos y tecnología, todas enfocadas en la protección de datos. La seguridad de última generación puede desempeñar un papel fundamental en el cumplimiento, ayudando a garantizar que la tecnología que se casa con las personas y el proceso sea efectiva". **Trend Micro***

Por el lado de **Imperva** lo principal es que el esfuerzo por el cumplimiento nazca y permee desde los mandos ejecutivos hacia abajo a los diferentes niveles de la organización. *"De otra manera, se convierte siempre en una responsabilidad indeseada por las áreas a las que invariablemente les cae el requerimiento".*

Hay que destacar que el GDPR es una de las iniciativas legales más importantes de la historia en términos de privacidad y protección de datos, y los requisitos básicos se harán eco en todo el mundo en los próximos años.

En este sentido, **Sophos** recomienda que las organizaciones, como mínimo, desarrollen un plan y lo documenten detenidamente. *"Por ejemplo, las organizaciones deben apropiarse de su preparación aprendiendo más sobre el tema y evaluar continuamente el riesgo, es decir, observar qué datos almacenan y por qué, descubrir qué es lo que falta y luego decidir cuánto esfuerzo deben invertir para mitigar ese riesgo. También es importante tener en cuenta que, debido a que las sanciones financieras por no cumplir con el GDPR podrían ser significativas, la aceptación de los altos ejecutivos de las empresas es importante para tener éxito".*

Tiempo de oportunidades para el canal

Teniendo en cuenta que un gran porcentaje de empresas desconoce o no tiene recursos suficientes para asegurar el cumplimiento normativo que exige la GDPR, esto supone grandes oportunidades para el sector de software de gestión empresarial.

Según **Sophos**, es una oportunidad significativa para la industria de la seguridad y sus canales. *"Muchas de las tecnologías que se requieren para cumplir con éxito con la normativa son de naturaleza bastante técnica y generarán considerables oportunidades de ventas de valor agregado para los revendedores y las organizaciones de servicios profesionales.*

Los socios de canal que trabajan con proveedores de seguridad consolidados que tienen ofertas para proteger muchos niveles de la infraestructura de una organización (red, endpoint, cifrado, correo electrónico, DLP, control web) probablemente estén en una buena posición para aprovechar la oportunidad de GDPR".

Desde el punto de vista de **Forcepoint**:

> *"Gracias a nuestros partners, podremos brindar nuestros servicios a través de los cuales las empresas podrán descubrir brechas en sus sistemas de seguridad. Somos expertos en el tema; es parte de un equipo que comprende lo que el cliente necesita y está en condiciones de proveer la tecnología necesaria para cumplir con la normativa", **Forcepoint**.*

Adicionalmente, la empresa está expandiendo su presencia y estrategia en 2018 mediante su estrategia de Human Point System en la cual los Socios Autorizados adoptarán esta oferta de soluciones para ampliar su oferta consultiva alrededor de GDPR. *"La protección del factor humano es la visión de Forcepoint y el enfoque de nuestros productos ya que además de integrarse, ayuda a las organizaciones a comprender el ritmo normal del comportamiento de los usuarios y el flujo de datos que entran y salen de su organización para poder identificar los riesgos y responder a ellos en tiempo real".*

La estrategia de Human Point System ayudará a los partners autorizados a elevar sus servicios de consultoría de seguridad a la mesa de dirección de las organizaciones ya que estarán apoyando a que las organizaciones estén en cumplimiento, sin frenar el ritmo del negocio y protegiendo a su vez los datos y propiedad intelectual. *"Esto hará más ágil la adopción de nuevos proyectos como adaptar nuevas tendencias tecnológicas, mejorar procesos a nivel TI y manejo de información confidencial en los múltiples departamentos dentro de las organizaciones"*, enfatizan desde la firma.

Trend Micro entiende que los socios deben ofrecer soluciones de vanguardia a través de una estrategia de seguridad, *"permitiendo a las organizaciones aprovechar la oferta de ciberseguridad que aborda las amenazas de hoy y de mañana, adaptándose a las necesidades de su negocio"*.

Ligado a ello, en **Imperva** asumen que el rol principal del canal es de concientizador:

> *"La mayoría de las empresas ignoran que la GDPR les podría aplicar y tener consecuencias reales para su negocio", argumentan al respecto y agregan: "El rol secundario es de trusted advisor, para ayudar a los clientes a encontrar la estrategia más efectiva de selección y aplicación de tecnologías para el cumplimiento y mejora de su postura general de seguridad de datos",* ***Imperva****.*

Sebastián Losada, Gerente Regional de Marketing y Alianzas Estratégicas de **Licencias OnLine**, adhiere de manera contundente sobre la importancia del rol de los canales. *"Sus servicios de consultoría con la dirección y con el Staff ejecutivo de sus clientes será un factor crítico que probablemente genere nuevos diálogos para adaptar tecnologías complementarias, mejorar procesos de TI y optimizar el manejo de información en múltiples departamentos dentro de las organizaciones. Para ello, necesitarán entender las soluciones que permiten a los clientes el cumplimiento de la norma y transmitir el sentido de urgencia que merece, por lo que deberán estudiar muy bien los alcances e impactos de la regulación".*

> *"Será fundamental el factor confianza que se genere entre los partners y los clientes, complementado con un buen nivel de conocimiento sobre el GDPR para entender los impactos, inversiones y cambios que quizá deban contemplarse. Se generarán nuevos proyectos que demandarán servicios profesionales especializados por lo que todos los partners que ya se están preparando tendrán una ventaja diferenciadora relevante y para los que aún no lo hicieron, implica grandes oportunidades",* ***Carolina Losada, CEO Licencias OnLine.***

Ante esta coyuntura, *"uno de los grandes desafíos que tienen muchas organizaciones no sólo es tener la tecnología correcta, sino también contar con la experiencia humana adecuada. Es ahí donde los expertos tienen una contribución crítica para el éxito, transformando las prácticas 'técnicas' en cultura organizacional. La responsabilidad de buscar las formas de cómo hacerlo es de todos y el compromiso ya está planteado"*, enfatiza Carolina Losada.

Cumplir con el Reglamento General de Datos Personales supone un avance significativo, pero también implicará una mayor inversión en procesos y tecnología necesarios para asegurar los datos, tanto los que permanecen al amparo del perímetro de TI como los que se depositan en la nube.

En este sentido, eleva las condiciones de seguridad y privacidad que protegen los datos de los ciudadanos europeos y exige una ardua tarea para los responsables de infraestructuras.

Al mismo tiempo, se presenta como una oportunidad para los partners tecnológicos en tanto que habilita una puerta de entrada a nuevos proyectos en materia de almacenamiento, seguridad y diseño estratégico de las compañías.

El Reglamento General de Datos Personales normalizará la protección de datos en toda la Unión europea y, si bien puede parecer oneroso, en un mundo con tantas brechas como las que hemos tenido en los últimos años, es el tipo de regulación que necesitamos.

Agradecemos a todos los vendors que participaron de este informe aportando información y recursos:

Alejandro Wasserlauf
Systems Engineering Manager Latam/MCA – ***Veeam Software***

Sebastian Brenner
Security Strategist LATAM – ***Symantec***

Petter Nordwall
Director of Product Management – ***Sophos***

Josué Ariza
Regional Sales Director Caribbean & Spanish South America - ***Forcepoint***

Alejandro Guízar
SE Manager – ***Imperva***

José De Abreu
Latin America Sales Engineer Manager - ***A10 Networks***

José Ramón Fernández G.
México Sales Channel Manager and Alliances - ***Veritas***

Juan Pablo Castro
Director of Technology & Cybersecurity Strategist – ***Trend Micro***

J.P. Tiengo
Archer Manager - Latin America ***RSA***