byte TI

ENCARTE ESPECIAL MAYO

Soluciones para sobrevivir a GDPR

2 CONTENIDOS

ESPECIAL GDPR

N.º 260 • ÉPOCA III

Director
Juan Manuel Sáez
(juanmsaez@mkm-pi.com)

Redactor Jefe
Manuel Navarro
(mnavarro@mkm-pi.com)

Coordinador Técnico
Javier Palazon

Colaboradores
S. Velasco, R.de Miguel, I. Pajuelo, O. González, D. Rodríguez, F. Jofre, JL. Valbuena, MªJ. Recio, MA. Gombáu, J. Hermoso, JC. Hernández, C. Hernández, M. Barceló, A.Barba.

Fotógrafos
E. Fidalgo, S. Cogolludo, Vilma Tonda

Ilustración de portada
Javier López Sáez

Diseño y maquetación
El Palíndromo Comunicación S.L.

WebMaster
NEXICA
www.nexica.es

REDACCIÓN
Avda. Adolfo Suárez, 14 – 2º B
28660 Boadilla del Monte
Madrid
Tel.: 91 632 38 27 / 91 633 39 53
Fax: 91 633 25 64
e-mail: byte@mkm-pi.com
PUBLICIDAD
Directora comercial: Isabel Gallego
(igallego@mkm-pi.com)
Tel.: 91 632 38 27
Ignacio Sáez (nachosaez@mkm-pi.com)

DEPARTAMENTO DE SUSCRIPCIONES
Tel. 91 632 38 27
Fax.: 91 633 25 64
e-mail: suscripciones@mkm-pi.com
Precio de este ejemplar: 5,75 euros
Precio para Canarias, Ceuta y Melilla:
5,75 euros (incluye transporte)

Impresión
Gráficas Monterreina
Distribución
DISPAÑA
Revista mensual de informática
ISSN: 1135-0407

Depósito legal
B-6875/95

MAYO de 2018
Printed in Spain

EDITA
Publicaciones Informáticas MKM

GDRP: Cumplir para obtener una ventaja competitiva

Por Juan Julián Moreno Piedra
Director de Preventa para el Sur de Europa, Micro Focus

A pocos días de la entrada en vigor de la normativa GDPR en Mayo de 2018, no todas las empresas han tomado las medidas necesarias para adecuarse a la nueva realidad. Uno de los motivos fundamentales es que embarcarse en este proyecto significa de hecho modificar toda la estructura de datos de las empresas y realizar importantes cambios en sistemas y procesos que implican inversiones económicas, y parece que no se adivina un retorno de la inversión para las organizaciones, pero, ¿es esto cierto? ¿qué ventajas se obtienen de la adecuación a la normativa?

Para saber qué ventajas se pueden obtener analicemos cómo se debe afrontar un proyecto de GDPR.

Todo proyecto de GDPR debe comenzar con la realización de una Consultoría Legal en la que se analice cómo afecta la ley a los procesos corporativos y qué cambios hay que implementar, sentando así la bases para estar preparados frente a futuras litigaciones.

A continuación se debe realizar un Análisis de Riesgos y definir medidas y respuestas adecuadas. Esto permitirá a las empresas rediseñar los procesos para buscar eficiencias y ahorros de coste además de evitar cuantiosos daños en su reputación si están protegidas contra posibles brechas.

El siguiente paso es convertir la Consultoría Legal y el Análisis de Riesgos en acciones que se puedan implantar por el departamento de TI, y para ello se necesita una Consultoría Estratégica de IT que analice el estado de madurez tecnológico de las organizaciones y diseñe un roadmap priorizando los proyectos necesarios para poner en marcha el cumplimiento en el plazo de tiempo necesario. Este estudio ayuda a identificar aplicaciones que, conteniendo datos personales, ya no sean y puedan ser retiradas proporcionando grandes ahorros a las organizaciones.

Es en este punto donde entran las compañías que, como Micro Focus, proporcionan las soluciones tecnológicas necesarias en áreas como la seguridad, el gobierno de la información o el archivado, permitiendo la identificación de la información de carácter personal, su protección y securización durante todo su ciclo de vida.

La Implementación de la tecnología se debe realizar usando metodologías ágiles, abordándolo por fases según la priorización que se determinó en la consultoría estratégica, disminuyendo así posibles incidencias y permitiendo demostrar al regulador que se están dando los pasos adecuados para el cumplimento.

En resumen, abordar una iniciativa de GDPR es un proyecto complejo que puede reportar beneficios adicionales muy positivos, como la gestión centralizada del dato, la protección contra demandas, la retirada de aplicaciones obsoletas o la mejora de procesos, además de evitar cuantiosas sanciones del organismo regulador y proteger la imagen pública.

"La empresa, tiene que trazar un plan para cumplir con GDPR"

ESET es una de las compañías que más tiempo lleva informando a sus clientes sobre las consecuencias de no adaptarse a los requerimientos del Reglamento General de Protección de Datos. Hablamos con Carlos Tortosa, responsable de grandes cuentas y desarrollo de negocio de la compañía sobre las consecuencias que puede tener no adaptarse a GDPR y cuál es la propuesta de ESET

¿Qué supone GDPR para la empresa?

Para una gran cantidad de empresas, GDPR supone un cambio sustancial porque al final, el cambio de pasar de la LOPD a la GDPR, significa utilizar una serie de herramientas que cuando se promulgó la LOPD no existían. Además también supone la realización de una serie de cambios a nivel organizativo porque ahora hay que implementar una serie de soluciones y de políticas que tendrán que ser revisadas todos los años. Además hay que tener en cuenta que cuando una empresa implante una determinada política, incluso la Agencia Estatal de Protección de Datos puede pedirnos en cualquier momento pruebas de cómo se está protegiendo la información que maneja una determinada empresa. Los cambios, son por tanto, muchos y muy importantes.

¿Se han adaptado las empresas a GDPR?

Desde ESET llevamos tiempo evangelizando sobre lo que hay que hacer para adaptarse a la GDPR y tengo la sensación de que, a día de hoy, las empresas todavía están bastante perdidas. Tal y como lo veo tengo la sensación de que están esperando a ver qué ocurre a partir del 25 de mayo y cómo va a actuar la Agencia Estatal de Protección de Datos. En general, diría que a 25 de Mayo estarán adecuadas al nuevo Reglamento entre el 25 y el 35 por ciento de las empresas. Además, empresas que hayan empezado a estudiar cómo tienen que adaptarse para cumplir con GDPR, tampoco hay muchas.

Aquí hay que diferenciar, empresas del IBEX 35 o grandes empresas, sí que llevan trabajando en esto desde hace tiempo pero una parte importante del resto de compañías, todavía no lo han hecho.

Aquellas empresas que aún no están adaptadas, ¿todavía están a tiempo?

Con la complejidad que tenemos hoy en día la mayor parte de las empresas en cuanto a gestión de la información y al almacenamiento de la misma y encontrándonos a menos de un mes de que entre en vigor el Reglamento de Protección de Datos, diría que si no se ha hecho nada, va a ser muy complicado que llegue al 25 de mayo con los deberes hechos. Desde ESET hemos hablado con partners de nuestro canal, que han comenzado a trabajar con empresas a principios de año, y van a intentar que sus clientes tengan implementada la política y las soluciones en esa fecha. Pero en menos de un mes es prácticamente imposible que una empresa se adecue al Reglamento, por muy pequeña que sea la empresa.

Quizá, sólo en el caso de un autónomo, que únicamente tiene un par de dispositivos, que lo tiene todo almacenado en local y no tiene nada en la nube, pues en ese caso, posiblemente sí pueda cumplir con GDPR el 25 de mayo, pero en el resto, no.

¿Qué tiene que hacer una empresa que no se haya puesto a ello?

Las empresas creo que, básicamente, están a la espera de ver cómo se actúa en el tema de las sanciones. Lo que tiene que hacer una empresa que todavía no se haya puesto a trabajar en cumplir con GDPR, es, en primer lugar, informarse. Una vez que se ha informado, tiene que darse prisa y posiblemente, tenga que buscar una consultora o una auditora que le diga los paso a seguir y que le haga una implantación que se adapte al Reglamento. Es algo que no se puede hacer a lo loco, no basta con hacer una encriptación de los datos. Las empresas tienen que estar formadas con respecto al tratamiento de los datos porque muchas veces trabajan con información sensible de carácter personal de los trabajadores, de los colaboradores, etc.

Una vez que se ha trazado el plan, hay que buscar las soluciones apropiadas y a la vez adecuar a los trabajadores a que cumplan con ese plan que se ha trazado. Los trabajadores tienen que saber qué implica que se reciba un dato de carácter personal y qué implica que ese dato se almacene en un lugar o en otro.

¿Cuál es la propuesta de ESET?

Nosotros, llevamos mucho tiempo trabajando en esto y lo primero que hemos hecho ha sido informar a las empresas y a nuestros clientes y partners sobre en qué consiste GDPR. A partir de aquí, nuestra aportación se refiere a niveles de soluciones de seguridad, para que la información con la que se trabaja esté cifrada. Para ello contamos con una

Carlos Tortosa,

responsable de grandes cuentas y desarrollo de negocio de ESET

solución, ESET Deslock Encryption, se encarga de cifrar los datos de una forma fácil. Una de sus ventajas es que puede realizar una instalación optimizada lo que reduce el tiempo de puesta a punto a los administradores. Además, por la parte del cliente requiere una mínima interacción del usuario, lo cual mejora el cumplimiento de políticas de seguridad de la información.

Además tenemos una aplicación de doble autenticación, ESET Secure Authentication, que GDPR también dice que se utilice que lo que hace es proteger el acceso a la información.

Sin embargo, creemos, que además de estas dos soluciones, no está de más, tener una solución que permita proteger la gestión de la información a nivel interno.

¿En qué se diferencia la propuesta de ESET de otras similares?

Nosotros proponemos utilizar las soluciones que propone GDPR. Lo que pide el Reglamento es que la información esté protegida y por eso nosotros sugerimos, además, tener una solución DLP que permita gestionar la información internamente y evitar fugas. Evidentemente la competencia también ofrece soluciones similares pero nosotros tenemos el gran valor añadido del soporte especializado e individualizado que ofrecemos.

El RGPD: un cambio de paradigma en la protección de datos

Por Èlia Urgell
Tax Product Manager
Wolters Kluwer Tax & Accounting

La implementación de la nueva normativa europea relativa a la protección de datos es inminente. A partir del próximo 25 de mayo, tanto las instituciones públicas como las empresas privadas que recopilan y hacen tratamiento de datos de personas físicas deberán cumplir con el nuevo Reglamento General de Protección de Datos (RGPD), también conocido por sus siglas en inglés GDPR. Se trata de una nueva normativa que modifica y unifica la legislación vigente en lo referente a la privacidad de los datos personales y a la libre circulación de estos datos entre los Estados miembros con un triple objetivo: reforzar el nivel de protección de los datos, impulsar las oportunidades de negocio y potenciar las garantías de cumplimiento. Pero se trata sobre todo de un cambio de paradigma en la protección de datos, ya que el RGPD transfiere a las empresas el deber de velar por el cumplimiento de esta normativa implementando las medidas técnicas y de seguridad que cada empresa considere adecuadas en función del tratamiento de datos que realice.

Este principio de responsabilidad proactiva por parte de compañías e instituciones es una de las novedades más destacadas y con mayor impacto que introduce el RGPD. Si hasta ahora las empresas tenían claro que cumplían la legislación en materia de protección de datos simplemente aplicando las medidas que ya estaban establecidas en la ley, a partir de la aplicación del RGPD, para hacer efectivo este principio de responsabilidad proactiva, las organizaciones tendrán la obligación de analizar qué datos tratan, con qué objetivos y qué tipo de operaciones de tratamiento llevan a cabo y, a partir de ahí, decidir qué medidas toman y aplican para asegurar su cumplimiento en función de los riesgos detectados y asumidos.

Junto con la introducción de este principio, otra de las modificaciones más importantes del RGPD es la referida al consentimiento, que una vez empiece a aplicarse el Reglamento deberá darse de forma inequívoca, informada y explícita por parte del interesado para cada una de las actividades de tratamiento. Si existiese más de una finalidad para los datos, deberá solicitarse para cada uno de ellas.

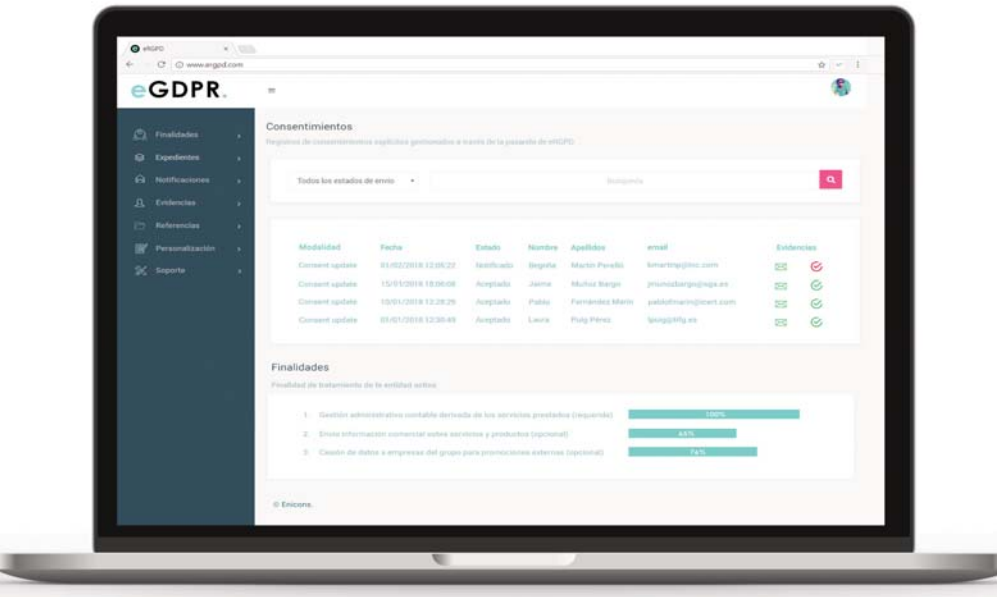
Además, se introducen nuevos derechos para los usuarios, de modo que tengan mayores garantías de evitar que se haga un uso ilícito o inapropiado de sus datos, como el derecho de supresión u olvido, el de la limitación del tratamiento o el de la portabilidad de los datos a otra empresa o país. Asimismo, en el Reglamento se refuerzan las figuras internas encargadas de la seguridad de los datos y del cumplimiento de la normativa, y en algunos casos se exige la existencia de un delegado de protección de datos. Ahora, además, las sanciones previstas por el RGPD se endurecen, con multas que pueden llegar hasta los 20 millones de euros.

UNA OPORTUNIDAD PARA EL CANAL DE DISTRIBUCIÓN

La nueva normativa conlleva cambios por parte de las compañías para adaptarse de forma óptima a los exigentes requerimientos legislativos, a la par que conlleva una actualización o renovación de las aplicaciones de gestión que usan. En este sentido, la aplicación del RGPD es sin duda una oportunidad para el canal de distribución de software de gestión, como lo es cualquier nueva regulación o cambio normativo.

Las novedades que introduce el RGPD hacen imprescindible esta actualización, y en este sentido la oportunidad para el canal que comercializa e implanta software de gestión es clara, no solo por la herramienta en sí, sino sobre todo por los servicios en torno al software que un cambio normativo como el RGPD requiere. Es fundamental para las empresas contar con el acompañamiento en servicios de consultoría y formación, y se trata de un acompañamiento que el canal de distribución puede ofrecer si bien requiere de una elevada especialización jurídica en la materia, más allá de la especialización técnica que el canal ya posee.

Enicons presenta eRGPD Corporate y Sector



Enicons, Electronic Certification Services, presenta su plataforma eRGPD.com en las modalidades de servicio Corporate y Sector

eRGPD Corporate ofrece soluciones específicas para grandes empresas o proveedores de servicios de adecuación al nuevo Reglamento General de Protección de Datos.

Actualización de Consentimientos. Solución para el envío masivo de notificaciones con enlace a formulario interactivo de consentimiento. Para cada respuesta genera acta de consentimiento certificada y fechada.

Evidencias de Información y Consentimiento. Solución de videocaptura certificada de navegación web que permite acreditar el contenido y comportamiento de los formularios de información y consentimiento.

Formulario interactivo de Ejercicio de Derechos. Permite automatizar la recepción y registro de ejercicios de derechos, integrando el proceso de autenticación del solicitante. Se integra con el módulo de notificaciones a responsables del tratamiento.

Módulo de autenticación para ejercicios de derechos. Para aquellas entidades que ya disponen de un proceso de ejercicio de derechos por vía electrónica se ofrece el módulo de autenticación mediante videocaptura certificada de documento identificativo y del propio solicitante.

Las soluciones integradas en eRGPD Corporate pueden ser integradas en los circuitos de información, consentimientos y atención de ejercicios de derechos mediante personalización de la interfaz web de eRGPD o a través de API para integración.

eRGPD Sector es una propuesta de adecuación y cumplimiento del RGPD orientado a PYMES y profesionales independientes. Mediante acuerdos de colaboración con entidades representativas de un sector de actividad o empresas titulares de aplicaciones informáticas verticales, se adaptan los soportes declarativos de actividades de tratamiento y análisis de riesgos y mediante un sencillo formulario interactivo de alta se personalizan estos soportes de forma individual para cada entidad cliente, gestionando las comunicaciones de procedimientos a operadores internos y proveedores responsables del tratamiento.

eRGPD Sector permite ofrecer una solución completa que combina la personalización adecuada para PYMES a muy bajo coste, con las prestaciones avanzadas de notificaciones certificadas, gestión automatizada de ejercicios de derechos y generación de evidencias de consentimiento disponibles en la plataforma eRGPD.

Más información: https://www.ergpd.com/

Solución de gestión de la disponibilidad del dato

Por François Castro, Director General Servicies IT de Grupo Econocom

El próximo año el alojamiento de información relativo a la protección de las personas físicas en Europa, estará sometido a una nueva legislación, más estricta en materia de seguridad y protección de datos, de obligada aplicación en los 28 estados miembros de la UE. El nuevo Reglamento (UE) 2016/679 (RGPD, en siglas en inglés) fue aprobado el año pasado y deberá ser respetado por todas las empresas a partir del 25 de mayo de 2018. A partir de esa fecha, la seguridad de los datos deberá extenderse a todas las fases de diseño y producción de las diferentes acciones comerciales, hasta el punto de que una vulneración de seguridad deberá ser notificada de inmediato a las autoridades y al usuario, en caso de que supongan pérdida de datos y/o si acceden a los datos indebidamente.

Garantizar la disponibiliad de los datos pasa entonces a ser tarea prioritaria en el Departamento de IT ya que la RGPD prevé que el incumplimiento de las obligaciones de los registros de tratamiento lleva aparejadas multas de hasta 10.000.000€ o el 2% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la mayor cuantía.

A nivel técnico, para garantizar la disponibilidad de acceso a los datos hay que controlar dos tiempos para la criticidad del servicio: el RTO (Recovery Time Objective) que es el tiempo necesario para recuperar un servicio que se ha caído y el RPO (Recovery Point Objective), que es el punto en el tiempo en el que recuperamos el servicio y que se corresponde al momento en el que podemos obtener los datos.

Hoy, los datos se clasifican en estructurados consumidos y generados por aplicaciones y que están guardados en formatos ordenados. Y, además, los datos no estructurados que son los generados por los propios usuarios.

Es también importante a nivel técnico la capacidad de certificar el tratamiento del "derecho al olvido" como manifestación del usuario de derechos de cancelación y oposición aplicados a los datos, para impedir la difusión de información personal cuando su publicación no cumpla con los requisitos de adecuación y pertinencia previstos en la normativa. Además se incorporan en la RGPD cambios en la securización de los datos de perfiles, minimización de datos en su tratamiento y en su plazo, nuevas condiciones en cuanto a consentimiento, portabilidad de la información sensible o la duración del período de almacenamiento. Estos son parte de los aspectos regulados que deberán ser tenidos en cuenta y donde los proveedores de aplicaciones y servicios Cloud estarán especialmente expuestos. Por otra parte, el responsable del tratamiento deberá asegurarse que los datos recogidos son los “adecuados, pertinentes y limitados a lo estrictamente necesario en relación con los fines para los que son tratados”.

Toda nueva regulación obliga a las organizaciones a cambiar y esto solamente se puede hacer con las suficientes dosis de planificación e inversión. Además, será necesario construir un nuevo ecosistema de tecnologías y servicios que cumplan con los nuevos requerimientos, nuevos perfiles organizativos que supervisen su cumplimiento y procesos de calidad de la seguridad de la información que soporten controles y auditorías futuras.

Un IT Manager tiene que preguntarse cómo se miden los tiempos de restauración, si se tienen o no, controlados los RTO´s y RPO´s de los modelos de negocio, si se tiene o no, una ruta pensada para gestionar la RGPD, si sabe dónde están los datos sensibles y quién accede a ellos, si se está evaluando quitarse las cintas y/o no tiene mas remedio que continuar con ellas... Desde Grupo Econocom, a partir de nuestra Solución de Gestión de Disponibilidad del Dato damos respuesta a todas estas preguntas y ayudamos a planificar junto al cliente una hoja de ruta. Los objetivos de esta solución consisten en poder ofrecer el dato no estructurado a todos los usuarios garantizando la disponibilidad de los mismos con calidad y poder introducir medidas correctivas en caso de degradación; en un segundo nivel, ayudar a las empresas al cumplimiento de la RGPD. Para ello, habrá que contar con herramientas y/o adecuar las que tenga el cliente de fabricantes premium.

Será muy importante el seguimiento del proyecto desde un punto de vista evolutivo, para revisar el entorno, y también desde un punto de vista proactivo y reactivo. Ninguna de estas soluciones requiere de infraestructura y la forma de pago puede ser plana, para que no implique una inversión inicial.

Una visión holística del esfuerzo y contar con un Partner especializado resulta determinante, aunque otros factores, como nivel de madurez de procesos de la organización y/o la profunda comprensión de la actividad de la compañía junto al conocimiento de la ley, se convierten en elementos clave que, en la mayoría de los casos, marcarán la diferencia.

MICROMOUSE
Soluciones Excelentes

GDPR

Artículo 32

"... se aplicarán medidas técnicas como la encriptación de los datos."

safend
A SuperCom company

no sólo encripta sus datos

No hay éxito de negocio sin adaptación al RGPD

Por Alfonso Ramírez
director general Kaspersky Lab Iberia

Cuando quedan escasos días para la entrada en vigor del nuevo Reglamento de Protección de Datos (RGPD), las empresas necesitan estar ya preparadas para cumplir con los requisitos. Estos requerimientos se traducen en una gran oportunidad para aportar aún más valor a los negocios y para convertirse en un impulso positivo a la salud de la información en las empresas, reforzando la protección de los datos personales a ellos confiados.

Desde el anuncio de la puesta en marcha de este reglamento, muchas organizaciones y entidades de todo tipo han comenzado a trabajar para fortalecer las medidas de protección de datos, sobre todo en lo relativo al almacenamiento y procesamiento de información personal. Sin embargo, muchos directivos han visto esta normativa como algo incómodo. No obstante, lo cierto es que los profesionales de TI consideran que esta nueva legislación les va a dotar de más fuerza en las empresas, según un estudio de Kaspersky Lab de 2017. En concreto, un 63% considera que asegurarán, de esta forma, la protección de la información en las empresas para las que trabajan.

Sin embargo, y de acuerdo a este mismo informe, el 18% de los profesionales TI españoles no creen que sus empresas se hayan adaptado completamente cuando entre en vigor la nueva normativa el 25 de mayo. De hecho, teniendo en cuenta que la seguridad de la información es parte de su responsabilidad diaria, no nos sorprende que los responsables TI estén especialmente preocupados por la adecuada protección de la información personal. Ven amenazas por todos los frentes y son perfectamente conscientes de las posibles repercusiones que una brecha de seguridad puede llegar a tener.

Ante esta situación, se hace necesario que, tanto los responsables de TI como los encargados, establezcan una serie de medidas para demostrar que el tratamiento que hacen sobre los datos es conforme con el nuevo reglamento. En este sentido, es muy importante que mantengan una responsabilidad activa y comiencen a trabajar cuanto antes en el análisis del posible riesgo y operen en base a un registro de actividades. Asimismo, deben ocuparse de la protección de datos desde el diseño y establecer medidas de seguridad desde el inicio para evitar posibles violaciones de seguridad de la información. En caso de que se produzca alguna infracción, es importante notificarla en un plazo máximo de 72 horas y evaluar el impacto que ha tenido sobre la protección.

No debemos olvidar tampoco la concienciación en materia de ciberseguridad. Este punto también es primordial para una buena adaptación al RGPD. En este sentido, la formación de empleados sea cual sea su escala profesional, desde trabajadores a directivos, es necesaria para responder ante incidentes y evitar posibles brechas que pongan en riesgo la protección de los datos.

Para nosotros, la seguridad y la protección de la información es primordial y la razón de ser de nuestra empresa. Por ello, es parte de nuestros valores ayudar tanto a directivos, profesionales TI y empleados, como a organizaciones de distinto ámbito y tamaño, a que entiendan la importancia de la salud de los datos, no sólo de cara al cumplimiento con la normativa, sino también de cara al éxito a largo plazo de la misma empresa.

Zaltor, de la mano de GFI Software, te ofrece soluciones en el área de comunicación y seguridad dirigidas a pequeñas y medianas empresas con el fin de mejorar la seguridad de red, web y correo, así como el control de sitios web gracias a sus funciones de monitorización. Estos productos te ayudarán a cumplir con la ley GDPR, solucionando las vulnerabilidades en tu sistema y red.
Necesidades que cubrirás con la implementación de estas soluciones:

SEGURIDAD WEB Y DESCARGAS FIABLES

GFI WEBMONITOR
Seguridad web, monitorización y control de acceso a Internet. Permite un control y monitorización de las descargas y la navegación web, con motores antivirus, para una excelente protección ante amenazas.
KERIO CONTROL
UTM de Nueva Generación. Incluye firewall y router de red, sistema de detección de intrusos (IPS), antivirus perimetral, VPN y filtro de contenidos y apps.

PROTECCIÓN DEL CORREO ELECTRÓNICO

GFI MAILESSENTIALS
Seguridad y anti-spam para tus servidores de correo. Permite crear y reforzar las políticas de filtrado de contenido para evitar la pérdida de datos.
GFI ARCHIVER
Servidor de archivado para emails, carpetas y entradas de calendario. Minimiza el riesgo legal, permitiendo un archivado en el servidor local del correo y de los documentos en su estado original.

PROTECCIÓN DE PUNTOS FINALES

GFI ENDPOINTSECURITY
Control de acceso y seguridad de los dispositivos de almacenamiento externos. Cifrado y auditoría de archivos.
GFI EVENTSMANAGER
Monitorización activa de red y análisis de logs. Consolida los registros de eventos de toda la red para obtener visibilidad completa de la infraestructura e informes de cumplimiento. Además, puede identificar brechas de seguridad y de datos.

SUPERVISIÓN Y AUDITORÍA DE LA RED

GFI ONEGUARD
Plataforma centralizada de seguridad de red y antivirus empresarial. Protege tu sistema identificando vulnerabilidades e incluye seguimiento de activos.
GFI LANGUARD
Administración de actualizaciones y análisis de vulnerabilidades. También permite analizar el estado centralizado de seguridad de tu red, inventario hardware/software y gestión de parches.

Más información:
www.zaltor.com/gdpr

Panda Adaptive Defense

Control y visibilidad de tus datos personales.

Simplifica el cumplimiento del GDPR

Con la entrada en vigor del GDPR (General Data Protection Regulation), aumentan las exigencias para empresas que manejan datos personales de consumidores europeos. Deberán, no solo proteger su privacidad, sino también controlar cómo se procesan, almacenan y utilizan sus datos. **Panda Adaptive Defense** y su módulo adicional **Data Control**, te ayudarán en el cumplimiento del GDPR.

Descubre y audita

Identifica a los usuarios, equipos o servidores con acceso a Información de Identificación Personal (PII) de tu empresa.

Monitoriza y detecta

Implementa medidas de acceso y operación sobre PII con la ayuda de los informes y las alertas en tiempo real.

Simplifica la gestión

Su activación es inmediata y se gestiona directamente desde la misma plataforma cloud.

Control de datos

Tu empresa tendrá un control exhaustivo de la PII ubicada en sus equipos.

Contacta con tu distribuidor habitual o llamando al

900 90 70 80

panda

pandasecurity.com/business/