Secure &MAGAZINE

Número 2 | Julio 2017

ESPECIAL GDPR

Ransomware: cómo actuar contra este malware

ENTREVISTA

Silvia Barrera

Inspectora jefa de la Sección Técnica de la Policía Nacional

MEDIDAS ORGANIZATIVAS Y TÉCNICAS DE ADECUACIÓN AL GDPR

Cambios en la normativa
Aumento de las sanciones
Sistema de Gestión de la Privacidad

¿Vacaciones? Los ciberdelincuentes no descansan

Secure&IT reconocida como "Mejor Empresa de Seguridad TIC del año"

Secure&IT
www.secureit.es

Editorial

Estimados lectores,

El editorial de este segundo número de la revista ***Secure&Magazine*** empieza con la palabra "incertidumbre". El porqué es sencillo: este es uno de los términos más repetidos en todo lo que se refiere a la implantación del nuevo Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés). Usuarios y, sobre todo, empresas se enfrentan con expectación a los cambios que implica este nuevo modelo de privacidad, que llega de manos de la Unión Europea y que ya ha entrado en vigor (será de obligado cumplimiento a partir del 25 de mayo de 2018).

Para dar alguna pincelada, podemos decir que el RGPD no se limita al cumplimiento de las normas, sino que deja en manos del responsable la adopción de las medidas que considere oportunas para cumplir con él. El aspecto positivo es que no es tan rígido y permite que empresa y norma se adapten. Pero, al contrario que la actual Ley Orgánica de Protección de Datos (LOPD) -que menciona las medidas de seguridad que se deben implantar- el nuevo Reglamento dice qué obligaciones hay que cumplir, pero no explica cómo hacerlo, y esto supone un reto.

La pregunta es: ¿están preparadas las empresas para abordar el nuevo Reglamento General de Protección de Datos? Podemos decir, sin duda, que no. Queda mucho por hacer y, por eso, desde **Secure&IT** recomendamos a las compañías que, si no se han puesto en marcha ya, empiecen a desarrollar un plan de acción para adaptar su forma de trabajar a los nuevos requisitos del RGPD (designar un Delegado de Protección de Datos –DPD-, actualizar las medidas de seguridad para proteger los datos personales según dicta el Reglamento, etc.).

Probablemente, la modificación más importante a la que se deban enfrentar las empresas (y que afectará en su forma de trabajar) tendrá que ver con las medidas de seguridad y con la obtención del consentimiento de los interesados (ya no sirve con el consentimiento tácito o implícito –casillas ya marcadas, aceptación por omisión, etc.-, sino que debe ser explícito). En cuanto a las medidas de seguridad, deberán implantar aquellas que resulten necesarias, basadas en los riesgos a los que estén expuestos los afectados por el tratamiento de sus datos personales. Por tanto, podemos decir que no sirve "reciclar" el documento de seguridad.

La Agencia Española de Protección de Datos ha publicado en su web varias guías (una sobre las novedades y otra específica para los responsables del tratamiento de datos personales) para que el RGPD sea más accesible y fácil de entender. Hay que concebirlas como lo que son: pautas para conformar un sistema de gestión de la privacidad. Por eso, lo mejor para adaptarse al nuevo Reglamento es contar con especialistas en la materia, y no solo del ámbito jurídico: son imprescindibles los expertos en procesos de seguridad de la información y, por supuesto, los técnicos con experiencia. Es la única forma de asegurar que el próximo mayo la empresa cumplirá adecuadamente con la nueva normativa.

De todo lo que rodea al nuevo GDPR (cambios con respecto a la normativa anterior, responsabilidades legales de las empresas ante el nuevo Reglamento, procedimientos y tecnologías necesarias para la adecuación) se habló en nuestra III Jornada de Ciberseguridad: *Seamos prácticos: medidas organizativas y técnicas de adecuación al GDPR*. Por este motivo, hemos decidido convertir esta edición de nuestra revista en casi un especial sobre el nuevo Reglamento General de Protección de Datos.

Pero, no queremos dejar de lado dos incidentes de seguridad que han movilizado al mundo entero, WannaCry y Petya, que también tienen relación con la nueva normativa. A partir del año que viene, las organizaciones o compañías que traten datos de carácter personal estarán obligadas a notificar a la autoridad de control competente cualquier tipo de brecha grave de seguridad que sufran, en un plazo de 72 horas desde que ocurra.

Aprovechamos también la ocasión para reiterar nuestro agradecimiento a los asistentes, patrocinadores y ponentes su participación en nuestra III Jornada de Ciberseguridad.

El equipo de Secure&IT

Sumario

4 Entrevista

Silvia Barrera, inspectora jefa de la Sección Técnica de la Policía Nacional

7 Reconocimiento

Secure&IT reconocida como "Mejor Empresa de Seguridad TIC del año"

8 Medidas organizativas y técnicas de adecuación a GDPR

Cambios en la normativa; aumento de las sanciones; Sistema de Gestión de la Privacidad

18 ¿Vacaciones? Los ciberdelincuentes no descansan

Recomendaciones y consejos para evitar ciberataques

20 GDPR, un serio toque de atención para todos nosotros

Horatiu Bandoiu, ISO 27001 LA y Channel Marketing Manager de Bitdefender

21 Tecnología colaborativa ante la nueva regulación de protección de datos

Fortinet

22 Ransomware: cómo actuar contra este malware

Silvia Barrera

"Los daños que causa una crisis de reputación o un robo de información pueden ser irreversibles. La red no da segundas oportunidades"

Silvia Barrera es inspectora jefa de la Sección Técnica de la Policía Nacional. Trabaja en cibeseguridad desde el año 2007: ha ocupado puestos en ciberinteligencia, redes sociales, cibercrimen y, en la actualidad, forensia digital. También ha participado en grupos de trabajo internacional en Europol e Interpol. Su primer libro *Claves en la Investigación de Redes Sociales* ha sido galardonado con el Premio de la editorial Círculo Rojo 2017 al Mejor Libro de Aprendizaje. Además, siempre que puede, imparte clases y ofrece ponencias y charlas divulgativas con el objetivo de prevenir y enseñar sobre ciberseguridad.

Sueles decir que la realidad siempre supera a la ficción. ¿Crees que la gente es consciente de los peligros de Internet?

Por supuesto que no. No lo son hasta que no lo viven. Son hechos que, como no causan alarma social, ni suelen tener difusión por parte de la víctima, pasan desapercibidos. Hasta que el usuario lo sufre en sus propias carnes y, entonces, comprende hasta dónde pueden llegar las consecuencias de una simple estafa.

¿Hasta qué punto se sorprenderían los usuarios si supieran lo que pasa "detrás"?

Se sorprenderían y serviría de mucho. El motivo por el que yo participo en eventos y hago difusión es precisamente este. No puedo hablar de casos concretos, pero sí advierto a la gente de que hay investigaciones muy dolorosas. Sobre todo, cuesta mucho decirle a una persona que no puedes hacer nada en 72 horas porque, según funciona Internet, no puedes hacer las cosas tan rápido. Es un proceso largo del que, en muchos casos, se desconoce la autoría.

Seguramente los niños dominan más el mundo digital que sus padres. Es un reto al que los padres se enfrentan. ¿Cómo se debe "acompañar" a los menores en este proceso que, a veces, a los padres se les escapa?

Tenemos que ponernos las pilas y hacernos con una cierta base de cómo funciona la Red: conocer que hay unas normas tácitas en cuanto a navegación y que existen unos límites. Y una vez que sepamos cuál es el impacto de la tecnología, hay que tratar de hablar con ellos sobre el tema como algo natural (no criminalizarlo, ni prohibirlo, como solemos hacer con las cosas que desconocemos). Hay que ser conscientes de que va a ser su instrumento de trabajo diario. Es su presente y va a ser su futuro y, por lo tanto, tenemos que guiarlos de forma natural en el uso y estar con ellos, e ir –incluso- descubriendo cosas con ellos.

"Tenemos que ponernos las pilas y hacernos con una cierta base de cómo funciona la Red "

Las redes sociales son utilizadas por todos, mayores y pequeños. Tu primer libro "Claves de la Investigación en Redes Sociales" habla de ellas. ¿Qué papel juegan cuando hablamos de peligros en Internet?

Todos. Por un lado, tenemos el escaneo masivo de red de sistemas, que hacen los cibercriminales para saber cuál es la "salud" de nuestras redes. Por otra parte, hay sistemas vulnerables, para los que existen exploits y códigos maliciosos que se aprovechan de esas vulnerabilidades y que se lanzan de forma masiva. Y, además, está la exposición a las redes sociales, que es un factor más de ataque. Esta última es una vía fundamental –sobre todo cuando hablamos de ataques dirigidos–, porque le damos a los atacantes una información muy valiosa (es una forma de entrada de ataques más sofisticados).

¿Se puede decir que no sabemos utilizar las redes sociales?

Depende de lo que entendamos. Lógicamente, un perfil lo puede hacer todo el mundo, hasta un niño de 5 años. El problema es saber las consecuencias que tiene; entender que las publicaciones tienen un impacto, que hay que tener una estrategia y que no nos valen todas las redes sociales. Una cosa es la posibilidad de usar la tecnología, que todo el mundo la sabe usar, y otra cosa es conocer en qué mundo se mueve y las consecuencias que generan las publicaciones.

¿Qué aspectos debería tener en cuenta una persona antes de publicar en una red o de, simplemente, descargársela o hacerse usuario?

Yo me daría primero una vuelta por Internet. Es necesario hacer búsquedas de esa red social, ver qué tipos de usuarios la tienen y qué comentarios hacen de ella. Es un trabajo laborioso, pero es lo mismo que hacemos cuando compramos un producto: mirar primero si es bueno, las opiniones, etc. En definitiva, hay que hacer un análisis: ver para qué sirve, qué peligros tiene, la configuración de la seguridad, qué rentabilidad le podemos sacar, etc., y luego decidir.

¿Pensamos que somos inmunes a los ciberdelitos?

Sí, porque no los percibimos. Todo lo que no podemos ver de forma objetiva y palpable no lo entendemos como un delito. Apreciamos el miedo cuando está cerca, cuando se ve, cuando nuestros sentidos lo pueden captar. Y la tecnología no se ve, se siente.

Es algo muy nuevo y, además, -de forma errónea- se suele asociar a la víctima con conductas estúpidas, con desconocimiento, con falta de formación… y no es así. Víctimas podemos ser cualquiera, dependiendo de la especialidad y de lo dirigido que sea el ataque.

Muchas veces pensamos que nadie nos va a querer atacar a nosotros. ¿Es uno de los motivos que nos hace caer en la trampa?

Tenemos que entender que pueden querer –simplemente- una foto nuestra, personal, que podemos guardar en nuestro móvil y que puede comprometer nuestra imagen reputacional en Internet.

"Víctimas podemos ser cualquiera, dependiendo de la especialidad y de lo dirigido que sea el ataque "

Acceder a esa información y hacerla pública genera unas consecuencias. Y el hecho de que nos pidan dinero por no publicarla hace que se convierta en una extorsión. Es información que, seguramente, no le interesa a nadie, pero es una forma de sacarte dinero a ti.

Cuando ya nos encontramos ante un delito de estas características. ¿Cómo tenemos que proceder?

Situaciones de ataque se pueden dar de muchos tipos. En el caso de las empresas, se debería de contar con un protocolo estandarizado, igual que lo hay en caso de incendio o terremoto. Es necesario hacer simulacros y ejercicios; contar con unas pautas para los trabajadores. Los empleados necesitan saber cómo actuar en caso de incidentes (si detectamos un empleado desleal, si ocurre un ataque de ransomware, etc.). Reglas sencillas como apagar los ordenadores, desconectarlos de la red, avisar al responsable de seguridad, no conectar dispositivos externos que no sean de uso corporativo, etc., son fundamentales.

Son cosas que se pueden hacer (no cuestan tanto dinero) y que, aunque tienen un periodo de adaptación, son efectivas. Lógicamente, hay que tener presente que es necesario invertir en recursos humanos y técnicos, y ser conscientes de que la vulnerabilidad de la empresa es una parte importante y hay que trabajar en ella.

"Es necesario formar a la gente. La tecnología va muy rápido y tenemos que recibir formación"

¿Y en el caso de los usuarios domésticos? Porque muchas veces no saben ni dónde acudir.

Hay tres creencias erróneas de los usuarios: "Esto no va conmigo", "Esto no me va a pasar a mi" y "Si me pasa lo denuncio y ya está". Pues nada de eso es así. Son tres cosas que no solucionan el problema. Si vas a estar en Internet, o vas a llevar determinadas acciones de intercambio de información, tienes que saber que hay unas normas y protocolos que cumplir para hacerlo de forma más segura. Pensamos que, como Internet ha llegado de esta forma tan rápida y radical, es un mundo sin normas. Tenemos que interiorizar que es una responsabilidad nuestra y que no podemos eludirla. Los daños que causa una crisis reputacional o un robo de información pueden ser irreversibles. La red no da segundas oportunidades.

Igual que los usuarios necesitamos formación en este sentido, ¿también es necesario que los cuerpos y fuerzas de seguridad del Estado se formen?

Por supuesto, hay que seguir formando a la gente. La tecnología va muy rápido y tenemos que recibir formación, por un lado, como simples usuarios que pueden tener conductas de riesgo para la Administración Pública (acceso a webs peligrosas, intercambio de información, uso de aplicaciones inseguras, descarga de ficheros infectados, etc.). Pero, además, nosotros -a nivel policial- tenemos que estar preparados para dar respuestas a las conductas delictivas. Por tanto, no podemos tener la misma formación que un usuario medio. Tenemos que adelantarnos en la búsqueda de soluciones que, a veces, tienen que ser imaginativas y creativas. Lo cierto es que contamos con medidas judiciales, de investigación o el propio Código Penal, pero no tenemos un sitio -en protocolo- que nos diga cómo hay que implementarlo. Por ejemplo, no existen protocolos de cómo rastrear o intervenir bitcoins o de cómo lanzar una botnet; no existe. Como medida, nos debemos formar constantemente y, en este punto, tenemos que colaborar y estar en contacto directo con la empresa privada. En ocasiones las compañías cuentan con tecnología y conocimientos que no tienen las fuerzas y cuerpos de seguridad de Estado, y nos pueden ayudar en este proceso.

https://sbarrera.es/

@sbarrera0

@sbarrera0

Secure&IT reconocida como "Mejor Empresa de Seguridad TIC del año"

Secure&IT ha sido reconocida como "Mejor Empresa de Seguridad TIC del año" en la XI edición de los Trofeos de la Seguridad TIC, concedidos por la revista Red Seguridad. El premio ha sido otorgado en reconocimiento al servicio de Seguridad 360º, a través del cual es posible ofrecer una cobertura completa al cliente: cumplimiento normativo y protección de datos; procesos corporativos de seguridad; seguridad informática y seguridad gestionada (a través del Centro de Operaciones de Seguridad).

En la ceremonia de entrega de los galardones, el director general de **Secure&IT** Francisco Valencia quiso agradecer el premio al jurado y a la organización. Además, apuntó que **Secure&IT** es una empresa especializada en proteger información: "*Nos gusta hacer hincapié en que no somos una empresa de seguridad informática, sino de seguridad de la información. Hace 7 años, tuvimos la idea de combinar derecho y tecnología de la forma más práctica posible, para empresas de cualquier sector y tamaño. Hoy por hoy hemos conseguido trabajar la seguridad 360º, combinando derecho, tecnología, hacking, expertos en procesos y un SOC*".

Don Javier Candau, jefe de Seguridad del Centro Criptológico Nacional (CCN), entregó el galardón a Francisco Valencia, director general de Secure&IT

La seguridad de la información en España

España es uno de los países más ciberatacados del mundo, ocupa el tercer lugar de la lista mundial (Estados Unidos y Reino Unido están en los primeros puestos). Los datos no dejan lugar a dudas: en nuestro país las denuncias por ciberdelitos han crecido un 20% en el primer trimestre de este año, y los ataques a infraestructuras estratégicas del Estado se han multiplicado por siete en dos años. Además, el Instituto Nacional de Ciberseguridad (INCIBE) ha informado de que registró 116.000 incidencias el año pasado.

Las empresas son cada vez más conscientes de la importancia de la gestión de la seguridad de la información, pero todavía queda mucho por hacer. Uno de los primeros pasos es conseguir que los responsables entiendan que las amenazas van más allá de los ciberdelincuentes: empleados descontentos, errores humanos, falta de medidas técnicas, formación insuficiente, incumplimiento legal o competencia desleal son factores a tener muy en cuenta, ya que ocasionan pérdidas a la empresa por lo que, intencionalmente o no, debemos denominar "ciberataque".

El impacto de un ciberataque puede afectar más de lo que pensamos: genera desconfianza, desprestigio, pérdida de datos, fuga de clientes, sanciones por incumplimiento de las normativas o, incluso, dificultad para entrar en ciertos mercados.

Seguridad 360°

A través de la "Seguridad 360°", **Secure&IT** ofrece una cobertura completa al cliente, ayudando a las organizaciones a establecer un Sistema de Gestión de Seguridad de la Información (SGSI), basado en cuatro aspectos fundamentales: la protección de datos y el cumplimiento normativo; los procesos corporativos de seguridad; la seguridad informática, y la seguridad gestionada, a través de un SOC.

De esta manera se puede hacer un seguimiento constante de la empresa; llevar a cabo auditorías en todas las materias (protección de datos, seguridad informática y procesos); establecer un plan de actuación; asegurarse del cumplimiento de la normativa por parte de la compañía; implantar las medidas tecnológicas necesarias; establecer procesos corporativos de gestión de la seguridad; certificar a la organización conforme la norma ISO27001; integrar los sistemas de TI en un Centro de Operaciones de Seguridad y, además, impartir formación continuada.

Seamos prácticos: medidas organizativas y técnicas de adecuación al GDPR

Las empresas españolas preocupadas por cumplir con el GDPR a tiempo

La rápida evolución tecnológica no deja de plantear desafíos. En el ámbito de la Protección de Datos de Carácter Personal, usuarios y empresas se enfrentan a la implantación de un nuevo modelo de privacidad, que viene impuesto por la Unión Europea: el Reglamento General de Protección de Datos (RGPD o GDPR, por sus siglas en inglés). Por este motivo, dedicamos nuestra III Jornada de Ciberseguridad, Seamos prácticos: medidas organizativas y técnicas de adecuación a RGPD, a analizar esta normativa.

En el acto, que fue inaugurado por Silvia Barrera, inspectora jefa de la Sección Técnica de la Policía Nacional, se examinaron los cambios con respecto a la normativa anterior, las responsabilidades legales de las empresas ante el nuevo Reglamento, así como los procedimientos y las tecnologías necesarias para la adecuación al RGPD.

Silvia Barrera: "*La protección de los datos personales no solo debe importar a las empresas por las sanciones que pueda imponerles la Agencia Española de Protección de Datos. Si sufren incidentes relacionados con esta materia, los daños a la reputación pueden ser incalculables. Además, es necesario que trabajen en la seguridad de los usuarios y de los propios trabajadores*".

Según la UE, el Reglamento ha sido adaptado al entorno digital y trata de que los ciudadanos recuperen el control de sus datos (sustituye a la Directiva del año 1995, cuando el uso de Internet no estaba tan extendido). Pero, algunos informes revelan que **casi el 60% de las empresas españolas no cuentan con un plan para afrontar esta nueva normativa**, que ya ha entrado en vigor y que será de obligado cumplimiento en mayo de 2018.

Durante su intervención, Francisco Valencia, director general de **Secure&IT**, recomendó a las empresas ponerse ya a trabajar en la adecuación a la norma, puesto que en mayo del año que viene tienen que cumplir con el RGPD. "***Uno de los principales retos reside en que el nuevo Reglamento de Protección de Datos te dice qué obligaciones tienes que cumplir, pero no cómo hacerlo.*** *Al contrario que la actual Ley Orgánica de Protección de Datos, que sí menciona las medidas de seguridad a implantar*".

Las sanciones aumentan

Con el nuevo Reglamento, las sanciones contra las empresas que incumplan la normativa aumentan. Sonia Martín, directora de Servicios Profesionales de **Secure&IT**, ha explicado que en caso de sufrir, por ejemplo, una fuga de datos, **se prevén multas que pueden alcanzar los 20 millones de euros o un 4% del volumen de negocio** (la cuantía que sea mayor de entre las dos opciones). A esto se suma que las empresas deberán notificar a las autoridades pertinentes las brechas de seguridad, en un plazo máximo de 72 horas, con el consiguiente daño que puede suponer a su reputación.

Entre los aspectos que más preocupan a las compañías se encuentran las evaluaciones de impacto, que tendrán que realizar las empresas cuando traten datos sensibles. Luis Cisneros, *compliance consultant* de **Secure&IT**: "*Este es un análisis de riesgos que deben hacer las compañías y que recoge los daños que pueden afectar a la privacidad de los titulares de los datos. De nuevo, el problema es que el Reglamento nos dice que hay que llevarlo a cabo, pero no nos cuenta cómo hacerlo*".

Según Cisneros, otro de los desafíos que plantea el RGPD es la revisión de los consentimientos. **La aprobación de los usuarios para el tratamiento de datos ya no puede ser tácita, el consentimiento tiene que ser explícito y claro**. Esto significa que ya no servirá que se pongan casillas ya marcadas, o se basen en el silencio o la inacción.

No solo eso, el nuevo Reglamento introduce el "derecho al olvido", esto significa que cualquier persona podrá exigir que su información personal sea eliminada de los proveedores de servicios de Internet cuando lo desee, siempre y cuando quienes posean esos datos no tengan razones justificadas para retenerlos.

José Luis Piñar, catedrático de Derecho Administrativo, abogado y exdirector de la Agencia Española de Protección de Datos, ha sido el encargado de clausurar la jornada y ha explicado que **estamos ante un nuevo modelo, muy anglosajón, que no se centra tanto en el cumplimiento de las normas, como en dejar en manos del responsable la adopción de las medidas oportunas para cumplir con el Reglamento.** La parte positiva, según él, es que no es tan rígido porque se puede adaptar la norma a la empresa y viceversa, pero el problema es que genera más incertidumbre.

Para complementar al Reglamento, se está elaborando la nueva propuesta de Ley Orgánica de Protección de Datos. Piñar, que preside la comisión que ha elaborado la propuesta, comentó que no va a ser una normativa completa y global, puesto que Ley y Reglamento se complementarán.

También participaron en la jornada Samuel Bonete, *Enterprise and Regional sales manager* de la empresa Fortinet; Juan Jesús Merino, *Sales director* de Bitdefender en España; Javier Nieto, *area manager Iberia & Italy* de Flowmon; y Joaquín De La Torre Valentín, *director de desarrollo de negocio* de Sealpath.

Novedades del nuevo Reglamento Europeo de Protección de Datos

Después de 4 años de trabajo, la nueva normativa comunitaria recibió el visto bueno del Parlamento Europeo en abril de 2016. El RGPD, que sustituye a la Directiva de 1995 (momento en el que el uso de Internet no estaba tan extendido), tiene como objetivo ofrecer a los ciudadanos un mayor control sobre su información privada.

Ahora, todos los países de la Unión Europea tendrán una normativa común. Pero, además, cuentan con la posibilidad de desarrollar lo recogido en el RGPD o en aquellos aspectos en los que la nueva normativa guarde silencio. Es decir, cada uno de los Estados tiene potestad para dictar normas sobre supuestos que no se encuentren expresamente previstos en el Reglamento. De hecho, en nuestro país ya se ha presentado un proyecto de ley para la modificación de la Ley Orgánica de Protección de Datos.

Pero, ¿cuáles son las principales novedades a la que se van a enfrentar empresas y usuarios?

1. Entrada en vigor y obligatoriedad

Este es uno de los aspectos más controvertidos y que genera más confusión. El RGPD se aprobó el 27 de abril de 2016 y entró en vigor en mayo de ese año (tras su publicación en el Diario Oficial de la Unión Europea). En ese momento, se produjo la derogación de la Directiva de Protección de Datos de 1995. Pero, **como se trata de una normativa complicada, se ha dado un periodo de dos años para que los afectados puedan adaptarse a los nuevos requisitos.**

Por tanto, **los responsables de tratamiento deberán estar totalmente adecuados a la nueva normativa en mayo de 2018**. A partir de ese momento, será completamente obligatoria y las autoridades reguladoras podrán exigir su cumplimiento.

2. Sujetos obligados y ampliación del ámbito de aplicación territorial

El RGPD es aplicable a los datos de las personas físicas (no de las jurídicas), independientemente de su nacionalidad o residencia. Pero, según el nuevo proyecto de ley, se exceptúan:

- Los tratamientos que lleven a cabo las personas físicas en su ámbito personal o doméstico.
- Los tratamientos que realicen las fuerzas y cuerpos de seguridad del Estado y los juzgados y tribunales, en investigaciones o tareas de prevención del delito.
- Los tratamientos sobre materias clasificadas.

Además, el nuevo Reglamento ha ampliado el ámbito de aplicación territorial. Hasta ahora, estaba dirigido a responsables o encargados del tratamiento de datos (empresas, asociaciones, autónomos o profesionales independientes) establecidos en la Unión Europea. Pero, en la nueva norma se amplía a aquellos no establecidos en la UE que realicen tratamientos a ciudadanos europeos (derivados de una oferta de bienes o servicios o como consecuencia de una monitorización y seguimiento de su comportamiento - siempre que esa monitorización se haga desde la UE-). Esto permite que la normativa sea aplicable a empresas que podían hacer tratamiento de datos de personas en la Unión Europea, pero que se regían por normativas de otros lugares, que no siempre ofrecen el nivel de protección del Reglamento europeo.

3. Obligatoriedad del consentimiento

Con el nuevo RGPD, los titulares de los datos deben aceptar el tratamiento de sus datos personales, mediante una declaración o una clara acción afirmativa. ¿Qué significa esto? Que **se refuerza la necesidad de que las personas den un consentimiento claro**, por lo que ya no sirve hacerlo "por defecto": poner casillas ya marcadas, basarnos en el silencio o la inacción, etc. Además, los términos y condiciones deberán tener un lenguaje sencillo.

Hay que tener en cuenta que el nuevo Reglamento **tiene dos características fundamentales: la privacidad desde el diseño y la privacidad por defecto**. Es decir, los titulares de los datos son los dueños de su privacidad y como tales pueden decidir sobre cada aspecto de la misma: quién, cuándo y cómo se van a tratar sus datos. El término "por defecto" hace referencia a que, en caso de silencio, se entiende como NO prestado el consentimiento.

En cuanto a la gestión de las finalidades (el uso que se va a dar a los datos), **es obligatorio que cada finalidad adicional (por ejemplo, el envío de comunicaciones comerciales es una finalidad adicional a un contrato de compra *online*) se encuentre claramente separada y tenga su propia aceptación.**

Por cierto, en todos los casos, el responsable del tratamiento debe ser capaz de demostrar que se ha obtenido ese consentimiento.

3.1. Consentimientos previos a la entrada en vigor del RGPD

Uno de los aspectos que está provocando mayor debate es la forma en que **se van a regular los consentimientos anteriores a la entrada en vigor de esta normativa**. En este sentido, el nuevo RGPD es tajante: **si el consentimiento no se encontraba claramente identificado o se basó en formas tácitas o por omisión, deberá volverse a solicitar**. Habrá que tenerlo muy en cuenta porque, según el nuevo proyecto de ley, el tratamiento de datos sin el consentimiento de los usuarios se entiende como una infracción muy grave.

4. Tipología de los datos personales

En la nueva normativa **desaparecen los tres niveles de seguridad** (básico, medio y alto). **Se sustituyen por una categoría general y por lo que han denominado "categorías especiales de datos".** A las categorías especiales ya recogidas (origen étnico o racial, opiniones políticas, etc.), se han añadido otras como el tratamiento de datos genéticos o los datos biométricos.

5. Derechos de los afectados

La normativa anterior ya reconoce los derechos ARCO (acceso, rectificación, cancelación y oposición). Con el nuevo Reglamento, se refuerza el derecho de acceso (hay que facilitar copia de los datos objeto del tratamiento) y **se añaden dos nuevos: el derecho a la portabilidad y el derecho al olvido.**

- Derecho a la portabilidad: se prevé la posibilidad de transmitir los datos de un responsable a otro, de forma que, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible. Por ejemplo, si un usuario quiere cambiar de prestador de servicios de correo electrónico o de telefonía, podrá solicitar el cambio de uno a otro, sin perder sus contactos o sus antiguos mensajes.
- Derecho al olvido: El nuevo Reglamento establece que cualquier persona tendrá derecho a que su información personal sea eliminada de los proveedores de servicios de Internet cuando lo desee, siempre y cuando quien posea esos datos no tenga razones legítimas para retenerlos. Además, esa empresa u organización deberá remitir la petición al resto de entidades que puedan haber replicado los datos.

El procedimiento, para que los usuarios ejerzan estos derechos, debe estar visible (en las webs o los documentos que acrediten el consentimiento), ser accesible y tener un lenguaje sencillo. Además, la presentación de solicitudes tendrá que ser posible a través de medios electrónicos.

6. Registro de actividades de tratamiento

Se ha eliminado la necesidad de notificar los ficheros ante las distintas autoridades nacionales de protección de datos (en el caso de España, el Registro General de la Agencia Española de Protección de Datos) y se ha cambiado por lo que el nuevo Reglamento ha definido como "Registro de actividades de tratamiento". Este registro se llevará a cabo de forma interna y, entre otros aspectos, contendrá: nombre y datos de contacto del responsable; nombre y datos del Delegado de Protección de Datos; finalidades del tratamiento; descripción de categorías de interesados y de datos tratados; y, en su caso, las transferencias internacionales de datos.

7. El Delegado de Protección de Datos

La figura del Delegado de Protección de Datos (DPD o DPO por sus siglas en inglés) no es siempre necesaria, aunque se considera recomendable. Pero, es obligatoria en estos casos:

- Si el tratamiento lo lleva a cabo un organismo público.
- Si las actividades del responsable o encargado consisten en operaciones que requieren una observación habitual y sistemática de los interesados a gran escala (por ejemplo, videovigilancia).
- Si las actividades del responsable o encargado consisten en el tratamiento a gran escala de categorías especiales de datos (por ejemplo, los datos de salud en un hospital).

Se van a revisar los consentimientos anteriores al RGPD. Si el consentimiento no se encontraba claramente identificado o se basó en formas tácitas o por omisión, deberá volverse a solicitar.

El DPD deberá contar con los conocimientos necesarios en derecho y protección de datos (aunque no tiene por qué ser jurista). Además, actuará de forma independiente (puede ser una persona física o jurídica, interna o externa) asesorando, informado y supervisando el cumplimiento del RGPD.

8. Análisis de riesgos y evaluación de impacto

Una de las principales novedades del RGPD es la realización de un análisis de riesgos, relativo al tratamiento de datos. El análisis tiene dos vertientes: los riesgos que existen para la propia organización (interno) y los riesgos que existen para los derechos y libertados de los ciudadanos.

El tipo de análisis variará en función de: los tipos de tratamiento; la naturaleza de los datos; el número de interesados afectados; y la cantidad y la variedad de tratamientos que lleve a cabo una misma organización.

El análisis deberá llevarse a cabo utilizando alguna de las metodologías existentes (ISO 31000, ENS, ISO27001, ISO 27018), por lo que **la protección de datos pasa a configurarse como un Sistema de Gestión de la Privacidad.**

Además, los responsables deberán realizar una Evaluación de Impacto en Protección de Datos (EIPD) antes de la puesta en marcha de aquellos tratamientos que conlleven un alto riesgo para los interesados, o traten categorías especiales de datos (tratamientos a gran escala de datos sensibles, observación a gran escala de una zona de acceso público, etc.).

9. Medidas de seguridad

Las medidas de seguridad **deberán confeccionarse con el objetivo de corregir aquello que se detecte en el análisis de riesgos, y tienen que ser aplicadas por el responsable antes de iniciar el tratamiento.**

Estas medidas pueden ser de carácter organizativo (políticas corporativas, procedimientos internos, etc.) o técnico (cifrado, controles de acceso, *backups*, etc.). Su finalidad es garantizar que solo se traten los datos necesarios y que se respeten los periodos de conservación y la accesibilidad de los datos.

Otra de las novedades (una de las más importantes) es que se deberán notificar las "violaciones de seguridad de los datos". Es decir, el responsable de tratamiento deberá notificar a la autoridad competente (en nuestro caso la AEPD) cualquier brecha de seguridad que se haya producido, en un plazo de 72 horas desde que ocurra (incluyendo en la notificación las medidas adoptadas para solventar el problema). Además, si la brecha implica un riesgo para los interesados, también se les deberá notificar a ellos.

10. Transferencias internacionales

Los datos solo podrán ser comunicados fuera de la UE en tres casos: si es a países o territorios a los que la Comisión reconoce un nivel adecuado; si se otorgan las garantías adecuadas sobre las medidas de seguridad; atendiendo al interés del titular de los datos o a intereses generales.

11. Las autoridades de protección de datos

La nueva normativa sigue manteniendo la existencia de los diferentes reguladores nacionales y sus funciones. Pero, ahora estarán coordinados por un organismo dependiente de la Comisión Europea: el Comité Europeo de Protección de Datos.

Pero, el RGPD establece novedades:

- Para los titulares de los datos se establece un sistema de ventanilla única. Es decir, en caso de que tengan que hacer reclamaciones dentro de los Estados miembros, podrán acudir ante la autoridad de su país.
- Los responsables y encargados de tratamiento, que tengan centros en diversos Estados miembros, podrán centralizar la organización de su Sistema de Gestión de la Privacidad en un único país (estableciendo una autoridad de control principal).

Las sanciones por incu
normativa de Protección

La Agencia Española de Protección de Datos tiene potestad para sancionar a organizaciones y particulares que incumplan la normativa de Protección de Datos de carácter personal. En la actualidad, estas sanciones están divididas en tres niveles: leves, graves y muy graves, y pueden oscilar entre los 900 y los 600.000 euros (por cada dato mal tratado).

El nuevo Reglamento General de Protección de Datos mantiene el poder sancionador de la Agencia, pero –además– endurece las multas. **A partir de mayo de 2018, las sanciones cambian y aumentan considerablemente.**

MAYOR CUANTÍA

10.000.000 € ó 2% volumen negocio total anual del ejercicio financiero anterior

- **Falta de obtención del consentimiento paterno cuando se ofrecen servicios de la sociedad de la información a menores sin capacidad de consentir.**
- **Falta de implementación de medidas de seguridad apropiadas.**
- **No realización de una evaluación de impacto relativa a la protección de datos cuyo tratamiento entrañe elevado riesgo o, en su caso, no realizar la consulta previa a la Autoridad de Control.**
- **No designar un Delegado de Protección de Datos, cuando se requiera.**
- **Falta de cooperación con la Autoridad de Control.**
- **Incumplimiento de las obligaciones por parte del encargado del tratamiento.**
- **Incumplimiento de las obligaciones como corresponsables.**
- **No cumplir con las obligaciones impuestas a los organismos de certificación: comunicación del otorgamiento o retirada de las certificaciones a las empresas, incumplimiento de las condiciones de acreditación, etc.**
- **No notificar las violaciones de seguridad:**

  √ **¿Cuáles? Las que supongan riesgo para los derechos y libertades de los titulares. Incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Ejemplos:**

  - **pérdida de un ordenador portátil,**
  - **acceso no autorizado a bases de datos de una organización (incluso por su propio personal) o**
  - **borrado accidental de algunos registros.**

  √ **¿A quién? A la Autoridad de Control. Y a los titulares si la brecha implica alto riesgo para los derechos y libertades de los titulares.**

Si ello requiere esfuerzos desproporcionados: medida alternativa → comunicación pública

√ **¿Cuándo? En el plazo de 72 horas.**

Derecho a la no auto incriminación: no confesión de culpabilidad sino cumplimiento

mplimiento de la
de Datos aumentan

Ya no estarán tipificadas en niveles, sino que se separarán en dos rangos, dependiendo de los artículos del Reglamento que las contengan. Las más bajas serán de 10 millones de euros o el 2 por ciento del volumen negocio total anual del ejercicio financiero anterior (la cifra que sea de mayor cuantía). Las más elevadas ascenderán a 20 millones de euros o el 4 por ciento del volumen de negocio total anual de ejercicio financiero anterior (también la que sea de mayor cuantía entre las dos).

El nuevo Reglamento incluye, además, la posibilidad de que los Estados miembros asocien las infracciones y sanciones administrativas con sanciones penales. Por lo que, aquel que cometa algún tipo de incumplimiento de este tipo, puede verse penalizado también por la vía penal (cada Estado miembro será el encargado de establecer esta regulación). Y lo mismo ocurrirá con la regulación del ámbito laboral.

Como decíamos, el RGPD recoge una serie de conductas susceptibles de ser sancionadas administrativamente, pero no están categorizadas. A pesar de eso, podemos extraer algunos ejemplos.

MAYOR CUANTÍA

20.000.000 € ó 4% volumen negocio total anual del ejercicio financiero anterior

- **Falta de cumplimiento de los principios básicos del tratamiento: licitud, fines explícitos y legítimos, adecuados y pertinentes, etc.**
- **No atender o no facilitar el ejercicio de los derechos ARCOPO de los interesados:**
  - Acceso, rectificación, cancelación y oposición;
  - Portabilidad → transmitirlos a otro responsable y
  - Olvido → supresión.
- **Incumplimiento de las normas del Estado Miembro.**
- **No permitir acceso a la Autoridad de Control a datos personales y/o locales para el ejercicio de sus poderes de investigación.**
- **No cumplir una orden de la Autoridad de Control en el ejercicio de sus poderes correctivos.**
- **Incumplimiento de los requisitos para transferencias de datos personales a terceros países u organizaciones internacionales.**
- **No informar a los interesados en el momento en el que se obtengan su datos.**
- **No contar con el consentimiento explícito del interesado.**
- **Incumplimiento del deber de secreto.**
- **Transferencia internacional de datos a un tercer país u organización que no ofrezca garantías adecuadas.**

El DPO debe tener unos conocimientos precisos en materia de protección de datos

Decálogo para establecer un Sistema de Gestión de la Privacidad

1. Identificar y registrar el sistema de tratamiento de datos pretendido

El registro de ficheros ante la AEPD ha desaparecido. Se ha cambiado por lo que el nuevo Reglamento ha definido como "Registro de Actividades de Tratamiento". Se llevará a cabo de forma interna y lo gestionará el responsable del tratamiento. Este registro debe contener: todos los datos que se traten en la organización; el lugar de almacenamiento; las empresas que acceden a él; si está subcontratada alguna parte de la gestión del mismo; las cesiones; si hay transferencias internacionales, etc.

Si en el fichero se tratan datos con un nivel especial de protección, se deberá llevar a cabo una "evaluación de impacto para los datos personales", teniendo en cuenta los perjuicios que pueden ocasionarse a los afectados (personas físicas titulares de los datos). En determinados casos será necesario solicitar autorización a la AEPD.

2. Nombrar un Delegado de Protección de Datos

Siempre que se traten categorías especiales de datos, y bajo otra serie de circunstancias (como el tratamiento indiscriminado o a gran escala de datos personales), será obligatorio nombrar a un Delegado de Protección de Datos (DPD o DPO por sus siglas en inglés). Está figura debe tener unos conocimientos precisos en materia de protección de datos y, además, debe contar con cierta independencia y responsabilidad en cuanto al ejercicio de sus funciones.

Dentro de esas laborales de nombramiento, es recomendable la adscripción a determinados códigos de conducta sectoriales, que ayuden a un mejor cumplimiento de las obligaciones establecidas en esta normativa.

3. Presentar información y pedir consentimiento al interesado

Un aspecto fundamental dentro de la nueva normativa, que será la base legal de la mayoría de los tratamientos, es el consentimiento del afectado. El nuevo Reglamento tiene dos características fundamentales: la privacidad desde el diseño y la privacidad por defecto. Es decir, los titulares de los datos son los dueños de su privacidad: pueden decidir sobre cada aspecto de la misma y, también, qué uso se va a dar a sus datos. El término "por defecto" hace referencia a que, en caso de silencio, se entiende como NO prestado el consentimiento.

La gestión de las finalidades (el uso que se va a dar a los datos) también tiene mucha importancia. Es obligatorio que cada finalidad adicional (por ejemplo, el envío de comunicaciones comerciales) se encuentre claramente separada y tenga su propia aceptación. No sirve que se haga por defecto (que pongamos casillas ya marcadas o nos basemos en el silencio o la inacción). La nueva normativa refuerza la necesidad de que la persona dé un consentimiento claro y afirmativo.

4. Realizar acuerdos contractuales con terceros encargados del tratamiento

Igual que con la anterior normativa, las relaciones con los encargados del tratamiento tienen que encontrarse reguladas por un contrato. Podemos hacerlo de dos formas: subcontratando un servicio para minimizar un riesgo o imponiendo al encargado del tratamiento unas medidas propias de seguridad.

Además, se facilita la transferencia internacional de datos. Deja de ser necesaria la autorización del director de la AEPD, siempre que se firmen las cláusulas contractuales tipo aprobadas por la Comisión Europea.

5. Realizar análisis de riesgos, para el interesado, ante la pérdida de confidencialidad, integridad o disponibilidad de sus datos (Magerit, ISO 31000, etc.)

Para saber cuáles son las medidas de seguridad que es necesario aplicar a los diversos tratamientos, hay que analizar los riesgos que pueden afectar a la organización y a los usuarios. Una vez analizados, hay que imponer medidas de seguridad y control que permitan reducir los niveles de riesgo detectados.

6. Selección de controles adecuados, comparar con un marco de controles (ISO 27002, ISO 27018, COBIT, etc.)

Una forma de establecer los controles más adecuados para reducir el riesgo es acudir a las diversas metodologías y estándares, que ya existen en el mercado, y aplicarlos al tratamiento. No solo se pueden utilizar para calcular el riesgo, sino que también es posible hacer una selección de controles específicos, que nos ayuden a establecer un marco adecuado y homogéneo. Además, al ser estándares de mercado, todos los clientes podrán conocer el nivel de cumplimiento y compromiso de la organización, con respecto a los datos personales.

7. Implantación de las medidas técnicas y organizativas resultantes del análisis de riesgos

La aplicación de los controles se traduce en imponer ciertas medidas, de cara a ofrecer un nivel de seguridad que garantice la protección de la información:

- Medidas organizativas: políticas y procedimientos internos, derechos y obligaciones de los empleados, custodia y mantenimiento de la documentación, etc.
- Medidas técnicas: control de accesos, criptografía, seguridad física, comunicaciones, continuidad de negocio, etc.

8. Monitorización, vigilancia continua del sistema continua

Es importante el control del sistema de forma continua, porque una de las obligaciones que impone la nueva normativa es que se notifiquen las brechas de seguridad en el plazo de 72 horas (desde que se produzcan). Se debe notificar la incidencia a la AEPD, junto con la solución que se ha tomado. Además, en el caso de que se vean afectados datos con un nivel de protección especial, también deberá comunicarse a los usuarios perjudicados.

9. Auditoría del sistema

Todos los sistemas de gestión deben ser regularmente reevaluados, según los criterios que establezca la organización. El objetivo es analizar el nivel de cumplimiento o, en su caso, las desviaciones que se hayan producido. De estas auditorías salen las oportunidades de mejora y el análisis de vulnerabilidades del sistema.

10. Certificación del Sistema de Gestión de Privacidad

Es algo voluntario pero muy recomendable. El hecho de que un tercero imparcial establezca que el sistema de gestión es seguro ofrece garantía a los potenciales clientes y usuarios de nuestros servicios. En este caso, la normativa comunitaria no impone la necesidad de auditoría, aunque sí es recomendable de cara a una mayor transparencia y seguridad.

¿Vacaciones?
Los ciberdelincuentes no de

Recomen

¡DESCONFÍA!

- **Comprueba que los proveedores son fiables** y las páginas, en la que hagas los trámites, seguras (verifica sus datos de contacto, el servicio de atención al cliente, el aviso legal y las políticas de privacidad).
- **Debes estar atento.** Lee con detenimiento los contratos. A veces, la letra pequeña esconde "extras" que no tenías previstos.
- **Cuidado con los correos fraudulentos.** Es una época perfecta para hacer ataques de phishing. No abras correos sospechosos, ni accedas a links o descargues archivos poco confiables.
- **No hagas compras en ordenadores públicos.** No conviene introducir nuestros datos personales (más si son bancarios) en dispositivos de lugares públicos.

ACTUALIZA Y PROTEGE TUS DISPOSITIVOS

- **Instala todas las actualizaciones.** De esta forma eliminamos las brechas de seguridad.
- **Instala un software de seguridad**. No solo en el ordenador, también en el resto de dispositivos (smartphones o tablets).
- **Haz copias de seguridad.** En vacaciones estamos más expuestos, por eso es muy importante hacer copias de seguridad.
- **Cifra la información más sensible.** De esta forma evitarás accesos no autorizados.

escansan

daciones

LA PREVENCIÓN ES FUNDAMENTAL

- **Cuidado con la información que das en redes sociales.** No reveles tu ubicación, ni des a conocer que tu casa está vacía.
- **Evita los correos de respuesta automática** en los que ofrezcas más información de la necesaria cuando estés de vacaciones.
- **Envía el correo no deseado a la papelera**. Si abres uno de estos mails, estás indicando a su remitente que la cuenta está activa.
- **Cuidado con las wifi gratuitas.** Asegúrate de que la red es fiable antes de conectarte y permanece conectado el menor tiempo posible.
- **Deshabilita las conexiones cuando no las necesites.** Es el caso del GPS, el wifi o el Bluetooth.
- **Activa la contraseña de tu teléfono o tablet.** De esta forma, será más difícil para los ladrones poder utilizar tus dispositivos.
- **Acuérdate de cerrar sesión**, especialmente cuando te conectes desde dispositivos que no son tuyos.
- **Protege a los menores cuando usen Internet.** En vacaciones, los más pequeños suelen utilizar más los dispositivos móviles. ¡Presta atención!

GDPR, un serio toque de atención para todos nosotros

Tengo que confesar desde el principio que esta opinión reflejará dos perspectivas: la de auditor y profesional de seguridad, por un lado, y la de fabricante de soluciones de seguridad que incluyen características de privacidad y confidencialidad.

Una vez hecha la confesión, entremos directamente en el asunto: el 25 de mayo de 2018 será de obligado cumplimiento el nuevo Reglamento Europeo de protección de Datos; la versión revisada y actualizada que genera un marco unitario para el tratamiento de la protección de datos en todos los países UE.

Aparte del interés que genera para los legisladores, que tienen que alinearse al GDPR y a los organismos de control que se van a crear, el nuevo reglamento es importante para el gremio de consultores y auditores porque está generando mercado para nuevos servicios. Además de la burocracia y el papeleo que va a introducir, todos los involucrados **esperamos que el nuevo Reglamento genere una oportunidad nueva para las empresas privadas y las organizaciones públicas de tomar en serio el tratamiento de datos de sus usuarios, empleados y proveedores**. Es un reto, pero igualmente es una gran oportunidad para: hacer un análisis serio a los procesos de negocio (artículos 44-50); ver cómo se generan, procesan y transmiten los datos privados y empezar a tomar medidas para su protección -que esperemos vayan un paso más allá de la designación de un Data Protection Officer- (art. 37-39); y para mantener un registro.

Y, si hacen este análisis, por qué no ir un paso más allá, examinando los procesos internos y actividades, desde la perspectiva de la seguridad, pensando en implantar un sistema de gestión (o al menos hacer un análisis de los riesgos de seguridad e implementar controles para disminuirlos a un nivel adecuado).

No todo lo relativo a la seguridad de la información significa tecnologías y costes extra, muchas veces las medidas organizativas son más eficientes que muchos productos. Además, el GDPR insiste en la necesidad de la formación del personal en su artículo 39. Por eso, un programa de *Security Awareness* puede reducir muchos riesgos, además de involucrar y preparar al personal en la protección de los activos informacionales.

Desde la perspectiva de un fabricante de seguridad innovador, que ha hecho de la protección de la experiencia digital su misión, ponemos muchas esperanzas en la implantación correcta y coherente del GDPR. Creemos que la gente se tomará aún más en serio la responsabilidad de proteger sus sistemas, infraestructuras y organizaciones con soluciones modernas y eficaces, sin dejar al azar los datos de los clientes o empleados. Confiamos en que los presupuestos reflejen esta necesidad, si no por impulso interno, al menos por el temor a las multas que se anuncian importantes (por no hablar de los daños de imagen asociados).

Anticipamos que muchas empresas van a pensar de nuevo sus procesos, y **es posible que este Reglamento sea un impulso determinante para la adopción de la transformación digital y la consolidación de los datos en *datacenters* y en la nube**. Como proveedor destacado de seguridad para el *datacenter* moderno, *hyperconvergence* y la nube híbrida, esperamos ser partícipes de esta evolución, porque sabemos que podemos aportar valor y una seguridad eficaz.

La obligación de informar sobre las incidencias que afectan la confidencialidad de los datos (art. 33,34, Rec. 85-88) supondrá que muchas organizaciones "discretas" deban informar de sus brechas de seguridad y cooperar con las autoridades y la industria. Pero, lo más importante es que tendrán que tomar precauciones que hoy en día descartan. Lo hacen porque, actualmente, si ocurre una incidencia nadie les obliga informar de que ha pasado algo grave. Tomemos como ejemplo las incidencias del último año, culminando con WannaCry, cuando empresas grandes han negado haber sufrido ataques o que los datos de sus clientes y empleados hayan sido secuestrados o extraídos.

Aparte de esto, esperemos que la responsabilidad de poner medidas para proteger los datos impulse a los consejos de administración a pensarlo dos veces cuando rechazan proyectos de inversiones necesarias en infraestructuras de seguridad (art. 32).

Quiero añadir una tercera perspectiva, la de usuario conectado y con sus datos en posesión de gigantes como Google, Apple o Facebook. Me alegro de que finalmente estas empresas súper poderosas, que controlan no solo nuestros datos sino también nuestras vidas digitales – con sus proyectos de correlación avanzada de Big Data–, nos tengan que tomar en serio cuando les pedimos que controlen a quién revelan nuestros datos y cómo influyen en nuestras decisiones.

Horatiu Bandoiu,
ISO 27001 LA
Channel Marketing Manager de Bitdefender

Tecnología colaborativa ante la nueva regulación de protección de datos

La continua digitalización y globalización de nuestra economía depende, cada vez más, del control y procesamiento de los datos personales. Nos enfrentamos a una cuestión que, por un lado, supone enormes oportunidades para el negocio pero que también **implica una creciente conciencia pública y preocupación por la importancia de la protección de los datos personales**.

Según algunos estudios, más de la mitad de los consumidores dijeron que habían abandonado el proceso de compra online debido a problemas de privacidad. Otra de las conclusiones es que menos del 10% de los entrevistados aseguró sentir el control sobre la forma en que las organizaciones gestionaban y usaban sus datos personales.

El Reglamento General de Protección de Datos de la Unión Europea (GDPR) responde a esta preocupación. Reconociendo el valor de tales datos, la nueva reglamentación impone un costo a su recogida, almacenamiento y uso, haciendo responsables a las organizaciones de su protección y obligándolas a devolver el control y la propiedad al individuo.

El GDPR se aplica a cualquier organización, de cualquier país, que recopile, almacene o procese los datos personales de los residentes de la UE. Estos datos pueden ser de empleados, socios comerciales o clientes potenciales y clientes. En la terminología de la regulación, estas organizaciones se definen como "controladores", que determinan cómo y por qué se procesan los datos personales, o "procesadores", que actúan en nombre del controlador. Ambos tienen obligaciones que deben cumplir y pueden enfrentarse a sanciones en caso de incumplimiento.

Dado el cambiante panorama de amenazas, garantizar un nivel de recursos e innovación puede ser complicado para una empresa o incluso para el gobierno nacional.

Parte del problema proviene de la forma en que ha evolucionado la ciberseguridad: la multiplicidad de vectores de ataque demanda soluciones específicas que guardan escasa o nula interacción con el resto de la infraestructura de seguridad. En este contexto, se complica la gestión y se producen lagunas e incoherencias en la respuesta a las nuevas amenazas, especialmente en un entorno multiproveedor.

El desafío se ve agravado por la adopción de tendencias como la movilidad, el *cloud computing* y el IoT, que amplían la superficie de ataque efectiva, exponen las redes a nuevas vulnerabilidades y erosionan el concepto tradicional de perímetro de red.

Aunque el cumplimiento del GDPR no es algo que solo se pueda lograr con la tecnología, la seguridad de la red es un primer paso esencial. Para reducir la exposición a las implicaciones que pueda provocar una violación grave de datos, es necesario minimizar tanto el número de intrusiones en la red como el tiempo de detección. Y es aquí donde estamos trabajando desde Fortinet, apostando por un enfoque en el que todos los componentes clave de la infraestructura de seguridad conforman una arquitectura sin fisuras.

La arquitectura *Fortinet Security Fabric* ofrece una respuesta única a los retos de proteger las actuales redes caracterizadas por su complejidad, un perímetro desdibujado y un elevado ancho de banda.

Las soluciones de seguridad que planteamos para responder a las exigencias de la GDPR están basadas en una seguridad escalable e interconectada, combinadas con una alta conciencia, inteligencia de amenazas y estándares de API abiertos, que permitirá ofrecer la protección automatizada extremo a extremo demandada por las organizaciones para sus entornos físicos, virtuales y en la nube.

FORTINET

Ransomware: cómo actuar contra este malware

Probablemente, hace apenas unos meses la mayoría de los usuarios no había oído la palabra *ransomware*. Pero, los acontecimientos han hecho que eso cambie. Dos ciberataques, WannaCry y Petya, han puesto en jaque al mundo y han conseguido dar visibilidad a un problema contra el que luchan las empresas de ciberseguridad desde hace años.

Los ciberdelincuentes utilizaron algunas vulnerabilidades de Microsoft para cifrar equipos de grandes compañías y gobiernos en cientos de países, bloqueando los archivos y exigiendo un rescate en *bitcoins*. En el caso de WannaCry, el *ransomware* establecía una conexión con un servidor de Internet (su creador) antes de actuar y un dominio que fue introducido en una *blakhole*-DNS (filtro de internet), consiguió su desactivación; no ha sido el caso de Petya que, aunque ha sido firmado por los fabricantes antimalware, sigue activo.

Como siempre, los parches no solucionan de forma definitiva el problema, habrá nuevas modificaciones, nuevas versiones y nuevo malware, así que no podemos bajar la guardia.

Como regla general, conviene mantener los equipos actualizados, realizar copias de seguridad de los ficheros, no abrir ficheros descargados de internet o recibidos por correo de fuentes no confiables. Pero, estos ataques suelen ser consecuencia de la combinación de varios factores:

- **Envío masivo de SPAM**
- **Ingeniería social, que consigue que algunos usuarios abran un fichero desconocido**
- **Malware del tipo *ransomware***
- **La explotación en forma de "gusano" de una vulnerabilidad Microsoft**

¿QUÉ DEBEMOS HACER?

- **Contra el SPAM:**

√ Disponer de sistemas *antispam* y *antimalware* en el perímetro de la red, de modo que se minimice la probabilidad de que este tipo de correos lleguen al usuario. Independientemente del sistema de correo empleado (incluso en sistemas *cloud*), la seguridad no está garantizada. Es necesario buscar medidas adicionales de seguridad en el correo electrónico.

√ Lo ideal es disponer de una plataforma de *antispam* dotada de *sandbox*, que ejecutará los ficheros sospechosos antes de que lo haga el usuario, reduciendo notablemente estas amenazas.

- **Contra la ingeniería social**

√ Formación, formación, formación y concienciación, concienciación, concienciación.

√ ¿Qué parte de "si no sabes lo que es, no lo abras" no entiendes?

√ En Internet, si algo es gratis, es que el producto eres tú.

- **Contra el *ransomware***

√ Disponer de un *antimalware* actualizado.

√ Elegir de entre los fabricantes de antivirus aquellos que aporten una protección específica contra *ransomware*, APT o amenazas desconocidas. Dada la variabilidad de los *ransomware*, el mero filtrado en base a firmas no siempre es suficiente.

√ Asegurar la existencia de una política de copias de seguridad, probada y con la periodicidad adecuada. En caso de infección, bastará con restaurar los ficheros.

√ El sistema no debería poder acceder a los ficheros de copia de seguridad ya que, en caso de infección, podrían cifrarse tanto los ficheros originales como sus copias. Es necesario desconectar el disco al acabarla copia, o hacerlo mediante protocolos que no impliquen crear unidades Microsoft (como FTP).

• Contra las vulnerabilidades de Microsoft

√ Activar firewall personal en todos los ordenadores y servidores basados en Windows.

√ Desactivar, siempre que no sean imprescindibles, las opciones de "Uso compartido de archivos e impresoras para redes Microsoft" de tus tarjetas de red. Si compartes impresoras o ficheros, basta con desmarcar esta opción.

√ Asegurar que el servidor o el ordenador estén actualizados, y mantener una política de actualización adecuada.

√ Segmentar la red, creando zonas aisladas (y solo cuando sea necesario) por los que puedan circular protocolos Microsoft. Estos protocolos viajan sobre los puertos 139 y 445.

Es importante que recuerdes que estos ataques no han sido los primeros, ni serán los últimos, ni los más graves. Estas medidas no son definitivas y no protegen contra todos los ataques. Por este motivo, en el caso de las empresas, se debe elaborar un plan de seguridad completo que incluya procesos, tecnología y vigilancia de la seguridad.

Secure&IT

www.secureit.es