Texto Laura del Río
Fotografía Santiago Ojeda
Vídeo Jorge Pariente

EL 25 DE MAYO NO ES UNA META, ES PARTE DEL CAMINO

<< No debería pillar por sorpresa a las empresas, pero procrastinar es, a veces, un hábito ineludible. El Reglamento Europeo de Protección de Datos (GDPR por sus siglas en inglés) es una normativa que lleva fraguándose desde el año 2012, que se aprobó en 2016, y que será de obligado cumplimiento a partir del 25 de mayo de 2018. Pero muchas empresas aún no están preparadas.

GDPR: una carrera de fondo

Sus antecesoras, la LOPD, que entró en vigor en 1999, y el reglamento de 1995, han establecido una buena base de preparación a lo que estaba por venir con el desarrollo del mundo digital. Pero el momento de dar un salto cualitativo, y también cuantitativo, en seguridad ha llegado. Cómo están afrontando el cambio las compañías y en qué nivel de adaptación se encuentran, con la obligatoriedad de GDPR pisándoles los talones, han sido algunos de los temas que han centrado la conversación en el encuentro organizado por Computing; en el que se han reunido expertos en seguridad de importantes empresas e instituciones a nivel nacional.

Según se contó en el evento, el objetivo de GDPR es armonizar las leyes de la Unión Europea sobre seguridad para crear un marco de colaboración público-privada homogéneo en todos los países, que facilite y fortalezca la protección de lo más valioso que tienen las empresas, los datos. Las estrictas sanciones que impone GDPR son 'la espada de Damocles' de las compañías, las protagonistas de sus pesadillas. No en vano, se ha pasado de multas por un importe máximo en torno a 600.000 euros, en el caso de las infracciones más graves según la LOPD, a multas que pueden alcanzar los 20 millones de euros o equivaler al 4% de la facturación anual de la empresa en cuestión, según GDPR.

Testimonios tranquilizadores aseguraban que "GDPR no implica nada revolucionario, aunque sí un tanto complicado de implementar". El nuevo reglamento europeo se asimila más al modelo anglosajón, no obstante, la LOPD era una de las normas más estrictas de los países de la Unión Europea, por lo que "si se cumplía con la norma anterior, no se debe temer a esta, otra cosa es que no se cumpliera".

JESÚS P. LÓPEZ, CONSULTOR DE TECNOLOGÍA Y PREVENTA DE HP

"CUALQUIER DISPOSITIVO PUEDE SER UNA VÍA DE ENTRADA A NUESTROS DATOS PARA EL CIBERDELINCUENTE"

Se ha extendido en las empresas una visión un tanto distorsionada de GDPR que juzga a la normativa como una amenaza de inminente castigo más que como una herramienta de apoyo para fomentar la seguridad. Desterrar este pensamiento es clave para afrontar el cumplimiento de la normativa como una forma de gestionar y conocer los riesgos a los que se expone nuestra organización y la manera de responder ante ellos.

Hay que ser conscientes de que cualquier dispositivo que utilicemos es susceptible de convertirse en una vía de entrada para el ciberdelincuente a nuestros documentos. Todos los equipos contienen información, desde la impresora hasta la nube, hardware y software. Por tanto, es indispensable diseñar una estrategia integral de seguridad que comprenda la trazabilidad de los datos en los diferentes dispositivos y la autenticación de acceso a los mismos.

VICENTE MANUEL MARTÍN, SPAIN PRESALES MANAGER DE PANDA SECURITY

"GDPR NO SE ENFOCA TANTO EN LAS INFRAESTRUCTURAS, SINO EN LAS PERSONAS"

Construir una protección sólida contra los ciberataques pasa por analizar el tratamiento que se da a los datos que recopila la empresa, sobre todo los no estructurados o dispersos. Este tratamiento se da directamente desde el puesto de trabajo, punto neurálgico de la actividad diaria por el que pasa un gran volumen de información y, por tanto, uno de los principales entornos que necesita ser securizado.

De esta forma, GDPR no se enfoca tanto en las infraestructuras, sino en las personas y sus métodos. Para conseguir una correcta adaptación al nuevo régimen, las empresas deben reestructurar tanto los modelos de protección de datos, como los requerimientos de autenticación. El Machine Learning y la monitorización van a jugar un papel fundamental a la hora de identificar procedimientos no acertados y potenciales amenazas.

FABIO CERIONI, CHIEF TECHNOLOGY OFFICER DE TECHEDGE EN ESPAÑA Y LATAM

"ES HORA DE QUE EL ÁREA IT LE COJA EL TESTIGO AL ÁREA LEGAL"

La gestión del ciclo de vida del dato es una cuestión a la que las empresas no le han prestado la suficiente atención y que ahora GDPR pone encima de la mesa. Cuándo un dato debe ser eliminado, cuándo prescribe su uso aunque tenga que continuar siendo guardado o cómo gestionarlo cuando está activo, son algunos de los aspectos indispensables para preservar la privacidad de las personas y empresas.

Tener localizados lo datos pero que estos no dejen un rastro que pueda poner en peligro su seguridad es otro de los retos a los que se enfrentan las compañías con el nuevo reglamento. Desarrollar un software para ubicar la información puede ser una solución para los grandes sistemas empresariales; aterrizar los requerimientos legales en casos prácticos es fundamental para cumplimentar la normativa.Es hora de que el área IT le coja el testigo al área legal.

Aplazame,
Jorge Valhondo

Cigna,
Henry Velásquez

Air Miles España,
Ana Aguirrezábal

Dutilh Abogados,
María Suárez

"GDPR nos hace mayores", fue una de las afirmaciones que generaron mayor debate. Lo que para algunos supone "disfrutar de mayor libertad y autogestión" siempre que se alcancen los mínimos impuestos en materia de seguridad, para otros sectores más regulados, como la Sanidad o la Administración, conlleva "moverse en arenas movedizas sin contar con una pauta coherente a seguir".

Así con todo, el término 'protección' también se torna ambiguo, ya que como algunos expertos señalaron, "la empresa puede considerar que cuenta con las barreras de seguridad suficientes y la Agencia Española de Protección de Datos (AEPD), no". Esto es porque "cada compañía esta expuesta a un grado de riesgo diferente". A pesar de todo, en la mesa hubo unanimidad respecto a que "por mucho que cumplas la normativa, el riesgo cero no existe".

Uno de los nuevos actores que han entrado en juego es el tiempo de conservación de la información. GDPR pone en jaque la gestión del ciclo de vida del dato, del que hasta ahora no se tenían que rendir cuentas. No obstante, la forma más adecuada de implantar las variaciones empieza por "determinar qué medidas afectan realmente a tu organización y cuáles no, para modificar solo lo estrictamente necesario, ya que cada empresa tiene sus particularidades y "no existe una receta única". Asimismo, en las grandes compañías internacionales es vital establecer sinergias entre los distintos stakeholders para "mapear los flujos de datos y crear estándares para diseñar una estrategia de seguridad uniforme".

GDPR como inhibidor del dato

Casi todos los presentes en el acto no dudaron en reconocer la laxitud de la mayoría de las empresas en cuanto a los métodos de compartición de archivos entre los trabajadores. En este sentido, muchos demandaron la implementación de una herramienta única para acotar el uso de dispositivos y el acopio de datos innecesarios. Si bien la cantidad de información recopilada no es directamente proporcional a la calidad de los misma, hay modelos de negocio para los que hacer un correcto balance entre la cantidad adecuada de datos capturados y la petición de permiso al usuario para capturarlos sin que este abandone el proceso, por ejemplo, de compra online, como ocurre en los eCommerce, se convierte en todo un desafío.

La cesión de datos de cualquier índole suele ser considerada una amenaza para la privacidad del usuario. Expertos en ciberseguridad expusieron la creciente falta de reparos a la hora de cumplimentar información online, sobre todo en las generaciones más jóvenes como los millennials. Hechos como dejar los datos de inicio de sesión guardados por defecto o predeterminados "dan facilidades al usuario, pero pueden suponer un peligro para su privacidad, y de esto también deben preocuparse los fabricantes". Sin embargo, no se debe pasar por alto que "compartir nuestros datos hace que las empresas nos ofrezcan mejores servicios", aunque no hay que obviar que con el uso de nuestra información en beneficio de las compañías "el cliente no siempre sale ganando".

En este sentido, algunos consideran que normativas como GDPR están "diseñadas para hacerle daño a los gigantes tecnológicos como Google y Facebook", que tienen que cumplir con la nueva política de protección de datos para operar en Europa. "Por más que he revisado Google Analytics, no entiendo cómo van a hacer que esa solución cumpla con GDPR",

Ymedia,
Sonia Casado

Idealista,
David Rey

Fundación para la Protección de Datos,
Jorge Badiola

Laliga,
Ignacio Gurpegui

Santander Consumer Finance,
Eduardo Laffarga

Iberdrola,
Teresa Rodríguez

Grupo Cortefiel,
Patricia Arias

apuntaron en la mesa. A ojos de algunos encargados de seguridad, esta acotación del comercio de datos también afecta a la evolución de tecnologías que se alimentan de los mismos, como el Machine Learning. Aunque otros se muestran más optimistas, pese a que la petición de permisos y la especificación del uso que se le va a dar al dato puedan ralentizar el proceso.

La figura del DPO

Con objeto de superar la exhaustiva evaluación de GDPR es primordial establecer una política de supervisión y registro continuo y la anteriormente mencionada sinergia entre departamentos, para la que los encargados en ciberseguridad propusieron nombrar a un responsable de cohesionar las actividades de cada área en este ámbito. Adicionalmente, según el tipo de actividad de la compañía y el tipo y volumen de datos que maneja, existen ciertas compañías que tienen que incluir en su plantilla la figura del Data Protection Officer (DPO).

Este perfil, representado en un único delegado o en un conjunto de personas, esta importado de las corporaciones alemanas y desempeña el papel de consultor para la entidad, aunque debe actuar de manera independiente a esta a la hora de hacer de interlocutor con la agencia y señalar las brechas de seguridad. Que GDPR "exhorta a las organizaciones a denunciarse a sí mismas mediante la figura del DPO", no es un pensamiento de unos pocos. Sin embargo, hubo expertos que alegaron en su defensa que "para quien de verdad trabaja el DPO es para la ley, en este sentido tiene un compromiso ético y, en base a eso, actúa como asesor, y también, haciendo una labor de concienciación en cuanto a la privacidad en la empresa".

Cunef,
Juan Manuel López

Selae,
Carlos Bachmaier

Ferrovial,
Maica Aguilar

Grupo Cortefiel,
David Moreno

En esta línea, el DPO no implementa soluciones, únicamente verifica la efectividad de las implantadas según la normativa; así, aunque no exista una titulación específica de DPO, este tiene que ser, en palabras de los expertos, un "superhombre o supermujer" que tenga conocimientos tecnológicos, jurídicos, técnicos, etcétera. Por este motivo, lo más lógico es que su tarea recaiga en un equipo de profesionales. En el evento supimos que "aún se están preparando las certificaciones del DPO" y dirimiendo si serán específicas de cada país o comunitarias de la Unión Europea, "aunque ya existen cursos formativos al respecto".

Pese a que con la normativa europea se persigue trasladar la responsabilidad sobre seguridad del departamento IT a toda la estructura corporativa, sigue siendo el área de Tecnología la que se encarga de supervisar que los proveedores y socios con los que trabaja la compañía cumplan con GDPR para no acabar "afectados", ya que "cualquier empresa, de producto o servicios, que opere en Europa debe atenerse a esta legislación".

Educación en GDPR

Los entendidos y responsables de seguridad son los que mejor conocen GDPR, y paradójicamente, el usuario se encuentra en el otro extremo, es decir, es un reglamento "para proteger al ciudadano, pero sin el ciudadano", ya que este apenas lo conoce. En este sentido, los expertos echan en falta un programa de información y concienciación por parte del Gobierno, para que "todos conozcamos las implicaciones que tiene, nuestros derechos y deberes", y no solo a nivel de empresa e instituciones. Una buena medida sería "incorporar la privacidad como una asignatura transversal en los colegios", para que, desde pequeños, "entendamos la importancia de mantenerla, y que esta solo se garantiza mediante la seguridad".

La consecución de iniciativas como la anterior ahorraría a las compañías grandes gastos en concienciación de los empleados, "ya que llegaríamos a adultos con un alto nivel de educación en esta materia", añadieron. Los trabajadores, en ocasiones, ven los datos de la compañía "desde la distancia", y no se dan cuenta de que "entre esos datos, están los suyos personales". De esta manera, "personalizar los robos de documentos y sus repercusiones es la única manera de crear conciencia".

El 25 de mayo de 2018 no es una meta, sino "un punto de inflexión en el camino después del cual hay que seguir trabajando". Algunos profesionales estiman que a partir de esta fecha "se concederá una moratoria de seis meses para la implementación", ya que hay muchas entidades "a las que ha pillado el toro", amén de "aquellas agencias de protección de datos a las que tampoco les ha dado tiempo a terminar sus deberes". Con moratoria o sin ella, no hay duda de que GDPR entraña una carrera de fondo. ■