Ciberseguros y cumplimiento del RGPD

José Luis Juárez
IT Security Consultant en vintegrisTECH

Navegando por la Red sin rumbo determinado, encontré un corto de Keiichi Matsuda, especialista en realidad aumentada y diseño de interfaces y usabilidad, sobre hiperrealidad y sus consecuencias. El vídeo me hizo pensar mucho sobre el punto en que nos encontramos y en el tremendo avance que necesitamos alcanzar en los próximos años en lo referente a la información personal, su valor, cómo gestionarla y cómo protegerla.

Ni que decir tiene que, aun cuando el vídeo es una ficción, se acerca mucho al ciclo de vida de la información hoy en día. Pero en cualquier caso, antes de alcanzar ese punto debemos culminar otros que faciliten su llegada. En estos momentos, uno de los principales retos consiste en disponer de los medios adecuados para realizar una gestión de la información con garantías.

Según la memoria de 2017 de la Fiscalía General del Estado, los procedimientos judiciales relacionados con delitos de estafa supusieron el mayor grupo de ciberdelitos registrados, el 61 por ciento, y sumaron 4.930. Este dato, aun cuando puede parecer bueno debido a la drástica reducción en relación con ejercicios anteriores (19% y 22% frente a las cifras de 2016 y 2015, respectivamente), denota que nuestra información no está debidamente tratada y protegida, por lo que tenemos por delante mucho trabajo que hacer.

Con la aplicación del Reglamento General de Protección de Datos (RGPD) desde el 25 de mayo de este año y las nuevas multas de hasta 20 millones de euros que se podrían imponer a las compañías que no observen ciertas normas –como, por ejemplo, la desaparición del consentimiento tácito a la hora de la recopilación de datos–, ahora más que nunca se hace necesario disponer de herramientas que faciliten y garanticen el cumplimiento de dicha norma.

Ciberseguros

En este sentido, los ciberseguros son una buena herramienta si nos centramos en los requisitos de contratación y de coberturas que garantizan. Para su contratación, por ejemplo, las aseguradoras exigen cumplir con una serie de medidas de seguridad que demuestran cierta madurez y responsabilidad en la gestión para mitigar los riesgos. Esto obliga a las organizaciones que deseen contratarlos a adoptar medidas de protección y procedimientos de gestión de incidentes para el cumplimiento legal. De lo contrario, el ciberseguro no se concede.

Tal y como señala el Instituto Nacional de Ciberseguridad (Incibe), como coberturas básicas se consideran las responsabilidades y procedimientos regulatorios; la defensa, perjuicios y multas regulatorias; los daños propios y la pérdida económica; y la gestión de crisis y los gastos pagados a expertos.

Los puntos anteriores son un resumen condensado de la lista completa en la que cada punto dispone de temas más desarrollados y que aplicarán según las necesidades de contratación de cada caso, coincidiendo todas en la protección de la información y su tratamiento adecuado, tanto para evitar un incidente como para abordarlo una vez ocasionado.

Cabe destacar, como es normal, que las empresas aseguradoras se reservan el derecho de no atender según qué reclamaciones, lo que generalmente denominamos las exclusiones, y que algunas son actos deshonestos, fraudulentos y deliberados por parte del asegu-

rado; daños personales o materiales; responsabilidades asumidas por contrato o acuerdo; reclamaciones previas y litigios previos e incidentes que hubieran ocurrido con anterioridad a la fecha de efecto del contrato; infracción de secretos comerciales y patentes; y, en algunos casos, guerra y terrorismo.

De todo lo anterior se desprende que, aun cuando una póliza puede ayudar a mitigar el impacto de un incidente, es importante que las empresas tomen conciencia de los riesgos digitales e inviertan en prevención. Asimismo, deben asumir la gran responsabilidad que la nueva ley les otorga y el coste de su incumplimiento. Aparte, existe un riesgo tanto o más grande que las pérdidas económicas y las sanciones: la pérdida de reputación, algo que una organización tarda muchos años en construir y que puede ser difícil de enmendar.

De hecho, uno de los grandes paradigmas que nos podemos encontrar en este ámbito es que gran parte de los incidentes de ciberseguridad tienen un origen humano, mientras que buena parte de los directivos consideran la seguridad TI una cuestión puramente tecnológica. Un estudio de PwC lo confirma: "el 50 por ciento de los directivos ve la ciberseguridad como un problema tecnológico, no de negocio, cuando en la realidad solo el 10 por ciento de los incidentes están ocasionados por la tecnología, mientras que el resto vienen de la mano del comportamiento humano".

> Las empresas deben poner más foco en la cada vez menos nítida franja entre negocio y tecnología

Cambio de mentalidad

Este complejo entorno exige un cambio radical de mentalidad por parte de los responsables en las corporaciones, las cuales deben poner más foco en la cada vez menos nítida franja existente entre el área de negocio y la tecnología utilizada para generarlo. Para facilitar esta tarea, Vintegris dispone de nebulaSUITE, que engloba los servicios imprescindibles para la protección integral de la identidad digital. Esta *suite* de tecnologías permite lo siguiente:

- **Gestionar identidades digitales.** Crear certificados digitales que actúen como números de identificación para las personas y los dispositivos. Gracias a disponer de su propia autoridad de certificación, está capacitada para emitir y administrar sus propios certificados digitales.
- **Controlar el acceso a los activos de la organización.** Autenticar a los usuarios y controlar su acceso mediante autenticación multifactor adaptativa (MFA), con capacidad para elegir en cada momento el método más adecuado para cada usuario y para adaptar fácilmente todo el entorno en cada caso.
- **Acelerar los procesos de firma**, ya que permite que empleados y clientes firmen documentos utilizando certificados digitales y/o firmas manuscritas, estando todo protegido por cifrado para obtener el máximo nivel de confianza. El sistema permite gestionar incluso los flujos de trabajo para hacer los procedimientos legales más sencillos, dentro del marco legal adecuado.

A ello se le suman las capacidades que proporciona la nube, como por ejemplo disponer de acceso global a estos servicios de forma casi instantánea, obteniendo una cobertura integral en temas como:

1. Identidad digital tanto para usuarios como dispositivos con certificados digitales cualificados.
2. Control centralizado de los certificados digitales con la plataforma de gestión de certificados.
3. Flujos de trabajo simples y personalizados que permiten la aprobación de documentos, transacciones y procesos para uno o múltiples signatarios.
4. Verificaciones de transacciones digitales en beneficio de los ciudadanos y las empresas de la Unión Europea, según el reglamento Europeo eIDAS 910/2014.
5. Autenticación y control sobre el acceso a la empresa y sus recursos.

En definitiva, contar con estas funcionalidades hará más sencillo para las empresas implementar las medidas de obligado cumplimiento del nuevo RGPD. ■