Secure
&MAGAZINE

Número 4 | Junio 2018

ESPECIAL
Protección de Datos

ENTREVISTA

Jesús Rubí Navarrete

Adjunto al director de la Agencia Española de Protección de Datos

EL RGPD HA LLEGADO. ¿Y AHORA QUÉ?

De un vistazo: cambios en la regulación de protección de datos

Siendo prácticos: Medidas organizativas, técnicas y legales de cumplimiento

¿Sabes cuáles son los derechos ARCOPO?

¿SEGURO QUE ESTÁS SEGUR@?

Responde a nuestras preguntas y averígualo

Secure&IT
www.secureit.es

Editorial

Estimados lectores,

En esta edición de ***Secure&Magazine*** vamos a empezar planteándonos: el RGPD ha llegado, ¿y ahora qué? Este fue el título de nuestra IV Jornada de Ciberseguridad, que tuvo lugar el 22 de mayo, en la misma semana en la que se aplicaba el Reglamento General de Protección de Datos. En este punto, queremos hacernos eco de las palabras del secretario general técnico del Ministerio de Justicia, José Amérigo Alonso, encargado de inaugurar el evento, quién destacó que nos encontramos en un cambio de época, y no en una época de cambios, en cuanto a seguridad de la información se refiere.

Este planteamiento confirma que cumplimiento del RGPD se ha convertido en una de las grandes preocupaciones de las empresas. Por este motivo, nos pareció interesante abordar su aplicación en nuestra jornada (igual que hicimos en la tercera edición). Pero, no solo eso, también hemos querido que el número cuatro de ***Secure&Magazine*** sea un especial sobre protección de datos, en el que vamos a tratar de responder a esa pregunta: el RGPD ha llegado, ¿y ahora qué?

Qué mejor manera de empezar a aclarar cuestiones sobre esta normativa que hablando con el adjunto al director de la Agencia Española de Protección de Datos, Jesús Rubí Navarrete, que lleva 20 años vinculado a la entidad. Rubí Navarrete destaca dos características del reglamento: la prevención y la flexibilidad. Y habla de un sistema mucho más proactivo, en el que cada organización debe analizar sus riesgos y ver qué medidas tiene que aplicar, según sus necesidades. Ya lo hemos comentado en otras ocasiones, esta proactividad es una de las principales novedades del RGPD, de estilo más anglosajón.

Otro de los aspectos que ha generado mayor preocupación en empresas y organizaciones es el régimen sancionador. En este sentido, desde la AEPD lanzan un mensaje tranquilizador: las sanciones previstas por el reglamento pueden ser de cuantías muy superiores a las de la anterior LOPD, pero, el modelo actual, por su flexibilidad y proactividad, no está tan focalizado en las sanciones. En algunos casos permitirá corregir errores o incumplimientos sin necesidad de imponer multas. Ahora bien, en cualquier caso, las autoridades apuntan que será necesario que las empresas sean diligentes y que puedan demostrar esa diligencia; de no ser así, estarán más cerca de ser sancionadas económicamente.

Como decíamos, con el RGPD, las medidas de seguridad deberán confeccionarse con el objetivo de corregir aquello que se detecte en el análisis de riesgos. Por tanto, estaremos permanentemente en una fase de mejora continua (revisiones periódicas, una mejora de los procesos, etc.). Seguramente, estáis pensando que es muy fácil decirlo, pero complicado llevarlo a la práctica. Por este motivo, os proponemos una lista de tareas con las medidas técnicas (cifrado, controles de acceso, back ups, etc.), organizativas (políticas corporativas, procedimientos internos, etc.) y legales de cumplimiento. Además, os mostramos de una forma muy visual, los cambios que se han producido en la regulación de protección de datos.

En este número contamos con la participación de varios colaboradores a los que, como siempre, agradecemos su dedicación; sin sus aportaciones esta revista no sería lo mismo: Horatiu Bandoiu (Bitdefender), Gorka Sainz (Fortinet) y Carlos Ferro (Thycotic).

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

El equipo de Secure&IT

Sumario

4 Entrevista

Jesús Rubí Navarrete, adjunto al director de la Agencia Española de Protección de Datos

9 Los derechos ARCOPO

Los derechos que puedes ejercer sobre tus datos personales

10 El RGPD ha llegado. ¿Y ahora qué?

De un vistazo: cambios en la regulación de protección de datos

Siendo prácticos: Medidas organizativas, técnicas y legales de cumplimiento

16 RGPD: lecciones aprendidas

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

18 El GDPR: añadiendo dientes a la privacidad de datos

Gorka Sainz, System Engineer Fortinet Iberia

20 Siete maneras de proteger las cuentas privilegiadas de tu organización

Carlos Ferro, Regional Director, Southern Europe, Middle East & Africa de Thycotic

22 ¿Seguro que estás seguro?

Responde a nuestras preguntas y averígualo

Jesús Rubí Navarrete

"El modelo de supervisión [del RGPD] es mucho más flexible y proactivo, y no está tan focalizado en las sanciones"

Adjunto al director de la Agencia Española de Protección de Datos, Jesús Rubí Navarrete lleva 20 años ligado a esta institución: ha ostentado en otras etapas el cargo que hoy ocupa, pero también ha sido subdirector general de Inspección de Datos. Con anterioridad fue director del Gabinete del Ministro de Justicia, secretario general técnico del Ministerio de Relaciones con las Cortes, director general de Relaciones con las Cortes y vocal del Tribunal de Defensa de la Competencia. Autor de diversas publicaciones en materia de publicidad, derecho de competencia, procedimiento administrativo y protección de datos personales, también colabora con diferentes universidades españolas. Pero, su actividad va más allá de nuestras fronteras: participa en reuniones y conferencias internacionales sobre protección de datos personales; colabora en proyectos con otras autoridades de protección de datos (República Checa, Bulgaria, Bosnia y Herzegovina, Israel y Croacia), y es coordinador de la Red Iberoamericana de Protección de Datos.

Podríamos decir que el RGPD supone un gran cambio en esta materia. ¿Lo están abordando las empresas como deberían? O, mejor dicho, ¿lo han abordado en estos dos años, desde que entró en vigor, como deberían?

Estamos pendientes de algunas encuestas que arrojen más resultados. Pero, tras las múltiples y muy variadas reuniones que hemos mantenido en todo tipo de foros (administraciones públicas; empresas pequeñas, medianas y grandes, etc.), podemos decir que hay una gran sensibilización con la aplicación de esta norma. Yo llevo 20 años en la agencia y diría que la sensibilización que ha habido con esta normativa no es comparable con ninguna otra anterior. Hay muchísima más sensibilización, urgencia e inquietud en el cumplimiento. Aunque, es cierto que esta predisposición al cumplimiento y al conocimiento no se ha aprovechado adecuadamente en el periodo de dos años, desde que entró en vigor. Digamos que esta predisposición creció de manera exponencial en los últimos 8-10 meses antes de su aplicación.

"La sensibilización que ha habido con esta normativa no es comparable con ninguna otra anterior"

¿Son las pymes la gran preocupación para la Agencia?

Sí, porque el reglamento supone una modificación en las modalidades de cumplimiento de esta normativa (además de los nuevos derechos que se reconocen y deberes que se imponen). En lo que se refiere al modelo de cumplimiento, es enormemente diferente al anterior porque se basa en la diligencia activa de cada uno, y hay toda una metodología de medidas que hay que ir adoptando para cumplir con la normativa de protección de datos.

En el caso de las pymes y micropymes (no de todas, porque hay algunas que hacen tratamientos muy intensivos de datos personales), cuyo tratamiento de datos es de muy bajo riesgo, la metodología que exige cumplir el reglamento es compleja. Por eso, hemos desarrollado una herramienta muy básica y muy sencilla que se llama Facilita (https://www.aepd.es/herramientas/facilita.html).

Es una herramienta que hace una preselección para saber si se es de bajo riesgo o no. Permite, en los ficheros más habituales, obtener documentalmente parte (o la mayor par-

te) de las obligaciones del reglamento, adaptadas a cada empresa. En este punto, es necesario recordar que, en este modelo de cumplimiento, uno de los aspectos fundamentales es la necesidad de documentar todo lo que se hace y por qué se hace.

Además de la herramienta, ¿qué otros materiales se han puesto a disposición de las pequeñas y medianas empresas para facilitarles la tarea?

Hemos creado una hoja de ruta, porque en el RGPD hay una serie de medidas con una sistemática jurídica (y no práctica). En esta hoja de ruta, hemos establecido con qué medidas hay que empezar: el registro actividades de tratamiento, el análisis de riesgos (y, en función de este, tienes que adoptar -o no- otras medidas, como hacer evaluaciones de protección de datos o nombrar un DPO), etc. Se han indicado los pasos que hay que ir dando, tanto para empresas como para las administraciones públicas. Y, además de la guía general sobre RGPD, se ha elaborado una guía práctica de cada uno de esos pasos. Todas ellas están a disposición de las empresas en nuestra página web (https://www.aepd.es/guias/index.html).

Comentabas que este es un régimen más preventivo y proactivo. ¿Cuáles son los pros y los contras de esta "autonomía"?

El reglamento tiene dos características fundamentales: la prevención y la flexibilidad. La prevención está basada en esta nueva metodología de cumplimiento que se fundamenta en analizar qué actividades de tratamiento realizo, el análisis de riesgos en base a criterios propios, y el resto de medidas de cumplimiento. Esta es la parte proactiva porque cada cual tiene que ver y analizar todo este tipo de medidas, desde una perspectiva de seguridad y de la "lesión" que se puede producir en los derechos de las personas. La flexibilidad se produce porque, precisamente, como resultado de esos análisis hay que establecer una serie de medidas acordes a las necesidades. No son iguales para todos: pueden ser más sencillas (por ejemplo, en el caso de la mayoría de las micropymes); más complejas, en medianas empresas, o de complejidad superior en grandes corporaciones. Hay ese margen de flexibilidad para que esas medidas se adapten a la tipología de tratamientos que realiza cada una de las compañías.

"El reglamento tiene dos características fundamentales: la prevención y la flexibilidad"

La figura del delegado de protección de datos (DPO) es un elemento clave en el reglamento. ¿Cómo valoran desde la Agencia esta figura?

Valoramos esta figura muy positivamente. El DPO es un profesional, o un equipo de profesionales, muy cualificado (interno o contratado de forma externa), que se encarga de asesorar, informar, resolver dudas y supervisar que las cosas se hagan de forma correcta. En este punto hay que matizar que el DPO no es quien tiene que cumplir la normativa; quien tiene que cumplir es la organización a la que presta sus servicios.

Toda su labor la tiene que llevar a cabo manteniendo un contacto muy fluido con la alta dirección de la empresa. Por este motivo, es una figura que va a contribuir de una manera muy especial a la adaptación y al cumplimiento del reglamento. Pero, además, tiene otras funcio-

nes ya que, por ejemplo, es el punto de contacto con las autoridades de protección de datos y con los ciudadanos.

Tiene ese papel interno de mejora y asesoramiento, y externo de tratar de resolver posibles reclamaciones relacionadas con la protección de datos. También es el punto de contacto más fluido con la propia autoridad de protección de datos.

Esta figura no es obligatoria en todos los casos, pero, ¿diría que es recomendable?

Aún en los casos en los que es voluntario, puede suponer una ventaja y una mayor facilidad y diligencia para el cumplimiento de esta normativa. Imaginemos profesionales que, por su actividad, tienen la obligación de pertenecer a un colegio profesional. El colegio puede facilitar a esos profesionales (repartiendo el coste entre todos) el asesoramiento del DPO. Y, aunque no sea obligatorio, es una manifestación y un plus de diligencia en el cumplimiento de la norma. En asociaciones empresariales se da la misma situación.

Uno de los casos en los que es obligatorio es aquel en el que las actividades del responsable, o encargado, consistan en operaciones que requieren una observación habitual y sistemática de los interesados a gran escala (por ejemplo, videovigilancia). ¿Podemos definir qué es un tratamiento a gran escala?

No hay una definición exacta de "gran escala", depende de muchas circunstancias. Hay unas directrices, que están en la web de la Agencia, del grupo de autoridades de protección de datos, que ofrecen orientación sobre cómo interpretar y cumplir el reglamento (qué criterios tener en cuenta para saber si son o no a gran escala). Pero, es algo que depende de las circunstancias. Un centro comercial, por ejemplo, tiene videovigilancia intensiva. Comparativamente con lo que es el resto de la ciudad no sería a gran escala, pero proporcionalmente con respecto a las personas que van allí a diario sí lo es.

"El modelo de supervisión es mucho más flexible y proactivo, y no está tan focalizado en las sanciones"

El régimen sancionador es mucho más estricto. ¿Cuáles son los aspectos que más va tener en cuenta la Agencia?

Con la normativa anterior de protección de datos existía un régimen sancionador que se ha considerado, en muchas ocasiones, duro. El modelo de cumplimiento estaba muy focalizado en el régimen de las sanciones económicas; la opción de apercibir y no imponer sanción económica era limitada. Esto cambia con el RGPD. Es verdad que las sanciones previstas en el reglamento pueden ser de unas cuantías enormemente superiores a las de la anterior LOPD. Pero, también es verdad que, en este modelo de supervisión que está en el reglamento, hay otro conjunto de medidas correctivas que puede adoptar la autoridad de protección de datos, y que no tienen por qué dar lugar a una sanción económica.

Por ejemplo, hay una medida que es la advertencia, que se pude hacer, incluso, cuando no se ha constatado una infracción. Por ejemplo, alguien presenta una denuncia sobre la videovigilancia de una comunidad de propietarios y, sin necesidad de constatar si se ha producido una infracción, desde la Agencia se podría informar al presidente o presidenta de la comunidad de cuáles son los requisitos para hacer videovigilancia, advertirle de que debe cumplirlos y consultar si los cumple o no, sin necesidad de una sanción.

Hay todo un abanico de medidas, con lo cual el modelo de supervisión es mucho más flexible y proactivo, y no está tan focalizado en las sanciones (aunque se les de mucha importancia). Es mucho más equilibrado que el anterior y cuenta con medidas que permiten corregir, en la práctica, posibles errores o incumplimientos puntuales sin necesidad de imponer una sanción económica.

Y, ¿de qué depende? Pues, de cómo se cumpla el reglamento: que se sea diligente, se siga la metodología prevista para el cumplimiento, que se documente todo lo que se hace (incluso cuando sea algo que consideremos no aplicable, se debe argumentar por qué no lo es), etc. El que no tenga diligencia, o no pueda acreditarla, estará más cerca del régimen de sanciones económicas.

Esto nos va a dar una flexibilidad mayor para que se garanticen los derechos de los ciudadanos, sin necesidad de imponer sanciones económicas, siempre que se haya adoptado una conducta diligente, incluso, aunque se haya hecho una interpretación que no coincide con la del regulador.

En el caso de multinacionales, y empresas con sede en un país diferente, el procedimiento sancionador puede complicarse. ¿Cómo se va a abordar este asunto?

Una de las grandes ventajas e innovaciones de este reglamento es que es la primera norma a nivel mundial que está adaptada adecuadamente al entorno de Internet. Y lo está en dos sentidos: porque ha reconocido nuevos derechos y porque ha establecido unos criterios que garantizan los derechos de los ciudadanos europeos, respecto de multinacionales que estén fuera de la Unión Europea. Y, en ese sentido, el reglamento establece dos criterios: si la organización está fuera de la UE, pero trata datos de europeos en los servicios que genera y esos servicios están dirigidos específicamente a ciudadanos europeos, tiene que cumplir con la normativa europea de protección de datos. O, si está fuera de la UE y monitoriza la conducta de los europeos (como hace Facebook para adaptar la publicidad), tiene que cumplir con esta normativa. Y, además, debe asignar un representante en la UE al que se puedan dirigir las autoridades europeas para obtener información o exigir responsabilidades. Es un avance enorme porque supone la posibilidad, en este mundo globalizado, de poder exigir a quienes tratan datos de ciudadanos europeos un sistema de garantías que, a lo mejor, no existe en su país.

Se hace muy necesario contar con una normativa nacional adaptada al reglamento. ¿En qué momento se encuentra la tramitación de la nueva Ley Orgánica de Protección de Datos?

Se encuentra en el Congreso de los Diputados, después del plazo de presentación de enmiendas, y está en manos de los grupos parlamentarios la negociación correspondiente para aprobar el proyecto. Lo deseable hubiera sido que la aprobación de este proyecto hubiese coincidido con el 25 de mayo, porque esa adaptación hubiese sido integral y hubiese generado mayor seguridad jurídica. Pero, los plazos parlamentarios tienen sus propios mecanismos. Ya se sabe cuál es la orientación de las enmiendas de los distintos grupos y hay que ver a qué consensos se llega para que se apruebe lo antes posible la nueva LOPD. Aunque, hay que tener en cuenta que la nueva ley por la que nos regimos es el Reglamento Europeo de Protección de Datos; la ley española es la que adapta, en los aspectos en los que permite el reglamento, nuestro sistema jurídico a las previsiones de la norma europea.

"Una de las grandes ventajas e innovaciones de este reglamento es que es la primera norma a nivel mundial que está adaptada adecuadamente al entorno de Internet"

Por su actividad, ¿qué sectores pueden tener un mayor impacto en la privacidad de los ciudadanos? ¿Va a centrar la Agencia sus recursos en ellos?

La Agencia promovió antes de la aplicación efectiva una serie de reuniones con los sectores en los que, por su volumen o por la incidencia que tienen en los derechos de las personas, han tenido tradicionalmente una mayor incidencia o tienen dudas respecto de la aplicación del reglamento. Estamos haciendo estas reuniones sectoriales para tratar de una manera presencial, directa y fluida las dudas de últi-

ma hora para que cumplan adecuadamente la norma. Algunos ejemplos son: sector de la publicidad, telecomunicaciones, turismo, grandes superficies comerciales, suministros de energía, etc. Aquellos en los que hay tratamientos masivos de datos.

Con el cambio normativo, han aparecido muchas empresas que ofrecen asesoramiento a muy bajo coste y, probablemente, pocas garantías. Según hemos visto en declaraciones de Mar España, es un tema que preocupa a la Agencia. ¿Cómo se plantean actuar ante este tipo de ofertas?

Por un lado, en aspectos como el DPO, hemos promovido un sistema de certificación, no para que sea obligatorio certificarse como delegado de protección de datos, pero sí para que haya una mayor transparencia en el mercado sobre el nivel de conocimientos y formación. Pero, por supuesto, se puede ser DPO sin seguir este esquema de certificación, siempre que se cumplan las previsiones del reglamento.

Pero, somos conscientes de que hay entidades que están ofreciendo sus servicios de una manera que no es leal ni transparente. Por ejemplo, hay algunas entidades que se están ofreciendo como DPO a empresas que no van a tener obligación de tenerlo y se auto designan. En esta situación están, también, aquellas compañías que ofrecen asesoramiento a "coste cero". Estas empresas, aprovechando la financiación de la fundación Tripartita y dando a entender que dan formación, ofrecen un asesoramiento gratuito. Por eso, hay que insistir en que ante la variedad de ofertas (que ha aumentado de una forma exponencial) hay que hacer una reflexión y tratar de obtener información sobre la calidad del asesoramiento que se va a recibir.

¿Quiere añadir algo más a modo de conclusión?

No estamos acostumbrados a este sistema de cumplimiento que depende de la diligencia de cada uno, ni a documentar todo lo que hacemos o analizamos (y que nos lleva a tomar determinadas decisiones). Es muy importante ese cambio de mentalidad que, además, tiene una perspectiva de futuro. Porque el análisis que se haga ahora hay que seguir haciéndolo y actualizándolo en el tiempo.

Vamos a tener que cambiar la mentalidad en varias cosas, pero, una vez cojamos esta rutina, el modelo de cumplimiento y de garantía de los derechos de los ciudadanos puede haber mejorado cuantitativa y cualitativamente de una manera importante.

https://www.aepd.es/

@AEPD_es

https://www.youtube.com/user/desdelaAEPD

LOS DERECHOS ARCOPO

Los derechos que puedes ejercer sobre tus datos personales

Derecho de acceso

Te ofrece la posibilidad de acceder a la información que has entregado a una empresa u organismo público y conocer, por ejemplo, qué datos tuyos tiene y desde cuándo están en su poder, o que tratamiento se hace de ellos.

Derecho de rectificación

Nos permite modificar los datos que sean inexactos o que estén incompletos. Para ello, debemos indicar al poseedor de esos datos qué modificación queremos hacer, aportando la documentación necesaria que lo justifique.

Derecho de cancelación

Te permite solicitar que se supriman los datos que resulten ser inadecuados o excesivos. En este caso, se tiene que indicar a la empresa o entidad qué dato queremos cancelar y justificar nuestra petición, aportando la documentación necesaria.

Derecho de oposición

Te permite decidir si la empresa o entidad que ha obtenido tus datos puede hacer un tratamiento de ellos.

Derecho a la portabilidad

Es una forma avanzada del derecho de acceso, por el cual la copia que se proporciona al interesado debe ofrecerse en un formato estructurado, de uso común y lectura mecánica. Implica que los datos personales del interesado sean transmitidos directamente de un responsable a otro, sin necesidad de que pasen por el usuario (siempre que sea técnicamente posible).

Derecho al olvido

No está considerado un derecho autónomo o diferenciado de los derechos ARCO, sino la consecuencia de la aplicación del derecho al borrado de los datos personales. Establece la supresión de los datos personales cuando ocurra alguno de los supuestos que contempla, por ejemplo, el tratamiento ilícito de los datos, o la desaparición de la finalidad del tratamiento. Según la AEPD, es una manifestación de los derechos de cancelación u oposición en el entorno online.

*Un dato personal es "*toda información sobre una persona física identificada o identificable*". No solo hace referencia al nombre o los apellidos, también incluye las fotos, la voz, el DNI, el número de historial clínico, las huellas dactilares o, incluso, la matrícula del coche. Deben hacer referencia a una persona física identificada (sabemos a quién pertenece el dato) o identificable (no sabemos a quién pertenece, pero lo podemos conocer fácilmente).

El RGPD ha llegado. ¿Y ahora qué?

Casi un 70% de los españoles asegura que ha recibido mensajes publicitarios de empresas, a través del teléfono o email, sin haber facilitado sus datos personales a estas organizaciones. Es una información del barómetro del Centro de Investigaciones Sociológicas (CIS) del pasado mes de mayo, que también revela que los principales temores a la hora de ceder los datos personales son: que puedan ser utilizados para enviar información comercial, que sean usados sin consentimiento o ser víctimas de un fraude.

Las denuncias de ciudadanos ante la Agencia Española de Protección de Datos (AEPD) relacionadas con el tratamiento de información personal en Internet también han aumentado considerablemente (casi un 40 % en los últimos dos años). Es un tema que preocupa a los ciudadanos y la mitad de ellos asegura que está poco o nada informado sobre el asunto.

A pesar de eso, parece que en el ámbito empresarial la tendencia es otra. A falta de encuestas que arrojen más resultados, el adjunto al director de la Agencia Española de Protección de Datos, Jesús Rubí Navarrete, asegura: "*Tras las múltiples y muy variadas reuniones que hemos mantenido en todo tipo de foros, podemos decir que* ***hay una gran sensibilización con la aplicación de esta norma****. Yo llevo 20 años en la Agencia y diría que la sensibilización que ha habido con esta normativa no es comparable con ninguna otra anterior*". Pero, apunta que, aunque hay una mayor predisposición al cumplimiento, no se ha aprovechado adecuadamente el periodo de dos años desde que entró en vigor el Reglamento General de Protección de Datos (RGPD).

Cumplir con el RGPD, una de las grandes preocupaciones de las empresas

Es la confirmación de que una de las grandes preocupaciones de las empresas y organizaciones en este año es cumplir con el RGPD, de aplicación desde el 25 de mayo. Por este motivo, dedicamos la cuarta edición de nuestra Jornada de Ciberseguridad al reglamento. El evento fue inaugurado por José Amérigo Alonso, Secretario General Técnico del Ministerio de Justicia, que habló del papel del legislador nacional y del proyecto de la nueva Ley Orgánica de Protección de Datos.

A la Secretaría General Técnica del Ministerio de Justicia le ha correspondido el impulso del este proyecto y, en este sentido, Amérigo apuntaba: "*El papel del legislador nacional tenía que ser importante en dos planos: la depuración del ordenamiento jurídico (para eliminar incompatibilidades) y ver de qué opciones, de las que deja el RGPD a los Estados miembros, hacía uso España*".

El Secretario General Técnico del Ministerio de Justicia también hizo un guiño a Leonardo Da Vinci para destacar que, en este momento de evolución continua en la tecnología, no podemos hablar de una época de cambios, sino de un cambio de época: "*El contexto en el que se aprobó la anterior norma europea y el actual no tienen nada que ver. La anterior es de 1995, un momento en el que se hablaba de entre 20.000 y 40.000 ordenadores conectados; nada que ver con el momento actual en el que hay más dispositivos conectados que ciudadanos.* ***La importancia que ha adquirido el dato en la actual economía pone de manifiesto que nos encontramos más que en una época de cambios, en un cambio de época***".

En esta línea intervino también Sonia Martín, directora de Servicios Profesionales de Seguridad de **Secure&IT**, que centró su ponencia en los cambios en la regulación de protección de datos: "*El legislador se ha dado cuenta de que está*

por detrás. Había una serie de normas muy divergentes y, además, la tecnología en 1995 (fecha de la directiva que teníamos) no estaba tan desarrollada. Por eso, necesitábamos una nueva regulación. Además, debe ser lo más homogénea posible a nivel internacional. Esta parte es la más difícil, porque intentar regular Internet con la protección de datos a nivel mundial es muy complicado".

Una de las principales novedades del RGPD, de estilo más anglosajón, es que **las empresas y organizaciones deben evaluar sus riesgos y, de acuerdo con el principio de responsabilidad activa, diseñar las medidas a aplicar en función de esos riesgos.** En este escenario, destaca la figura del Delegado de Protección de Datos (puede ser interno o externo) cuyas funciones deben desarrollarse en el ámbito del asesoramiento, la supervisión y la cooperación con las autoridades de protección de datos.

Con el RGPD, 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. Francisco Valencia, director general de **Secure&IT**, se muestra positivo en este sentido y considera que, aunque parece demasiado podemos conseguirlo marcándonos una lista de tareas con las medidas técnicas (cifrado, controles de acceso, *back ups*, etc.), organizativas (políticas corporativas, procedimientos internos, etc.) y legales de cumplimiento.

Uno de los momentos más esperados es la aprobación del proyecto de Ley Orgánica de Protección de Datos, al que se presentaron 369 enmiendas, y que se encuentra en el proceso de tramitación parlamentaria. Aunque instituciones y empresas tiene mucho interés en que se apruebe cuanto antes, es difícil hacer previsiones con los plazos. Esta ley complementa algunos aspectos del reglamento y aclara otros, por tanto, será necesario manejar las dos normativas (LOPD y RGPD) al mismo tiempo. Por este motivo, se ha buscado una estructura pareja para que se puedan leer ambas normas de forma simultánea.

El modelo actual es más flexible y proactivo, y no está tan focalizado en las sanciones

El régimen sancionador

Este es uno de los aspectos que más preocupa a las compañías porque el RGPD endurece las sanciones considerablemente. 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). Por su parte, 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).

En este sentido, desde la AEPD apuntan que, aunque las sanciones previstas por el Reglamento pueden ser de cuantías muy superiores a las de la anterior LOPD, **el modelo actual es más flexible y proactivo, y no está tan focalizado en las sanciones.** Por tanto, en algunos casos permitirá corregir posibles errores o incumplimientos sin necesidad de imponer una sanción económica. Ahora bien, en cualquier caso, apuntan que será necesario que las empresas sean diligentes y que puedan demostrar esa diligencia; de no ser así, estarán más cerca de ser sancionadas económicamente.

Teresa Granda, Letrada del Consejo General de la Abogacía Española fue la encargada de recoger el mensaje más importante de cada intervención y poner las conclusiones a la primera parte del evento.

También participaron en la jornada Rubén Aparicio, *Regional account manager* de la empresa Fortinet; Juan Jesús Merino, *National Channel Country manager*, de Bitdefender; Óscar Maire-Richard, *Prot-On founder & Product manager*; Carlos Ferro, Regional director, Southern Europe, Middle East & Africa de la empresa Thycotic; Blanca Pedrera, *responsable de Proyectos Digitales y Bases de Datos*, del Grupo Corporativo Consejo General de Enfermería, que intervino en la mesa redonda Impacto de GDPR sobre la actividad económica de las empresas, junto con José Andrés Jiménez, *asesor facultativo TIC* del Congreso de los Diputados.

Por primera vez, la jornada se dividió en dos partes. La tarde, que fue inaugurada por Ángel Pablo Avilés "Angelucho", se destinó a la realización de varios talleres, en los que los participantes pudieron comprobar, de forma práctica, cómo las tecnologías pueden ayudar a las empresas y organizaciones en el cumplimiento del Reglamento de Protección de Datos.

De un vistazo: cambios en la regulación de protección de datos

El legislador siempre ha sido más lento de lo que los nuevos escenarios (globalización, competencia, *IoT*, *e-commerce*, redes sociales, etc.) requieren, ya que estos contextos suponen nuevas amenazas y nuevos riesgos constantes: ciberdelincuencia, ataques a infraestructuras críticas, ciberguerra, etc.

Por este motivo, se han ido tomando diversas medidas, tanto a nivel europeo como nacional. En el ámbito de las acciones europeas destacan: las directivas (relativas a los ataques contra los sistemas de información y sobre ciberseguridad), el Reglamento Europeo sobre Protección de Datos y la creación del Centro Europeo de Lucha contra el Cibercrimen. En España se ha modificado el Código Penal, se aplica el RGPD, contamos con el Esquema Nacional de Seguridad y se han creado organismos y entidades como el Instituto Nacional de Ciberseguridad (INCIBE), el Mando Conjunto de Ciberdefensa o el CCN-CERT.

En materia de privacidad, el legislador ha dado cuenta de que iba por detrás. La normativa estaba obsoleta, porque el contexto en el que se aprobó la anterior norma europea (de 1995) y el actual no tienen nada que ver. Con la llegada del Reglamento General de Protección de Datos, de aplicación desde el 25 de mayo, esto cambia.

¿Qué cambia legalmente?

- **Este Reglamento es de aplicación directa → no ha sido necesaria la transposición de la norma.**
- **Será igual en todos los países de la UE, aunque no su desarrollo en cada uno de ellos.**
- **Se derogan: la Directiva Europea 95/46/CE, la Ley Orgánica 15/1999 de Protección de datos y el Real Decreto 1720/2007.**
- **Estamos esperando la publicación de la nueva Ley Orgánica de Protección de Datos.**

¿Qué cambia conceptualmente?

LOPD	RGPD
Consentimiento tácito	Consentimiento expreso
3 niveles: alto, medio y básico	2 niveles: especiales y no especiales
Inscripción pública de ficheros	Registro interno de actividades de tratamiento
Regulación externa	Autorregulación (y desde el diseño)
Medidas de seguridad establecidas en RD	Medidas de seguridad definidas por la entidad
Seguridad reactiva	Seguridad proactiva → Vigilancia
Derechos: ARCO	Derechos: ARCO + limitación + supresión (olvido) + portabilidad

Siendo prácticos: Medidas organizativas, técnicas y legales de cumplimiento

Probablemente, usuarios, empresas y organizaciones se han visto abrumados por la gran cantidad de información que, en los últimos meses, han recibido o visto publicada sobre el Reglamento General de Protección de Datos (RGPD). Incluso, no sería atrevido decir que algunas compañías han sufrido ataques de nerviosismo según se acercaba el 25 de mayo. Por eso, vamos a tratar de ser prácticos. Aunque pueda parecer demasiado, vamos a elaborar una lista de tareas con las medidas técnicas (cifrado, controles de acceso, continuidad de negocio, etc.), organizativas (políticas corporativas, procedimientos internos, derechos y obligaciones de los empleados, custodia y mantenimiento de la documentación, etc.) y legales de cumplimiento, que nos ayude en la tarea.

¿QUÉ QUEREMOS HACER? (para qué quiero los datos y qué quiero hacer con ellos)

√ Identificar los tratamientos.

√ Crear un Registro de Actividades de Tratamientos (RAT): en ocasiones hay que hacerlo.

√ Realización de Análisis de Impacto: posiblemente, sea necesario llevarlo a cabo para saber el impacto que puede tener el tratamiento que queremos hacer en los titulares de los datos, ya que puede ser alto.

√ Consulta previa a la Agencia de Protección de Datos: si el impacto es alto, tendré que pedir permiso a la AEPD o el organismo de control correspondiente.

¿CÓMO NOS ORGANIZAMOS?

√ Nombrar un Delegado de Protección de Datos: no siempre es obligatorio, pero es recomendable. Va a ser el contacto entre la Agencia Española de Protección de Datos y la empresa. Es el defensor del titular de los datos dentro de la organización. No es el que ejecuta el cumplimiento, es el que se encarga de que alguien lo haga.

√ Establecer roles, responsabilidades y autoridades: responsable del ejercicio de los derechos, responsable de las notificaciones a la AEPD, responsables técnicos, etc.

√ Identificar un Código de Conducta Sectorial: estos códigos servirán como herramientas para que los responsables y encargados puedan demostrar el cumplimiento, teniendo en cuenta las características y necesidades específicas de los distintos sectores.

GARANTIZAR LOS DERECHOS DE LOS TITULARES

√ Informar a los titulares de lo que se pretende hacer y cómo ejercer sus derechos.

√ Pedir consentimientos de cada tratamiento.

√ Realizar acuerdos contractuales con terceros encargados del tratamiento.

√ Implantar un procedimiento de atención a los derechos ARCOPO:

- Derecho de acceso
- Derecho de rectificación
- Derecho de cancelación
- Derecho de oposición
- Derecho a la portabilidad
- Derecho al olvido

√ Si alguien quiere hacer uso de sus derechos, debemos saber qué hacer.

Estaremos permanentemente en una fase de mejora continua

MEDIDAS DE SEGURIDAD (ANTES RD1720)

Antes el legislador especificaba qué medidas técnicas había que cumplir para garantizar la seguridad de los datos, pero la tecnología es tan rápida que se esas medidas se quedaban obsoletas casi a la par que nacían. Ahora hay que autorregularse: hacer el análisis de riesgos, seleccionar controles de mitigación (por ejemplo, los de la ISO 27002).

√ Realizar un Análisis de Riesgos (ISO 31000 - MAGERIT)

Existe una probabilidad de que me pase algo y, cuando me suceda, voy a tener un impacto: Probabilidad X Impacto = Riesgo

Este análisis responde a la pregunta: ¿cómo afecta a los usuarios la pérdida de confidencialidad, integridad y disponibilidad de sus datos?

Pretende analizar de un modo sistemático cómo pueden verse afectados los datos ante distintos escenarios de riesgo, que tenemos que definir. Para cada escenario de riesgo, definiremos una probabilidad de ocurrencia y un impacto estimado.

De la correcta selección de escenarios, y de la buena estimación de probabilidad e impacto, dependerá la exactitud del modelo.

√ Seleccionar controles de mitigación (ISO 27002 - ENS)

Conocidos los riesgos, hay que establecer un Plan de Tratamiento. Este Plan puede derivarse de un conjunto de controles (ISO 27002 establece un conjunto adecuado, completo y sencillo).

√ Implantación de las contramedidas de reducción de riesgo

Para cada control seleccionado, debemos aplicar la denominada "seguridad por capas", que permitirá la gestión completa de cada control.

√ Implantar un mecanismo de vigilancia y control: será necesaria la monitorización avanzada y un sistema de control.

RESPUESTA ANTE INCIDENTES

√ Implantar planes de respuesta a incidentes de seguridad.

√ Implantar un procedimiento de notificación de brechas.

MEJORA CONTINUA

Estaremos permanentemente en una fase de mejora continua. Cada año habrá una revisión, una mejora de los procesos, etc.

√ Auditoría periódica

√ Planes de mejora

√ Certificación del sistema

RGPD: lecciones aprendidas

Ha pasado más de un mes desde la fecha de aplicación del RGPD y constatamos que no ha marcado tanto un punto de inflexión en la seguridad de los datos, tal y como anunciamos todos. Parece que las organizaciones se toman con calma la tarea del cumplimiento y esta es una buena señal: las prisas no son buenas, especialmente en las cosas importantes.

Como nos hemos involucrado en ayudar a varias organizaciones a cumplir con el RGPD, pensamos oportuno destacar algunas lecciones aprendidas:

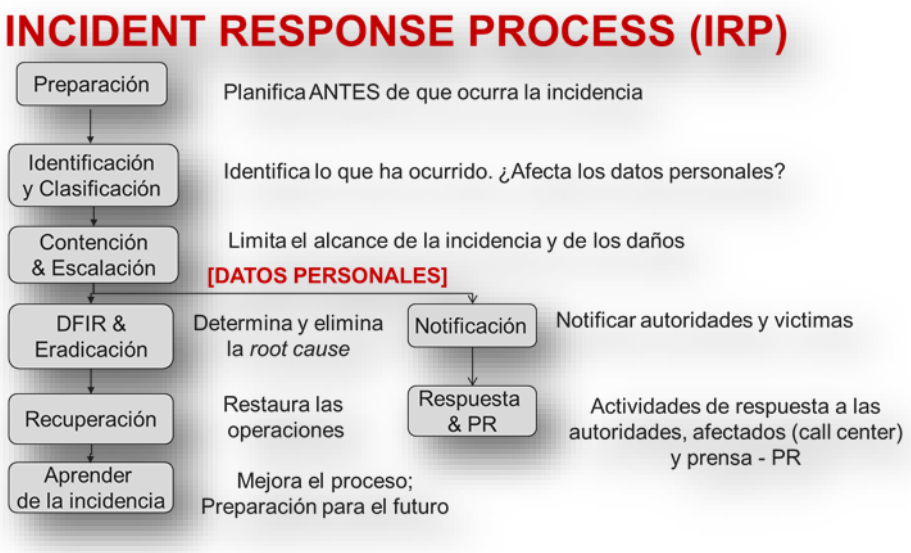
1. Nunca es tarde para echar un vistazo a los datos que manejas, a su carácter y a su importancia. Algo bueno que hemos podido extraer de toda la revolución generada por el RGPD es el hecho de forzarnos a reflexionar sobre algo básico: qué es lo que queremos proteger, qué riesgos le corresponden y qué se puede, convenientemente, hacer. Hacía tiempo que muchas de las organizaciones importantes que conocemos no revisaban sus **planes de mitigación y gestión de los riesgos**, y esta oportunidad ha sido bienvenida.

2. Revisar los **derechos de acceso y** el refuerzo de las **políticas de acceso**. Hemos visto casos en los que existían políticas muy buenas de control del acceso, que se "relajan" con el tiempo. Por eso, el Reglamento de Protección de Datos, forzándonos a retocarlas, nos ha ayudado de nuevo pensar en las prioridades y las restricciones de acceso necesarias para disminuir los riesgos asociados con el personal; no solo por las posibles malas intenciones, sino también por desconocimiento y error humano.

3. Poner **barreras contra el acceso injustificado** a los datos personales. Aparte de los cortafuegos y el acceso por canales encriptados, hemos vuelto a plantearnos los casos en los que los datos personales salen de la empresa por varios medios: portátiles, discos duros externos, dispositivos móviles, etc. En este caso las protecciones básicas como el *full disk encryption* y la protección de los dispositivos móviles nos pueden salvar de muchos dolores de cabeza.

4. Usar de manera responsable tecnologías de ***patch management***. Analizando los riesgos, hemos visto que muchos ataques avanzados han aprovechado vulnerabilidades que tenían ya un parche, pero no había sido aplicado (Equifax, Target, o la explosión de WannaCry). Las tecnologías de *patch management* que protegen de vulnerabilidades (no solo de Windows y Office, también de las otras aplicaciones) ya no son tan caras y hacen bien su trabajo.

5. Uno de los aspectos que hay que priorizar con el RGPD es el proceso de ***incident response***. Aunque algunas cosas no estén bien implementadas, nos podemos librar de multas si tenemos un proceso de respuesta bien organizado, efectivo y provisto de herramientas de trabajo coherentes y modernas. En la imagen, se puede ver el proceso de *incident response*



según recomiendan las buenas prácticas, ligeramente modificado para adaptarse a la RGPD.

Como ya es sabido, en un intervalo de 72 horas hay que avisar las autoridades y a los usuarios afectados; hacer un informe bien documentado con lo que ha pasado, y demostrar las medidas que se han tomado para identificar, contener y parar/remediar la incidencia. Es un proceso sencillo pero que implica a varios actores de la entidad, hasta el nivel más alto. Tenemos la suerte de disponer de una herramienta que se adapta perfectamente a este proceso y permite dar un paso efectivo hacia delante: Bitdefender GravityZone Ultra Security, la primera y única herramienta que se adaptada perfectamente a los requerimientos de un proceso de *incident response*:

- Contiene varios mecanismos de identificación de los Indicadores de Compromiso (IoC) y de Ataque (IoA);

- permite hacer la contención automática (en el caso de que la empresa no tenga un equipo de respuesta ante incidencias bien formado y en activo), pero también la contención manual, dejando libertad a los administradores en los casos en los que quieren ejecutar y estudiar el ataque en entornos seguros tipo *sandbox*;

- permite la preservación de las pruebas y el estudio del desarrollo del ataque y de los dispositivos afectados;

- puede llevar a cabo la eliminación del ataque, de los códigos usados y la vuelta a un estado seguro;

- se puede integrar con varias plataformas de tipo SOC y proporciona herramientas de forense digital y conexión con comunidades de expertos que pueden ayudar en el tratamiento de las incidencias;

- proporciona información detallada para la redacción de los informes de tratamiento de la incidencia que se necesitan para las autoridades de protección de los datos personales.

Hay que tener en cuenta que esta herramienta ayuda al cumplimiento de RGPD, pero es necesario unir esfuerzos a todos los niveles. Bitdefender está siempre dispuesto a aportar su granito de arena en este sentido, y puede guiar a las compañías (no solo para asegurar el cumplimiento, sino también para comprobar que el trabajo que se desarrolla es correcto) y mantenerlas preparadas para proteger los datos personales.

Horatiu Bandoiu,
ISO 27001 LA
Channel Marketing Manager de Bitdefender

Bitdefender®

El GDPR: añadiendo die
de dat

Las violaciones de datos y el robo de identidades han alcanzado unas proporciones epidémicas. Según algunas encuestas, más de la mitad de los consumidores (55%) han abandonado las compras online por problemas de privacidad. Estos estudios también detectan que solo el 10% de los encuestados tiene la sensación de controlar la forma en que las empresas procesan y utilizan su información personal.

Esta tendencia es sin duda una mala noticia para un mundo que avanza hacia la adopción de una economía digital. Las compras *online*, el acceso inmediato a la información financiera, y la capacidad de acceder y proteger los servicios electrónicamente está cambiando la vida de las personas y la forma en la que las empresas realizan sus negocios. No es el momento adecuado para que decaiga la confianza del consumidor.

El Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) es la respuesta de la Unión Europea a los riesgos asociados con el papel que desempeña, cada vez más, la tecnología en la vida cotidiana. GDPR fue ratificado por los estados miembros en abril de 2016 y empezó a ser de obligado cumplimiento el 25 de mayo de este año. Aunque se trata de una regulación de la UE, también se aplica a cualquier organización, independientemente de su ubicación física, si recopila datos personales de consumidores de la UE.

El objetivo de la nueva regulación es garantizar que se incorpore una protección adecuada en el proceso de recogida de datos personales "por defecto y por diseño". La normativa requiere que las organizaciones recopilen solo los datos mínimos necesarios para un propósito específico, y que sean eliminados por completo cuando ya no sean necesarios. La regulación también define a las personas como los únicos propietarios de sus datos personales, y no las instituciones y corporaciones. Como dueños, estas personas deben poder retirar su consentimiento para la recogida de datos con la misma facilidad que para otorgar su permiso.

Privado significa privado

El reto para muchas organizaciones radica en que el GDPR otorga a las personas el "Derecho a ser olvidado" (RTBF, por sus siglas en iglés), lo que implica que cuando se acaba su relación con una organización pueden llevarse sus datos con ellos y se debe eliminar toda la información de identificación personal. Esto incluye cualquier dato que pueda identificar a una persona en concreto, que se pueda usar para distinguir a un individuo de otro, o que pueda utilizarse para que datos anónimos dejen de serlo.

Protección eficaz

En el caso de una violación de datos, el GDPR también establece las condiciones de cuándo debe hacerse la notificación y establece dos niveles de sanciones, según la gravedad de la infracción. Las infracciones menores acarrean penas de hasta el 2% de la facturación mundial o 10 millones de euros, la que sea mayor, y las infracciones mayores requieren penas de hasta el 4% de la facturación mundial o 20 millones de euros, quedándose también con la cifra mayor.

Debida a la rápida evolución de la tecnología, el GDPR también hace responsable de la "evaluación continua de riesgos" a la institución que controla los datos y requiere que cualquier organización externa que procese los datos también cumpla con GDPR.

entes a la privacidad
tos

Como resultado, tanto el esfuerzo de lograr el cumplimiento como los riesgos asociados con el incumplimiento se incrementarán con el GDPR. De hecho, se estima que más del 50% de las organizaciones no cumplirán la normativa.

¿Quién está afectado?

El GDPR aplica a cualquier organización, independientemente del país, que recoja, almacene o procese datos personales de residentes de la UE. Esto incluye datos de empleados, socios, clientes actuales y potenciales. En terminología de regulación, estas organizaciones se definen como controladores, es decir, aquellos que determinan cómo y por qué se procesan los datos personales, o 'procesadores' que actúan en nombre del controlador. Ambos tienen mayores obligaciones con el GDPR, y ambos podrían enfrentarse a sanciones por incumplimiento de la normativa o en el caso de una violación de datos.

Las implicaciones van más allá de una regulación regional que solo afecte a las empresas u organizaciones de la UE que manejan datos personales de la Unión. Es posible que esto conduzca a una expectativa más amplia que afecte a personas de todo el mundo, ya que el nivel de protección requerido por el GDPR debe convertirse en la "nueva normalidad", lo que significa que los clientes esperan que, si las compañías pueden ofrecer ese nivel de visibilidad y control de datos para los consumidores de la UE, ¿por qué no extenderlo al resto del mundo? Esto tiene tremendas implicaciones en lo que se refiere a "como de seguros son tus datos" y conducirá a que los consumidores exijan soluciones que cumplan sus expectativas en términos de seguridad y control de su información personal.

Para la mayoría de las organizaciones, especialmente empresas internacionales, cumplir con el GDPR será un desafío significativo y a largo plazo. Además del impacto en las tecnologías de información y seguridad, el cumplimiento del GDPR requerirá cambios en algunos procesos de negocio, incluidos los flujos de procedimientos de datos, las estructuras organizativas e incluso las políticas comerciales. A diferencia de regulaciones similares, el modelo de negocio digital actual, que está viviendo una rápida evolución, exigirá una evaluación continua de los riesgos asociada a la adopción de nuevas tecnologías.

Este proceso va a requerir una nueva revisión de las soluciones y estrategias de seguridad existentes. La seguridad en la red no solo debe evitar de forma activa las intrusiones que se producen desde cualquier punto de los sistemas de red distribuidos. También deberá minimizar el riesgo de violaciones graves, reduciendo el tiempo necesario para detectar y responder a nuevas amenazas. La solución para lograrlo pasa por un enfoque amplio, potente y automatizado de la seguridad.

Gorka Sainz
System Engineer Fortinet Iberia
FORTINET

Siete maneras de proteger las cuentas privilegiadas de tu organización

El incremento de las amenazas dirigidas y sofisticadas, por parte de atacantes internos y externos, ha provocado que sea muy complicado para las organizaciones proteger su información crítica y sensible. Esta tarea se vuelve cada vez más difícil cuando los entornos IT se hacen más complejos y distribuidos a gran escala en diferentes localizaciones y en la nube.

La mayoría de las brechas de alto nivel tienen en común el haber sido comprometidas mediante la obtención de *passwords*, que suelen ser hackeadas con técnicas de ingeniería social, y luego utilizadas para conseguir acceso a las cuentas privilegiadas. Este acceso no autorizado puede pasar desapercibido durante semanas o, incluso, meses, permitiendo a los atacantes ver y robar información a su antojo.

La realidad es que muchos usuarios de IT no tienen un conocimiento adecuado de cómo funcionan las cuentas privilegiadas, así como los riesgos asociados por un mal uso o robo, lo que les hace más vulnerables a daños tanto económicos como de reputación.

Según el informe de Thycotic *Global Channel Partner Survey 2018*, donde han participado más de 250 integradores y proveedores de servicios gestionados, más del 70% de sus clientes han sufrido alguna brecha de seguridad en el ultimo año. De ellos, el 55% no solucionó completamente la causa de la brecha y el 18% no buscó ninguna solución para evitar que la brecha se repitiera. Pero, el dato más alarmante es que el 62% de los ataques implicaron cuentas privilegiadas de los clientes para aprovecharse de las vulnerabilidades.

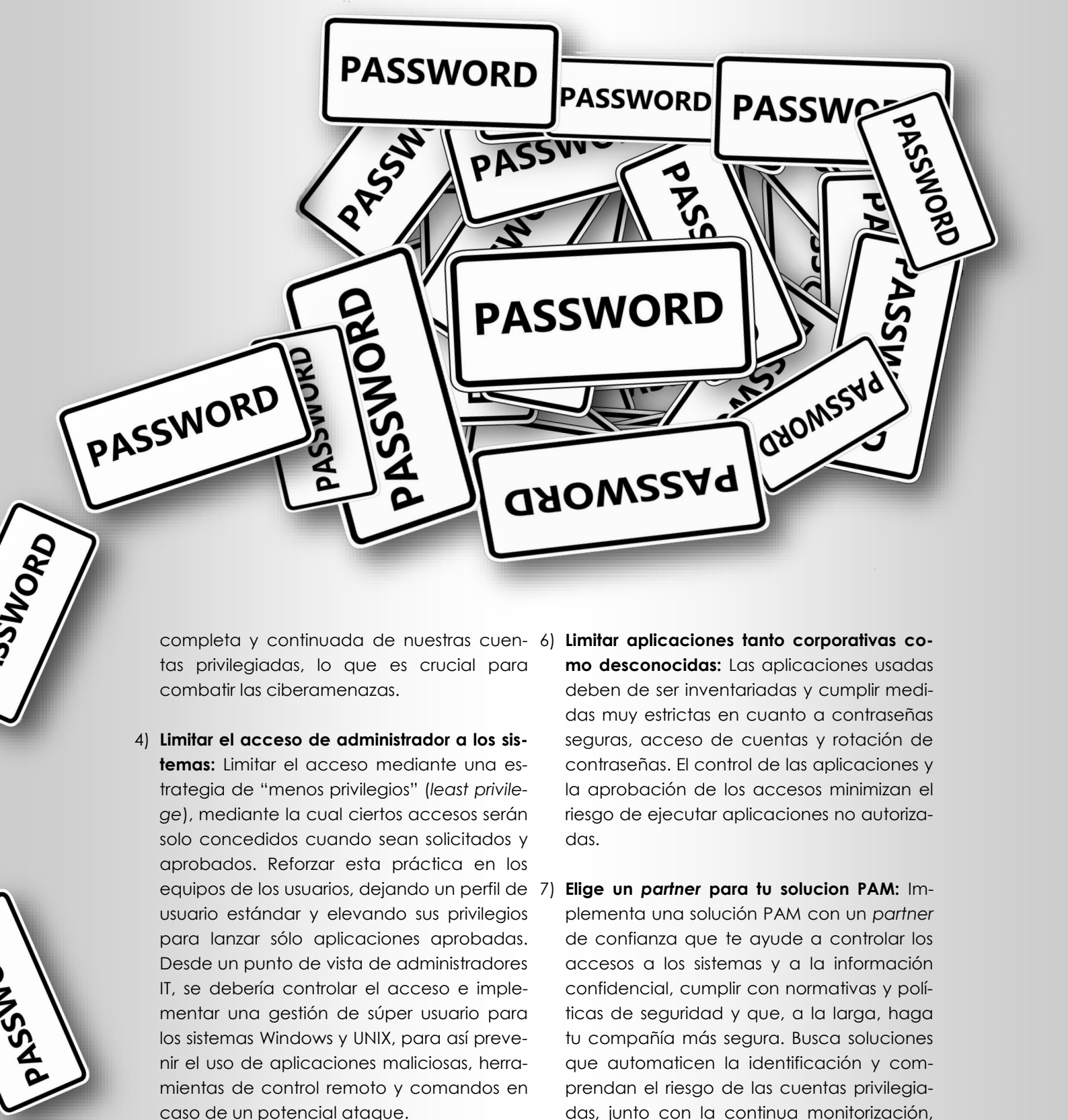
Hacking the Hacker

Privileged account management (PAM) no es un reto insuperable. Cualquier organización puede controlar, proteger y securizar sus cuentas privilegiadas (y así hacer el trabajo de los *hackers* más complicado) con estos sencillos pasos:

1) **Mantenerse alejado de métodos manuales de gestión de cuentas privilegiadas:** demasiadas hojas (que además son compartidas) de Microsoft Excel para hacer seguimiento y control de las contraseñas. Esta práctica manual es peligrosa e ineficiente, sobre todo teniendo en cuenta que una solución PAM puede instalarse de manera rápida y sencilla.

2) **Educar a los empleados:** el eslabón más débil (en términos de seguridad) que tienen las empresas es el factor humano. Según aumenta el número de ataques sofisticados de ingeniería social y *phishing*, las empresas deben ampliar sus programas de concienciación relativos a seguridad. Cada vez más, los dispositivos personales son utilizados para cuestiones laborales, por lo que educar a los empleados en buenas prácticas de seguridad IT se ha convertido en una obligación

3) **Descubrir y automatizar la gestión de cuentas privilegiadas y claves SSH (*Secure Shell*):** usar una solución PAM dedicada y focalizada en las cuentas más críticas y sensibles e implementar medidas de descubrimiento para detectar la extensión de cuentas privilegiadas; identificar potenciales abusos internos y revelar amenazas externas. Con esto aseguramos una visibilidad



completa y continuada de nuestras cuentas privilegiadas, lo que es crucial para combatir las ciberamenazas.

4) **Limitar el acceso de administrador a los sistemas:** Limitar el acceso mediante una estrategia de "menos privilegios" (*least privilege*), mediante la cual ciertos accesos serán solo concedidos cuando sean solicitados y aprobados. Reforzar esta práctica en los equipos de los usuarios, dejando un perfil de usuario estándar y elevando sus privilegios para lanzar sólo aplicaciones aprobadas. Desde un punto de vista de administradores IT, se debería controlar el acceso e implementar una gestión de súper usuario para los sistemas Windows y UNIX, para así prevenir el uso de aplicaciones maliciosas, herramientas de control remoto y comandos en caso de un potencial ataque.

5) **Proteger las contraseñas de las cuentas privilegiadas:** Gestionar, monitorizar y controlar de manera proactiva el acceso privilegiado con una herramienta de protección de contraseñas que debería, de forma automática, descubrir y almacenar las cuentas privilegiadas, rotar las contraseñas, auditar, analizar y gestionar la actividad de cuentas con privilegios.

6) **Limitar aplicaciones tanto corporativas como desconocidas:** Las aplicaciones usadas deben de ser inventariadas y cumplir medidas muy estrictas en cuanto a contraseñas seguras, acceso de cuentas y rotación de contraseñas. El control de las aplicaciones y la aprobación de los accesos minimizan el riesgo de ejecutar aplicaciones no autorizadas.

7) **Elige un *partner* para tu solucion PAM:** Implementa una solución PAM con un *partner* de confianza que te ayude a controlar los accesos a los sistemas y a la información confidencial, cumplir con normativas y políticas de seguridad y que, a la larga, haga tu compañía más segura. Busca soluciones que automaticen la identificación y comprendan el riesgo de las cuentas privilegiadas, junto con la continua monitorización, grabación y almacenaje seguro.

Carlos Ferro
Regional Director, Southern Europe, Middle East & Africa de Thycotic

thycotic

¿Seguro que e

- **¿Seguro que cambias tus contraseñas periódicamente?**

Para evitar riesgos, lo más recomendable es que cambies tus contraseñas periódicamente y que no reutilices las anteriores. Además, trata de no ponerlo fácil: no utilices fechas importantes para ti (aniversarios, fecha de nacimiento, etc.) o nombres de familiares o mascotas; usa contraseñas complejas, que sean largas e incluyan números, mayúsculas, minúsculas y símbolos.

Para recordar una contraseña compleja, puedes utilizar usar las "*passphrases*": elige una frase fácil de recordar para ti, cambia algunas letras a mayúscula, añade símbolos a modo de separación y, por último, puedes sustituir letras por números que se parezcan.

- **¿Seguro que has tapado la *webcam* de tu ordenador?**

Aunque parezca mentira, los ciberdelincuentes son capaces de manipular y controlar la cámara de tu ordenador a distancia (lo consiguen infectando tus dispositivos con algún archivo malicioso). Para evitarlo, no descargues archivos o abras links que no sean de confianza. Pero, además, es importante que cubras las *webcams* de tus dispositivos.

- **¿Seguro que no te conectas a redes wifi desconocidas?**

Cuando nos conectamos a una red wifi pública desconocemos quién es el administrador o qué medidas de seguridad utiliza. Por eso, debemos tomar precauciones y tratar de evitar las gratuitas. Por supuesto, nunca utilices redes no confiables para acceder a servicios de información bancaria, recursos corporativos, correo electrónico o acceso a las redes sociales.

- **¿Seguro que realizas copias de seguridad de forma periódica?**

Seguramente, en el trabajo tendrás a tu disposición carpetas compartidas y será el departamento de sistemas el encargado de realizar las copias de seguridad. De esta forma, si sufres alguna pérdida, robo o avería no habrá problema. Pero, en el ámbito personal solemos ser más descuidados. Si es así, ¡cambia el chip! Haz copias de seguridad y, aunque es un consejo clásico, ten especial cuidado en las épocas de vacaciones, en las que estamos más expuestos a imprevistos.

- **¿Seguro que te mantienes al tanto de las noticias de ciberseguridad?**

Para evitar las brechas de seguridad, te conviene estar al tanto de las novedades y las últimas noticias relacionadas con la materia. Por eso, te recomendamos que, de vez en cuando, visites webs y blogs de ciberseguridad que ofrecen consejos y contenido interesante para los usuarios. Aquí van algunas propuestas:

- √ Blog del Instituto Nacional de Ciberseguridad (INCIBE)
- √ Web de la Oficina de Seguridad del Internauta
- √ Web del Grupo de Delitos Telemáticos de la Guardia Civil
- √ Blog de "Angelucho"
- √ Web de la Agencia Española de Protección de Datos
- √ Blog de **Secure&IT**

- **¿Seguro que actualizas los sistemas operativos y programas de tus dispositivos?**

Es importante que mantengas en todo momento actualizado el equipo (tanto las aplicaciones como el sistema operativo) para eliminar las brechas de seguridad. Debes saber que es poco práctico ser precavido y prestar atención, si después no tienes tus dispositivos actualizados y protegidos.

- **¿Seguro que utilizas las redes sociales de forma apropiada?**

¿Informas a extraños de dónde vas o les proporcionas datos personales de tus amigos? ¿Dejas las llaves puestas cuando sales de casa? Seguro

estás segur@?

que no. En el uso de redes sociales deberías hacer lo mismo y, para eso, es necesario que configures tu privacidad de forma apropiada. Así evitarás que cualquiera lo sepa todo sobre ti, simplemente echando un vistazo a tus perfiles.

- **¿Seguro que eliminas los *emails* de remitentes desconocidos?**

Los correos de *phishing* tratan de engañarte haciéndose pasar por un banco, por la administración pública o por uno de tus proveedores. A través de estos emails, los ciberdelincuentes también pueden infectar tus dispositivos con un *ransomware* que cifra tu información. Por este motivo, no debes abrir ningún correo electrónico, si no tienes la certeza de que proviene una fuente confiable. No obstante, si lo abres y ves que contiene algún link o archivo adjunto, no lo ejecutes ni lo descargues. Lo mejor, si tienes dudas, es llamar a la fuente del correo y verificar que te lo ha mandado.

- **¿Seguro que no te conectas a sitios web fraudulentos?**

Probablemente, cuando entras por primera vez en una página -en la que vas a hacer una compra o vas a descargar un programa- una de las cosas que te preguntas es cómo puedes comprobar si es segura. ¿Quieres saber si una web te ofrece unas garantías mínimas? Comprueba lo siguiente: asegúrate de que la URL empieza por "https" y que la barra de direcciones del navegador está en verde; revisa el aviso legal de la página, que debe recoger la dirección e información de contacto de la empresa; revisa las políticas de privacidad para saber qué tratamiento se va a hacer de tus datos; infórmate de las condiciones generales de contratación (en el caso de que vayas a hacer una compra); y comprueba si tiene certificados (algunas empresas cuentan con sellos y certificados que garantizan su seguridad).

- **¿Seguro que evitas las descargas ilegales?**

¿Descargas música, series o *software* pirata? Debes saber que la piratería es una conducta ilegal en España, que está castigada y se sanciona. Pero, además, al descargarte música, videojuegos, películas, o, sencillamente, al tratar de ver algún partido de fútbol de forma gratuita en webs con dudosa reputación, te expones a otros riesgos: infección de tus dispositivos con algún tipo de *malware* (el problema se agrava si lo haces en el trabajo); o robo de tus datos para actividades ilegales (venderlos en la Deep web; robarte imágenes a través de la webcam para venderlas; enviar *spam*; realizar ataques de denegación de servicio; cometer delitos o fraudes desde tu ordenador; etc.).

- **¿Seguro que tienes instalado un buen antivirus?**

Es uno de los principales consejos que se suele dar y el motivo es obvio: siempre viene bien contar con una herramienta que nos proteja de las amenazas. No solo hablamos de instalarlo en el ordenador, conviene disponer de ellos también en el resto de tus dispositivos (*smartphones* o *tablets*).

- **¿Seguro que eres precavid@ y usas el sentido común?**

Puede parecer algo muy obvio, pero ante ciertas propuestas y ofertas perdemos la prudencia y nos olvidamos de la lógica. ¿Has recibido algún *email* o mensaje en el que un millonario te había nombrado su único heredero? ¿Alguien, desde un número extraño, te ha enviado un SMS porque quiere contactar contigo por Whatsapp y no puede? ¡Sospecha! Nadie regala nada porque sí, ni se complica tanto para contactar con una persona. Tanto *online* como *offline*, hay que estar alerta y aplicar el sentido común para estar protegidos.

Después de leer esto, podrías responder afirmativamente al a pregunta "¿Seguro que estás segur@?". Si es así, enhorabuena; no bajes la guardia, la seguridad 100% no existe. Si no, ¿a qué esperas para empezar a trabajar en ello?

Secure&IT

www.secureit.es