ARBOR NETWORKS

Informe sobre la obligación legal de notificar o denunciar brechas de seguridad que afecten a datos personales

Informe elaborado por Abanlex para Arbor Networks

ABANLEX

Índice

Resumen ejecutivo 3

1.Toda empresa sufre ataques informáticos 4

2. Las brechas afectan a empresas y particulares 5

3. Quién está obligado a notificar o denunciar 5

4. Primer paso: Investigación de la brecha 6

5. Segundo paso: Anotación de los detalles de la brecha y aplicación de las medidas correctoras 7

6. Tercer paso: Notificar la brecha o denunciar 8

6.1. Notificar brechas de seguridad 8

6.1.1. Brechas de seguridad que se deben notificar 8

6.1.2. Quién está obligado a notificar una brecha de seguridad 10

6.1.3. Se ha de notificar la brecha a la AEPD y al particular afectado 10

6.1.4. Circunstancias de la notificación 12

6.1.4.1. Cuándo se debe notificar a la AEPD y al particular afectado 12

6.1.4.2. Cómo debe ser la notificación a la AEPD y al particular afectado 12

6.1.4.3. Cómo se debe notificar a la AEPD y al particular afectado 13

6.1.4.4. Debe registrarse la brecha 13

6.1.4.5. Se sanciona al que no notifica 13

6.1.4.6. Casos en los que se puede evitar notificar al particular afectado 14

6.1.4.7. Otras obligaciones de notificación 15

6.1.4.8. Proyecto europeo: Incluir otros sectores en la obligación de notificar 16

6.2. Denunciar la comisión de una infracción 16

7. Amenazas avanzadas/Analítica de seguridad: PRAVAIL SECURITY ANALYTICS 22

Descarga gratis este informe: http://go.abanlex.com/Arbor1

Esta obra está bajo una Licencia Creative Commons Atribución-SinDerivar 4.0 Internacional.

Resumen ejecutivo

Los operadores que explotan redes públicas de comunicaciones electrónicas o que prestan servicios de comunicaciones electrónicas disponibles al público tienen la obligación de notificar a la Agencia Española de Protección de Datos las brechas de seguridad que sufran cuando supongan la pérdida, destrucción, alteración o acceso ilegítimo a datos de carácter personal. Asimismo, el operador deberá notificar también la violación al abonado o particular sin dilaciones indebidas.

Las demás empresas, distintas a las referidas del sector de las comunicaciones electrónicas, no están habilitadas para notificar sino que están obligadas a denunciar dicha afección sufrida sobre los ficheros que están obligadas a custodiar. En caso de que la brecha no haya afectado a datos personales, solo las empresas que formen parte de las infraestructuras críticas del estado podrán, si lo desean, informar al CNPIC español.

En todos los casos, las empresas están obligadas a mantener un documento de seguridad en el que deberá figurar un registro actualizado de las incidencias y brechas de seguridad sufridas. Este documento deberá reflejar las medidas de seguridad que establezca la empresa con respeto a la ley y en función del nivel de riesgo -alto, medio o bajo-, al que se enfrente. El documento, que reflejará un sistema de control de acceso a los datos, establecerá si se deben implementar medidas incluso de cifrado sobre los datos para su protección.

Las empresas españolas sufren ataques informáticos de forma constante. Muchas lo ignoran por no tener un sistema técnico adecuado que les permita conocerlo; a otras les falta información sobre quién o cómo las están atacando. Solo unas pocas cuentan con tecnología para identificar tentativas de intrusión o brechas exitosas, para extraer la información necesaria y para establecer nuevas medidas de seguridad.

La información sobre los ataques sufridos permite realizar las siguientes cuatro acciones:

1 Mejorar la protección de los activos de la empresa, así como cumplir con la obligación de reflejar en el documento de seguridad el detalle de las incidencias y poder comunicárselo, en su caso, a los organismos pertinentes entre los que destaca el CNPIC para las infraestructuras críticas.

2 Entregar pruebas del ataque a la Policía o a la Guardia Civil en el momento de la denuncia de los hechos, con el objetivo de facilitarles la investigación.

3 Denunciar los hechos a la Agencia Española de Protección de Datos cuando la brecha de seguridad sufrida afecte a datos de carácter personal. Los operadores de comunicaciones electrónicas, en lugar de denunciar, podrán notificar en dos tiempos: primero mediante una notificación inicial dentro de las primeras 24 horas; y, segundo, en los tres días siguientes, mediante una notificación complementaria

4 Informar a los usuarios cuyos datos se hayan visto comprometidos.

La normativa española obliga a obtener información y notificar brechas de seguridad. La falta de cumplimiento puede derivar en la siguiente tanda de multas: una primera con valor total de hasta 340.000 euros; una de hasta 300.000 euros por no haber evitado la brecha; y otra de hasta 600.000 euros en casos concretos tasados en la normativa de protección de datos.

Los sistemas técnicos que permiten conocer las tentativas de intrusiones y las brechas exitosas son necesarios por utilidad y obligatorios por imposición legal. Su implantación y monitorización es una tarea a la que hay que dedicar el tiempo y los recursos necesarios.

1 Toda empresa sufre ataques informáticos

Una brecha de seguridad puede suponer la pérdida de datos o el acceso de un tercero a los mismos. Esta circunstancia es causa suficiente para que la empresa española que lo haya sufrido tenga que auto-denunciarse o deba notificar el hecho a la Agencia Española de Protección de datos.

Que se va a sufrir un ataque informático es seguro. La forma adecuada de protegerse ante ellos es combinar dos tipos de medidas: por un lado, el establecimiento de una serie de mecanismos de seguridad robusta; por otro, el de un sistema de análisis en tiempo real que sea capaz de detectar tanto las brechas producidas como los intentos de ataque o de entrada. La robustez de las medidas depende de varias acciones que deben operar sobre la organización del activo humano y sobre la disposición de soluciones tecnológicas.

La normativa vigente en España establece a las empresas del sector de las comunicaciones electrónicas la obligación de notificar las brechas de seguridad que supongan la pérdida, destrucción, modificación o acceso ilegítimo a información personal. Esta obligación, que vincula solo al sector de las comunicaciones electrónicas, alcanzará probablemente a las empresas del resto de los sectores en los próximos años. Mientras llega esta ampliación de la norma de notificación, seguirá imperando en España y para el resto la obligación de auto-denunciarse en caso de que las brechas de seguridad hayan afectado a los datos de carácter personal que la empresa está obligada a proteger y custodiar. Es decir, **las empresas de los demás sectores están obligadas a auto-denunciarse**.

Las amenazas en la Red crecen en sofisticación. Esto supone que las herramientas de defensa o de seguridad informática convencionales no son suficientes: o bien no evitan el éxito de estas intromisiones o bien ni siquiera las detectan.

"Hoy día, la mayoría de las organizaciones confía en tecnología y procedimientos diseñados para disminuir los riesgos asociados con virus y troyanos, que no están dirigidos y no son suficientes para combatir las avanzadas amenazas actuales", confirma la Lockeed Martin Corporation, referencia global en defensa militar y seguridad de la información.

Para lograr un blindaje efectivo ante las nuevas amenazas es imprescindible conocerlas en profundidad, de modo que las herramientas de detección y enfrentamiento estén diseñadas específicamente para detectarlas y hacerlas fracasar.

Los ataques informáticos están siendo dirigidos a todo tipo de sujetos: grandes corporaciones, pequeñas y medianas empresas y Administración Pública. Todos ellos disponen de información personal, en soportes informáticos, que debe ser custodiada y protegida. Por este motivo, todas ellas deben implementar las medidas necesarias que garanticen su seguridad.

En ocasiones, el cifrado de datos es una medida recomendable o incluso legalmente obligatoria, que no exime del deber de notificar o auto-denunciarse, pero sí reduce la carga de responsabilidad sobre el sujeto afectado, así como el daño real sufrido. **El Gabinete Jurídico de la Agencia Española de Protección de Datos recuerda, en su Informe 494/2009, cuál es la importancia de la protección adecuada de los datos**, de manera que sea legal y suficiente:

"La seguridad en el intercambio de información de carácter personal en la que hay que adoptar medidas de seguridad de nivel alto, en particular los requisitos de cifrado de datos, no es un tema baladí, ni un mero trámite administrativo, ni una cuestión de comodidad. ***Es el medio técnico por el cual se garantiza la protección de un derecho fundamental y al que hay que dedicar el tiempo y los recursos que sean necesarios para su correcta implementación"****.*

La vulnerabilidad de la información en formato electrónico se confirma también atendiendo al Informe sobre brechas de seguridad en Europa elaborado por la Universidad Europea Central. Según los analistas de esta universidad, 229 ataques con intromisión lograda a centros de datos europeos fueron reportados entre los años 2004 y 2014. En estos ataques, más de 640 millones de archivos que incluían información personal se vieron afectados. El 40% de los mismos fue comprometido a través de ataques informáticos, mientras que los archivos restantes se vieron afectados debido a errores administrativos, a la pérdida o la sustracción de hardware, a los abusos de los sujetos con acceso autorizado o a la falta de diligencia en la red. Es reseñable el hecho de que millones de archivos con datos personales han sufrido ataques y que, independientemente de la causa, en todos los supuestos la obligación de notificar persiste.

Los ataques informáticos son constantes. El mayor problema que presentan es que son silenciosos: entran, extraen y desaparecen sin dejar rastro. Es muy probable que la empresa jamás lo llegue a conocer, a pesar de que sus datos hayan quedado ya comprometidos. Lo que esa empresa debe preguntarse es: ¿Está preparada mi empresa para conocer los ataques que está sufriendo? ¿Está preparada para prevenir el siguiente?

2 Las brechas afectan a empresas y particulares

La notificación obligatoria pretende que "*los consumidores sepan cuándo sus datos personales han sido comprometidos de forma que, si es necesario, puedan poner remedio*", afirma Neelie Kroes, ex-comisaria encargada de la Agenda Digital de la Unión Europea y Vice-Presidenta de la Comisión Europea

> *"Consumers need to know when their personal data has been compromised, so that they can take remedial action if needed, and businesses need simplicity. These new practical measures provide that level playing field." (Digital Agenda: New specific rules for consumers when telecoms personal data is lost or stolen in EU)*

Las personas físicas cuyos datos hayan sido afectados, son los principales sujetos sobre los que la norma presta atención.

Sin embargo, un aspecto de extrema importancia para las empresas es el de la incidencia real de las brechas de seguridad en su gestión de marca e imagen pública. **Los ataques informáticos que tumban la protección de los datos personales afectan a la imagen corporativa de la empresa que los haya sufrido y, consecuentemente, restan credibilidad a la marca, merman la confianza de los clientes y lastran la reputación online de la entidad**. Es este motivo el principal causante de que los ataques constantes no sean portada más a menudo.

Los efectos adversos más graves los sufren los particulares, cuya información personal se ve comprometida. Las consecuencias de los daños son desde los materiales o reputacionales, hasta la usurpación de su identidad. Quizá el aspecto más interesante de todo esto sea que estas consecuencias no tienen por qué ser inmediatas: la información sobre las personas físicas es poder y el hecho de contar con datos de los individuos hace posible que puedas atacarlos en cualquier momento, presente o futuro. **Los ataques silenciosos pueden tener como objetivo la extracción de datos con objetivos a medio y largo plazo** contra los particulares o contra la propia empresa. Afortunadamente, aunque el adverbio no sea el más idóneo, hoy en día las consecuencias suelen verse en periodos de tiempo breves de entre pocas horas y menos de un año.

En caso de que se sufra una brecha de seguridad, la empresa debe saber cómo actuar. Si opera en el sector de las comunicaciones electrónicas, debe poner la fuga de información en conocimiento de la autoridad nacional competente que, en España, es la Agencia Española de Protección de Datos. En el caso de empresas de otros sectores, si la fuga de información afecta a datos de carácter personal, está obligada a denunciar los hechos ante la misma autoridad citada. En ciertas ocasiones, el titular de los datos, que es la persona física cuyos datos se hayan visto afectados, deberá ser igualmente notificado. Este debe conocer los casos en los que la fuga haya comprometido su información, de modo que pueda realizar con la mayor celeridad posible actuaciones como el cambio de contraseñas o la revisión de sus cuentas bancarias. Por su parte, la AEPD se encargará de proponer medidas correctoras adecuadas con el objetivo de minimizar el daño o de abrir directamente el procedimiento de inspección oportuno, que puede terminar en archivo, apercibimiento o sanción.

3 Quién está obligado a notificar o denunciar

La diferencia entre la notificación y la denuncia es sutil. Por medio de la notificación, se pone en conocimiento del órgano de control que se ha sufrido una brecha de seguridad. Por medio de la denuncia, se hace lo mismo pero con intención de que se abra un procedimiento de inspección que puede acabar en sanción, apercibimiento o archivo.

Estos son los sujetos que, en España, están obligados a notificar o denunciar brechas de seguridad que sean causa de una violación de datos de carácter personal:

- **Notificación:** Están obligados a notificar sin dilaciones indebidas las brechas de seguridad que sean causa de la violación de datos:

- Los operadores de servicios de comunicaciones electrónicas disponibles al público.

- **Denuncia:** Están obligados a denunciar todas las personas jurídicas y los ciudadanos que tengan conocimiento de la brecha y la violación de datos. En relación con las empresas, destacamos el siguiente listado abierto:

- Comercios de todo tipo

- Empresas relacionadas con productos alimenticios, bebidas y tabacos

- Entidades de sanidad: clínicas, hospitales, etc.

- Contables, auditores y asesores fiscales
- Asociaciones y clubes
- Inmobiliarias
- Empresas de la industria química y farmacéutica
- Constructoras
- Turismo y hostelería
- Fabricantes y vendedores de maquinaria
- Fabricantes y vendedores de medios de transporte
- Escuelas, universidades y otros centros de formación
- Prestadores de servicios de transporte
- Aseguradoras privadas
- Empresas de servicios informáticos
- Agricultura, ganadería, explotación forestal, caza y pesca
- Entidades bancarias y financieras
- Producción de bienes de consumo
- Sector energético
- Despachos de abogados, notarios y registradores
- Actividades diversas de servicios personales
- Organizaciones empresariales
- Servicios sociales
- Empresas dedicadas a la publicidad directa
- Servicios de telecomunicaciones
- Casinos y casas de apuestas
- Empresas de seguridad
- Selección de personal
- Actividades postales y de correo
- I+D
- Partidos políticos y sindicatos
- Entidades religiosas
- Mutualidades
- Empresas de organización de ferias, exhibiciones y congresos
- Solvencia patrimonial y crédito
- ITV y similares
- Comercio y servicios electrónicos
- Comunidades de propietarios
- Empresas y entidades con otras actividades

La normativa española y, en particular, el artículo 41 de la Ley General de Telecomunicaciones, impone a los operadores que explotan redes públicas de comunicaciones electrónicas o que prestan servicios de comunicaciones electrónicas disponibles al público la obligación de adoptar las medidas necesarias, tanto técnicas como de gestión, para garantizar la seguridad y protección de los datos personales. Deben destacarse tres consideraciones fundamentales de este artículo:

• Por un lado, que ***"los operadores que exploten redes públicas de comunicaciones electrónicas*** *o que presten servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos,* ***deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad*** *en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar la protección de los datos de carácter personal".*

• Por otro, que *"en caso de violación de los datos personales, el operador de servicios de comunicaciones electrónicas disponibles al público* ***notificará sin dilaciones indebidas dicha violación a la Agencia Española de Protección de Datos"****.*

• Por último, que, *"si la violación de los datos pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o particular,* ***el operador notificará también la violación al abonado*** *o particular sin dilaciones indebidas".*

4 Primer paso: Investigación de la brecha

Todos los sujetos obligados a cumplir la normativa española de protección de datos, que pueden ser consultados en el artículo 2 de la Ley Orgánica 15/1999 (LOPD), están obligados a contar con un sistema adecuado de investigación de incidencias y brechas de seguridad.

Esta obligación se impone a través de dos artículos de la citada LOPD: el artículo 9.1, que establece la necesidad de adoptar medidas concretas de seguridad sobre los datos; y el artículo 10, que establece los deberes de guarda y custodia de los datos con el fin de que permanezcan en secreto e inaccesibles a terceros.

Artículo 9.1 LOPD. Seguridad de los datos.

> *El responsable del fichero, y, en su caso, el encargado del tratamiento* ***deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal*** *y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del*

estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Artículo 10 LOPD. Deber de secreto.

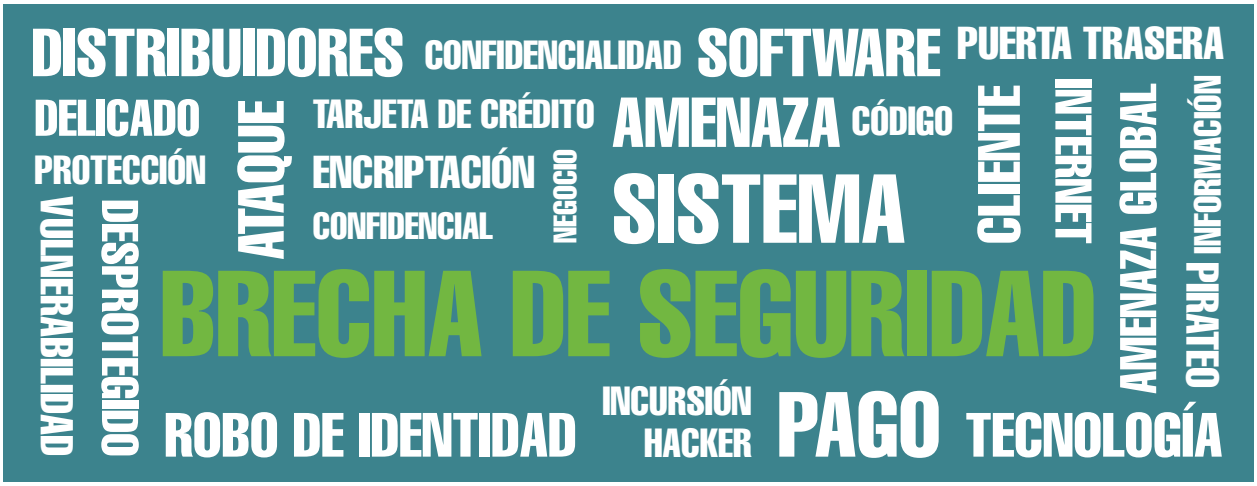
El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal ***están obligados al secreto profesional*** *respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.*

La normativa española de protección de datos convierte al responsable de los datos en custodio de los mismos. La implantación de medidas de seguridad se establece como imperativo y, de forma expresa, se determina que han de ser las necesarias para garantizar la seguridad de los datos.

El estado de la técnica hoy permite contar con sistema eficientes que analizan los ataques que la empresa sufre y que extraigan datos de ellos para definir las estrategias necesarias de prevención. El coste de estos sistemas varía en función de las características con las que se le quiera dotar. A pesar de ser tecnología de alto rendimiento, su precio no es elevado, sino accesible a cualquier empresa que quiera cumplir la ley.

Un ejemplo de herramienta asequible de seguridad ante ataques informáticos lo encontramos en el Jetpack Protect, que se ofrece de forma gratuita como plugin instalable dentro del popular CMS WordPress, de Attomatic, y que es usado por algunas de las principales empresas de antivirus del mundo. Esta herramienta de WordPress cuenta con una funcionalidad sencilla: previene de ataques por fuerza bruta con tecnología en la nube, identifica IP malintencionadas y las bloquea. Gracias a sistemas como este, los datos volcados en el gestor de contenidos están más seguros. Si una empresa con blog puede contar con algo más de protección de forma sencilla ante ataques informáticos, una empresa del sector de la salud o de las comunicaciones debería ya tener un sistema completo implantado en sus servidores para cubrir la obligación legal que les impone la LOPD de forma imperativa.

Las herramientas de análisis ante ataques informáticos permiten crear un mapa histórico completo de todos los intentos fallidos de crear brechas de seguridad, así como de las intrusiones realizadas con éxito. Estos sistemas son los únicos que permiten con cierto grado de eficacia poder conocer cuántos ataques se han recibido, cuál es su tipo y procedencia, así como estimar su resultado. En definitiva, permiten conocer, prevenir y actuar con información real, de manera rápida y sin dilaciones.



5 Segundo paso: Anotación de los detalles de la brecha y aplicación de las medidas correctoras

En caso de que el ataque haya afectado a los datos personales, que la empresa ha de guardar y custodiar, se deben registrar los detalles de la incidencia en el Documento de Seguridad interno de la empresa.

La normativa de protección de datos establece la obligación de registrar todas las incidencias que afectan a los datos personales. Esta obligación pesa sobre todos los sujetos obligados, desde una floristería local hasta una empresa de la industria militar.

Todas las empresas están obligadas a contar con un Documento de Seguridad completo y actualizado en el que figuren estas incidencias, de haberse producido. La falta

del documento o de la inscripción de los detalles de las brechas de seguridad sufridas pueden ser consideradas infracciones graves o muy graves, que son sancionadas con multas de hasta 600.000 euros. La decisión de registrar internamente estas incidencias debería estar motivada, primero, por la obligación legal a hacerlo, que imponen la LOPD y su reglamento, y, segundo, porque, si se llegase a investigar, este registro podría permitir la graduación de la cuantía de la sanción, según dispone el artículo 45.4 LOPD. Solo el hecho de no registrar las incidencias, además de ser una irresponsabilidad, es una infracción grave de la Ley.

Todas las empresas y demás sujetos obligados, sin excepción, deberán registrar las incidencias de forma que quede constancia de los siguientes datos en su Documento de Seguridad (artículo 90 del Real Decreto 1720/2007 o RLOPD):

- El tipo de incidencia.
- El momento en que se ha producido, o en su caso, detectado.
- La persona que realiza la notificación.
- La persona a quién se realiza la notificación.
- Los efectos que se hubieran derivado de la misma.
- Las medidas correctoras aplicadas.

Asimismo, además de establecer el registro, estas empresas deben contar con un procedimiento establecido de notificación y gestión de las incidencias que afecten a los datos de carácter personal.

En caso de los sujetos que están obligados a notificar las brechas de seguridad, han de anotarse en el Documento de Seguridad los detalles ya indicados, con especial atención a los relativos al tipo de brecha de seguridad sufrida, la notificación a la AEPD y, en su caso, la notificación a los particulares afectados.

Por último, en caso de que la empresa o el sujeto obligado que correspondiese realizasen un tratamiento de datos de nivel medio o alto, estarían igualmente obligadas a registrar las incidencias que los afecten, derivadas de brechas de seguridad. Sin embargo, según se dispone en el artículo 100 del RLOPD, a estas empresas **se les exige que incluyan algunos datos adicionales en el registro:**

- Los procedimientos realizados de recuperación de los datos.
- La persona que ejecutó cada proceso de recuperación de los datos.
- Los datos restaurados.
- Una indicación sobre los datos que ha sido necesario grabar manualmente en el proceso de recuperación, en su caso.

En todos los casos, la normativa exige indicar el tipo de brecha sufrida. Esta información solo se puede conocer si se cuenta con un sistema que detecte y analice los ataques informáticos sufridos y que permita prever acciones concretas para evitarlos o protegerse ante ellos.

6 Tercer paso: Notificar la brecha o denunciar

Las brechas de seguridad no siempre producen consecuencias sobre información o datos personales. Pero, en caso de que sí lo hagan, la empresa está obligada a consignar la incidencia en su documento interno de seguridad, al tiempo que realiza una de estas dos acciones: notificar el ataque o denunciar la intrusión.

6.1. Notificar brechas de seguridad

6.1.1. Brechas de seguridad que se deben notificar

En España, tres textos normativos vigentes regulan de forma expresa la obligación de notificar quiebras de seguridad: la Directiva 2002/58/CE; la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, que transpone a España la citada directiva; y el Reglamento (UE) nº 611/2013, que desarrolla también la misma directiva. Las dos últimas normas parten de la primera, así que se basan en los principios y conceptos jurídicos de esta.

Dicha Directiva 2002/58/CE, también llamada 'Directiva sobre la privacidad y las comunicaciones electrónicas', indica que la obligación de notificar surge cuando se produce una *"violación de datos personales"*. Una violación de datos es definida por la norma como la *"violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público en la Comunidad"*.

Las conclusiones que obtenemos de la Directiva sobre la privacidad y las comunicaciones electrónicas acerca de qué tipo de brechas deben notificarse son las siguientes:

1. Se deben notificar las brechas que hayan afectado a datos personales.

Una entidad no está obligada a notificar todas las violaciones de seguridad que sufra, sino solo aquellas que afecten a datos de carácter personal. Es decir, a información que identifique o permita identificar a una persona física. En particular, la Directiva 95/46/CE, origen de la normativa de protección de datos

en Europa, define los datos personales como *"toda información sobre una persona física identificada o identificable (el «interesado»)"*. Además, aclara que *"se considerará identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"*. De este modo, la obligación de notificar que establece la Directiva 2002/58/CE opera únicamente cuando la brecha de seguridad afecte a datos que identifiquen o puedan llegar a identificar a un individuo concreto.

2. La causa que haya provocado la brecha de seguridad es intrascendente.

Hay que notificar siempre. Toda brecha de seguridad se debe notificar, con independencia de la causa. Ya se ha indicado que una violación de seguridad puede tener orígenes diversos. Una de las más habituales es la de los ataques informáticos externos, aunque la brecha también se puede deber a la pérdida de un dispositivo de almacenamiento, a la mala administración de personas autorizadas al acceso o a la exposición indeseada de la información en la Red. Si el culpable es un empleado, la responsable es la empresa para la que trabaja, bien por haberlo elegido o bien por no haberlo vigilado. Sea cual fuera la causa de la brecha, habrá que notificarla adecuadamente.

La Ley General de Telecomunicaciones no añade más a lo ya dispuesto por la Directiva. Y, por su parte, el Reglamento (UE) nº 611/2013 tan solo desarrolla cuestiones de índole práctica.

Ley General de Telecomunicaciones señala una serie de medidas técnicas y de gestión mínimas adecuadas para preservar la seguridad en la explotación de la red o en la prestación de los servicios de los operadores que explotan redes públicas de comunicaciones electrónicas o que prestan servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos. Estas medidas obligatorias, técnicas y de gestión, que tienen el fin de garantizar la protección de los datos de carácter personal, deberán incluir, como mínimo:

- La garantía de que **solo el personal autorizado tenga acceso a los datos** personales para fines autorizados por la Ley.
- **La protección de los datos personales del acceso o revelación no autorizados o ilícitos**, así como de la destrucción accidental o ilícita y la pérdida o alteración accidentales o el almacenamiento o tratamiento, no autorizados o ilícitos.
- **La garantía de la aplicación efectiva de una política de seguridad** con respecto al tratamiento de datos personales.

La Agencia Española de Protección de Datos, en el ejercicio de su competencia de garantía de la seguridad en el tratamiento de datos de carácter personal, podrá examinar las medidas adoptadas por los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público y podrá formular recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad que debería conseguirse con estas medidas.

En caso de violación de los datos personales, el operador de servicios de comunicaciones electrónicas disponibles al público está obligado a notificar sin dilaciones indebidas dicha violación a la Agencia Española de Protección de Datos.

La ley establece dos escenarios en los que es necesario informar a los particulares:

1) Si la violación de los datos pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o particular,

el operador está obligado a informar de la violación al abonado o particular sin dilaciones indebidas.

2) En caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas deberá informar a los abonados sobre dicho riesgo y sobre las medidas a adoptar.

6.1.2. Quién está obligado a notificar una brecha de seguridad

Las empresas del sector de las comunicaciones electrónicas están obligadas a notificar las brechas de seguridad que comprometan información personal.

La obligación de notificar, en la fecha de cierre de este informe, recae sobre:

1. **Los operadores que explotan redes públicas de comunicaciones electrónicas.**
2. **Los prestadores de acceso a Internet o ISP (Internet Service Providers).**

Esta obligación solo se establece para los casos en los que la brecha de seguridad suponga la pérdida, modificación, destrucción o acceso no consentido a datos de carácter personal.

En los próximos años, esta obligación de notificar brechas de seguridad recaerá sobre más sujetos. La Comisión Europea considera necesario ampliar la operatividad del régimen de notificaciones al resto de sectores. Esta consideración se ha plasmado por escrito en la Directiva 2009/136/CE.

Considerando 59 de la Directiva 2009/136, de 25 de noviembre:

> *"la notificación de violaciones de la seguridad refleja un interés general de los ciudadanos por ser informados acerca de fallos en la seguridad que puedan implicar la pérdida de sus datos personales o algún otro riesgo para dichos datos […] por lo que deben introducirse, a escala comunitaria y con carácter prioritario, requisitos de notificación explícitos y obligatorios en todos los sectores".*

Es previsible que esta obligación de notificar las violaciones de seguridad que afectan a datos personales vaya a extenderse a todos los sectores por medio del esperado Reglamento General Europeo de Protección de Datos, que se encuentra en fase de negociación en el seno de la Unión Europea.

Las empresas que prestan servicios de comunicaciones electrónicas están obligadas a notificar las brechas de seguridad que supongan una violación de datos personales en virtud del artículo 4.3 de la Directiva 2002/58/CE, el artículo 41 de la Ley General de Telecomunicaciones y los artículos 2 y 3 del Reglamento (UE) nº 611/2013.

Artículo 2 c) de la Directiva 2002/21/CE:

> *"Servicio de comunicaciones electrónicas: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos; quedan excluidos asimismo los servicios de la sociedad de la información […]".*

La obligación afecta a las empresas de telecomunicaciones y a los proveedores de acceso a Internet o ISP, pero no a las empresas que ofrecen contenido a través de la red ni a las que prestan otros servicios de la sociedad de la información.

6.1.3. Se ha de notificar la brecha a la AEPD y al particular afectado

La empresa debe notificar las brechas de seguridad por tres medios: a sí misma a través del registro de la incidencia en el Documento de Seguridad interno; a la Agencia Española de Protección de Datos por medio de una comunicación con contenido definido en la normativa; y, en ciertos casos, al usuario cuyos datos personales hayan sido violados.

La obligación de notificar las quiebras de seguridad que afecten a datos personales se introdujo por primera vez en la Directiva 2002/58/CE, en la redacción dada por la Directiva de modificación 2009/136/CE.
El artículo 4 de la Directiva 2002/58/CE obliga a comunicar dicha violación:

1. **A la autoridad nacional competente, que en España es la AEPD**
2. **Al particular afectado**, solo en el caso de que las consecuencias de la brecha puedan afectar negativamente a su intimidad o a sus datos personales.

3. **La brecha de seguridad deberá anotarse en un inventario**, según dispone el artículo 90 del RLOPD, donde se recojan todas las brechas que vaya sufriendo la empresa. Respecto de cada brecha, habrán de anotarse los hechos que la han provocado, sus efectos y las medidas adoptadas.

La Directiva 2002/58/CE habilita a la Comisión Europea a determinar las medidas técnicas de ejecución sobre el procedimiento, circunstancias y forma de presentación de la notificación de la quiebra. La Comisión lo ha hecho a través del Reglamento (UE) nº 611/2013, que se estudia en el apartado 5 de este Informe.

La obligación de notificación que se analiza, introducida por la Directiva citada, ha sido objeto de transposición al Ordenamiento jurídico español a través del actual artículo 41 de la Ley General de Telecomunicaciones. Este se limita a reproducir, casi íntegramente, las disposiciones establecidas por el artículo 4 de la Directiva 2002/58/CE.

Únicamente difiere en un extremo. Establece que el contenido y el formato del inventario donde se anoten todas las brechas de seguridad que sufra una empresa se va a determinar por real decreto. En relación con esto último, ha de tenerse en cuenta que la normativa española de protección de datos, en concreto el Real Decreto 1720/2007, dispone en su artículo 90 que es en el Documento de Seguridad donde han de registrarse todas las incidencias, incluidas las brechas de seguridad, que afecten a datos personales.

El Reglamento (UE) nº 611/2013, directamente aplicable en todos los Estados de la UE sin necesidad de transposición, no amplia el catálogo de sujetos obligados. Este reglamento se elaboró para dar respuesta a otra cuestión y que es la siguiente: toda violación de datos personales sufrida por una empresa del sector de las comunicaciones electrónicas se debe de notificar siempre a la autoridad nacional competente, que en España es la AEPD.

Artículo 2.1 del Reglamento (UE) nº 611/2013:

> *"Los proveedores notificarán todos los casos de violación de datos personales a la autoridad nacional competente".*

La normativa no incluye un ámbito competencial que delimite cuándo ha de recibir la notificación la Autoridad de un Estado y cuándo la de otro. Esta deficiencia es especialmente problemática si se tiene en cuenta, como plantea el Grupo de Trabajo del artículo 29 en su Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments, que **es posible que la empresa que sufre la quiebra esté establecida en un Estado; que la brecha tenga lugar en otro, donde tenga sus instalaciones; y que los afectados se encuentren en varios Estados. Ante qué organismo se presenta la notificación es un problema que trata de resolver, en la medida de lo posible, el Reglamento (UE) nº 611/2013, que prevé, en su artículo 2.5, que la autoridad a la que se haya notificado informe a las demás autoridades afectadas**.

En cuanto a **la notificación al propio interesado, no es obligatoria siempre; solo en algunos casos: cuando pueda afectar negativamente a sus datos personales o a su intimidad**. Para determinar si concurre o no este requisito, es decir, si afecta negativamente a los datos personales o intimidad del afectado, se ha de atender a las circunstancias contempladas en el artículo 3.2 del Reglamento (UE) nº 611/2013. Así, deben evaluarse:

- La naturaleza y el contenido de la información personal comprometida. Especialmente, ha de evaluarse si se trata de datos financieros, de datos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas o la pertenencia a sindicatos del particular, de datos sobre salud o sexualidad, de datos de localización, de registros de Internet, de registros de navegación en Internet, de datos de correo electrónico o de listas de llamadas.
- Las posibles consecuencias de la violación para el particular. Especialmente, si puede conllevar fraude o usurpación de su identidad, daños físicos, sufrimiento psicológico humillación o perjuicio reputacional.
- Las propias circunstancias en que se haya producido la violación de datos personales, atendiendo particularmente a su origen y al momento en que la empresa afectada haya llegado a conocer que la información personal se encuentra en poder de un tercero no autorizado.

El Dictamen 03/2014 sobre la notificación de violación de datos personales elaborado por el Grupo de Trabajo del artículo 29 resulta muy ilustrativo a la hora de interpretar estas circunstancias. Este texto contiene una lista de supuestos en los que la empresa que sufre la brecha de seguridad está obligada a notificar a los particulares. Junto a cada ejemplo, se detallan una serie de medidas

que hubieran podido evitar el compromiso de los datos. A pesar de que esta lista es simplemente ejemplificativa, se erige como una referencia comparativa muy útil para determinar cuándo una brecha afecta negativamente al interesado y, por ende, cuándo ha de notificársele la violación.

Ejemplo obtenido del Dictamen 03/2014 sobre la notificación de violación de datos personales:

Un empleado de un ISP facilita a un tercero un nombre de usuario y contraseña con el que puede accederse a la base de datos de los clientes. Este podría acceder a datos de pago, lo que conllevaría repercusiones financieras para los afectados. Asimismo, podría utilizar la dirección de correo electrónico y la contraseña de los clientes para tratar de acceder a otros servicios en línea.

Los particulares han de ser notificados de la brecha de seguridad, de forma que modifiquen cuanto antes la contraseña comprometida y cancelen cualquier cargo producido de modo fraudulento en su cuenta bancaria.

Es evidente que esta brecha de seguridad puede afectar negativamente al perjudicado, por lo que debe conocerla y tomar las precauciones adecuadas.

6.1.4. Circunstancias de la notificación

El sistema de notificación se detalla en el Reglamento (UE) nº 611/2013, aplicable desde el 25 de agosto de 2013. Su artículo 2 describe el sistema de notificación a la autoridad nacional competente, mientras que el artículo 3 del mismo Reglamento se encarga de la notificación al titular de los datos. Creando un sistema único, la Comisión pretende evitar que cada Estado introduzca regímenes diferentes, excesivamente complejos o excesivamente costosos.

6.1.4.1. Cuándo se debe notificar a la AEPD y al particular afectado

El Reglamento (UE) nº 611/2013 establece un sistema de notificación en dos fases:

1) Fase 1: Notificación inicial. Se ha de realizar una notificación inicial, si fuera posible, en el plazo de 24 horas desde la detección del incidente.

2) Fase 2: Notificación complementaria. Posteriormente, en el plazo de 3 días desde la notificación inicial, se realizará una segunda notificación complementaria que añada las circunstancias desconocidas en un primer momento.

El Grupo de Trabajo del artículo 29 ha apoyado este sistema de dos fases en su Dictamen 06/2012, ya que permite combinar una rápida capacidad de reacción con el máximo rigor posible.

Desde el momento en que la entidad del sector de las comunicaciones electrónicas, a las que el Reglamento se refiere como proveedores, tenga conocimiento suficiente de que ha sufrido un incidente de seguridad que comprometa datos personales, es decir, desde que detecte la violación de datos personales, deberá notificar el caso a la Autoridad Nacional competente en el plazo de 24 horas, en la medida de lo posible. En el caso de que en ese momento no disponga de toda la información exigida por el Anexo I del Reglamento, que detallamos también en este informe, el proveedor notificará al menos la de la Sección 1 de la misma norma.

Desde ese momento, dispondrá de otras 72 horas para remitir una segunda notificación que ya incluya también los extremos de la Sección 2 del Anexo I. Cuando, a pesar de la labor de investigación realizada en ese plazo, no pueda disponer de toda la información necesaria, notificará la que tenga justificando el motivo del retraso y enviará el resto en el plazo más breve posible.

En cuanto a la notificación al particular afectado:

- **Debe enviarse sin dilaciones injustificadas**, aunque puede demorarse con la autorización de la Agencia Española de Protección de Datos.
- **Tiene que enviarse completa y en una sola fase**.

El Reglamento no exige remitir la notificación al particular afectado en un plazo determinado, pero sí establece que se realice sin dilaciones injustificadas. Por otro lado, esta notificación no puede dividirse en dos fases.

Aunque estas diferencias son relevantes, la diferencia más importante con respecto a la notificación a la autoridad competente es la posibilidad de que la notificación a los particulares sea demorada, previa autorización de la autoridad competente, cuando esta pueda comprometer la investigación de la violación.

6.1.4.2. Cómo debe ser la notificación a la AEPD y al particular afectado

El contenido de la notificación a la Autoridad Nacional competente será más completo que el contenido de la notificación que debe realizarse, en su caso, al particular afectado.

Cuando una entidad del sector de las

comunicaciones electrónicas se vea obligada a notificar una quiebra de seguridad a la autoridad nacional competente, **dicha notificación deberá de tener el siguiente contenido mínimo**, según dispone el Anexo I del Reglamento (UE) Nº 611/2013 de la Comisión:

- **Sección 1**

Contenido mínimo para la notificación inicial.

- **Deberá identificar al proveedor**, detallando su denominación, identidad y un punto de contacto que podrá ser los datos de contacto del responsable de protección de datos, de forma que la autoridad pueda obtener más información. Además, se hará referencia a si se trata de una primera o una segunda notificación.
- **Incluirá la información disponible sobre el incidente**, que podrá completarse mediante notificaciones posteriores. Fecha y hora en que ha tenido lugar la brecha, fecha y hora en que se ha detectado, causa u origen, naturaleza y contenido de los datos comprometidos, medidas que se han aplicado o se van a aplicar.

- **Sección 2**

Contenido mínimo adicional para la notificación complementaria.

- **Información suplementaria sobre la violación de datos personales**. Resumen del incidente, incluyendo la ubicación física de la violación y del soporte de almacenamiento comprometido; número de particulares afectados; posibles efectos negativos para estos; medidas adoptadas para paliarlos.
- **Posible notificación adicional a los particulares:** número de particulares notificados, contenido y medio utilizado.
- **Notificación a las autoridades competentes de otros Estados Miembros**, en caso de que la violación tenga carácter transfronterizo.

Por su parte, **cuando sea obligatorio notificar a los particulares que pueden sufrir efectos adversos por la violación, dicha notificación hará referencia a los extremos siguientes**, detallados en el Anexo II del Reglamento:

- **Nombre del proveedor, identidad y datos de contacto**.
- **Resumen del incidente**.
- Fecha estimada en que se ha producido.
- Naturaleza y contenido de los datos personales comprometidos.
- Posibles efectos adversos para los particulares.
- Causa u origen de la violación.
- Medidas adoptadas por el proveedor y medidas que propone al particular.

6.1.4.3. Cómo se debe notificar a la AEPD y al particular afectado

El Reglamento exige que la autoridad competente en cada Estado Miembro facilite un procedimiento de notificación electrónico, además de información suficiente sobre su acceso y utilización.

La AEPD habilitó un formulario online accesible a través de la Sede Electrónica de la AEPD en el apartado *"Notificación de quiebras de seguridad"*. La AEPD lo puso a disposición de los sujetos obligados el 23 de marzo de 2014. Es "*un canal rápido y seguro para que los proveedores de servicios de comunicaciones electrónicas notifiquen a la Agencia los casos previstos en la legislación*", en palabras de la AEPD, según el artículo 'Protección de Datos lanza un nuevo sistema para *"reforzar garantías"* en las notificaciones de quiebras de seguridad' publicado por Europa Press el 23 de abril de 2014.

La notificación a los particulares se realizará *"por vías de comunicación que garanticen una pronta recepción de la información y sean seguras con arreglo al estado actual de la técnica"*, según dispone el artículo 3.6 del Reglamento. Además, esta norma aclara que esta notificación no podrá hacer referencia a cuestiones distintas de la propia brecha de seguridad. Por ejemplo, la notificación no podrá utilizarse para promocionar nuevos servicios, pero tampoco será posible notificar la violación en una factura corriente.

6.1.4.4. Debe registrarse la brecha

La brecha de seguridad, la notificación a la AEPD y, en su caso, la notificación a los particulares afectados han de anotarse en el Documento de Seguridad de la empresa que la sufra, en cumplimiento del artículo 90 RLOPD.

6.1.4.5. Se sanciona al que no notifica

Si una empresa sufre una violación de datos personales y no lo notifica a la autoridad de control y, en su caso, a los particulares afectados, está incumpliendo una obligación legal. La Ley General de Telecomunicaciones no incluye en su catálogo de infracciones la ausencia de notificación de una brecha, por lo que podría parecer que incumplir esta obligación carece de consecuencias. Sin embargo, sí hay consecuencias.

El artículo 41.4 de la Ley General de Telecomunicaciones aclara que la LOPD y el Real Decreto 1720/2007 también son aplicables.

Así, las sanciones derivadas de incumplir el deber de notificación se contemplan en la LOPD. Su artículo 44.2 a) considera infracción leve la no remisión a la AEPD de las notificaciones previstas en la Ley. Entre ellas, se puede incluir la ausencia de notificación de una brecha de seguridad que, por tanto, podría conllevar una multa de entre 900 y 40.000 euros. Por su parte, no notificar a los afectados cuando fuere necesario podría constituir una infracción grave, conforme al artículo 44.3 g) de la LOPD. La sanción derivada de este incumplimiento sería una multa comprendida entre los 40.001 € y los 300.000 euros.

A las cuantías de la sanciones por no notificar habría de sumarse la cuantía de la sanción por no haber implementado las medidas de seguridad necesarias para evitar la quiebra de seguridad, considerada infracción grave conforme al artículo 44.3 h). Esta podría fijarse entre los 40.001 € y los 300.000 euros. Y si la brecha fuera la causa de una infracción muy grave, según los casos tasados en el artículo 44.4 LOPD, la sanción sería de una multa de entre los 300.001 y los 600.000 euros.

En definitiva, no notificar una brecha de seguridad podría dar lugar a:

- Varias multas por valor en suma de hasta 340.000 euros.

- Una multa de hasta 300.000 euros por no haber evitado la brecha.

- Hasta 600.000 euros de multa en casos concretos.

Es conveniente notificar. Y, para ello, es muy recomendable contar con un sistema que detecte y analice las intrusiones y los ataques en general.

6.1.4.6. Casos en los que se puede evitar notificar al particular afectado

La Directiva 2002/58/CE y la Ley General de Telecomunicaciones exigen que las empresas del sector de las comunicaciones electrónicas adopten las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios[1]. Estas medidas deberán, como mínimo:

- Garantizar que solo el personal autorizado pueda acceder a los datos personales protegidos.

- Protegerlos de la destrucción, pérdida, alteración, almacenamiento, acceso o revelación no autorizados.
- Garantizar la aplicación efectiva de una política de seguridad.

La violación de datos personales puede deberse a que alguna de esta medidas ha fallado, lo que genera la obligación de comunicar la brecha a la autoridad

1 La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) ha publicado unas Directrices Técnicas que hacen referencia a las medidas técnicas y de gestión más adecuadas.

competente. Esta obligación de notificar a la autoridad competente no será objeto de excepción en ningún caso. Es decir, siempre habrá que notificar a la Agencia Española de Protección de Datos, cuando los datos personales se vean afectados.

Tan solo existe un tipo de brecha sobre la que no se debe informar a la AEPD: aquella sobre la que se tiene certeza de que no ha afectado en modo alguno datos personales, aun habiendo podido ponerlos en riesgo. **En este caso, la brecha debe registrarse internamente**, pudiendo ser en el propio Documento de Seguridad, para desarrollar e implementar las medidas de precaución y seguridad necesarias por si volviese a tener lugar esa intrusión u otra similar.

La notificación a los particulares no es necesario realizarla en estos supuestos:

- **Cuando la intrusión y la violación de datos no pueda afectar negativamente a los datos personales o a la intimidad del particular.**
- **Cuando los datos extraídos estén debidamente cifrados y sean incomprensibles** y, consecuentemente, la intrusión y la violación de datos no pueda afectar negativamente a los datos personales o a la intimidad del particular.

El supuesto de la inteligibilidad está contemplado tanto en la Directiva 2002/58/CE como en la Ley General de Telecomunicaciones: cuando la empresa que haya sufrido la quiebra de seguridad pruebe a la autoridad competente que ha aplicado a los datos afectados las medidas de seguridad necesarias para hacerlos incomprensibles no tendrá la obligación de notificar la brecha a los particulares afectados.

Es decir, la obligación de notificar se excepciona cuando los terceros no autorizados no puedan acceder a la información comprometida. El Reglamento (UE) nº 611/2013 considera los datos incomprensibles en dos casos:

- **Cuando se hayan cifrado de forma segura y la clave no haya sido comprometida .**
- **Cuando se hayan sustituido por su valor resumen (hash value), calculado mediante una función resumen cuya clave no haya quedado comprometida[2].**

Esta excepción es lógica ya que, si los sujetos que han obtenido la información personal sin estar legitimados no pueden comprenderla, el riesgo para los particulares será nulo. Las personas físicas no podrán verse negativamente afectados por la quiebra.

Dictamen 03/2014 sobre la notificación de violación de datos personales del Grupo de Trabajo del artículo 29:

"La razón de ser de esta excepción a la notificación de las personas es que unas medidas adecuadas pueden reducir los riesgos residuales para la privacidad del interesado a un nivel insignificante. La violación de la confidencialidad de datos personales cifrados mediante un algoritmo de tecnología avanzada sigue siendo una violación de datos personales que debe notificarse a la autoridad. No obstante, si la clave de confidencialidad está intacta, los datos, en principio, resultarán incomprensibles para las personas no autorizadas, así que la violación probablemente no afectará negativamente al interesado y, por tanto, no será necesario notificársela".

Aun así, aclara posteriormente en el mismo Dictamen que no puede afirmarse de forma absoluta que la adopción de medidas de cifrado sea suficiente para que la obligación de notificar ceda. Podría darse el caso de que la empresa que sufre la quiebra no tenga una copia de seguridad de esos datos. Es cierto que los datos serán inaccesibles, pero la pérdida de estos también supone una violación si no se pueden recuperar.

6.1.4.7. Otras obligaciones de notificación

Las entidades del sector de las comunicaciones electrónicas no solo deben notificar las violaciones de datos personales que sufran. Existen otros dos supuestos de hecho que generan obligaciones de notificación:

1. Estas empresas están obligadas a notificar a sus abonados los riesgos particulares de violación de seguridad en la red, según los artículos 4.2 de la Directiva 2002/58/CE y 41.2 de la Ley General de Telecomunicaciones.

2. Las empresas del sector de las comunicaciones electrónicas deberán notificar a la autoridad de reglamentación, que es en España la Comisión Nacional de los Mercados y la Competencia (CNMC), *"las violaciones de la seguridad o pérdidas de integridad que hayan tenido un impacto significativo en la explotación de las redes"*, según el artículo 13 bis de la Directiva 2002/21/CE, en la redacción introducida por la Directiva 2009/140/CE. Sin embargo,

2 Informe sobre la necesidad legal de cifrar información y datos personales, (Abanlex, 2014)

esta obligación no ha sido transpuesta al Ordenamiento jurídico español.

6.1.4.8. Proyecto europeo: Incluir otros sectores en la obligación de notificar

La obligación de notificar las violaciones de datos personales introducida por la Directiva 2002/58/CE, transpuesta a nuestro Ordenamiento jurídico en el artículo 41 de la Ley General de Telecomunicaciones y desarrollada a través del Reglamento (UE nº 611/2013), solo afecta expresamente a las empresas de un sector: el de las comunicaciones electrónicas. Por tanto, las empresas de cualquier otro sector no están obligadas a notificar las quiebras de seguridad que comprometan información personal ni a la autoridad competente ni a los particulares afectados.

Sin embargo, la entrada en vigor del futuro Reglamento general europeo de protección de datos va a ampliar, según se estima, el catálogo de sujetos expresamente obligados. Con su entrada en vigor, deberá notificar cualquier responsable del tratamiento, no ya solo las empresas del sector de las comunicaciones electrónicas. De esta manera, la Comisión Europea podrá materializar un objetivo en el que llevaba trabajando varios años. Ya en 2009, cuando se introdujo la obligación de notificar limitada a las empresas del sector de las comunicaciones electrónicas, la Comisión declaró ante el Parlamento Europeo que iba a comenzar el trabajo preparatorio para extender la obligación a otros sectores. Luego, lo corroboró a través del Considerando 59 de la Directiva 2009/136/CE:

> *"la notificación de violaciones de la seguridad refleja un interés general de los ciudadanos por ser informados acerca de fallos en la seguridad que puedan implicar la pérdida de sus datos personales o algún otro riesgo para dichos datos […] por lo que deben introducirse, a escala comunitaria y con carácter prioritario, requisitos de notificación explícitos y obligatorios en todos los sectores".*

El régimen de notificación de la todavía Propuesta de Reglamento es similar al regulado en la Directiva 2002/58/CE y en la Ley General de Telecomunicaciones. Se recoge, previsiblemente, en los artículos 31 y 32 del futuro Reglamento. El primero regulará la notificación a la autoridad nacional competente y el segundo la notificación a los particulares afectados.

Al igual que la Directiva 2002/58/CE habilitaba a la Comisión para elaborar una norma de desarrollo, que fue el Reglamento (UE) nº611/2013, la Propuesta de Reglamento procede de la misma forma. Así, el régimen no estará completo hasta la aprobación de dicha norma de desarrollo. Sin embargo, lo más eficiente sería, en lugar de aprobar un nuevo texto normativo, ampliar el ámbito de aplicación del Reglamento (UE) nº611/2013, de forma que sirviera para detallar el régimen de notificación de cualquier violación de datos personales, sin importar el sector al que pertenezca la entidad que la sufra.

La única diferencia en el futuro Reglamento es que sí contemplará las sanciones que habría de afrontar quien sufriera un ataque con violación de datos personales y no cumpla la obligación de notificar. Según su artículo 79.6 h), aún solo propuesto, la autoridad competente podría imponer una multa de hasta 1.000.000 de euros o, si se trata de una empresa, de hasta el 2% de su volumen anual mundial de negocio.

6.2. Denunciar la comisión de una infracción

Los responsables de datos que tengan conocimiento de la comisión de una infracción de protección de datos están obligados a denunciar los hechos, con el objetivo de garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar (artículo 1 LOPD).

Del hecho de que la Propuesta de Reglamento vaya a introducir la obligación de notificar de forma expresa no se puede colegir que los responsables del tratamiento no tengan la obligación de denunciar ya en la actualidad. Al menos en España, la tienen, pero no la suelen cumplir cuando los responsables que merecen sanción son ellos mismos.

La normativa vigente en España exige la auto-denuncia en caso de sufrir una brecha de seguridad que afecte a datos de carácter personal de los que se es responsable.

Hoy día, la existencia de esta obligación se fundamenta en tres motivos:

1. **Primer motivo: Como responsable del fichero o del tratamiento, una persona física o jurídica está obligada tanto a guardar secreto** sobre los datos que posea, conforme al artículo 10 de la LOPD, **como a implementar todas las medidas técnicas y organizativas que garanticen la seguridad de los datos**, como establece el artículo 9 de la LOPD. Cuando se produce una brecha

de seguridad que pone al descubierto información personal, la medida más idónea para evitar ciertas consecuencias negativas consiste en comunicar los hechos a la AEPD y a los particulares afectados, de forma que puedan poner remedio con la máxima celeridad y, con ello, minimizar el daño. **Puesto que a la AEPD a día de hoy no se puede notificar esta circunstancia, lo establecido en la ley y obligatorio es presentar una denuncia contra uno mismo, así como una comunicación de los hechos dirigida a las personas físicas cuyos datos se hayan visto comprometidos.**

Artículo 9.1 LOPD:

"El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".

El derecho a la protección de datos se ha configurado como un derecho fundamental en el artículo 18.4 de la Constitución Española, como un derecho fundamental que otorga a cada individuo la facultad de decidir el destino de sus datos personales, de forma que pueda combatir las agresiones que provengan del uso mecanizado de estos. A un responsable de datos la ley le obliga a presentar una denuncia con el objetivo de contribuir decisivamente a la preservación de

este derecho fundamental, limitando los efectos adversos de una quiebra en su seguridad, con independencia de si el responsable de los hechos es él mismo.

2. **Segundo motivo: El Reglamento 1720/2007 establece una obligación de notificar las incidencias que afecten a datos personales**. En este caso, dos interpretaciones de la norma son posibles: que la notificación haya de hacerse al particular afectado; o que la notificación haya de hacerse a la AEPD.

Artículo 90 del Real Decreto 1720/2007:

"Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la

notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas".

3. **Tercer motivo:** El artículo 45.5 de la LOPD establece una serie de supuestos en los que la AEPD puede establecer la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate. Los más significativos son los siguientes: *"cuando la entidad infractora haya regularizado la situación irregular de forma diligente"*; y *"Cuando el infractor haya reconocido espontáneamente su culpabilidad"*. En el primer supuesto se establece una relación directa con el correcto registro de la incidencia en el Documento de Seguridad y la consecuente aplicación de las medidas para solventar el fallo. El segundo supuesto es un complejo ya que puede ser interpretado ese reconocimiento espontáneo como aquel que sucede en uno de estos casos: cuando se auto-denuncia; cuando notifica los hechos a los afectados; cuando recibe una mera solicitud de información de la AEPD como parte del proceso de inspección.

Uniendo los tres motivos con el artículo primero de la LOPD, que establece el objeto de la ley, se determina que existe una obligación de presentar una denuncia ante el conocimiento cierto de una infracción consistente en la violación de datos de carácter personal.

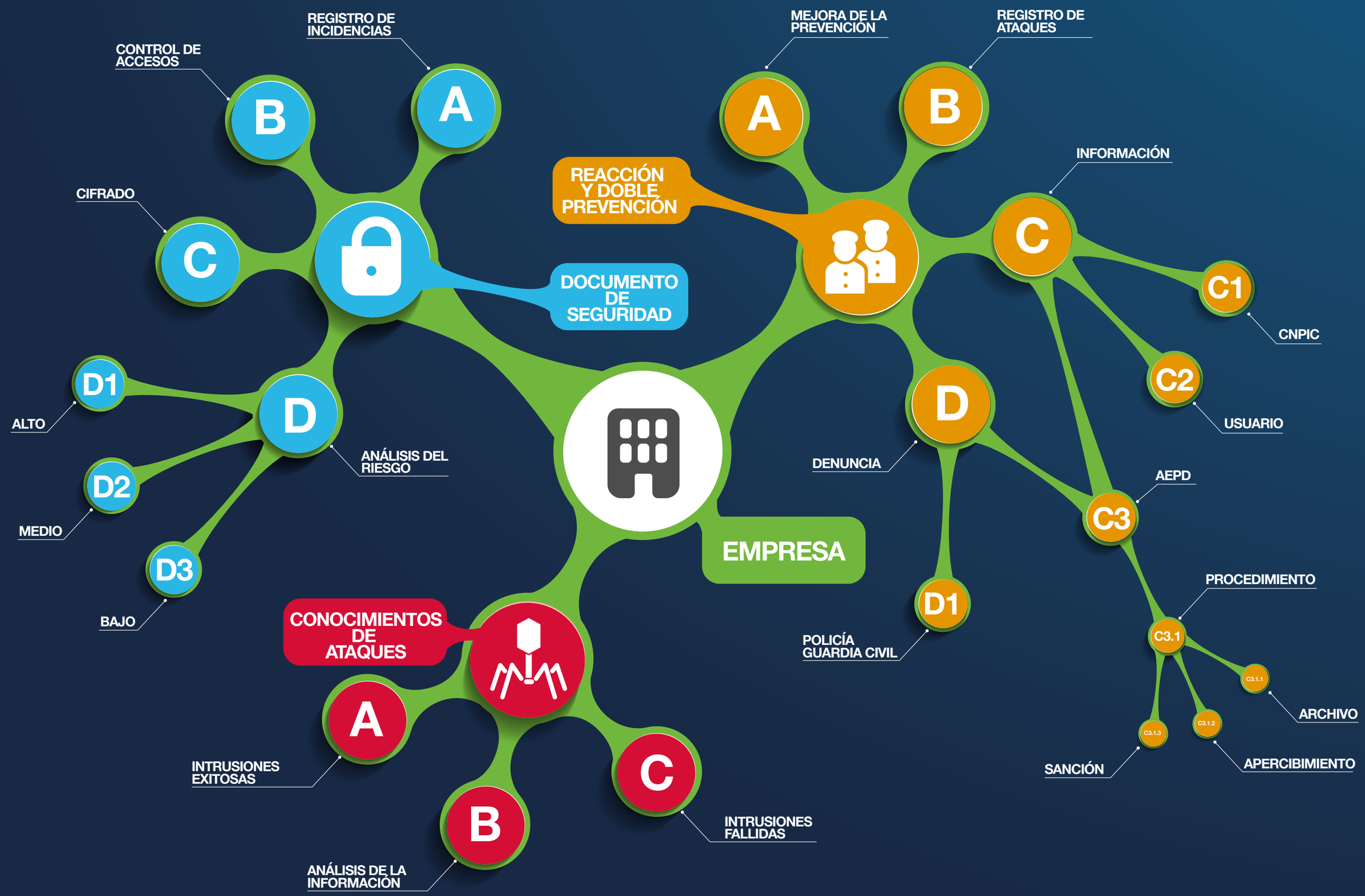
La mayoría de las empresas incumplen esta obligación y no realizan notificación alguna, tratando de evitar cualquier inspección y sanción por parte de la AEPD. No obstante, ya existen varias empresas que han actuado correctamente, notificando sus fallos de seguridad a la AEPD a través de auto-denuncias. Estas han conseguido minimizar el daño que han provocado las brechas de seguridad, además de lograr que la AEPD pusiera fin a los procedimientos sancionadores con su archivo o con una reducción sustancial de la cuantía de la sanción, gracias a la aplicación de los artículos 45.4 y 45.5 o 45.6 de la LOPD.

Así, los procedimientos PS/00279/2013, PS/00623/2012, E/00364/2013 y A/00192/2013, todos relativos a entidades que se auto-denunciaron por haber sido víctimas de brechas de seguridad, terminaron archivados. Tan solo el procedimiento PS/00496/2013 finalizó con una sanción de 3.000 euros.

El resultado es positivo si se tiene en cuenta que las infracciones que habían cometido al sufrir la brecha de seguridad eran graves, por lo que la AEPD les podía haber impuesto sanciones de hasta 300.000 euros. Habían infringido la obligación de implementar medidas de seguridad adecuadas, el deber de secreto y la obligación de no ceder datos personales a terceros sin la autorización de los afectados y, a pesar de ello, los procedimientos terminaron en archivo o con una multa de cuantía mínima.

En relación con la obligación de notificar la brecha de seguridad a los particulares, las normas que se deben seguir son las mismas que en el caso de los obligados a notificar las brechas de seguridad a la AEPD.

En conclusión: La implantación de las medidas de seguridad adecuadas, incluidos los sistemas de detección y análisis de intrusiones necesarios, permiten proteger los datos de los particulares y la información privada de la empresa, establecer mecanismos de prevención de ataques informáticos y evitar brechas de seguridad o violaciones de datos. Ante las obligaciones legales de notificar y denunciar, una adecuada implementación de medidas de seguridad, análisis y control es la mejor defensa.


EMPRESA
DOCUMENTO DE SEGURIDAD
A
REGISTRO DE INCIDENCIAS
B
CONTROL DE ACCESOS
C
CIFRADO
D
ANÁLISIS DEL RIESGO
D1
ALTO
D2
MEDIO
D3
BAJO
REACCIÓN Y DOBLE PREVENCIÓN
A
MEJORA DE LA PREVENCIÓN
B
REGISTRO DE ATAQUES
C
INFORMACIÓN
C1
CNPIC
C2
USUARIO
C3
AEPD
C3.1
PROCEDIMIENTO
C3.1.1
ARCHIVO
C3.1.2
APERCIBIMIENTO
C3.1.3
SANCIÓN
D
DENUNCIA
D1
POLICÍA GUARDIA CIVIL
CONOCIMIENTOS DE ATAQUES
A
INTRUSIONES EXITOSAS
B
ANÁLISIS DE LA INFORMACIÓN
C
INTRUSIONES FALLIDAS

7 Amenazas avanzadas/Analítica de seguridad PRAVAIL SECURITY ANALYTICS

Pravail Security Analytics le permite ver los ataques a su red global mucho más rápido y de forma más detallada que antes. Visualizaciones potentes que aportan contexto de seguridad significativo a cantidades masivas de datos para que pueda identificar las amenazas tanto en tiempo real como en conjuntos de datos históricos.

Detección de amenazas, respuesta ante incidentes y ciencia forense

Para poder comprender realmente los ataques enfocados y sutiles necesita un registro completo de todo el tráfico de la red. Pravail Security Analytics usa las tecnologías de grandes datos que le permiten recoger de forma rentable y almacenar todo el tráfico que entra y sale de su red. Con Pravail Security Analytics puede avanzar o retroceder en los datos de redes, ver los ataques y atacantes desde distintas perspectivas, así como identificar ataques de día cero y precisar la ex-filtración de los datos. Asimismo, realizar análisis forenses para determinar la eficacia de los controles, reforzar la seguridad y el compliance.

Funciones y ventajas

CONTROLE TODO EL TRÁFICO DE LA RED

Cuando se trata de la seguridad de red, Arbor cree que la detección es la clave y la prevención el objetivo. Y la detección comienza con una gran visibilidad, Pravail Security Analytics le permite cargar capturas completas desde cualquier parte de la red, no solo donde tiene un refuerzo de seguridad; de esto modo tiene una visión sin precedentes del tráfico en toda su red global.

REPRODUZCA, DETENGA Y REBOBINE SUS DATOS

Interactúe con sus datos como nunca antes. Visualizaciones potentes que muestran los datos desde múltiples perspectivas (atacante, objetivo, localización o tipo de ataque) le permiten un análisis de seguridad para comparar con rapidez las estadísticas de ataque desde distintos periodos o ubicaciones, a lo largo de los años o terabytes de tráfico.

HACIENDO ANÁLISIS REITERATIVOS PARA IDENTIFICAR ATAQUES NO DETECTADOS CON ANTERIORIDAD

Pravail Security Analytics se puede usar para decisiones de ataque en tiempo real, y para almacenar los datos para futuras revisiones. Además se realizan análisis reiterativos para identificar amenazas no detectadas con anterioridad usando la última inteligencia de amenazas.

INTELIGENCIA DE ATAQUE GLOBAL, PROTECCIÓN LOCAL

La inteligencia de ataque que mantiene Pravail Security Analytics a la vanguardia de la seguridad de red procede de datos derivados del ATLAS® de Arbor (Active Threat Level Analysis System, sistema de análisis de las amenazas activas). Con este sistema, Arbor supervisa el tráfico de Internet para detectar nuevas amenazas que están dirigidas a la empresa. Estos datos se analizan por expertos de seguridad dentro del Equipo de Respuesta e Ingeniería de Seguridad de Arbor (ASERT) y se vierten en eficaces metodologías de detección o análisis.

HERRAMIENTA DE CUMPLIMIENTO

Use Pravail Security Analytics para facilitar el cumplimiento de políticas de uso interno o regulaciones de la industria/gubernamentales, tales como HIPAA, PCI, Directiva de Retención de datos de la UE, NERC, ITIL e ISO 17799.

DESARROLLO RÁPIDO, EN LA NUBE O EN UN SITIO CONCRETO

Pravail Security Analytics usa las tecnologías de Grandes Datos que disminuyen la barrera para las organizaciones que buscan desplegar y manejar análisis de seguridad de clase mundial. Una organización puede cargar con seguridad capturas de paquete a Pravail Security Analytics en la Nube y estar analizando sus datos en cuestión de minutos para detectar amenazas. Para las empresas que no pueden cargar sus capturas de paquete a la Nube por motivos prácticos o de seguridad, Pravail Security Analytics se puede usar como una solución en un sitio concreto.

ABANLEX

Despacho de abogados con especialización en tecnología y protección de datos

La principal función de Abanlex es resolver casos complejos de Derecho Tecnológico. El bufete está especializado en la innovación jurídica, que emplea para desarrollar soluciones legales que protejan de forma efectiva la información de las empresas ante las nuevas amenazas. Los abogados de Abanlex permanecen en la vanguardia de los movimientos legislativos, colaborando en la elaboración de las normas que afectan a sus áreas de ejercicio.

Las soluciones que ha creado y ejecutado Abanlex para resolver casos de extraordinaria complejidad sitúan a la firma como despacho de referencia en diferentes materias como los nuevos sistemas de pago electrónico, el cifrado o los dispositivos de seguimiento y detección de intrusiones. Sus últimos casos de relevancia internacional son: el Derecho al Olvido contra Google, que ha llevado ante el TJUE, y los avances en criptomonedas, gracias a los cuales colabora en estos asuntos con las Fuerzas y Cuerpos de Seguridad del Estado y figura citado en varios documentos del Gobierno de España y del de Estados Unidos.

Abanlex tiene su sede en Madrid, España.

Más información disponible en www.abanlex.com

Abanlex. c/ Velázquez, 109, 7ª Planta. 28006 Madrid. Correo electrónico: info@abanlex.com (@abanlex)

ARBOR™ NETWORKS

Arbor Networks, Inc. ayuda a proteger a las principales empresas y proveedores de servicios mundiales de los ataques DDoS y amenazas avanzadas. Arbor es el proveedor líder mundial de protección DDoS para la empresa, operadores y segmentos del mercado móvil, según Infonetics Research. Las soluciones para hacer frente a las amenazas avanzadas de Arbor ofrecen una visibilidad completa de la red a través de una combinación de captura de paquetes y la tecnología NetFlow, lo que permite una rápida detección y mitigación de malware e insiders maliciosos. Arbor también ofrece análisis del mercado para la respuesta dinámica ante incidentes, análisis histórico, visualización y análisis forense. Arbor se esfuerza por ser un *"multiplicador de fuerza"*, para convertir a los equipos de seguridad y red en expertos. Nuestro objetivo es proporcionar una visión más detallada de las redes y un mayor contexto de seguridad, por lo que los clientes pueden resolver problemas más rápidamente y reducir el riesgo para su negocio.

Arbor Networks es distribuido en España a través de Exclusive Networks

Arbor Networks

C/ Caleruega, 102-104. Planta 10. 28033 Madrid

Tel: 902 108 872. Fax: 917 662 634

www.arbor.net

Arbor Networks Iberia

C/ Caleruega, 102-104. Planta 10. 28033 Madrid

Tel: 902 10 88 72. Fax: 917 662 634

es.arbornetworks.com