ENJOY SAFER TECHNOLOGY™

Guía sobre el Reglamento General de Protección de Datos (GDPR)

Una guía detallada para conocer cómo te afecta el nuevo Reglamento de la Unión Europea.

Informe elaborado por abanlex

ENJOY SAFER TECHNOLOGY™

Guía sobre el Reglamento General de Protección de Datos

Informe elaborado por

abanlex

DESCRIPCIÓN BREVE

La entrada en vigor del ***Reglamento General de Protección de Datos (UE)***, cuyo cumplimiento será exigible a partir del 25 de mayo de 2018, amplía las obligaciones de implantación de medidas de seguridad para todas las empresas europeas, los autónomos y la Administración Pública entre otros. Estas medidas incluyen la obligación de implementar cifrados y sistemas de 2FA incluso sobre datos considerados de nivel básico, cuando el riesgo lo exige. Otros sujetos también obligados son los ubicados fuera de la Unión Europea que dirijan sus servicios a usuarios de países miembros o que reciban datos personales desde Europa. Este documento también aporta datos sobre sectores específicos, describe las consecuencias de una brecha de seguridad con y sin cifrado previo aplicado y trata los tipos de certificaciones.

INFORME ELABORADO POR ABANLEX PARA ESET

Contenido

I. Introducción al cifrado y al doble factor de autenticación 7

II. Los sistemas de cifrado 7

A. Sistemas de cifrado aceptados por la ley en España 8

B. Sistemas no aceptados para cifrar en el marco empresarial 8

III. Cifrado. *Reglamento General de Protección de Datos (UE)* 9

A. Entrada en vigor del ***Reglamento General de Protección de Datos (UE)***

Alcance y exigibilidad 9

B. Cuándo es obligatorio y cuándo es voluntario implementar cifrados 10

C. Qué es la evaluación de impacto y cómo afecta al cifrado 10

D. Cuándo no cifrar puede ser ilegal 11

E. Características obligatorias del sistema de cifrado 12

F. Cifrado de datos de nivel básico cuando el riesgo lo exige 12

G. Cifrar exime de tener que comunicar las brechas de seguridad 13

IV. Sectores que requieren cifrar información o datos personales 14

A. Norma básica de cifrado (LOPD) 14

B. Prevención del blanqueo de capitales y obligaciones de cifrado 15

C. Defensa Nacional, Administración Pública y Seguridad del Estado 17

D. Sector Jurídico: abogados, notarios y procuradores 18

E. Sector Sanitario: hospitales, clínicas y centros de salud 19

F. Sector de las telecomunicaciones 20

G. Sector del periodismo: el secreto profesional periodístico 21

H. Sector creativo: propiedad intelectual e industrial y secretos comerciales 22

V. Sistemas de doble factor de autenticación (2FA) 23

A. Marco de utilidad del 2FA 23

B. El 2FA en el ***Reglamento General de Protección de Datos (UE)*** 24

C. Sistemas de autenticación única con 2FA 25

D. Protección frente a ataques informáticos mediante 2FA 25

E. Empresas y fuerzas de seguridad recomiendan implementar 2FA 26

VI. Bring Your Own Device (BYOD) 28

VII. Notificación de brechas de seguridad informática 29
A. Obligaciones ante una brecha de seguridad, según la LOPD 29
1. Los operadores de telecomunicaciones están obligados a notificar brechas de seguridad 29
2. Cuándo se debe notificar una brecha de seguridad 31
3. Qué debe contener la notificación de una brecha de seguridad 32
4. Cómo se debe informar al usuario afectado por la brecha 32
5. Cifrar permite, según el caso, no comunicar la brecha de seguridad a los usuarios 33
6. Sanciones por no notificar, según la LOPD 33
B. Obligaciones ante una brecha de seguridad, según el nuevo *Reglamento General de Protección de Datos (UE)* 33
1. Todas las empresas están obligadas a notificar las brechas de seguridad sufridas 34
2. Cuándo se debe notificar una brecha de seguridad 34
3. Qué debe contener la notificación de una brecha de seguridad 34
4. Cómo se debe informar al usuario afectado por la brecha 35
5. Cifrar puede permitir no comunicar la brecha de seguridad a los usuarios 35

VIII. Certificaciones informáticas requeridas por la ley 36
A. El concepto de certificación informática 36
B. Clasificación de certificaciones 36
1. Certificaciones para empresas y certificaciones para usuarios 36
2. Certificaciones genéricas y certificaciones específicas 37
C. Algunas de las principales certificaciones 37
D. Normas que exijan o recomienden contar con un certificado 38

IX. Sanciones con el nuevo *Reglamento General de Protección de Datos (UE)* 39

ENJOY SAFER TECHNOLOGY™

Guía sobre el Reglamento General de Protección de Datos

Informe elaborado por

abanlex

I. Introducción al cifrado y al doble factor de autenticación

Las medidas de seguridad informática correctamente implementadas aportan un escudo de seguridad y de protección frente a los ataques informáticos. **El cifrado robusto y los sistemas de Doble Factor de Autenticación (en adelante, 2FA) son los principales pilares de la seguridad, y su incorporación en la empresa es económicamente asequible y demuestra beneficios inmediatos desde el primer momento.**

La normativa exige la implementación de soluciones de cifrado y de barreras denominadas de Doble Factor de Autenticación (en adelante, 2FA) para proteger los mayores activos de un gran número de empresas. A través de ataques informáticos, una importante cantidad de información confidencial, datos personales y secretos comerciales son sustraídos a diario. Por este motivo, las empresas de seguridad informática han perfeccionado herramientas de prevención y defensa que dificultan e impiden la intrusión y el acceso a la información.

Las empresas que cifran sus datos son extraordinariamente escasas. Debido a que muchas de ellas carecen de sistemas antivirus, muchas veces ignoran que están sufriendo brechas de seguridad a través de las cuales son sustraídos los datos que deben custodiar. Al desconocimiento se le une una importante falta de concienciación y una preocupante falta de interés. Por lo general, se mantiene la errónea creencia de que cifrar e implantar soluciones de 2FA es complejo, caro e ineficiente. Sin embargo, las soluciones que se ofrecen hoy en día son sencillas y de coste asequible, además de que pasan totalmente desapercibidas al usuario, por lo que no requieren conocimiento informático ni una especial pericia en tecnología.

Hoy, cifrar está al alcance de todo aquel que desee proteger su información. No hace mucho, Arturo Ribagorda, Catedrático de Informática de la Universidad Carlos III, según la nota informativa de la AEPD y la UCM publicada en 2006, afirmaba que "*la idea de la dificultad en la aplicación de las Medidas de Seguridad en materia de Protección de Datos es una idea errónea y falaz*", ya que, en ese año, existían herramientas que permiten el cifrado de datos y la obtención de copias de respaldo "*sin excesiva dificultad*". Desde entonces hasta ahora, **la industria de la seguridad ha evolucionado creando herramientas de cifrado de fácil implementación, con servicio de soporte a distancia y con capacidad de funcionar sin que el usuario sea consciente de que su equipo y su trabajo están protegidos.**

II. Los sistemas de cifrado

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.

El cifrado de datos es una medida recomendable y, en muchos casos, legalmente obligatoria, que no exime del deber de notificar, 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*".

Para la Agencia Española de Protección de Datos (en adelante, AEPD), la seguridad informática en la transmisión e intercambio de datos personales es una cuestión de máxima importancia, en especial cuando las medidas que hay que adoptar incluyen el cifrado. Implementar de forma correcta un sistema de cifrado robusto no es un tema baladí, ni un mero trámite administrativo, ni una cuestión de comodidad,

según la AEPD, sino 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.

A. Sistemas de cifrado aceptados por la ley en España

La normativa europea en materia de cifrado, así como el ***Reglamento español de desarrollo de la Ley Orgánica de Protección de Datos*** (en adelante, RLOPD) en su artículo 104, otorgan a las empresas obligadas la posibilidad de elegir entre las siguientes dos opciones:

- **Opción de cifrado:** sistema profesional de cifrado robusto.
- **Opción alternativa al cifrado convencional:** cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Algunos ejemplos pueden ser los siguientes:

- ***Esteganografía:*** a través de este sistema, el emisor oculta mensajes a nivel de aplicación para su envío en forma de imágenes por medio de diferentes vías electrónicas, incluida la satelital.
- ***Spread-spectrum:*** el sistema de transmisión mediante espectro ensanchado permite el envío de mensajes ocultos para el caso inalámbrico a nivel físico.

Las opciones alternativas al cifrado convencional requieren una implementación difícil y una gestión compleja, habitualmente problemática, a diferencia de la sencillez que ofrecen los actuales sistemas de cifrado. En 2009 la Agencia afirmó que aún no se disponían de tecnologías más ágiles para preservar la confidencialidad de la información que emplear herramientas de cifrado, aunque en un futuro estas puedan aparecer. A día de hoy, el cifrado sigue siendo la tecnología más eficiente para este fin.

El RLOPD abre la vía al desarrollo de nuevos mecanismos que garanticen las mismas consecuencias que las que se logran por medio de la implementación de los sistemas profesionales de cifrado.

> ***Artículo 104 del Reglamento de la LOPD:***
>
> *"Cuando, conforme al artículo 81.3, deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros".*

Los sistemas de cifrado robustos o los mecanismos alternativos aceptados por la normativa se caracterizan por no estar comprometidos y por contar tanto con un sistema de gestión de claves, como con un procedimiento de administración de material criptográfico.

Los sistemas adecuados de cifrado cifran de forma que la información no sea inteligible ni manipulada por terceros, de manera que: el sistema de cifrado a emplear no esté comprometido y que se cuente con un sistema de gestión de claves, en particular, y con un procedimiento de administración de material criptográfico, en general. Las herramientas profesionales de cifrado de prestadores de confianza suelen cumplir estos requisitos.

B. Sistemas no aceptados para cifrar en el marco empresarial

Los sistemas inadecuados y que no deberían usarse en el entorno profesional son los provistos por herramientas destinadas al uso particular, como los programas de compresión de archivos o los de cifrado doméstico, habitualmente gratuitos y disponibles en Internet. La Agencia Española de Protección de Datos, a través de su Gabinete Jurídico, ha sido tajante al respecto cuando se le consultó acerca de los sistemas de cifrado de ciertas herramientas, como las de compresión de archivos (ZIP) y los sistemas de

claves de los PDF. La respuesta clave fue que ese tipo de herramientas son ineficaces por las vulnerabilidades propias de aquellas que no han sido diseñadas para el cumplimiento de la normativa vigente en el ámbito profesional.

Esta información se publicó en el Informe 0494/2009 del Gabinete Jurídico de la Agencia Española de Protección de Datos:

> *"Los productos que generan archivos PDF o el realizado por WinZip tienen vulnerabilidades conocidas y se disponen de herramientas de libre distribución que aprovechan dichas vulnerabilidades. Más concretamente, no sólo se pueden obtener en Internet fácilmente utilidades que rompen las protecciones de los archivos PDF o ZIP, sino que el propio algoritmo en el que descansa la cifra de documentos PDF, el algoritmo RC4, es manifiestamente vulnerable".*

La AEPD concluye que los sistemas generales de cifrado son insuficientes para el intercambio de información con las garantías que se precisan en el Reglamento para un uso profesional. En cambio, para un uso estrictamente particular, personal o doméstico estos sistemas generales de cifrado (ZIP, PDF, etc.) podrían considerarse adecuados, según el caso.

Para cumplir de manera correcta la normativa vigente en España en materia de cifrado, deben ser empleadas las herramientas profesionales pensadas, diseñadas y probadas para ello.

III. Cifrado. Reglamento General de Protección de Datos (UE)

El Reglamento General de Protección de Datos (UE) sienta un antes y un después en la protección de los datos de carácter personal. Esta norma es de obligado cumplimiento no solo para las empresas europeas, sino también para las extranjeras que tengan acceso a datos, bien porque sean estos enviados desde Europa, bien porque dirijan sus servicios hacia personas físicas ubicadas en alguno de los países miembros de la Unión Europea.

El Reglamento ya está en vigor. Se dio un plazo prudente, hasta el 25 de mayo de 2018, para que todos los sujetos obligados comprendan la norma, sean conscientes de su alcance e implementen las medidas de seguridad acordes con los niveles marcados en el texto. Esta norma no debe ser transpuesta a una ley española para que sea aplicable en España. Ya es aplicable, de forma directa, sobre todos los sujetos privados y públicos obligados por esta misma. Es momento de considerar si se está o no cumpliendo la norma antes de que llegue la fecha antedicha y se convierta en exigible.

A. Entrada en vigor del Reglamento General de Protección de Datos (UE). Alcance y exigibilidad

El *Reglamento General de Protección de Datos (UE) (RGPD)*, que impone obligaciones a las empresas europeas, a los autónomos y a las Administraciones Públicas de los estados miembros de la Unión Europea, fue aprobado el día 27 de abril de 2016, **ya está en vigor en España y empezará a ser exigible el 25 de mayo de 2018.**

Entre los sujetos obligados al cumplimiento de esta norma europea están los mentados y aquellos que traten datos personales con fines diferentes a los personales o domésticos, entre otros. Además, deberán cumplir la norma los sujetos obligados que, estando fuera de la Unión Europea, reciban datos personales desde Europa o traten estos para algún otro sujeto obligado, así como aquellos que dirijan sus servicios a personas físicas europeas a través de, por ejemplo, Internet.

Al tratarse de un Reglamento de la Unión Europea, se aplica de manera automática y directa en todos los estados miembros ***(artículo 288 del Tratado de Funcionamiento de la Unión Europea)***, a diferencia de la Directiva de Protección de Datos que debía ser transpuesta a través de leyes nacionales. Esto quiere decir que no será necesaria una nueva norma para que sea obligatorio su cumplimiento, sino que ya lo es y comenzará en breve a ser exigible.

B. Cuándo es obligatorio y cuándo es voluntario implementar cifrados

Con el Reglamento General de Protección de Datos (UE) se establecen varios niveles de empresas que deben o pueden implementar medidas de cifrado:

Cifrados obligatorios

- **Imposición estatal**

  Los estados establecen determinadas categorías de datos y de tratamientos que exigen el establecimiento de sistemas de cifrado a las empresas que los tratan. En España, el ejemplo más práctico de esta indicación del ***Reglamento General de Protección de Datos (UE)*** lo encontramos en la obligatoriedad del cifrado sobre los datos de nivel alto, entre los que están aquellos que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical.

- **Código de conducta o certificado**

  Las empresas tienen que implementar de forma obligatoria sistemas de cifrado en caso de que voluntariamente se hubieran adherido a un código de conducta que lo exija o si el cifrado es requisito en el certificado que muestren como acreditación.

- **Evaluación de impacto**

  Determinadas empresas, por el tipo de tratamiento que realizan, deben cifrar los datos personales que gestionan, según las conclusiones de la evaluación de impacto que hayan realizado por imperativo legal. Estas empresas son, entre otras, las que tratan datos biométricos o las que observan sistemáticamente y a gran escala zonas de acceso público.

- **Mitigación del riesgo**

  Debe aplicarse la medida de cifrado si su implantación mitiga un riesgo cierto.

Cifrados convenientes

Aquellas empresas que hayan implementado un sistema de cifrado y sufran una brecha de seguridad que afecte a los datos personales que gestiona, pueden no informar sobre la intrusión a los usuarios. En cambio, aquellas empresas que no cifren están compelidas a informar a los usuarios sobre los ataques que sufran si las consecuencias incluyen la afección de sus datos personales.

Cifrados voluntarios

La empresa que almacena datos disociados o datos personales de los indicados en el artículo 11 del ***Reglamento General de Protección de Datos (UE)*** a través de los cuales no sea ya posible identificar a una persona física, siempre que no haya una norma que le obligue a cifrarlos, puede implementar medidas de cifrado para aumentar la seguridad sobre estos.

El cifrado es una de las medidas más adecuadas para mitigar los riesgos inherentes al tratamiento de datos de carácter personal de manera que se pueda mantener la seguridad, según dispone el ***Reglamento General de Protección de Datos (UE)*** en su Considerando 83. La norma concreta quiénes son los sujetos a los que se les impone este deber de aplicar, cuando proceda, medidas de cifrado: el responsable o el encargado del tratamiento.

C. Qué es la evaluación de impacto y cómo afecta al cifrado

El tipo y la robustez del cifrado que el *Reglamento General de Protección de Datos (UE)* exige deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse.

La evaluación de impacto es el análisis de los riesgos propios del tratamiento de datos personales para conocer las medidas de seguridad informática necesarias que deben ser implementadas.

Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los peligros que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

En determinados casos la implantación de medidas específicas, como las de cifrado, se estima necesaria, según el Considerando 84 del ***Reglamento General de Protección de Datos (UE)***, **cuando sea probable que las operaciones de tratamiento entrañen un alto riesgo** para los derechos y libertades de las personas físicas. **En estos casos, incumbe al responsable del tratamiento la realización de una evaluación de impacto** relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con la normativa vigente en relación con el tratamiento de datos personales.

Si no se toman a tiempo las medidas adecuadas, como la de implementar un sistema de cifrado robusto cuando sea necesario, habida cuenta de los riesgos localizados por medio de la evaluación de impacto, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas. A través del Considerando 85 del ***Reglamento General de Protección de Datos (UE)*** se nos aportan los siguientes ejemplos de consecuencias sobre las personas físicas afectadas:

- *Pérdida de control sobre sus datos personales o restricción de sus derechos*
- *Discriminación*
- *Usurpación de identidad*
- *Pérdidas financieras*
- *Reversión no autorizada de la seudonimización*
- *Daño para la reputación*
- *Pérdida de confidencialidad de datos sujetos al secreto profesional*
- *Perjuicios económicos o sociales significativos*

Este hecho podría dar lugar a responsabilidades directas, frente a la Administración y los afectados, para los sujetos que debían haber implantado sistemas de cifrado adecuados u otras medidas adicionales de seguridad, como el doble factor de autenticación.

D. Cuándo no cifrar puede ser ilegal

Para tratar datos personales es necesario que estos se destinen al fin para el que se recogieron o para algún otro necesario y proporcional recogido en el Derecho de la Unión o de los Estados miembros. **La implantación de medidas de cifrado siempre es conveniente, sea cual sea el dato o el tratamiento de que se trate.**

La existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización, es uno de los requisitos o exigencias que se tendrán en cuenta, según dispone el ***artículo 6 del Reglamento General de Protección de Datos (UE)***, cuando el tratamiento al que fueran a someterse los datos personales sea distinto de aquel para el que se recogieron los datos personales y no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros.

En estos casos, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, el responsable tiene la obligación de comprobar y tener en cuenta las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de sistemas de cifrado aplicados a los datos personales, entre otros indicadores recogidos en el mentado artículo.

El ***Reglamento General de Protección de Datos (UE)*** dispone que, para los casos anteriores, **la falta de cifrado sobre los datos personales podría ser causa suficiente para que su tratamiento sea ilegal.**

Dicho de otra forma, los sistemas de cifrado robusto facilitan el tratamiento de datos y permiten que puedan ser empleados para un número mayor de fines.

E. Características obligatorias del sistema de cifrado

El cifrado de los datos de carácter personal es la primera de las medidas básicas de seguridad que el *Reglamento General de Protección de Datos (UE)* dispone para garantizar un nivel de seguridad adecuado al riesgo.

Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, a través del ***artículo 32 del Reglamento General de Protección de Datos (UE)*** **se establece la obligación de que tanto el responsable como el encargado del tratamiento deban aplicar medidas técnicas y organizativas apropiadas, que en su caso incluyan, entre otros:**

- **La seudonimización y el cifrado** de datos personales;
- La capacidad de garantizar **la confidencialidad**, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- **La capacidad de restaurar la disponibilidad y el acceso a los datos** personales de forma rápida en caso de incidente físico o técnico;
- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

La norma europea establece que la implantación de medidas de cifrado es imprescindible, además de elemental y básica, a la hora de evitar, entre otras consecuencias indeseables, el acceso no autorizado a la información por parte de terceros no autorizados. Al evaluar la adecuación del nivel de seguridad, el ***Reglamento General de Protección de Datos (UE)*** establece que deben tenerse en cuenta los riesgos que presenta el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, además de la comunicación o el ya mencionado acceso no autorizado a dichos datos.

F. Cifrado de datos de nivel básico cuando el riesgo lo exige

Con el nuevo ***Reglamento General de Protección de Datos (UE)***, **toda empresa está obligada a cifrar los datos que trata cuando sea probable que un tipo de tratamiento**, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, **entrañe un alto riesgo** para los derechos y libertades de las personas físicas, siempre que la solución de cifrado sea la medida más razonable para mitigar el riesgo. Esta evaluación del riesgo se lleva a cabo por medio de una evaluación de impacto exigida solo a determinados tipos de empresas por el tipo de tratamiento que hacen y su alcance.

La evaluación de impacto, definida en el ***artículo 35 del Reglamento General de Protección de Datos (UE)***, relativa a la protección de los datos **para determinar si es o no necesaria la medida de cifrado, se requerirá en particular en caso de que la empresa vaya a realizar una evaluación sistemática y**

exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; **cuando vaya a llevar a cabo un tratamiento a gran escala de las categorías especiales de datos** o de los datos personales relativos a condenas e infracciones penales; **o si va a realizar tareas de observación sistemática a gran escala de una zona de acceso público**.

Los datos, antes mentados, que forman parte de categorías especiales son aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. El manejo de estos datos, cuando sea legal su tratamiento según el artículo 9 del Reglamento General de Protección de Datos (UE), requiere que se apliquen siempre y en todo caso mecanismos de cifrado robusto.

La evaluación de impacto, cuando es obligatoria y cuando se hace por voluntad del responsable, deberá incluir como mínimo:

- Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
- Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
- Una evaluación de los riesgos para los derechos y libertades de los interesados; y
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con la normativa de protección de datos, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

La evaluación del impacto debe incluir, en el punto cuarto de los indicados, las medidas para prevenir y afrontar los peligros, entre las que destaca el cifrado, como apunta expresamente el Considerando 83 del Reglamento o los sistemas de doble factor de autenticación como medida para mitigar el riesgo.

G. Cifrar exime de tener que comunicar las brechas de seguridad

Las empresas que han adoptado medidas de cifrado de datos no están obligadas a comunicar a los afectados las brechas de seguridad que sufren, en determinados casos. Dispone el Reglamento, en su artículo 34, que cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

La comunicación, obligatoria para todas las demás empresas obligadas, no será necesaria, salvo que la AEPD determine otra cosa estudiado el caso particular, si el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.

IV. Sectores que requieren cifrar información o datos personales

El Reglamento General de Protección de Datos (UE) indica que se debe analizar el riesgo al que estarán sometidos los datos que se vayan a tratar, de manera que se puedan implementar las medidas de seguridad adecuadas, según el estado de la técnica.

A diferencia de otras normas que indican que solo se debe aplicar obligatoriamente el cifrado a datos o tratamientos de cierto nivel, en este Reglamento europeo se abre el abanico para que sea obligatoria la implementación de determinados tipos de cifrado y sistemas de 2FA a todo tipo de dato o tratamiento, sin distinción, en función del riesgo que exista para estos y para sus titulares.

Adicionalmente, encontramos muchas otras normas sectoriales que extienden la obligatoriedad del cifrado a actividades concretas: hospitales, medios de comunicación, despachos de abogados... e incluso anticuarios y vendedores de sellos.

A. Norma básica de cifrado (LOPD)

Las empresas que deben cifrar datos, según la Ley Orgánica de Protección de Datos (en adelante, LOPD) y su Reglamento de Desarrollo (en adelante, RLOPD), **son aquellas que deben implantar medidas de nivel alto** por razón de los datos que tratan o el tratamiento que realizan con ellos.

El cifrado, que forma parte de las medidas de nivel alto, es obligatorio aplicarlo, según el artículo 83 RLOPD, **en los siguientes ficheros** o tratamientos de datos de carácter personal:

- ✔ Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- ✔ Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
- ✔ Aquéllos que contengan datos derivados de actos de violencia de género.

El RLOPD, en su artículo 104, obliga también a aplicar sistemas de cifrado en la transmisión a través de redes públicas o redes inalámbricas de comunicaciones electrónicas de datos de carácter personal relativos a los tres conjuntos de datos referidos. La norma exige implementar sistemas de cifrado o bien utilizar cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero, también deben ser cifrados, por así disponerlo el artículo 101 RLOPD. En aquellos portátiles, móviles o tabletas en los que no sea posible implementar sistemas de cifrado debe evitarse el tratamiento de datos de carácter personal, salvo que sea estrictamente necesario, en cuyo caso tiene que hacerse constar motivadamente en el documento de seguridad y se deben adoptar medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Por último, como regla general, la norma ***(art. 103 RLOPD)*** exige, de cada intento de acceso, guardar como mínimo la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. El período mínimo de conservación de los datos registrados será de dos años. Estos mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir su desactivación ni su manipulación.

Este tipo de exigencias legales sobre cifrado robusto es posible cubrirlas con sistemas de cifrado profesional provistas por empresas de confianza y renombre en el sector de la seguridad informática.

B. Prevención del blanqueo de capitales y obligaciones de cifrado

La integridad del sistema financiero y de otros sectores de actividad económica cuenta en España con un sistema de protección especial articulado a través de la ***Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo*** (en adelante LPBC). Esta norma establece obligaciones concretas de prevención del blanqueo de capitales y de la financiación del terrorismo que obliga a determinados tipos de empresas, tanto residentes en España como no residentes, a recabar información de determinados sujetos con los que opera y cifrarla para garantizar tanto la seguridad de los datos como la obtención de los fines que la normativa prevé.

A través de la LPBC, se requiere a empresas de diferentes sectores cifrar los ficheros en los que estas deben integrar datos e información de tipo económico y social de un gran número de grupos de personas. Están sujetas al cumplimiento de esta Ley las personas o entidades españolas listadas en la norma, como también lo están las no residentes que desarrollen en España actividades de igual naturaleza a aquellas a través de sucursales o agentes o mediante prestación de servicios sin establecimiento permanente.

El elenco de empresas obligadas a cifrar datos recogidos para prevenir el blanqueo de capitales y la financiación del terrorismo **se encuentra en el artículo 2 de la LPBC** y alcanza a abogados, profesionales del arte, joyerías, promotores inmobiliarios, servicios postales, entidades de crédito, notarios y sociedades de garantía recíproca, entre otros muchos.

A continuación, los detallamos de manera literal:

Artículo 2.1 LPBC

"1. La presente Ley será de aplicación a los siguientes sujetos obligados:

***a)** Las **entidades de crédito**.*

***b)** Las **entidades aseguradoras** autorizadas para operar en el ramo de vida y los corredores de seguros cuando actúen en relación con seguros de vida u otros servicios relacionados con inversiones, con las excepciones que se establezcan reglamentariamente.*

***c)** Las empresas de **servicios de inversión**.*

***d)** Las sociedades gestoras de instituciones de **inversión colectiva** y las sociedades de inversión cuya gestión no esté encomendada a una sociedad gestora.*

***e)** Las entidades gestoras de **fondos de pensiones**.*

***f)** Las sociedades gestoras de entidades de **capital-riesgo** y las sociedades de capital-riesgo cuya gestión no esté encomendada a una sociedad gestora.*

***g)** Las sociedades de **garantía recíproca**.*

***h)** Las **entidades de pago** y las entidades de dinero electrónico.*

***i)** Las personas que ejerzan profesionalmente actividades de **cambio de moneda**.*

***j)** Los **servicios postales** respecto de las actividades de giro o transferencia.*

***k)** Las personas dedicadas profesionalmente a la intermediación en la concesión de **préstamos** o créditos, así como las personas que, sin haber obtenido autorización como establecimientos financieros de crédito, desarrollen profesionalmente alguna de las actividades a que se refiere la Disposición adicional primera de la Ley 3/1994, de 14 de abril, por la que se adapta la legislación española en materia de Entidades de Crédito a la Segunda Directiva de Coordinación Bancaria y se introducen otras modificaciones relativas al Sistema Financiero.*

***l)** Los **promotores inmobiliarios** y quienes ejerzan profesionalmente actividades de agencia, comisión o intermediación en la compraventa de bienes inmuebles.*

***m)** Los **auditores de cuentas**, contables externos o asesores fiscales.*

***n)** Los **notarios** y los registradores de la propiedad, mercantiles y de bienes muebles.*

***ñ)** Los **abogados**, procuradores u otros profesionales independientes cuando participen en la concepción, realización o asesoramiento de operaciones por cuenta de clientes relativas a la compraventa de bienes inmuebles o entidades comerciales, la gestión de fondos, valores u otros activos, la apertura o gestión de cuentas corrientes, cuentas de ahorros o cuentas de valores, la organización de las aportaciones necesarias para la creación, el funcionamiento o la gestión de empresas o la creación, el funcionamiento o la gestión de fideicomisos («trusts»), sociedades o estructuras análogas, o cuando actúen por cuenta de clientes en cualquier operación financiera o inmobiliaria.*

o) *Las personas que con carácter profesional y con arreglo a la normativa específica que en cada caso sea aplicable presten los siguientes servicios a terceros: **constituir sociedades** u otras personas jurídicas; ejercer funciones de dirección o secretaría de una sociedad, socio de una asociación o funciones similares en relación con otras personas jurídicas o disponer que otra persona ejerza dichas funciones; **facilitar un domicilio social** o una dirección comercial, postal, administrativa y otros servicios afines a una sociedad, una asociación o cualquier otro instrumento o persona jurídicos; ejercer funciones de fideicomisario en un fideicomiso («trust») expreso o instrumento jurídico similar o disponer que otra persona ejerza dichas funciones; o ejercer funciones de accionista por cuenta de otra persona, exceptuando las sociedades que coticen en un mercado regulado y estén sujetas a requisitos de información conformes con el derecho comunitario o a normas internacionales equivalentes, o disponer que otra persona ejerza dichas funciones.*

p) *Los **casinos** de juego.*

q) *Las personas que comercien profesionalmente con **joyas**, piedras o metales preciosos.*

r) *Las personas que comercien profesionalmente con objetos de **arte o antigüedades**.*

s) *Las personas que ejerzan profesionalmente las actividades a que se refiere el artículo 1 de la Ley 43/2007, de 13 de diciembre, de protección de los consumidores en la **contratación de bienes con oferta de restitución del precio**.*

t) *Las personas que ejerzan actividades de **depósito**, custodia o transporte profesional de fondos o medios de pago.*

u) *Las personas responsables de la gestión, explotación y comercialización de loterías u otros **juegos de azar** respecto de las operaciones de pago de premios.*

v) *Las personas físicas que realicen movimientos de **medios de pago**, en los términos establecidos en el artículo 34.*

w) *Las personas que **comercien profesionalmente con bienes**, en los términos establecidos en el artículo 38.*

x) *Las **fundaciones** y asociaciones, en los términos establecidos en el artículo 39.*

y) *Los gestores de sistemas de pago y de compensación y liquidación de valores y productos financieros derivados, así como los gestores de **tarjetas de crédito** o débito emitidas por otras entidades, en los términos establecidos en el artículo 40".*

Estos sujetos están obligados al cifrado de determinada información debido a que la LPBC impone la aplicación de las medidas de nivel alto, recogidas en la LOPD, a los ficheros en los que integran los datos para su tratamiento, todo ello por los siguientes motivos:

- Los sujetos obligados *"aplicarán medidas reforzadas de diligencia debida"* en las relaciones de negocio u operaciones de personas con responsabilidad pública (***art. 14 LPBC***). Estos sujetos obligados podrán proceder a la creación de ficheros donde se contengan los datos identificativos de las personas con responsabilidad pública. *"En todo caso deberán implantarse sobre el fichero las medidas de seguridad de nivel alto"*, que exige el cifrado de los datos (***art. 15 LPBC***).

- El tratamiento de datos de carácter personal, así como los ficheros, automatizados o no, creados para el cumplimiento de las disposiciones de toda la LPBC se someterán a lo dispuesto en la LOPD. Además, "***serán de aplicación a estos ficheros las medidas de seguridad de nivel alto***", que exigen el cifrado de datos (***art. 32 LPBC***).

La implantación de medidas de nivel alto, que la LPBC impone para datos, información y tratamientos diferentes de los recogidos en la LOPD, indica que las obligaciones de cifrado van más allá de la protección de los datos de carácter personal. En este caso, por razón del grado de protección que se establece, los sujetos al cumplimiento de la LPBC obligados a cifrar están igualmente compelidos a someter los sistemas de información e instalaciones de tratamiento y almacenamiento de datos, "***al menos cada dos años, a una auditoría interna o externa***" (***art. 96 RLOPD***) en la que se verificará que el cifrado es correcto y acorde a lo exigido por la normativa.

C. Defensa Nacional, Administración Pública y Seguridad del Estado

Las Administraciones Públicas españolas se ven obligadas por ley a cifrar en algunas de las tareas que realizan para asegurar el acceso, la integridad, la disponibilidad, la autenticidad, la confidencialidad, la trazabilidad y la conservación de los datos, las informaciones y los servicios utilizados en los medios electrónicos que gestionen en el ejercicio de sus competencias.

El Esquema Nacional de Seguridad o ENS introduce y compila en España muchas de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. El objetivo es permitir a los ciudadanos y a las Administraciones Públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. El ENS fue aprobado por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

El cifrado de gran parte de la información, tanto en local o remoto, como en su tránsito a través de comunicaciones, que manejan las Administraciones Públicas se determina como obligatorio a través de varias secciones del ENS. Según esta norma, desde el Estado se deben aplicar medidas específicas de cifrado en comunicaciones y en los soportes en los que se recoja y mantenga la información.

Estas son algunas de las principales indicaciones del cifrado en el ENS:

- **Cifrado obligatorio durante el mantenimiento y la transmisión**:
  "*La información con un nivel alto en confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella*" (***artículo 5.7.3 ENS***).

- **El cifrado débil se considera inseguro**:
  "*Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil*" (***art. 21 ENS***).

- **Las copias de respaldo deben ser cifradas**:
  "*Las copias de respaldo disfrutarán de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad de que las copias de seguridad estén cifradas para garantizar la confidencialidad*" (***5.7.7 Anexo II ENS***).

- **Los portátiles deben ser cifrados**:
  "*La información de nivel alto almacenada en el disco se protegerá mediante cifrado*" (***5.3.3 Anexo II ENS***)

Las Administraciones Públicas están obligadas a aplicar sistemas de cifrado robusto a la información confidencial, así como a la de nivel alto que tratan y gestionan, tanto durante su mantenimiento como durante su comunicación. Los sujetos obligados deberán prestar especial atención al cifrado que apliquen a sus dispositivos portátiles, tales como tabletas, ordenadores, relojes inteligentes u otros similares, ya que sobre ellos también se debe aplicar uno robusto y un proveedor confiable. Las copias de seguridad y de respaldo tienen que estar igualmente cifradas.

El ENS exige que las medidas de cifrado que se apliquen garanticen la integridad, la confidencialidad, la autenticidad y la trazabilidad de toda la información sobre la que se apliquen, ya sean o no datos de carácter personal. Para ello, nuevamente se recomienda, y la AEPD incluso exige, que la solución de cifrado elegida sea robusta y provenga de un proveedor confiable, además de que el sistema de cifrado no esté comprometido y de que cuente con un procedimiento de administración de material de cifrado y un sistema de gestión de claves.

D. Sector Jurídico: abogados, notarios y procuradores

Los abogados, los procuradores y los notarios están obligados a cifrar los datos que manejan, tanto al mantenerlos y custodiarlos, como al transmitirlos o comunicarlos. La información, con independencia de si se trata o no de datos de carácter personal, solo podrá estar en claro mientras se está haciendo uso de ella.

La información manejada por los abogados tiene el carácter de secreta y debe ser tratada de manera confidencial. El Código Deontológico de la Abogacía Española, que establece unas normas deontológicas para la función social de la Abogacía (***Preámbulo CDAE***), establece el deber de secreto para aquellos datos y otro tipo de información que manejan los abogados. El carácter de secreto y confidencial de la información exige su cifrado con el objetivo de convertirla en inteligible e inaccesible a terceros.

El abogado, "*está obligado a no defraudar la confianza de su cliente*" (***art. 4 CDAE***), dado que la relación entre ambos sujetos, cliente y abogado, se fundamenta en la confianza y exige del profesional una conducta íntegra, honrada, leal, veraz y diligente.

El secreto profesional exigido a los abogados y a los procuradores, así como a los notarios, por la normativa en cada caso aplicable, obliga a los profesionales a aplicar medidas de cifrado robusto. En algunos casos los datos cuya custodia requiere el cifrado están relacionados con la comisión de delitos, de los que salen impunes o por los que se les condena. El cliente deposita su confianza en el profesional sabiendo que este está obligado a no defraudar su confianza, a guardar secreto sobre todos los datos de su vida personal e íntima que le revele y a que esta información permanezca confidencial e inaccesible a terceros para siempre, durante la relación contractual de asesoramiento jurídico y después de esta. Todo el contenido que el cliente revele tiene que permanecer a resguardo bajo las más altas y estrictas medidas de seguridad, lo que exige el establecimiento de medidas de nivel alto y, por tanto, del cifrado de todos los datos que se encuentren recogidos en formato digital, así como de las comunicaciones que el abogado mantenga con su cliente.

El cliente del abogado, además de verse protegido por lo dispuesto en el Código Deontológico en relación con la obligación de secreto, se ve amparado por una serie de derechos fundamentales entre los que destaca el recogido en el artículo 24 de la Constitución Española y que le otorga el derecho "a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia" (***art. 24 CE***).

> ***Artículo 24.2 Constitución Española***
>
> *"[...] todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia. [...]"*

La Constitución Española y el CDAE entregan al cliente la seguridad de que su información va a ser guardada con el mayor de los esmeros. Tanto es así, que el deber de confidencialidad del abogado es casi absoluto, además del mayor de los existentes en derecho español. El cliente desnuda su intimidad ante el abogado revelando los detalles de delitos que ha o no ha cometido. Los datos del cliente no pueden trascender en ningún caso.

> ***Artículo 5 CDAE***
>
> *"**1**. La confianza y confidencialidad en las relaciones entre cliente y abogado, ínsita en el derecho de aquél a su intimidad y a no declarar en su contra, así como en derechos fundamentales de terceros, impone al abogado el deber y le confiere el derecho de guardar secreto respecto de todos los hechos o noticias que conozca por razón de cualquiera de las modalidades de su actuación profesional, sin que pueda ser obligado a declarar sobre los mismos como reconoce el **artículo 437.2 de la vigente Ley Orgánica del Poder Judicial**.*
>
> ***2**. El deber y derecho al secreto profesional del abogado comprende las confidencias y propuestas del cliente, las del adversario, las de los compañeros y todos los hechos y documentos de que haya tenido noticia o haya recibido por razón de cualquiera de las modalidades de su actuación profesional.*
>
> ***3**. El abogado no podrá aportar a los tribunales, ni facilitarle a su cliente las cartas, comunicaciones o notas que reciba del abogado de la otra parte, salvo expresa autorización del mismo.*
>
> ***4**. Las conversaciones mantenidas con los clientes, los contrarios o sus abogados, de presencia o por cualquier medio telefónico o telemático, no podrán ser grabadas sin previa advertencia y conformidad de todos los intervinientes y en todo caso quedarán amparadas por el secreto profesional.*

5. En caso de ejercicio de la abogacía en forma colectiva, el deber de secreto se extenderá frente a los demás componentes del colectivo.

6. En todo caso, el abogado deberá hacer respetar el secreto profesional a su personal y a cualquier otra persona que colabore con él en su actividad profesional.

7. Estos deberes de secreto profesional permanecen incluso después de haber cesado en la prestación de los servicios al cliente, sin que estén limitados en el tiempo.

8. El secreto profesional es un derecho y deber primordial de la Abogacía. En los casos excepcionales de suma gravedad, en los que la obligada preservación del secreto profesional pudiera causar perjuicios irreparables o flagrantes injusticias, el Decano del Colegio aconsejará al Abogado con la finalidad exclusiva de orientar y, si fuera posible, determinar medios o procedimientos alternativos de solución del problema planteado ponderando los bienes jurídicos en conflicto. Ello no afecta a la libertad del cliente, no sujeto al secreto profesional, pero cuyo consentimiento por sí solo no excusa al Abogado de la preservación del mismo."

El secreto profesional es un derecho y deber primordial de la Abogacía que merece el mayor de los respetos y que obliga a la implantación de medidas de nivel alto a los ficheros en los que se guarden datos de clientes. Por tanto, todo abogado está obligado al cifrado de, al menos, las carpetas relativas a los casos que lleva.

El empleo de servidores en la nube para la gestión de casos, para abogados y procuradores, está permitido por la normativa siempre que se respeten y se cumplan las medidas de seguridad de nivel alto. La manera adecuada de usar estos servicios sería mediante el cifrado en local de los datos, manteniendo a salvo y sin subir la clave privada con la que pueden descifrarse. Del mismo modo, la transmisión de los datos personales y del resto de información que traten los profesionales debe ser cifrada para los demás medios de conservación además de para su transmisión y comunicación por redes.

E. Sector Sanitario: hospitales, clínicas y centros de salud

En el sector sanitario, hospitales, clínicas y centros de salud están obligados al cifrado de todos los datos personales que traten de los pacientes en tanto en cuanto hubiera que aplicar niveles de protección alta sobre estos o sobre los tratamientos que se realicen sobre ellos, según la ***Ley 41/2002 de Autonomía del Paciente*** (en adelante, Ley de Autonomía del Paciente) y la LOPD.

La Ley de Autonomía del Paciente tiene por objeto "*la regulación de los derechos y obligaciones de los pacientes, usuarios y profesionales, así como de los centros y servicios sanitarios, públicos y privados, en materia de autonomía del paciente y de información y documentación clínica*" (***art. 1 Ley 41/2002***).

Los ficheros que tratan los sujetos obligados por esta norma deben ser objeto de aplicación de nivel alto de medidas seguridad. Esto resulta en que el cifrado es directamente aplicable y obligatorio.

Las entidades del sector sanitario deben orientar sus actividades a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica debe ser orientada por "*la dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad*", según el ***artículo 2 de la Ley de Autonomía del Paciente***. Estos derechos fundamentales hacen imprescindible el máximo celo a la hora de tratar la información concerniente a las personas físicas que serán atendidas por los sujetos obligados.

El cifrado de los datos por hospitales, clínicas y todo tipo de centro sanitario, así como por sus encargados del tratamiento, es una de las medidas esenciales a las que obliga la normativa de protección de datos. Asimismo, se impone la obligación, a la persona que elabora o tiene acceso a la información y la documentación clínica, de guardar la reserva debida. Esta obligación de guardar reserva se refuerza con un sistema adecuado de cifrado de datos que impida el envío por error de datos, que se compartan indebidamente o que se acceda a ellos en caso de extravío de uno de los soportes que los contienen.

Uno de los factores de mayor relevancia a la hora de llevar a cabo cifrados adecuados y conformes a la normativa es el derecho a la intimidad de la persona. Los datos tratados tendrán en todo caso el carácter de confidenciales, por lo que se debe llevar un control de quién y para qué accede a los datos. Por este motivo,

la normativa, además de exigir auditorías bianuales de cumplimiento, impulsa a las entidades del sector a contar con un código de conducta específico con normas y procedimientos protocolizados para garantizar el acceso legal a los datos de los pacientes.

> ***Artículo 7 Ley 41/2002***
>
> *"**1**. Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.*
>
> ***2**. Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes."*

El "*acceso a los datos*" debe realizarse, en todo caso, por un "*profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto*", según se dispone el artículo 16 de la Ley de Autonomía del Paciente. De igual forma, "el personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto". Este deber de secreto unido a la salvaguarda efectiva del derecho fundamental hacen imprescindible el recurso al cifrado de datos, obligatorio, por otro lado, por el tipo de datos que van a ser tratados y la implantación debida de las medidas de seguridad de nivel alto.

El cifrado de datos es la medida técnica necesaria que permite a los centros sanitarios cumplir con su obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad.

> ***Artículos 17.1, 17.5 Y 17.6 Ley 41/2002***
>
> *"**1**. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.*
>
> ***5**. Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen.*
>
> ***6**. Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal."*

El paciente tiene derecho a que los centros sanitarios establezcan un "*mecanismo de custodia activa y diligente de las historias clínicas*" (***art. 19 Ley 41/2002***). Por tanto, los centros sanitarios tienen la obligación de establecer e implementar dichos mecanismos.

F. Sector de las telecomunicaciones

Las empresas del sector de las telecomunicaciones, en particular los operadores que explotan redes públicas de comunicaciones electrónicas y los prestadores de acceso a Internet o ISP (Internet Service Providers), **cifran los datos de sus clientes para evitar tener que informarles sobre las brechas de seguridad** que sufren en caso de que los atacantes hayan tenido acceso a los archivos encriptados.

La ***LGT*** y el ***Reglamento (UE) nº 611/2013*** obligan a las empresas del sector de las comunicaciones electrónicas a notificar las brechas de seguridad que pongan en peligro información personal. En concreto, vincula a los operadores que explotan redes públicas de comunicaciones electrónicas y a los prestadores de acceso a Internet o ISP (Internet Service Providers). Todas ellas han de notificar tales brechas (i) a la AEPD y (ii) a los sujetos interesados cuya información personal se haya visto comprometida, además de (iii) anotar la incidencia en su Documento de Seguridad.

Esta obligación fue introducida por la ***Directiva 2002/58/CE***, transpuesta en España mediante el actual artículo 41 de la LGT y desarrollada en un Reglamento europeo específico: el ***Reglamento nº 611/2013***.

Artículo 41.3 I LGT

"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. 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".

Artículos 2.1 y 3.1 del Reglamento europeo 611/2013

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

3.1: *"Cuando un caso de violación de datos personales pueda afectar negativamente a los datos personales o a la intimidad de un abonado o particular, el proveedor, además de remitir la notificación contemplada en el artículo 2, también notificará el caso al abonado o particular".*

En caso de que la compañía haya aplicado un cifrado robusto a los datos personales afectados por la brecha que los haya hecho incomprensibles, no tendrá que poner en conocimiento de sus clientes, y de sus demás usuarios en general, este ataque sufrido.

La ***Ley 9/2014, General de Telecomunicaciones y el Reglamento (UE) nº 611/2013*** permiten que la compañía que ha sufrido el ataque informático no notifique la fuga de información y datos a los afectados solo en caso de que los archivos en los que los datos están contenidos estén debidamente cifrados con un sistema de cifrado robusto.

El propio Reglamento europeo 611/2013, directamente aplicable en todos los Estados de la UE, menciona expresamente el cifrado seguro como la medida idónea para convertir la información en incomprensible:

Artículo 4.2 del Reglamento europeo 611/2013

"Los datos se considerarán incomprensibles cuando: se hayan cifrado de forma segura con un algoritmo normalizado, y la clave usada para descifrar los datos no haya quedado comprometida por ningún fallo de seguridad y haya sido generada de modo que no pueda ser determinada por los medios tecnológicos disponibles por ninguna persona que no esté autorizada a acceder a ella".

La aplicación de sistemas de cifrado robusto como medida idónea para convertir la información en incomprensible protege a las compañías ante las crisis reputacionales que pueden derivar de comunicar públicamente las consecuencias de los ataques informáticos sufridos cuando estos afectan a datos de carácter personal.

G. Sector del periodismo: el secreto profesional periodístico

Los periodistas de investigación deben ejercer su profesión bajo la obligación de mantener secreto profesional sobre sus fuentes. Este deber de secreto profesional periodístico se sustenta sobre el artículo 20.1.d) de la Constitución Española, que reconoce el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de la actividad de los periodistas.

El secreto profesional periodístico implica, por un lado, el derecho a no publicar los datos que se quieren proteger y, por otro, a ocultar la fuente de la información dentro del mismo medio de comunicación, incluso ante superiores jerárquicos. Este deber de secreto convierte los datos, que no siempre son personales, en confidenciales y, por tanto, deben ser protegidos como tales.

Para el sector periodístico, el cifrado se erige como la herramienta idónea para mantener la información a salvo del acceso no consentido por parte de terceros no autorizados.

El secreto profesional periodístico es la consecuencia natural del ejercicio del derecho a la libertad de expresión. Este cuenta con una doble vertiente:

- Vertiente positiva de la libertad de expresión periodística: el periodista, en el ejercicio de sus funciones, puede revelar información, salvo que con ello perjudique los derechos de terceros de manera desproporcionada e injustificada. En caso de que la información trate de una persona, el periodista deberá ponderar siempre la naturaleza de la información de que se trate, el carácter sensible de esta información para la vida privada del individuo afectado, el interés público en disponer de dicha información y el papel que dicha persona desempeñe en la vida pública.

- Vertiente negativa de la libertad de expresión periodística: el periodista, en el ejercicio de sus funciones, puede ocultar información. No obstante, existen casos en los que la normativa le exige revelar dichos datos en determinadas circunstancias y, de no hacerlo, tendrá que atenerse a las consecuencias. Uno de estos casos lo encontramos en la Ley de Enjuiciamiento Criminal, que obliga a los periodistas, en ciertas circunstancias, a revelar ante los tribunales la fuente de la información para la persecución de delitos, a pesar de que se hubiese querido ocultar dicha información haciendo uso del secreto profesional periodístico.

El ***artículo 20.1 d) de la Constitución Española*** establece que"la l*ey regulará el derecho a la cláusula de conciencia y al secreto profesional*". No obstante, a pesar de que sí existe una norma que regula el derecho a la cláusula de conciencia (***Ley Orgánica 2/1997***), no hay, hasta la fecha, ninguna ley orgánica que haya regulado el secreto mentado para los periodistas. Asimismo, la ***Ley 14/1966***, de 18 de marzo, de Prensa e Imprenta afirma que"*un Estatuto de la profesión periodística, aprobado por Decreto, regulará los requisitos para el ejercicio de tal actividad*". Sin embargo, tampoco ha visto la luz tal "*Estatuto de la profesión periodística*" que pudiera haber regulado los límites del secreto profesional periodístico. Pese a la inexistencia de la normativa específica esperada, los periodistas fundamentan la relación con sus fuentes en la confianza, lo cual, al igual que en la relación abogado-cliente, exige de este una conducta profesional íntegra y honrada, y, por ende, el periodista está obligado a cifrar todos los ficheros que guarden información conseguida a raíz de una relación periodística basada en el secreto profesional.

H. Sector creativo: propiedad intelectual e industrial y secretos comerciales

Los sistemas de cifrado se están empleando en la industria del entretenimiento para tratar de garantizar con ello la confidencialidad de las obras hasta el momento de su divulgación (***art. 4 LPI***). El objetivo que se busca con el cifrado es claro: preservar el control sobre el destino de la obra hasta que se haga accesible por primera vez al público.

> ***Artículo 4 Ley de Propiedad Intelectual***
>
> *"A efectos de lo dispuesto en la presente Ley, se entiende por divulgación de una obra toda expresión de la misma que, con el consentimiento del autor, la haga accesible por primera vez al público en cualquier forma; y por publicación, la divulgación que se realice mediante la puesta a disposición del público de un número de ejemplares de la obra que satisfaga razonablemente sus necesidades estimadas de acuerdo con la naturaleza y finalidad de la misma."*

Existe una tipología diversa de sistemas de cifrado, desde los que simplemente cifran los discos de los dispositivos, hasta los que se basan en la ofuscación del código fuente de programas de ordenador y páginas web. Un sistema de adecuado de cifrado de la información protege la creación del autor y permite diseñar con mayor tranquilidad el destino de las obras. De otra manera, en caso de que no se aplicase el cifrado, un despiste en la custodia de los dispositivos o una brecha de seguridad podrían derivar en la sustracción de los bienes culturales cuya explotación comercial controlada estaba prevista. El cifrado es la medida que ayuda a prevenir consecuencias indeseadas ante este tipo de riesgos.

Los sistemas de cifrado también son la solución para que las meras ideas, que cuentan con una protección legal un tanto indefinida, los secretos comerciales y los datos confidenciales puedan permanecer a la vista de unos pocos privilegiados y ocultos para la sociedad en general.

La divulgación o explotación, sin autorización de su titular, de secretos industriales o de cualquier otra especie de secretos empresariales a los que se haya tenido acceso legítimamente, pero con deber de reserva, o ilegítimamente, se consideran desleales (***art. 13 LCD***). Sin embargo, el problema no es si son o no desleales estas conductas, sino que las acciones legales que puedan ejercitarse contra los infractores solo tienen cabida cuando el daño se ha producido; esto es, en materia de secreto comercial, la norma solo

protege después de que se hayan divulgado o explotado los secretos. La persecución de las violaciones de secretos precisa que la violación haya sido efectuada con ánimo de obtener provecho, propio o de un tercero, o de perjudicar al titular del secreto, con lo que la acción se hace aún más complicada.

> ***Artículo 13 Ley de Competencia Desleal***
>
> *"**1**. Se considera desleal la divulgación o explotación, sin autorización de su titular, de secretos industriales o de cualquier otra especie de secretos empresariales a los que se haya tenido acceso legítimamente, pero con deber de reserva, o ilegítimamente, a consecuencia de alguna de las conductas previstas en el apartado siguiente o en el artículo 14.*
>
> ***2**. Tendrán asimismo la consideración de desleal la adquisición de secretos por medio de espionaje o procedimiento análogo.*
>
> ***3**. La persecución de las violaciones de secretos contempladas en los apartados anteriores no precisa de la concurrencia de los requisitos establecidos en el artículo 2. No obstante, será preciso que la violación haya sido efectuada con ánimo de obtener provecho, propio o de un tercero, o de perjudicar al titular del secreto."*

La solución para proteger los secretos comerciales es el cifrado. Cifrando los datos se dificulta la divulgación y a la explotación no autorizada de secretos comerciales, así como la adquisición de secretos por medio de espionaje o procedimiento análogo.

V. Sistemas de doble factor de autenticación (2FA)

La tecnología 2FA (doble factor de autenticación o two factor authentication) es aquella que requiere al usuario de dos elementos para demostrar su identidad. El primero de ellos puede ser una contraseña, es decir, la información confidencial frecuentemente constituida por una cadena de caracteres que puede ser usada en la autenticación de un usuario o en el acceso a un recurso, según el artículo 5 del RLOPD.

A. Marco de utilidad del 2FA

El éxito del 2FA tardó en llegar debido a dos factores: el primero fue que los sistemas digitales que se usaban al principio consistían en el empleo de tokens y otras herramientas que requerían de cierta pericia por parte del interesado; y el segundo fue que era necesaria una concienciación sobre la necesidad de dedicar tiempo a asegurar los perfiles digitales de uno mismo, como las cuentas en redes sociales o el correo electrónico.

La finalidad de esta tecnología es impedir o, por lo menos, poner mayores trabas para la intrusión o el acceso no autorizado a cuentas, información o datos personales de los usuarios.

El primer impulso a la implantación del 2FA se dio, a principios del siglo XXI, en el mercado del consumidor final. Fueron las grandes corporaciones norteamericanas del sector de los servicios a través de Internet las que comenzaron su introducción en la sociedad.

El segundo impulso a la implantación del 2FA fue aportado por las entidades del sector bancario por medio del empleo de tarjetas de coordenadas. Una tarjeta de coordenadas es "una tabla -normalmente de las dimensiones de una tarjeta de crédito- con un conjunto de claves", según apunta la Comisión de Seguridad en la Red de la Asociación de Internautas en su 'Informe técnico sobre los posibles riesgos de la Banca Electrónica (2006)'. Para poder acceder a un perfil, el sistema requiere al usuario de la tarjeta la introducción de un número específico ubicado en una coordenada concreta de la tarjeta.

El tercer impulso en Europa viene de la mano de la Autoridad Bancaria Europea o European Banking Authority (en adelante, EBA), a través de las Directrices definitivas sobre la seguridad de los pagos por Internet. En su sección de definiciones aporta una concreta para lo que se conoce como autenticación fuerte del cliente, exigiendo al menos un 2FA, pudiendo ser triple o superior.

> *"Por autenticación fuerte del cliente se entiende, a efectos de estas Directrices, un procedimiento basado en el uso de dos o más de los siguientes elementos, clasificados como conocimiento, posesión*

e inherencia: i) algo que solo conoce el usuario, por ejemplo, una contraseña, código o número de identificación personal fijos; ii) algo que solo posee el usuario, por ejemplo, token, tarjeta inteligente, teléfono móvil; iii) algo que caracteriza al propio usuario, por ejemplo, una característica biométrica, como su huella dactilar. Además, los elementos seleccionados deben ser independientes entre sí; es decir, la violación de uno no debe comprometer la seguridad de los otros. Al menos uno de los elementos no debe ser reutilizable ni reproducible (salvo para la inherencia) y su sustracción, de manera subrepticia, a través de Internet no debe resultar posible. El procedimiento de autenticación fuerte se debe diseñar de tal forma que proteja la confidencialidad de los datos de autenticación."

De esta forma, con la aprobación de las directrices de la EBA y su entrada en vigor, las entidades bancarias que operan en Europa deben dejar de aceptar el acceso de los clientes por medio de una contraseña y un código de una tarjeta de coordenadas, dado que ambas son reutilizables y reproducibles. En cambio, se impone como factor adecuado el token, la tarjeta inteligente, un SMS recibido en el móvil o un dato biométrico, como la huella dactilar. Es decir, **el 2FA se impone como requisito para todas las entidades bancarias en su relación con el cliente por medios electrónicos**.

El cuarto y definitivo impulso para la implantación del 2FA ha llegado a través del Reglamento General de Protección de Datos (UE). En el considerando 83 de la norma y en los artículos 32 y 35, se establece la necesidad de implantar medidas de seguridad acordes al estado de la técnica y adecuadas para impedir el acceso no consentido a los datos personales. Con ello, se pretende mitigar el riesgo que pueden causar determinadas brechas de seguridad sobre la empresa y los ataques sobre los usuarios.

B. El 2FA en el Reglamento General de Protección de Datos (UE)

Establece el Considerando 83 del Reglamento General de Protección de Datos (UE) que se deberán aplicar las medidas adecuadas para mitigar riesgos. La norma menciona expresamente el cifrado, debido a que es quizá la más conocida y ya que a través de ella se puede mantener a salvo la práctica totalidad de los datos. Sin embargo, de cara al usuario, al empleado o a los directivos de la compañía, el Considerando también deja abierta la posibilidad de implantar medidas que cubran la falibilidad humana:

"A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

La tecnología 2FA es cada vez más solicitada por los propios usuarios como consecuencia de importantes sustracciones de información con gran cobertura mediática, como, por ejemplo, la sufrida en 2012 por la red social profesional LinkedIn. Los delincuentes que atacaron la red obtuvieron los datos de más de 117 millones de usuarios, sustrayendo sus contraseñas. En esta ocasión, en vez de tratarse de un ataque informático complejo, los delincuentes accedieron por medio de algo tan simple como probar contraseñas que jamás deberían haberse empleado por los usuarios, como 123456, password o LinkedIn.

La pasividad de los usuarios a la hora de cambiar sus contraseñas o cuidar la seguridad de sus redes hace necesario contar con tecnologías activas de 2FA para salvaguardar los datos personales y ofrecer un sistema seguro y confiable. El usuario habitual usa la misma contraseña para la mayor parte de sus servicios online: el código de acceso al móvil suele ser el PIN de la tarjeta de crédito, coincidente a su vez con su fecha de nacimiento o los primeros dígitos de su DNI; y la contraseña del correo electrónico suele ser un nombre o un color seguido de un año. El ser humano resulta tan predecible, que el acceso a su información se convierte en un juego de niños. Este hecho aumenta la inseguridad del usuario al generar un efecto bola de nieve: si un servicio resulta atacado, los delincuentes obtendrán una contraseña que será la llave de acceso a todos los demás servicios. Los sistemas 2FA ayudan a detener o minorar este efecto, salvaguardando los datos del usuario bajo un factor adicional de seguridad.

Uno de los casos mediáticos que ha provocado mayor interés por la implantación de la tecnología 2FA es el conocido como 'Caso Celebgate', por el que las cuentas de almacenamiento en la nube de más de 50 actrices y modelos americanas fueron hackeadas. Las fotos más privadas de estas usuarias fueron publicadas en Internet creando un gran revuelo mediático. La intrusión, lejos de llevarse a cabo mediante complicadas técnicas, fue realizado a través de *phishing* por correo electrónico. Las afectadas entregaron sus contraseñas al recibir un correo en el que se pedían estas credenciales. Una vez las contraseñas se encontraron en manos de los delincuentes, estos pudieron acceder a sus datos e incluso a copias de seguridad de sus dispositivos. Acto seguido, filtraron la información obtenida a la Red a través de diferentes foros públicos. Esto provocó un cambio a nivel global sobre la conciencia de los usuarios sobre la seguridad de sus cuentas. A partir de este momento, el uso de 2FA por los grandes prestadores de servicios de Internet se convirtió en una práctica común.

C. Sistemas de autenticación única con 2FA

Los sistemas de 2FA comenzaron a usarse en nuevos servicios a través de Internet y reforzaron su presencia en la banca electrónica. Los OTP, o *one-time password*, también reforzaron su implantación en servicios bancarios. Estos dispositivos personales, los OTP, permiten la generación de un código único y temporal que autentica al usuario con una contraseña adicional. Los sistemas basados en firma electrónica cualificada de persona física o de representante de persona jurídica han sido y están siendo también empleados por proveedores de servicios como sistema de autenticación único y, en ocasiones, se refuerza con el envío de un número al móvil o el uso de la huella dactilar.

La proliferación de los teléfonos inteligentes está permitiendo que el sistema de 2FA se extienda. **Ahora, cada usuario con un smartphone lleva consigo una herramienta capaz de generar un código OTP o un SMS de duración limitada, con la ventaja de que, además, puede ser utilizado simultáneamente por cualquier servicio que requiera de este tipo de autenticación**. Aplicaciones como Google Authenticator, Latch o Authy permiten mejorar el control de acceso a los diferentes perfiles del usuario por medio de la generación de códigos o el bloqueo y desbloqueo de sitios o dispositivos.

En un principio el 2FA se implementaba únicamente para los servicios más críticos, como la banca online. Sin embargo, el aumento en la sensibilización de los usuarios sobre su privacidad y la seguridad de sus datos en Internet ha llevado a que cada vez servicios de todo tipo, como el correo electrónico o las redes sociales, permitan activar la opción de acceso a través de la autenticación por dos pasos. A esto hay que añadir la reciente inclusión de tecnología de identificación por datos biométricos, como la huella dactilar o el iris, que trae la posibilidad de realizar segundas o terceras autenticaciones con seguridad reforzada.

La inseguridad de la Red tiene como consecuencia la necesidad de establecer un mecanismo de seguridad adicional a la simple contraseña, que contrarreste las acciones de los atacantes y el olvido, despiste o desidia del usuario a la hora de proteger lo suyo, que tanto puede ser una cuenta en una red social como su dinero de la tarjeta o de una cuenta bancaria.

D. Protección frente a ataques informáticos mediante 2FA

Los sistemas de 2FA ayudan a pequeñas, medianas y grandes empresas, entidades bancarias incluidas, a luchar contra los delincuentes que explotan las vulnerabilidades electrónicas y las humanas, por medio de ingeniería social para hacerse con las contraseñas de acceso a los perfiles privados. Gracias al 2FA, la mayoría de los ataques no llegan a consumarse debido a que el atacante no puede acceder al recurso específico que conforma ese segundo factor de autenticación.

Cada día se denuncian algo más de 47 estafas informáticas, de acuerdo con los datos incorporados en la ***Memoria de 2015 de la Fiscalía General del Estado***. Este número podría haber sido menor si se hubiera empleado tecnología de 2FA. La estafa informática es, de hecho, el delito informático que acumula más procedimientos judiciales. Los datos rescatados de la memoria de la Fiscalía General del Estado, sin embargo, no reflejan todos los que sufren los ciudadanos y las empresas en España, sino naturalmente solo aquellos que han sido denunciados. El número de afectados y el importe sustraído es probable que sea mucho mayor del que reflejan los datos, teniendo en cuenta ese número de víctimas que no denuncia las estafas que sufre, bien por no saber cómo debe actuar, bien por no estimar eficiente la inversión de su tiempo en el procedimiento habida cuenta de la cantidad que se le haya sustraído, o bien porque nunca llega a saber siquiera que ha sido estafado.

El número de estafas informáticas crece cada año de manera exponencial, junto con el resto de delitos informáticos registrados por el Estado. Así, mientras que en 2011 se constataron 6.532 delitos informáticos, en 2013 fueron 11.990 y 20.534 en 2014, lo que representa un incremento de un 210% en 3 años. Del total de 20.534, se consignaron 17.328 estafas informáticas, esto es, un 84,39% del total de los delitos informáticos sufridos en España.

La mayoría de las estafas suceden, según reconoce la Fiscalía en el informe referido, en relación con: ventas fraudulentas de productos; *phishing*, o suplantación de identidad para la obtención de datos personales o bancarios; *carding*, o uso de tarjetas de crédito o de sus datos o incluso de tarjetas virtuales; y actividades engañosas relacionadas con el juego *online*. Los tribunales reciben cada vez más casos de estafas informáticas de distintos tipos que afectan a consumidores y usuarios de todos los sectores de la industria.

E. Empresas y fuerzas de seguridad recomiendan implementar 2FA

La implantación de los sistemas de 2FA en las cuentas de los clientes bancarios protegen a las entidades bancarias frente a la devolución de cantidades en caso de que alguno de ellos sea objeto afectado de un delito informático. O de un conato de delito, ya no podría terminar de realizarse gracias el 2FA. Según indica el Banco de España en su ***Memoria del Servicio de Reclamaciones***, publicada en 2012, "*cuando el titular de la cuenta no reconozca su autoría en la operación de pago —en este caso, una transferencia— ni la falta de diligencia en el cumplimiento de sus obligaciones de custodia —tarjeta de coordenadas, etc.—, su entidad deberá reembolsarle de inmediato los fondos detraídos, salvo que pueda acreditar que aquel actuó de manera fraudulenta o incumpliendo, de manera deliberada o por negligencia grave, una o varias de las obligaciones que le incumben; y ello, con independencia de que la entidad pueda llevar a cabo, una vez efectuado el reembolso, las investigaciones que estime oportunas en defensa de sus legítimos intereses*". El 2FA permite añadir al banco una necesaria capa de protección, puesta en el cliente, ante este tipo de ataques.

Además de en sistemas de banca en línea u otras conexiones del usuario, es probable que las empresas comiencen a implementar en los próximos meses sistemas de 2FA en lugares electrónicos clave, incluyendo puntos de acceso móvil de los empleados, redes privadas virtuales (VPN), la infraestructura de escritorio virtual (VDI), servidores en la nube y diferentes redes, según un Informe Anual de Amenazas 2015 publicado por Dell Security en 2016. Según esta empresa, es posible reforzar las medidas de 2FA solicitando a todos los usuarios el empleo de contraseñas diferentes para todos sus servicios; la elaboración de códigos de conducta internos y procedimientos detallados sobre qué hacer cuando un empleado extravía el móvil o le es sustraído su dispositivo portátil; y educar a los empleados sobre las medidas de seguridad básicas, tales como la protección de contraseña.

Si bien la implantación del 2FA es de extremada conveniencia, habida cuenta del crecimiento en número de los ataques informáticos y la ruptura de medidas basadas en simples contraseñas, la Policía Nacional Española y EUROPOL advierten de que las nuevas tendencias del cibercrimen tienen como foco la instalación de malware en dispositivos móviles en los que se reciben las coordenadas con el objetivo de saltarse la protección del 2FA. Por este motivo, **la confianza en sistemas de 2FA debe depositarse en un prestador adecuado que, además, esté directamente involucrado en la prestación de servicios de seguridad informática contra infecciones de cualquier tipo**.

En este mismo sentido se presenta sus conclusiones el Informe Akamai Q3 sobre el estado de Internet de 2014, publicado en 2015:

> *"Another method to foil these types of phishing attacks is to enable two-factor authentication (2FA) on employees' email. When someone tries to log in to the email from an unknown or untrusted computer, a text message or voice message will be sent to the user, containing a short alphanumeric code that must to be entered to gain access to the mail account. With 2fa enabled, even if the user is successfully phished, the attacker will not be able to get into the mail account. Even better, when the attacker tries to access the mail account, it will trigger a message, effectively notifying the victim that someone is trying to log in to their mail account.*
>
> *At that point, the victim should know to notify their company's help desk and/or security team to make the company aware of the attack and take necessary steps to lock down accounts and services.*
>
> *Additionally, when the user does enter the 2fa code, they should be attentive and ensure that the site they are entering the code into is the site they are expecting. Phishers are capable of presenting false screens mimicking the 2fa code screen to capture the code to go with the password they have previously recovered."*

Confiar en la tecnología 2FA no es suficiente. También debe comprobarse la fiabilidad del prestador de la solución con el objetivo de obtener una confianza plena en la herramienta.

El informe de la Policía Nacional Alemana, titulado '*Perspectivas de Ciberseguridad Europea 2015*' (European Cyber Security Perspectives 2015), publicado en 2016, **señala también la importancia de la tecnología 2FA para combatir el cibercrimen**, creando una barrera entre la intención de obtener datos, información o dinero, de la consecuencia realmente obtenida, que suele ser nula. El informe hace especial hincapié en dos aspectos fundamentales: el hecho de que los terminales móviles se hayan convertido en los token personales de los usuarios; y la realidad que constituye el que estas herramientas puedan validar al usuario por medio de los datos biométricos tales como la huella dactilar. Aunque el informe no mencione otras formas de análisis biométrico, el reconocimiento del iris o la forma facial también son aspectos a tener en cuenta y que entran en lo que se conoce como tecnología disponible dentro del estado de la ciencia.

> *"In 2011, some online service providers introduced two-factor authentication, also called two-step authentication or 2FA. We now see that 2FA mechanisms increasingly involve the end user's smartphone. On top of the normal username/password, this setup involves a separate code that is acquired by the user by SMS or generated by a personalized app on their mobile phone. An example of the latter is the Google Authenticator. It can generate one-time passwords, and is implemented using open standards from the Initiative for Open Authentication (OATH). The large number of users that possess a smartphone has greatly contributed to the relatively easy implementation of 2FA. Notably, most service providers offer 2FA as an opt-in, it's use is not mandatory. Since 2013, we have seen a rapid growth in the service providers that offer two-factor authentication. We expect this trend to continue, especially given the fact that several smartphones have been released in 2013 and 2014 which include built-in biometrics (the third authentication factor), such as the Apple iPhone 5S/6 with its touch ID and the Samsung Galaxy S5 with a similar fingerprint scanner."*

La tecnología del 2FA también ha sido objeto de tratamiento en otros muchos informes de las Fuerzas y Cuerpos de Seguridad de diferentes estados de la Unión Europea, de Estados Unidos y Canadá, así como por empresas y organizaciones dedicadas al estudio de la seguridad en el empleo de recursos electrónicos. La ENISA (*European Union Agency for Network and Information Security*) publicó en 2013 el Informe "*e-ID Authentication methods in e-Finance and e-Payment services Current practices and Recommendations*" en el que ya recomendaba el empleo de esta tecnología, especialmente para el sector bancario.

> *"For medium and high risk operations, a strategy of using at least two authentication mechanisms that are mutually independent, where one is non-replicable and other non-reusable, exchanging credentials through different communication channels or devices should be implemented. Non-re-usability may be implemented by linking the authentication (e.g. OTP challenge) to the amount and payee of every transaction."*

La cantidad y calidad de informes en relación con la utilidad de los sistemas 2FA es creciente. Gracias a esta tecnología es posible disponer de un sistema de defensa avanzada ante ataques informáticos basados en estrategias de fuerza, en el uso sistemas complejos de intrusión o en el empleo de esquemas de ingeniería social. Desde los estados hasta las empresas del sector lo recomiendan, y es el usuario el que lo pide como uno de los mejores mecanismos de protección de sus activos, incluyendo sus perfiles, información, dinero y datos personales.

VI. Bring Your Own Device (BYOD)

BYOD (Bring Your Own Device) es una práctica corporativa consistente en permitir que el empleado haga uso de su propio dispositivo para fines profesionales o que emplee el que ha recibido de la empresa para fines personales. Esta práctica, que es tendencia, implica una cantidad importante de riesgos en relación con la protección de la información en todos sus niveles: datos personales, creaciones, secretos comerciales...

Los riesgos más importantes derivados del BYOD se han puesto de manifiesto con la aparición de aplicaciones móviles que, una vez instaladas en el dispositivo, empujan al usuario a compartir la agenda de contactos y la ubicación o permitirle el acceso al carrete de fotos o la tarjeta de memoria del terminal. Habitualmente, los usuarios suelen almacenar de manera mezclada los datos corporativos y los personales,

por lo que, tanto en estos casos como en los supuestos de extravío, sustracción o robo del terminal, todos quedan afectados.

Los sistemas de bloqueo de aplicaciones, las agendas separadas y los sistemas de cifrado implementados en los terminales complican el acceso a datos por parte de terceros no autorizados. Un sistema portable con contraseña de acceso en remoto a datos cifrados permitiría al usuario hacer uso de su terminal personal para fines profesionales, así como los sistemas que cifran el disco completo y permiten el acceso a los datos según parámetros y permisos otorgados por el administrador en función de los privilegios del usuario.

INCIBE, el Instituto Nacional de Ciberseguridad, recomienda a las compañías que apuesten por el BYOD que conciencien al empleado, "*para que en caso de que este lo use para temas de trabajo, incorpore las mismas medidas de seguridad que los dispositivos utilizados dentro de la compañía*". Asimismo, ofrece una recomendación clara en cuanto al cifrado de datos en su artículo '***Móviles personales y otros «wearables» en la empresa: los riesgos del BYOD.*** "*No permitir el almacenamiento de información sensible dentro del dispositivo. Y en caso de que se produzca, recomendar el uso de cifrado.*"

La normativa obliga a aplicar cifrados en los dispositivos de los empleados, en las áreas que admitan BYOD de todas las empresas que tienen obligación de cifrar alguno de sus ficheros, siempre que el trabajador vaya a almacenar o tratar dicha información. Las empresas que desean proteger determinados archivos deben también cifrar los dispositivos de los empleados que tengan acceso a ellos.

El riesgo del BYOD es alto en materia de seguridad. El empleado puede: extraviar el dispositivo, permitir que lo utilicen familiares o amigos, olvidar cambiar la contraseña de acceso, conectarse a través de una red 2G permitiendo la extracción de datos por medio de falsas antenas, enchufar su equipo a un cargador USB falso en un bar, instalar malware que envía archivos al exterior o, simplemente, anclar su dispositivo a una red 4G ajena a la propia de la compañía para realizar a través de ella lo que a través de la red de la compañía no podría.

El CERT Gubernamental español (**CNN-CERT**), que forma parte del Centro Nacional de Inteligencia (**CNI**), realizó una encuesta a empleados BYOD. Según el CERT, "*el dato más preocupante es que cerca de la mitad de los encuestados no manejan la información corporativa de forma cifrada en su dispositivo personal, incluso el 15,6% dice no saber cómo se debe manejar dicha información*" ('***Riesgos y amenazas del Bring Your Own Device (BYOD)***'). Este tipo de trabajadores podría llegar conectarse a redes desconocidas inseguras haciendo posible, sin quererlo, que se produzcan sobre sus dispositivos "*ciberataques de tipo man-in-the-middle, que podrían interceptar e incluso modificar los datos en tránsito*". Para evitar esta consecuencia, la primera medida de seguridad que recomienda el CERT es "*usar mecanismos de cifrado fuerte*", tales como el uso de redes privadas virtuales o VPN y sistemas de cifrado de datos.

Dentro del análisis de riesgos que el CERT realiza en su informe sobre BYOD, indica un aspecto que convendría tener en cuenta: "*[La] seguridad jurídica en caso de pérdida, robo o finalización de la relación de trabajo del empleado, requiriendo el uso de contraseñas de acceso, bloqueo de dispositivos, cifrado de información, así como el derecho institucional a borrar remotamente los datos corporativos del equipo*". El cifrado de la información vuelve a resultar una medida esencial.

Las empresas que vayan a permitir el BYOD deben realizar un cifrado completo de todos los dispositivos del empleado que vayan a ser utilizados también para el trabajo. El ***artículo 101 RLOPD*** impone esta obligación en el caso de que los dispositivos vayan a ser empleados para tratar datos o realizar un tratamiento de datos que exijan la implantación de medidas de seguridad de nivel alto. Además, es recomendable que configuren medidas que permitan al empleado abrir determinados archivos o le impidan enviar otros. Una precaución adicional para casos de emergencia es prever el bloqueo y borrado en remoto de los datos si fuera necesario.

VII. Notificación de brechas de seguridad informática

Una brecha de seguridad informática es un fallo o una vulnerabilidad de un programa de ordenador que conduce a la destrucción de información, a su pérdida o a la extracción de esta por un tercero no autorizado.

Con la norma antigua, las brechas de seguridad informática debían notificarse a la AEPD en caso de que fuera un determinado tipo de empresa del sector de las telecomunicaciones la que la sufriera, en términos generales.

Con el Reglamento General de Protección de Datos, todas las empresas están obligadas a notificar las brechas de seguridad, por lo que deberán extraer información constante sobre los intentos de intrusión y los accesos exitosos no autorizados para poder realizar la notificación en plazo. Además, se establece la obligación de comunicar determinados detalles de la brecha a las personas cuyos datos se hayan visto expuestos o se hayan podido ver afectados de alguna forma.

A. Obligaciones ante una brecha de seguridad, según la LOPD

La LOPD y la normativa sectorial o vinculada establecen que solo deberán notificarse las brechas de seguridad en determinados casos, sin que expresamente se obligue a comunicar detalle alguno a los posibles afectados.

1. Los operadores de telecomunicaciones están obligados a notificar brechas de seguridad

La normativa vigente en España establece que **los operadores que explotan redes públicas de comunicaciones electrónicas o que prestan servicios de comunicaciones electrónicas disponibles al público están obligados a notificar a la AEPD las brechas de seguridad que sufran cuando supongan la pérdida, destrucción, alteración o acceso ilegítimo a datos de carácter personal**. Asimismo, el operador debe notificar también al abonado o particular, sin dilaciones indebidas, la violación sufrida.

Las demás empresas, distintas a las referidas del sector de las comunicaciones electrónicas, no están obligadas ni habilitadas legalmente para notificar. En caso de que la brecha no haya afectado a datos personales, solo las empresas que formen parte de las infraestructuras críticas del estado pueden, si lo desean, informar al CNPIC español.

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.

"*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.

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 las intromisiones o bien ni siquiera las detectan.

Los sujetos obligados a cumplir la normativa española de protección de datos (artículo 2 de la LOPD), están obligados a contar con un sistema adecuado de bloqueo 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.

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, excomisaria 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)***

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:

- Obligación de adoptar medidas técnicas y de gestión: 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, deben 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.

- Obligación de notificar determinadas brechas de seguridad a la AEPD: 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 AEPD.

- Obligación de comunicar determinadas brechas de seguridad a los afectados: 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.

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*".

La 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:

- Obligación de implementar herramientas que limiten el acceso a los datos: la empresa debe articular un sistema que ofrezca la garantía de que solo el personal autorizado tenga acceso a los datos personales para fines autorizados por la Ley.

- Obligación de adoptar medidas específicas de protección de datos personales: la empresa debe adoptar medidas para la protección de los datos personales del acceso o revelación no autorizados o ilícitos, así como para actuar en caso de destrucción accidental o ilícita y ante la pérdida o alteración accidentales o el almacenamiento o tratamiento no autorizados o ilícitos.

- Revisar el cumplimiento de las políticas de protección de datos: la empresa debe garantizar la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.

La AEPD, 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.

2. Cuándo se debe notificar una brecha de seguridad

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 AEPD.

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

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.

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.

3. Qué debe contener la notificación de una brecha de seguridad

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 tener el siguiente contenido mínimo, según dispone el Anexo I del ***Reglamento (UE) Nº 611/2013***:

Sección 1. Contenido mínimo para la notificación inicial.

- Deberá identificar al proveedor, detallando su denominación, identidad y un punto de contacto que podrán 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 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.

La comunicación a la AEPD se debe hacer a través de un formulario online accesible a través de la Sede Electrónica de esta Agencia en el apartado ***"Notificación de quiebras de seguridad"***. 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.

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 puede registrarse internamente para desarrollar e implementar las medidas de precaución y seguridad necesarias por si volviese a tener lugar esa intrusión u otra similar.

4. Cómo se debe informar al usuario afectado por la brecha

En cuanto a la notificación al particular afectado, debe enviarse sin dilaciones injustificadas, aunque puede demorarse con la autorización de la AEPD, y tiene que enviarse completa y en una sola fase.

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.

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.

5. Cifrar permite, según el caso, no comunicar la brecha de seguridad a los usuarios

La notificación a los particulares no es necesario realizarla cuando la intrusión y la violación de datos no pueda afectar negativamente a los datos personales o a la intimidad del particular; y 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.

Para poder evitar la notificación a la AEPD, la empresa que haya sufrido la quiebra de seguridad debe estar en disposición de probar a la autoridad competente que ha aplicado a los datos afectados las medidas de seguridad necesarias para hacerlos incomprensibles, según dispone en la ***Directiva 2002/58/CE*** y la ***Ley General de Telecomunicaciones***.

En relación a qué debe considerarse un dato incomprensible, el ***Reglamento (UE) nº 611/2013*** considera que es cuando se hayan cifrado de forma segura y la clave no haya sido comprometida, así como cuando se hayan sustituido por su valor resumen (*hash value*), calculado mediante una función resumen cuya clave no haya quedado comprometida.

> ***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. Sanciones por no notificar, según la LOPD

La normativa española obliga a implementar medidas suficientes de seguridad para prevenir intrusiones y, para determinados tipos de empresas, a notificar las brechas cuando tienen lugar y a comunicarlas a los afectados. La falta de cumplimiento de esta obligación, así como la de no notificar o, en su caso, comunicar puede derivar en sanciones: 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.

Asimismo, los afectados podrían tener derecho a ser indemnizados por determinados daños y perjuicios que la brecha de seguridad, con la consecuente afección de sus datos, les hubiera ocasionado.

B. Obligaciones ante una brecha de seguridad, según el nuevo Reglamento General de Protección de Datos (UE)

El Reglamento General de Protección de Datos (UE) amplía las obligaciones de notificación y comunicación de las brechas de seguridad sufridas.

1. Todas las empresas están obligadas a notificar las brechas de seguridad sufridas

La entrada en vigor del Reglamento General de Protección de Datos (UE) extiende a todas las empresas, autónomos y administración pública la obligación de notificar las violaciones de la seguridad de los datos personales a la autoridad de control y la de comunicársela a los interesados.

Las empresas no son las únicas obligadas a notificar las brechas de seguridad. Los sujetos obligados a notificar las violaciones de la seguridad de los datos personales a la autoridad de control y a comunicársela a los interesados son, según el artículo 4 del Reglamento General de Protección de Datos (UE), la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como, entre otros, los siguientes:

- Pérdida de control sobre sus datos personales o restricción de sus derechos
- Discriminación
- Usurpación de identidad
- Pérdidas financieras
- Reversión no autorizada de la seudonimización
- Daño para la reputación
- Pérdida de confidencialidad de datos sujetos al secreto profesional
- Perjuicios económicos o sociales significativos para la persona física

Para evitar los daños y perjuicios derivados de una brecha de seguridad, se deben tomar a tiempo medidas adecuadas, como la implementación de antivirus, cortafuegos, sistemas de cifrado o la activación de herramientas de 2FA.

Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento pueden elaborar códigos de conducta o modificar o ampliar dichos códigos, según se dispone en el ***artículo 40 del Reglamento General de Protección de Datos (UE)***, con objeto de especificar la aplicación del ***Reglamento General de Protección de Datos (UE)***, como en lo que respecta a la seudonimización de datos personales o la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados.

2. Cuándo se debe notificar una brecha de seguridad

Tan pronto como la empresa, en su calidad de responsable del tratamiento, **tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, debe notificar esta a la AEPD o la autoridad de control competente**.

El responsable debe hacer esta notificación lo antes posible y, de ser posible, dentro de las 72 horas posteriores al momento en que haya tenido constancia de la brecha, a menos que pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

Si no es posible realizar dicha notificación en el plazo de 72 horas, cuando se presente el escrito este debe acompañarse de una indicación de los motivos de la dilación.

Los encargados del tratamiento también están obligados a notificar de forma inmediata al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. Qué debe contener la notificación de una brecha de seguridad

La notificación que hay que hacer a la AEPD deberá, como mínimo:

- **Describir la naturaleza de la violación de la seguridad** de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

- **Comunicar el nombre y los datos de contacto del delegado de protección de datos** o de otro punto de contacto en el que pueda obtenerse más información;

- **Describir las posibles consecuencias de la violación** de la seguridad de los datos personales;

- **Describir las medidas adoptadas** o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si al sujeto que ha sufrido el ataque informático no le fuera posible facilitar toda la información

simultáneamente, podrá facilitarla gradualmente, a medida que la tenga y sin dilación indebida; esto es, cuanto antes y sin dejar pasar más tiempo del estrictamente imprescindible.

Así mismo, el responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Según el ***artículo 33 del Reglamento General de Protección de Datos (UE)***, dicha documentación permitirá a la AEPD verificar el cumplimiento de la normativa por parte del sujeto que ha sufrido la brecha de seguridad.

4. Cómo se debe informar al usuario afectado por la brecha

La empresa responsable del tratamiento debe comunicar al interesado, también lo antes posible, la violación de la seguridad de los datos personales en caso de que pueda entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias.

La comunicación de la brecha de seguridad a las personas físicas cuyos datos personales hayan sido afectados por ella debe contener los siguientes apartados mínimos:

- Una descripción de la naturaleza de la violación de la seguridad de los datos personales
- Las recomendaciones concretas para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.
- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

5. Cifrar puede permitir no comunicar la brecha de seguridad a los usuarios

La comunicación al interesado no será necesaria si se cumple alguna de las condiciones siguientes:

- El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
- El responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado;

La comunicación de la brecha de seguridad deberá realizarse de forma pública en un medio de comunicación adecuado cuando suponga un esfuerzo desproporcionado ponerse en contacto con los interesados. La finalidad de esta comunicación pública es que se informe de manera igualmente efectiva a los interesados.

Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la AEPD, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle, según el ***artículo 58.2.e del Reglamento General de Protección de Datos (UE)***, que lo haga directamente o a través de una comunicación pública o podrá decidir que se cumple alguna de las condiciones para poder evitar la comunicación.

La aplicación de sistemas de cifrado, que hacen ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, permiten no tener que realizar ningún tipo de comunicación a los interesados en caso de que se sufra un ataque de seguridad, a menos que, por motivos justificados, la AEPD ordenase realizar el envío de la información directa o públicamente.

Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la AEPD, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. El ***Reglamento General de Protección de Datos (UE)***, en su Considerando 86, indica que, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

VIII. Certificaciones informáticas requeridas por la ley

El ***Reglamento General de Protección de Datos*** dedica un breve apartado a las certificaciones, consciente de que la especialización en esta compleja materia, así como la necesidad de conocer la capacidad de las empresas y los profesionales es cada vez más necesaria.

A. El concepto de certificación informática

Una certificación en materia de seguridad informática es una acreditación otorgada por un tercero independiente que asegura que un sujeto que haya sido auditado cumple una condición concreta en esa área de seguridad.

Las certificaciones suelen ser empleadas cuando dos o más sujetos van a establecer una relación contractual, ya sea comercial o laboral, y uno de ellos requiere al otro una prueba de que ha superado un proceso de certificación determinado. En estas circunstancias, un tercero independiente audita y, si la prueba es satisfactoria, emite un documento de certificación positiva.

Las certificaciones de seguridad informática no demuestran conocimientos informáticos, sino el hecho de que el sujeto auditado ha superado un proceso dado de certificación. Cuanto mayor sea el reconocimiento del certificado en la industria, mayor será el valor de este en sí mismo.

Los certificados obtenidos incrementan la confianza entre empresas, especialmente en transacciones internacionales. Cuando una empresa desconoce los métodos, los controles de calidad o la legislación a la que otra empresa se encuentra sometida, encontrará en los certificados emitidos por organizaciones internacionales un sistema reconocido con el que valorar su estado dentro del mercado competitivo y, con ello, tomar una decisión sobre si debe o no llevar a cabo la contratación.

B. Clasificación de certificaciones

Las certificaciones pueden ser de distintos tipos según la materia que traten y a quién se encuentren dirigidas: por un lado, tenemos las certificaciones para empresas y usuarios; y, por otro, las certificaciones genéricas y las específicas.

1. Certificaciones para empresas y certificaciones para usuarios

Las certificaciones emitidas sobre empresas son aquellas que acreditan que una empresa cumple ciertas condiciones relativas al proceso de producción o servicio, la calidad de estos o el proceso de entrega o prestación. Suelen estar enfocadas a crear elementos de confianza entre empresas que se plantean contratar entre ellas. Ejemplos claros de este tipo de certificaciones son aquellos que acreditan un nivel de seguridad informático determinado o las relacionadas con la protección ambiental en todas las actividades de una empresa.

Las certificaciones para usuarios son aquellas que acreditan que el usuario que las recibe posee unas habilidades o características específicas para el desarrollo de una función determinada. Estas certificaciones suelen tener un carácter más académico o de habilidad personal. Sirven para demostrar a una empresa la capacidad del usuario para desarrollar una función determinada, que puede ir desde el procesamiento de textos hasta el hecho de contar con conocimientos avanzados en materia de seguridad.

2. Certificaciones genéricas y certificaciones especificas

Las certificaciones generales son aquellas que se centran en el resultado y no en la herramienta a utilizar. Estas suelen ser emitidas por organizaciones internacionales, como por ejemplo ECDL o ISO.

La ECDL (*European Computer Driving Licence*) es una organización internacional nacida en Europa que expide acreditaciones reconocidas a nivel internacional que certifican los conocimientos de los usuarios en distintas áreas ofimáticas. Mediante distintos centros distribuidos por todo el mundo, aquellos usuarios interesados en obtener una acreditación de sus habilidades informáticas pueden obtener los certificados ofrecidos por ECDL y, con ello, demostrar sus conocimientos para el desarrollo de determinadas actividades. Actualmente, muchas empresas comienzan a solicitar a los candidatos a puestos de trabajo que acrediten mediante estos títulos el conocimiento que tienen en ciertas áreas.

Las ISO son las certificaciones más importantes a nivel global. Son expedidas por la Organización Internacional de Normalización (ISO de sus siglas en inglés). Esta organización tiene como objetivo la creación de estándares internacionales para todos los países miembros. Para ello, emite las llamadas certificaciones ISO, las cuales permiten a las empresas acreditar el cumplimiento de los estándares internacionales en un área concreta de su actividad. Estas certificaciones están directamente relacionadas con la calidad del servicio que ofrecen las empresas y suponen un importante factor de confianza, sobre todo en las transacciones comerciales.

Por último, las certificaciones también pueden ser específicas para el uso de una herramienta concreta. Un ejemplo de esto lo encontramos en las certificaciones que se otorgan para acreditar la capacidad en el procesamiento de textos. Así, una certificación genérica sería aquella que acredita que el usuario tiene las habilidades necesarias para procesar textos o para usar sistemas operativos. Por otro lado, la específica acredita el uso de, por ejemplo, herramientas ofimáticas concretas o determinadas distribuciones de sistemas operativos. Este tipo de acreditaciones pueden aplicarse a cualquier área informática para la cual existan distintas herramientas para el desarrollo de una actividad concreta.

C. Algunas de las principales certificaciones

Actualmente, los Comités de Conjunto técnico de ISO trabajan en las siguientes áreas:

- **ISO/IEC JTC 1/SG 1** Smart Cities
- **ISO/IEC JTC 1/SWG 2** Directives
- **ISO/IEC JTC 1/SWG 3** Planning
- **ISO/IEC JTC 1/SWG 6** Management
- **ISO/IEC JTC 1/WG 7** Sensor networks
- **ISO/IEC JTC 1/WG 9** Big Data
- **ISO/IEC JTC 1/WG 10** Internet of Things (IoT)
- **ISO/IEC JTC 1/SC 2** Coded character sets
- **ISO/IEC JTC 1/SC 6** Telecommunications and information exchange between systems
- **ISO/IEC JTC 1/SC 7** Software and systems engineering
- **ISO/IEC JTC 1/SC 17** Cards and personal identification
- **ISO/IEC JTC 1/SC 22** Programming languages, their environments and system software interfaces
- **ISO/IEC JTC 1/SC 23** Digitally Recorded Media for Information Interchange and Storage
- **ISO/IEC JTC 1/SC 24** Computer graphics, image processing and environmental data representation
- **ISO/IEC JTC 1/SC 25** Interconnection of information technology equipment
- **ISO/IEC JTC 1/SC 27** IT security techniques
- **ISO/IEC JTC 1/SC 28** Office equipment
- **ISO/IEC JTC 1/SC 29** Coding of audio, picture, multimedia and hypermedia information
- **ISO/IEC JTC 1/SC 31** Automatic identification and data capture techniques
- **ISO/IEC JTC 1/SC 32** Data management and interchange
- **ISO/IEC JTC 1/SC 34** Document description and processing languages
- **ISO/IEC JTC 1/SC 35** User interfaces
- **ISO/IEC JTC 1/SC 36** Information technology for learning, education and training
- **ISO/IEC JTC 1/SC 37** Biometrics
- **ISO/IEC JTC 1/SC 38** Cloud Computing and Distributed Platforms
- **ISO/IEC JTC 1/SC 39** Sustainability for and by Information Technology
- **ISO/IEC JTC 1/SC 40** IT Service Management and IT Governance

La Organización Internacional de Normalización emite actualmente miles de certificaciones sobre numerosos aspectos, desde la manipulación de alimentos hasta cuestiones medioambientales. **Las certificaciones ISO relevantes en el campo de la seguridad informática son aquellas pertenecientes a la serie 27000 y que van desde 27001 a 27004. Estas engloban todos los aspectos relacionados con el uso de herramientas informáticas.**

- **27001**: especifica los requisitos para establecer, implementar, mantener y mejorar la seguridad del sistema informático en el contexto de la organización. También incluye los requisitos para lidiar con los riesgos que pueden derivarse en el funcionamiento de cada organización.

- **27002**: establece las líneas a seguir a la hora de gestionar las prácticas en seguridad informática como la selección, la implementación y el control de las herramientas necesarias para los posibles riesgos a los que cada empresa puede verse enfrentada.

- **27003**: se concentra en los aspectos clave necesarios para el desarrollo y diseño de los sistemas de seguridad en una empresa.

- **27004**: establece una guía sobre el desarrollo de medidas que aseguren la efectividad en la implementación de los sistemas de seguridad en la empresa.

En cuanto a las certificaciones relativas a los usuarios, actualmente la ECDL ofrece acreditar competencias en tres niveles distintos (Base, Standard y Avanzado) para las áreas de ofimática, diseño web, diseño o edición de imágenes, herramientas online y seguridad informática.

D. Normas que exijan o recomienden contar con un certificado

El Reglamento General de Protección de Datos (UE), en su artículo 42 promueve el uso de certificaciones por parte de empresas europeas en materia de protección de datos para demostrar su cumplimiento en esta materia. Las empresas que soliciten las certificaciones deberán entregar, a las organizaciones que las emiten, toda la información que se les solicite y, si se les concede, podrán disfrutar del certificado por un máximo de tres años, plazo que podrá ser renovado según el desarrollo de la empresa.

El uso de estas certificaciones será voluntario y transparente por parte de las empresas y de los organismos que emiten estas certificaciones. Estos organismos, que se encuentran regulados en el ***artículo 43 del Reglamento General de Protección de Datos (UE)***, deben cumplir ciertos requisitos, tales como ser independientes, establecer revisiones periódicas, tener procedimientos para tratar reclamaciones de infracción y que en ningún caso exista conflicto de intereses.

La inclusión de los certificados en el nuevo reglamento de protección de datos, junto con la tendencia de las compañías de exigir a sus proveedores el estar en posesión de muchas de estas acreditaciones, muestran que en el futuro los certificados serán un elemento indispensable en las relaciones comerciales entre empresas.

La creciente globalización hace que las empresas contraten cada vez más de forma internacional. Para ello, las certificaciones son una herramienta indispensable sobre la que basar la confianza cuando no existe una experiencia previa.

IX. Sanciones con el nuevo Reglamento General de Protección de Datos (UE)

El Reglamento General de Protección de Datos (UE) establece un marco de sanciones para aquellos casos en los que los sujetos obligados (empresas, autónomos o Administraciones Públicas) incumplan la normativa aplicable a la protección de los datos de carácter personal.

Las sanciones se podrán imponer tras un procedimiento de investigación, seguido por uno sancionador. Este tipo de procedimientos pueden ser iniciados a instancia de parte, a través de una denuncia o una solicitud de amparo, o de oficio. La AEPD, además, lleva a cabo inspecciones sectoriales enfocadas a analizar el estado del cumplimiento normativo en sectores concretos como el sanitario o el automovilístico, entre otros.

Una inspección de oficio podría iniciarse cuando una empresa notifique a la AEPD una brecha de seguridad sufrida por ella misma. En ese momento, la autoridad realizará las tareas siguientes:

- ✓ Se verificará si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y a interesado.

- ✔ Se verificará que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado.

En caso de que la AEPD resuelva sancionar, según el ***artículo 83 del Reglamento General de Protección de Datos (UE)*** **se podrían llegar a imponer multas administrativas de 10 millones de euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global** del ejercicio financiero anterior, optándose por la de mayor cuantía.

Y si, tras haber sido advertido, apercibido u ordenado por la AEPD para hacer algo, se continúa en el incumplimiento de las resoluciones de la autoridad de control, **se podrán imponer multas administrativas de 20 millones de euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global** del ejercicio financiero anterior, optándose por la de mayor cuantía.

La implementación de sistemas robustos de cifrados y de herramientas de 2FA para minorar riesgos son esenciales para prevenir las consecuencias de un procedimiento sancionador. El escudo de protección ofrecido por estas soluciones tecnológicas es, además de obligatorio en muchos casos, un sistema para evitar sanciones y aumentar la confianza del cliente.

Como dijo la AEPD en relación con la seguridad y la protección de datos de carácter personal, "*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*".

Los sistemas de cifrado y de 2FA son soluciones al alcance de cualquiera, comúnmente aceptadas y de implantación económica. Contar con esta tecnología en la empresa, ya sea por decisión voluntaria o por obligación legal, protege frente a ataques informáticos y ante las sanciones, ofrece un escudo de seguridad y es, en la actualidad, el definitivo certificado de calidad.

Informe elaborado por

abanlex

CONTACTA CON NOSOTROS

96 291 33 48