LA SEGURIDAD DE LOS DATOS PERSONALES Y LA OBLIGACIÓN DE NOTIFICAR LAS BRECHAS DE SEGURIDAD

THE SECURITY OF PERSONAL DATA AND THE OBLIGATION TO NOTIFY SECURITY BREACHES

María Cumbreras Amaro
Abogada y Economista
Experta en Derecho Tecnológico en Procesia

Fecha de recepción: 12/02/2020
Fecha de aceptación: 03/03/2020

RESUMEN: El presente trabajo tiene como objetivo facilitar la interpretación de la normativa de protección de datos en lo relativo a la obligación de notificar las brechas de seguridad a la autoridad competente y, en su caso, a los interesados de modo que la notificación se gestione siguiendo unas pautas orientativas, se comunique por el canal adecuado y contenga información suficiente en base a las nuevas exigencias de la legislación.

ABSTRACT: The objective of this work is to facilitate the interpretation of the data protection regulations with regard to the obligation to notify data breaches to the competent authority and, where appropriate, to the data subjects so that the notification is managed according to a guideline, is communicated through the appropriate channel and contains sufficient information based on the new requirements of the legislation.

PALABRAS CLAVE: protección de datos, brechas de seguridad, seguridad de los datos, RGPD, riesgos, derechos y libertades de los interesados.

KEYWORDS: data protection, data breaches, data security, GDPR, risks, rights and freedoms of data subjects.

SUMARIO: 1. EL DERECHO A INTIMIDAD Y EL DERECHO A LA PROTECCIÓN DE DATOS: BREVE INTRODUCCIÓN. 2. LA PROTECCIÓN DE DATOS PERSONALES ESTABLECIDA EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS. 2.1. Tipos de brechas de seguridad. 2.2. La obligación legal de notificar las brechas de seguridad. 3. LA GESTIÓN Y NOTIFICACIÓN DE BRECHAS DE SEGURIDAD. 3.1. Gestión de incidentes de seguridad: Valoración de la brecha de seguridad. 3.2. Criterios para la notificación de brechas de seguridad e información que debe facilitarse. 3.3. Métricas e indicadores. 4. CONCLUSIONES. 5. BIBLIOGRAFÍA.

1. EL DERECHO A INTIMIDAD Y EL DERECHO A LA PROTECCIÓN DE DATOS: BREVE INTRODUCCIÓN

E El desarrollo de la sociedad de la información ha propiciado que la mayoría de los tratamientos de datos personales se realicen en el llamado ciberespacio. Pero ¿qué se entiende por ciberespacio? WILLIAN GIBSON describe por primera vez el ciberespacio como *"una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano. Una complejidad inimaginable"*. Han transcurrido ya casi 36 años desde esta forma de percibir el ciberespacio y que lejos de equivocarse, no puede ser más acertada teniendo en cuenta la realidad que vivimos. Hoy Internet está presente en la gran mayoría de hogares de los países desarrollados y no hace más que crecer, provocando, entre otros factores, la existencia de un deseo de comunicación recíproco y la generación de inteligencia colectiva, respondiendo a la perfección, a este deseo humano.

Con la llegada de las nuevas tecnologías, además de importantes ventajas para la ciudadanía, estas han supuesto también, un incremento de los riesgos para el derecho al respeto de la vida privada, lo que ha desencadenado en la necesidad de contar con normas que regulen específicamente el tratamiento de información personal de los ciudadanos. El derecho a la intimidad o respeto de la vida privada y el derecho a la protección de los datos personales, aunque están estrechamente relacionados, son derechos distintos. El primero establece que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. Apareció en la legislación internacional sobre derechos humanos en la Declaración Universal de Derechos Humanos (DUDH) en 1948, y más tarde, como uno de los derechos humanos fundamentales en el Convenio Europeo de Derechos Humanos (CEDH). La protección de datos surge en Europa en 1970 y poco a poco fue tomando un valor distinto desligándose del derecho al respeto de la vida privada[1].

En el ordenamiento jurídico de la Unión Europea (UE), la protección de datos está reconocida como un derecho fundamental distinto del derecho fundamental al respeto de la vida privada[2]. Con ánimo de simplificar tal distinción, podríamos decir que ambos derechos se diferencian en su formulación y alcance, siendo el

[1] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA Y CONSEJO DE EUROPA, *Manual de legislación europea en materia de protección de datos,* Editorial Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2019, pp. 21-22.

[2] La UE proclamó en el año 2000 la Carta de Derechos Fundamentales de la Unión Europea (la Carta) donde no solo garantiza el respeto de la vida privada y familiar (artículo 7), sino también establecía el derecho a la protección de los datos personales (artículo 8) elevando así el nivel de dicha protección al de un derecho fundamental en el Derecho de la UE. Si bien, fue con la adopción del Tratado de Lisboa cuando confiere a la carta el estatuto de documento jurídico vinculante -al nivel del Derecho primario-, y por consiguiente se establece el derecho a la protección de los datos personales.

derecho al respeto de la vida privada un derecho "clásico" de prohibición genérica de la injerencia -sujeta a ciertas excepciones en base a criterio de interés general- y la protección de los datos personales se considera un derecho "moderno" y activo[3], que establece un sistema de control mediante mecanismos que protegen a los ciudadanos cuando sus datos personales sean objeto manipulación indebida. El derecho a la protección de los datos personales es más amplio que el derecho al respeto de la vida privada, ya que entra en juego siempre que se traten datos personales.

Desde 1995 hasta mayo de 2018, el principal instrumento jurídico de la UE en materia de protección de datos fue la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva sobre protección de datos). Una directiva que establecía un amplio y detallado sistema de protección de datos en la UE y que obligaba a ser transpuesta a las legislaciones nacionales de los Estados miembros lo que inevitablemente generaba cierta discrecionalidad. Con el fin de armonizar la protección de los datos personales de los ciudadanos de la UE, se adopta en abril de 2016, el Reglamento General de Protección de datos (RGPD o Reglamento)[4] después de años de intensos debates, entrando en vigor el 25 de mayo de 2018. Un Reglamento que aún siendo de aplicación directa, ha obligado a los Estados miembros ha actualizar su legislación nacional en materia de protección de datos para ajustar debidamente su legislación al RGPD, así en España, se derogó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y se aprobó la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) al objeto de adaptar el ordenamiento jurídico español al RGPD.

2. LA PROTECCIÓN DE DATOS PERSONALES ESTABLECIDA EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Tal y como deja claro el propio título del Reglamento, el ámbito de protección de este cuerpo legal es siempre la persona física. El diseño de la protección de los datos personales que instaura el RGPD gira en torno a la noción de "riesgo" para los derechos y libertades de los interesados[5] y se basa principalmente en una serie de medidas de garantía tales como: i) principios generales (arts. 5 a 10); ii) Derechos de los interesados (Capítulo III, arts. 12 a 23); iii) Obligaciones a cargo del responsable del tratamiento y del encargado del

[3] HUSTINX, P., *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, EDPS Speeches & Articles, 2013. Disponible en: https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf

[4] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

[5] Al objeto de entender mejor algunos de los aspectos analizados en este estudio, pasaremos a enumerar los distintos agentes intervinientes en las operaciones de tratamiento de datos personales. Así, el responsable del tratamiento es la persona física o jurídica o autoridad que solo o junto con otros, determina los fines y medios en base a los que se realizará el tratamiento de datos; el encargado del tratamiento normalmente es el prestador de servicios que actúa por cuenta del responsable del tratamiento; y el interesado, el titular de los datos personales objeto de tratamiento.

tratamiento contenidas tanto en los principios generales como en el otorgamiento de los derechos de los interesados, así como aquellas otras contenidas en los artículos 24 a 36 RGPD; y por último, el establecimiento de autoridades de control y supervisión para la correcta aplicación de las disposiciones del RGPD[6].

El Reglamento instaura un sistema más reforzado de protección de los datos de los interesados. Una muestra de ello, es la inclusión del principio de responsabilidad activa o *accountability,* el cual establece la obligación de garantizar y poder demostrar que el tratamiento es conforme con las exigencias de la normativa.

Entre el conjunto de exigencias que se imponen a los responsables y encargados del tratamiento nos detendremos en aquellas relativas a la seguridad del tratamiento que obligan a aplicar medidas técnicas y organizativas oportunas para evitar cualquier injerencia no autorizada en las operaciones de tratamiento de datos y garantizar la confidencialidad, integridad y disponibilidad de la información personal de los titulares de los datos. Estableciéndose un nivel de seguridad determinado por[7]:

a) Las características de seguridad disponibles en el mercado (estado de la técnica) para un determinado tipo de tratamiento;
b) Los costes;
c) Los riesgos del tratamiento de los datos para los derechos y las libertades de los interesados;

Se impone una obligación genérica de transparencia y responsabilidad proactiva en el tratamiento de datos personales, y en particular, además de la obligación de adoptar las medidas oportunas para garantizar la seguridad del tratamiento, en caso de que se produzcan brechas de seguridad de los datos, la empresa deberá notificar la brecha sin dilación indebida, y como máximo en 72 horas desde que se tiene conocimiento de la misma a la autoridad competente, y a los interesados, en caso de que sea probable que entrañe alto riesgo para los derechos y libertades de los afectados.

2.1. Tipos de brechas de seguridad

Aunque todas las brechas de seguridad son incidentes de seguridad de la información, no todo incidente de seguridad es necesariamente una brecha de datos personales. Una brecha de seguridad puede tener efectos adversos considerables en los titulares de los datos, y que podrían ocasionar daños y perjuicios, tangibles e intangibles. Entre los efectos, se podría incluir la pérdida de control sobre su información personal, la restricción de derechos, usurpación de identidad o fraude, problemas de discriminación, pérdidas financieras o daños materiales, daño para la imagen o reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo. El Grupo de Trabajo del Artículo 29 (ahora denominado, Comité Europeo de Protección de Datos) en su Dictamen 03/2014 sobre notificación de violaciones de datos personales clasificó las brechas de seguridad en base a tres conocidos principios de la seguridad de la información:

[6] REYES, KAHANSKY, C. M. "El deber de notificar y el derecho a la no autoinculpación en la protección de datos personales", *Revista de Derecho UNED,* núm. 4, 2019, p. 288.
[7] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA Y CONSEJO DE EUROPA, *Manual de legislación europea en materia de protección de datos,* Editorial Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2019, p. 186.

a) «Violación de la confidencialidad»: cuando se produce un acceso no autorizado o accidental de los datos personales, o la revelación de los mismos.
b) «Violación de la integridad»: cuando se produce una alteración no autorizada o accidental de los datos personales.
c) «Violación de la disponibilidad»: cuando se produce una pérdida de acceso accidental o no autorizada a los datos personales, o la destrucción de los mismos.

A pesar de la distinción, una brecha de seguridad puede afectar a la tres dimensiones, confidencialidad, integridad y disponibilidad al mismo tiempo, así como la combinación de estas. Si bien, mientras que una violación de la confidencialidad o integridad puede resultar relativamente obvia, no es tan sencillo determinar una violación de la disponibilidad, que será preciso notificar solo cuando se haya producido una pérdida o destrucción permanente de los datos personales, por ejemplo, cuando los datos se hayan borrado accidentalmente o por una persona no autorizada o cuando los datos se encuentren cifrados de forma segura y se haya perdido la clave de descifrado. También estaremos ante una violación de la disponibilidad cuando se haya producido un interrupción del normal funcionamiento del servicio, esto es, cuando se detecte un fallo temporal en el suministro o un ataque de denegación de servicio que haga temporalmente inaccesibles los datos personales Por tanto, un incidente de seguridad de estas características que provoque la indisponibilidad de los datos personales durante un período de tiempo es también un tipo de brecha de seguridad, porque esta ausencia de acceso a los datos puede tener un impacto significativo en los derechos y las libertades de las personas físicas que habrá que valorar caso por caso, evaluando la probabilidad y gravedad del impacto de la ausencia de disponibilidad de los datos personales en los derechos y libertados de las personas físicas[8]. Además, este tipo de brecha deberá documentarse de conformidad con lo establecido en el artículo 33.5 RGPD, lo que ayuda al responsable del tratamiento a demostrar el cumplimiento de acuerdo con el principio de *accountability*.

2.2. La obligación legal de notificar las brechas de seguridad

Se entiende por brecha de seguridad de los datos personales a todo incidente de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales tratados o la comunicación o acceso no autorizados a dichos datos[9]. Aunque algunas empresas o entidades ya disponen de medidas de seguridad como el cifrado, medidas que ofrecen más posibilidades de garantizar la seguridad del tratamiento, las violaciones o brechas de seguridad siguen siendo un problema habitual en la actualidad.

Hasta la aplicación del RGPD, la obligación de notificar este tipo de brechas de seguridad a la Autoridad de Control (en el caso de España, la Agencia Española de Protección de datos, AEPD) se reducía únicamente a operadores de servicios de comunicaciones electrónicas[10] y prestadores de servicios de confianza[11]. Ahora, es

[8] Grupo de Trabajo del Artículo 29, Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679, adaptadas el 3 de octubre de 2017, pp. 8-9.
[9] Reglamento general de protección de datos, artículo 4, apartado 12; véase además Grupo de Trabajo del Artículo 29 (2017), Directrices sobre la notificación de violaciones de datos personales conforme al Reglamento 2016/679, WP250, 3 de octubre de 2017, p. 8.
[10] Véanse los artículos 41 y 44 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

una obligación, una parte de un todo en la gestión de la seguridad de la información, aplicable a cualquier responsable del tratamiento de datos personales.

De acuerdo con lo establecido en el RGPD, tan pronto como la empresa tenga conocimiento de que se ha producido una brecha de seguridad de los datos personales, deberá efectuar la correspondiente comunicación a la AEPD y, en su caso a los afectados, sin dilación y como máximo en las 72 horas siguientes. En caso de que no sea posible facilitar toda la información dentro del plazo indicado, se facilitará de manera gradual y a la mayor brevedad posible.

Aunque el responsable del tratamiento conserva la responsabilidad general de la protección de los datos personales, el prestador de servicios o encargado del tratamiento desempeña un papel importante para que el responsable del tratamiento pueda cumplir sus obligaciones, entre las que se incluye la notificación de las brechas de seguridad[12].

Hay que tener en cuenta que la notificación podría no realizarse cuando, una vez evaluada la brecha, se determine que es improbable que la misma constituya un riesgo para los derechos y libertades de las personas físicas, mientras que, por ejemplo, en la Ley de servicios de la sociedad de la información (LSSI)[13] hay que notificar todas con independencia de su gravedad. Si bien, cuando sea probable que la brecha de seguridad de los datos personales entrañe un alto riesgo para los derechos y las libertades de las personas físicas afectadas, el responsable del tratamiento deberá notificar, además de a la autoridad de control, a los afectados (titulares de los datos)[14].

En *strictu sensu*, cada brecha de seguridad individual es un incidente que debe ser notificado. No obstante, para evitar una carga excesiva, el responsable del tratamiento podría presentar una "notificación agrupada" donde se incluyesen todas las brechas de seguridad identificadas, siempre que:

a) afecten al mismo tipo de datos personales
b) cuando la brecha de la seguridad se haya producido de la misma manera, en un período de tiempo relativamente corto.

En el caso de que las brechas de seguridad afecten a diferentes tipos de datos personales y que se hayan producido de forma diferenciada, la notificación deberá realizarse de la forma habitual, notificándose cada brecha de conformidad con el artículo 33[15].

Una brecha de seguridad puede tener una serie de efectos negativos importantes sobre las personas, susceptibles de ocasionarles daños y perjuicios.

---

[11] Véase el artículo 19.2 del Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

[12] El artículo 28, apartado 3, letra f), dispone que el contrato u otro acto jurídico estipulará que el encargado del tratamiento *"ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, naturaleza del tratamiento y la información a disposición del encargado"*.

[13] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

[14] Véase el artículo 34 del Reglamento general de protección de datos.

[15] Grupo de Trabajo del Artículo 29, Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679, adaptadas el 3 de octubre de 2017, p. 18.

Por ello, el RGPD exige al responsable del tratamiento que sea notificada a la autoridad de control competente sin dilación indebida, y en aquellos casos, en los que sea probable que exista un alto riesgo de que se produzcan estos efectos adversos para los interesados, el RGPD exige al responsable del tratamiento que comunique la violación de la seguridad a las personas afectadas tan pronto como sea razonablemente posible[16].

En caso de que debiendo hacerlo, el responsable del tratamiento no notificara a la AEPD y, en su caso, a los interesados, la empresa se podría enfrentar a una multa administrativa[17], junto con una medida correctiva en su caso, que puede ser 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 con arreglo al artículo 83, apartado 4, letra a), del RGPD.

El hecho de no notificar una brecha puede revelar la ausencia de medidas de seguridad (artículo 32 RGPD), y por ese motivo, las autoridades de control también tendrán la posibilidad de imponer sanciones por no notificar o comunicar la brecha de seguridad, por una parte, y por la ausencia de medidas de seguridad (adecuadas), por otra, ya que se trata de dos infracciones diferenciadas[18].

En cifras, según las estadísticas ofrecidas por la AEPD en su Memoria de 2019[19], en España se notificaron 1.459 brechas de seguridad, de las cuales 498 incluyen notificaciones a los interesados, con un total de 14 resoluciones de requerimiento de notificación a los interesados emitidas por la AEPD. En particular, las notificaciones de brechas de seguridad trasladadas a inspección han crecido de las 16 de 2018 a las 79 de 2019, lo que supone un incremento de casi un 400%.

3. LA GESTIÓN Y NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

Desgraciadamente, sufrir un incidente de seguridad no es una opción, sino una cuestión de probabilidades. Ésta es una realidad difícil de asumir, no sólo desde el punto de vista técnico, sino también por las consecuencias económicas que puede ocasionar en la empresa los impactos directos e indirectos derivados de este hecho. Por ello, es necesario tomar conciencia e implementar medidas de prevención -que llevan implícitos costes económicos- aunque a priori no se traduzcan en un retorno de la inversión claro. Con independencia de la obligación legal de notificar, este estudio tiene como objetivo proporcionar directrices generales en la gestión de brechas de seguridad y, en especial, aquellos casos en los que la brecha tenga o pueda tener incidencia en el ámbito del RGPD, es decir, en aquellos casos en los que la brecha de seguridad pueda afectar a los derechos y libertades de las personas.

Bien es cierto que la gestión de las brechas de seguridad no constituye una novedad para las empresas ya que es una obligación contenida en otras

[16] Véase también el considerando 86 RGPD.

[17] Para más detalle sobre la aplicación y fijación de multas administrativas, consulte las Directrices del Grupo de Trabajo del Artículo 29, disponible aquí: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

[18] Grupo de Trabajo del Artículo 29, Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679, adaptadas el 3 de octubre de 2017, p. 11.

[19] Agencia Española de Protección de Datos (AEPD), *Memoria AEPD 2019.* Disponible en: https://www.aepd.es/sites/default/files/2020-05/memoria-AEPD-2019.pdf

normativas[20] y, además, ya en el Reglamento de desarrollo de la antigua LOPD[21] se hacía referencia a la obligación de incluir en el documento de seguridad un procedimiento relativo a la notificación, gestión y respuesta ante incidencias. A pesar de no ser una obligación preceptiva en la nueva normativa la llevanza de este registro de incidencias, si resulta útil y necesaria para garantizar la proactividad de los responsable en sus registro de actividades de tratamiento.

3.1. Gestión de incidentes de seguridad: Valoración de la brecha de seguridad.

Cuando detectamos e identificamos un incidente de seguridad es necesario entrar en una primera fase de análisis donde se pueda recabar la información y clasificar el incidente con mayor conocimiento y precisión[22]. Es de vital importancia que la organización esté concienciada y haya recibido formación en la materia a la hora de detectar e identificar una brecha de seguridad, sobre todo los empleados con acceso a datos, son clave fundamental para garantizar la seguridad de los tratamientos y en concreto, la gestión eficaz de las brechas de seguridad[23].

Identificado el incidente, -aún no hemos confirmado si es o no una brecha de seguridad notificable- es preciso tener definido el plan de actuación para solucionar el incidente ya que de la clasificación del mismo dependerán las acciones a emprender durante los procesos de respuesta y notificación.

Es habitual que exista cierto solapamiento entre las distintas fases de la gestión de la brecha de seguridad, así podemos listar las siguientes:

1) **Preparación**: Se trata de la primera fase del proceso, donde se determinarán las medidas de contención tempranas y se definirán las figuras implicadas en la gestión de la brecha.
2) **Detección e identificación**: A través de mecanismos de detección apropiados se determinará si estamos o no ante un incidente de seguridad, momento en el que se deberá realizar una clasificación preliminar del mismo. Para identificar incidentes de seguridad es de gran ayuda contar con servicios de notificación o aviso como los que proporciona INCIBE y CCN-CERT o de los propios fabricantes de sistemas de información[24].

---

[20] Para las Administraciones públicas, 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 (ENS), otorga el papel de coordinación en materia de respuesta a incidentes de seguridad al Centro Criptológico Nacional (CCN) (Art. 36) con el objetivo de articular mecanismos de respuesta a los incidentes de seguridad mediante la estructura CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team) obligando a la notificación de incidentes de seguridad a las Administraciones Públicas y, a su vez, la necesidad de gestionar las brechas de seguridad. Al objeto de facilitar esta labor el CCN dispone de la guía para la *"Gestión y Notificación de Ciberincidentes"* (CCN-STIC 817) y, además, proporciona de forma gratuita la herramienta *LUCIA* como canal para llevar a cabo las notificaciones de brechas de seguridad.

[21] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[22] Agencia Española de Protección de Datos (AEPD), *Guía para la gestión y notificación de brechas de seguridad,* 2018, p.24.

[23] MARTÍN SAN CRISTÓBAL, A., "Detección de incidentes y violaciones de seguridad", Thomson Reuters, 2020, p. 4.

[24] MARTÍN SAN CRISTÓBAL, A., "Detección de incidentes y violaciones de seguridad", Thomson Reuters, 2020, p. 4.

Además, en esta fase la empresa deberá anotar en su registro de incidencias aquellos incidentes de seguridad detectados e identificados como incidencias de seguridad que afectan a datos personales.

3) **Análisis y clasificación**: Es el momento donde se deberá recabar la máxima información y clasificar el incidente con mayor precisión, con el objetivo de confirmar la brecha, es decir, determinar si efectivamente estamos ante una brecha de seguridad, y valorar una posible notificación temprana a la AEPD y/o a los afectados.

Según la AEPD en su Guía para la gestión y notificación de brechas de seguridad, la brecha se podrá clasificar por:

i. Tipo de amenaza (0-day, ataque dirigido, denegación de servicio, acceso no autorizado, etc);
ii. Contexto u origen de la amenaza;
iii. Categoría de seguridad de los sistemas y datos afectados;
iv. Vector de ataque o método

Para valorar si el incidente de seguridad es o no una brecha de seguridad, así como su alcance, la empresa debe determinar la peligrosidad teniendo en cuenta la categoría o nivel de criticidad o peligrosidad; la naturaleza, sensibilidad y categorías de datos afectados; si los datos son o no legibles; el volumen de datos afectados; la facilidad de identificación de los afectados (inferencia); la severidad de las consecuencias del incidente para los afectados por la brecha, características especiales y número de afectados; entre otras.

4) **Proceso de respuesta y, en su caso, notificación**: Una vez, contenido el incidente, la erradicación puede ser necesaria para solventar determinados efectos del mismo, y así mitigar todas o parte de las vulnerabilidades que hubiesen sido explotadas. No se trata solo de aplicar medidas activas en el momento, sino de implementar controles periódicos y eficaces tendentes a minorar el riesgo en aquellos procesos de alto impacto, en este sentido resulta muy útil seguir alguno de los estándares internacionales de seguridad[25].

Asimismo, es importante recabar toda la documentación del proceso de cara a comunicaciones con las partes interesadas tanto de carácter interno como externo, y a la elaboración de un informe de cierre que permita extraer conclusiones y acciones de mejora en base a lecciones aprendidas[26].

En cuanto al proceso de notificación, sería conveniente formalizar un procedimiento al efecto, donde se evalúe la gravedad de la brecha[27] para, en su caso, notificar a la Autoridad de Control y/o a los interesados, y que contenga los

[25] Véanse, UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos; UNE-EN ISO/IEC 27002:2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información

[26] Agencia Española de Protección de Datos (AEPD), *Guía para la gestión y notificación de brechas de seguridad,* 2018, p. 28.

[27] A modo orientativo, la AEPD en su Guía para la gestión y notificación de brechas de seguridad propone en el Anexo III un posible modelo que puede ser utilizado como referencia en la toma de decisiones tanto para la notificación a la Autoridad de Control como para los propios afectados, valorando determinados umbrales bajo los cuales la empresa procederá a la notificación.

detalles sobre cómo escalar las notificaciones de brechas de seguridad a nivel interno.

5) **Seguimiento y cierre**: El plan de actuación requiere una serie de tareas de seguimiento y cierre tales como, la valoración de la contratación de un informe *forensic* que analice los hechos y recopile todas las evidencias precisas -siendo de gran utilidad en caso de disputa judicial o infracción administrativa-; valoración de las acciones legales oportunas analizando previamente los fines de imputación y la reparación del daño; y emisión de un informe de cierre sobre la trazabilidad del suceso y su análisis valorativo.

3.2. Criterios para la notificación de brechas de seguridad e información que debe facilitarse

Cuando un responsable del tratamiento notifica una brecha de seguridad a la autoridad de control, el artículo 33, apartado 3, establece que, como mínimo, debe:

a) 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;
b) 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;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) 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.

En este sentido, es preciso destacar que es muy posible que en las primeras 72 horas no se disponga de toda la información, y en la mayoría de los casos, no se conozca el volumen de datos total afectados, por ello, se recomienda una notificación gradual como forma segura de cumplir las obligaciones de notificación.

No será necesaria la comunicación a los afectados siempre que se haya adoptado las medidas técnicas y organizativas adecuadas con anterioridad a la brecha de seguridad (por ejemplo, en caso de que se pierda un dispositivo que contiene datos, pero está cifrado) o con posterioridad mitigando total o parcialmente el impacto de la brecha de seguridad, y cuando la notificación a los afectados suponga un esfuerzo desproporcionado a nivel técnico y organizativo.

3.3. Métricas e indicadores

De cara la evaluación de la implantación, eficacia y eficiencia del proceso de gestión y notificación de brechas de seguridad es preciso contar con métricas e indicadores de referencia para medir y así, mejorar el proceso en la organización. Podemos destacar las siguientes: i) alcance del sistema de gestión; ii) resolución de incidentes de nivel de impacto alto, muy alto y crítico; iii) resolución de incidentes de nivel de impacto bajo y medio; iv) recursos consumidos; v) estado de cierre de los incidentes.

4.CONCLUSIONES

El Reglamento General de Protección de Datos implanta un nuevo modelo de protección de datos que incluye, entre otras obligaciones, garantizar la seguridad de los datos que están sometidos a tratamiento y notificar las brechas de seguridad de los datos personales a las autoridades de control y a los interesados. La comunicación de brechas de seguridad se convierte en una herramienta de suma importancia en lo que respecta a la protección de los derechos fundamentales de las personas, por ello, este nuevo paradigma de protección que introduce el RGPD coacciona a responsables y encargados con la imposición de sanciones administrativas en caso de incumplimiento.

Como hemos comentado, brechas de seguridad pueden producirse con independencia de si el tratamiento es efectuado por un responsable o por un encargado, y por este motivo, el RGPD obliga a los encargados también a notificar las brechas de seguridad al responsable del tratamiento sin dilaciones indebidas. Siendo el responsable del tratamiento el encargado de notificar a las autoridades de control y a los interesados afectados, con arreglo a las normas y plazos antes mencionados.

La implicación del todo el personal de la organización es una de las cuestiones clave para garantizar la seguridad del tratamiento y, también, para gestionar de forma eficaz y eficiente las brechas de seguridad.

5. BIBLIOGRAFÍA

- HUSTINX, P., *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, EDPS Speeches & Articles, 2013. Disponible en: https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf
- REYES KAHANSKY, C. M. "El deber de notificar y el derecho a la no autoinculpación en la protección de datos personales", *Revista de Derecho UNED,* núm. 4, 2019, pp. 281-318.
- GIBSON W., *Neuromante,* Barcelona, Editorial Planeta, 1984.
- GARCÍA LÓPEZ, M. *El impacto de Internet en el libre desarrollo de la personalidad,* Wolters Kluwer, 2018.
- PLATERO ALCÓN, A. "La seguridad como elemento clave en el tratamiento de datos personales en Europa: especial referencia al régimen de responsabilidad civil derivado de las brechas de seguridad", *LEX,* núm. 23, 2019, pp. 55-73.
- MARTÍN SAN CRISTÓBAL, A., "Detección de incidentes y violaciones de seguridad", *Thomson Reuters*, 2020, pp. 2-20.

Guías y Estándares:

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), *Guía para la gestión y notificación de brechas de seguridad,* 2018.
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), *Memoria AEPD 2019.* Disponible en: https://www.aepd.es/sites/default/files/2020-05/memoria-AEPD-2019.pdf
- AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA Y CONSEJO DE EUROPA, *Manual de legislación europea en materia de protección de datos,* Editorial Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2019.
- CONSEJO NACIONAL DE CIBERSEGURIDAD DEL GOBIERNO DE ESPAÑA, *Guía nacional de notificación y gestión de ciberincidentes,* 2020.
- GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679*, adaptadas el 3 de octubre de 2017
- UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- UNE-EN ISO/IEC 27002:2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información

Legislación:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.