REGLAMENTO DE EJECUCIÓN (UE) 2018/151 DE LA COMISIÓN

de 30 de enero de 2018

por el que se establecen normas para la aplicación de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo en lo que respecta a la especificación de los elementos que han de tener en cuenta los proveedores de servicios digitales para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información, así como de los parámetros para determinar si un incidente tiene un impacto significativo

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Vista la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión ([1]), y en particular su artículo 16, apartado 8,

Considerando lo siguiente:

(1) De conformidad con la Directiva (UE) 2016/1148, los proveedores de servicios digitales pueden tomar las medidas técnicas y de organización que consideren adecuadas y proporcionadas para gestionar los riesgos existentes para la seguridad de sus redes y sistemas de información, siempre que dichas medidas garanticen un nivel adecuado de seguridad y tengan en cuenta los elementos previstos en dicha Directiva.

(2) Cuando determinen las medidas técnicas y de organización adecuadas y proporcionadas, los proveedores de servicios digitales deben plantear la seguridad de la información de forma sistemática, utilizando un enfoque basado en los riesgos.

(3) Con el fin de garantizar la seguridad de los sistemas e instalaciones, los proveedores de servicios digitales deben realizar procedimientos de evaluación y análisis. Estas actividades deben atañer a la gestión sistemática de las redes y sistemas de información, la seguridad física y del entorno, la seguridad de abastecimiento y los controles de acceso.

(4) Cuando se realice un análisis de riesgos dentro de la gestión sistemática de las redes y sistemas de información, se debe animar a los proveedores de servicios digitales a que determinen riesgos concretos y cuantifiquen su importancia, por ejemplo identificando amenazas para los activos críticos y la forma en que pueden afectar a las operaciones, y determinando la mejor manera de atenuar dichas amenazas en función de las capacidades disponibles y de las necesidades de recursos.

(5) Las políticas en materia de recursos humanos pueden referirse a la gestión de capacidades e incluir aspectos relativos al desarrollo de capacidades de seguridad y a la sensibilización. Cuando se tomen decisiones sobre un conjunto adecuado de políticas en materia de seguridad de las operaciones, debe animarse a los proveedores de servicios digitales a que tengan en cuenta aspectos de la gestión de cambios, la gestión de la vulnerabilidad, la formalización de prácticas operativas y administrativas y la cartografía del sistema.

(6) Las políticas relativas a la arquitectura de la seguridad pueden incluir, en particular, la segregación de redes y sistemas, así como medidas de seguridad específicas para operaciones críticas como las de administración. La segregación de redes y sistemas puede permitir a un proveedor de servicios digitales hacer distinciones entre elementos como los flujos de datos y los recursos informáticos que pertenecen a un cliente, a un grupo de clientes, al proveedor de servicios digitales o a terceros.

(7) Las medidas adoptadas en relación con la seguridad física y del entorno deben garantizar la seguridad de las redes y sistemas de información de una organización frente a los daños provocados por incidentes como robos, incendios, inundaciones u otros efectos de fenómenos meteorológicos, fallos de telecomunicaciones o de suministro de electricidad.

(8) La seguridad de suministros tales como la energía eléctrica, el combustible o la refrigeración puede englobar la seguridad de la cadena de suministro, que incluye en particular la seguridad de los contratistas y subcontratistas terceros y la gestión de estos. La trazabilidad de los suministros críticos se refiere a la capacidad del proveedor de servicios digitales de determinar y registrar las fuentes de tales suministros.

(9) Los usuarios de servicios digitales deben englobar a las personas físicas y jurídicas que sean clientes o subscriptores de un mercado en línea o un servicio de computación en nube o que sean visitantes del sitio web de un motor de búsqueda en línea con el fin de realizar búsquedas por palabras clave.

([1]) DO L 194 de 19.7.2016, p. 1.

(10) A la hora de definir la importancia del impacto de un incidente, los casos que figuran en el presente Reglamento deben considerarse como una lista no exhaustiva de incidentes significativos. De la aplicación del presente Reglamento y del trabajo del Grupo de cooperación deben extraerse conclusiones en lo referente a la recopilación de información de mejores prácticas sobre los riesgos e incidentes y las discusiones sobre las modalidades para informar sobre notificaciones de incidentes a que hace referencia el artículo 11, apartado 3, letras i) y m), de la Directiva (UE) 2016/1148. El resultado podría ser unas orientaciones exhaustivas sobre los umbrales cuantitativos de los parámetros de notificación que pueden dar lugar a la obligación de notificación para los proveedores de servicios digitales en virtud del artículo 16, apartado 3, de la Directiva (UE) 2016/1148. En su caso, la Comisión también podría estudiar la revisión de los umbrales fijados en el presente Reglamento.

(11) Con el fin de que las autoridades competentes estén informadas de nuevos riesgos potenciales, debe animarse a los proveedores de servicios digitales a que notifiquen voluntariamente cualquier incidente cuyas características hubieran sido desconocidas previamente para ellos, como nuevos *exploits*, vectores de ataque, actores de amenazas, vulnerabilidades y peligros.

(12) El presente Reglamento debe aplicarse a partir del día siguiente a la fecha de expiración del plazo de transposición de la Directiva (UE) 2016/1148.

(13) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité de Seguridad de las Redes y Sistemas de Información a que se hace referencia en el artículo 22 de la Directiva (UE) 2016/1148.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Objeto

El presente Reglamento precisa los elementos que han de tener en cuenta los proveedores de servicios digitales a la hora de establecer y adoptar medidas para garantizar un nivel de seguridad de las redes y sistemas de información que utilizan en el marco de la oferta de los servicios contemplados en el anexo III de la Directiva (UE) 2016/1148, y detalla los parámetros para determinar si un incidente tiene un impacto significativo en la prestación de dichos servicios.

Artículo 2

Elementos de seguridad

1. La seguridad de los sistemas e instalaciones a que hace referencia el artículo 16, apartado 1, letra a), de la Directiva (UE) 2016/1148 se refiere a la seguridad de las redes y sistemas de información y de su entorno físico, e incluirá los siguientes elementos:

a) la gestión sistemática de redes y sistemas de información, es decir, una cartografía de los sistemas de información y la creación de un conjunto de políticas adecuadas en materia de gestión de la seguridad de la información, incluidos el análisis de riesgos, los recursos humanos, la seguridad de las operaciones, la arquitectura de la seguridad, la gestión segura del ciclo de vida de datos y sistemas, y, si procede, el cifrado y su gestión;

b) la seguridad física y del entorno, es decir, la disponibilidad de un conjunto de medidas para proteger la seguridad de las redes y sistemas de información de los proveedores de servicios digitales frente a los daños, utilizando un enfoque basado en los riesgos que abarque todos los peligros y tenga en cuenta, por ejemplo, los fallos del sistema, los errores humanos, las acciones malintencionadas o los fenómenos naturales;

c) la seguridad de abastecimiento, es decir, el establecimiento y mantenimiento de políticas adecuadas con el fin de garantizar la accesibilidad y, en su caso, la trazabilidad de los suministros críticos utilizados en la prestación de los servicios;

d) el control del acceso a las redes y sistemas de información, es decir, la disponibilidad de un conjunto de medidas para garantizar que el acceso físico y lógico a las redes y sistemas de información, incluida la seguridad administrativa de las redes y sistemas de información, se autorice y restrinja sobre la base de requisitos de actividad de negocio y de seguridad.

2. En relación con la gestión de incidentes a que hace referencia el artículo 16, apartado 1, letra b), de la Directiva (UE) 2016/1148, las medidas adoptadas por los proveedores de servicios digitales incluirán:

a) procesos y procedimientos de detección mantenidos y ensayados para garantizar el conocimiento oportuno y adecuado de sucesos anómalos;

b) procesos y políticas sobre la notificación de incidentes y la detección de deficiencias y vulnerabilidades en sus sistemas de información;

c) una respuesta acorde con procedimientos establecidos y la comunicación de los resultados de la medida adoptada;

d) la evaluación de la gravedad del incidente, documentando las enseñanzas extraídas del análisis del incidente, y la recopilación de información pertinente que pueda servir como prueba y apoyo a un proceso de mejora continua.

3. La gestión de la continuidad de las actividades a que hace referencia el artículo 16, apartado 1, letra c), de la Directiva (UE) 2016/1148 se refiere a la capacidad de una organización de mantener o, en su caso, restablecer, después de un incidente perturbador, la prestación de los servicios a niveles aceptables preestablecidos, e incluirá:

a) el establecimiento y la utilización de planes de contingencia basados en un análisis de impacto en la actividad para garantizar la continuidad de los servicios prestados por proveedores de servicios digitales, que serán evaluados y ensayados con carácter periódico, por ejemplo mediante ejercicios;

b) capacidades de recuperación en caso de catástrofe, que serán evaluadas y ensayadas con carácter periódico, por ejemplo mediante ejercicios.

4. La supervisión, auditorías y pruebas a que hace referencia el artículo 16, apartado 1, letra d), de la Directiva (UE) 2016/1148 incluirán el establecimiento y el mantenimiento de políticas sobre:

a) la realización de una secuencia programada de observaciones o mediciones para evaluar si las redes y sistemas de información están funcionando según lo previsto;

b) la inspección y verificación para comprobar si se está siguiendo una norma o una serie de directrices, si los registros son exactos, y si los objetivos de eficiencia y eficacia se están cumpliendo;

c) un proceso destinado a revelar fallos en los mecanismos de seguridad de una red y sistema de información que proteja los datos y mantenga la funcionalidad según lo previsto; dicho proceso incluirá procesos técnicos y personal encargado del flujo de operaciones.

5. Las normas internacionales a que hace referencia el artículo 16, apartado 1, letra e), de la Directiva (UE) 2016/1148 designan las normas adoptadas por un organismo internacional de normalización contemplado en el artículo 2, apartado 1, letra a), del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo ([1]). De conformidad con el artículo 19 de la Directiva (UE) 2016/1148, también podrán utilizarse normas y especificaciones aceptadas a nivel europeo o internacional que sean pertinentes en materia de seguridad de las redes y sistemas de información, incluidas normas nacionales existentes.

6. Los proveedores de servicios digitales garantizarán la disponibilidad de documentación adecuada para permitir que la autoridad competente verifique la conformidad con los elementos de seguridad a que se refieren los apartados 1, 2, 3, 4 y 5.

Artículo 3

Parámetros que han de ser tenidos en cuenta para determinar si el impacto de un incidente es significativo

1. En relación con el número de usuarios afectados por un incidente, en particular los usuarios que dependen del servicio para la prestación de sus propios servicios, a que hace referencia el artículo 16, apartado 4, letra a), de la Directiva (UE) 2016/1148, el proveedor de servicios digitales deberá estar en condiciones de estimar cualquiera de estos elementos:

a) el número de personas físicas y jurídicas afectadas con las que se haya celebrado un contrato de prestación de servicios, o

b) el número de usuarios afectados que hayan utilizado el servicio basándose en particular en el tráfico de datos previo.

2. La duración de un incidente a que hace referencia el artículo 16, apartado 4, letra b), de la Directiva (UE) 2016/1148 designa el plazo transcurrido desde la perturbación de la correcta prestación del servicio en cuanto a su disponibilidad, autenticidad, integridad o confidencialidad hasta el momento de su restablecimiento.

3. En relación con la extensión geográfica con respecto a la zona afectada por el incidente a que hace referencia el artículo 16, apartado 4, letra c), de la Directiva (UE) 2016/1148, el proveedor de servicios digitales deberá estar en condiciones de determinar si el incidente afecta a la prestación de sus servicios en Estados miembros concretos.

4. El grado de perturbación del funcionamiento del servicio a que hace referencia el artículo 16, apartado 4, letra d), de la Directiva (UE) 2016/1148 se medirá en relación con una o varias de las siguientes características afectadas por un incidente: la disponibilidad, autenticidad, integridad o confidencialidad de los datos o de los servicios correspondientes.

([1]) Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, p. 12).

5. En relación con el alcance del impacto sobre las actividades económicas y sociales a que se hace referencia en el artículo 16, apartado 4, letra e), de la Directiva (UE) 2016/1148, el proveedor de servicios digitales deberá poder concluir, basándose en indicaciones tales como el carácter de sus relaciones contractuales con el cliente o, en su caso, el número de usuarios potencialmente afectados, si el incidente ha causado pérdidas significativas materiales o inmateriales a los usuarios, por ejemplo relativas a la salud, a la seguridad o daños a la propiedad.

6. A los efectos de los apartados 1, 2, 3, 4 y 5, no se exigirá a los proveedores de servicios digitales que recopilen información adicional a la que no tengan acceso.

Artículo 4

Impacto significativo de un incidente

1. Se considerará que un incidente tiene un impacto significativo cuando se haya producido al menos una de las siguientes situaciones:

a) El servicio prestado por el proveedor de servicios digitales ha estado indisponible durante más de 5 000 000 horas de usuario, donde la expresión «horas de usuario» se refiere al número de usuarios afectados en la Unión por una duración de sesenta minutos.

b) El incidente ha dado lugar a una pérdida de autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o de los servicios correspondientes ofrecidos, o accesibles mediante una red y sistema de información del proveedor de servicios digitales, que ha afectado a más de 100 000 usuarios en la Unión.

c) El incidente ha creado un riesgo para la seguridad pública o de pérdida de vidas humanas.

d) El incidente ha causado daños materiales como mínimo a un usuario en la Unión, y el daño causado a dicho usuario es superior a 1 000 000 EUR.

2. Partiendo de las mejores prácticas recopiladas por el Grupo de cooperación en el ejercicio de sus funciones de conformidad con el artículo 11, apartado 3, de la Directiva (UE) 2016/1148 y de los debates en virtud del artículo 11, apartado 3, letra m), de la misma Directiva, la Comisión podrá revisar los umbrales establecidos en el apartado 1.

Artículo 5

Entrada en vigor

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

2. Será aplicable a partir del 10 de mayo de 2018.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 30 de enero de 2018.

Por la Comisión

El Presidente

Jean-Claude JUNCKER