EBA/GL/2025/02

11/02/2025

Directrices

por la que se modifican las Directrices EBA/2019/04 sobre gestión de riesgos de TIC y de seguridad

1. Obligaciones de cumplimiento y de notificación

Rango jurídico de las presentes directrices

1. El presente documento contiene directrices emitidas en virtud del artículo 16 del Reglamento (UE) n.º 1093/2010[1]. De conformidad con el artículo 16, apartado 3, del Reglamento (UE) n.º 1093/2010, las autoridades competentes y las entidades financieras harán todo lo posible para atenerse a ellas.

2. En las directrices se expone el punto de vista de la ABE sobre las prácticas de supervisión más adecuadas en el marco del Sistema Europeo de Supervisión Financiera o sobre cómo debería aplicarse el Derecho de la Unión en un determinado ámbito. Las autoridades competentes definidas en el artículo 4, apartado 2, del Reglamento (UE) n.º 1093/2010 a las que sean de aplicación las directrices deberían cumplirlas incorporándolas a sus prácticas de la forma más apropiada (modificando, p. ej., su marco jurídico o sus procedimientos de supervisión), incluso en aquellos casos en los que las directrices vayan dirigidas principalmente a las entidades.

Requisitos de notificación

3. De conformidad con el artículo 16, apartado 3, del Reglamento (UE) n.º 1093/2010, las autoridades competentes deberán notificar a la ABE, a más tardar el 20.05.2025, si cumplen o se proponen cumplir estas directrices indicando, en caso negativo, los motivos para no cumplirlas. A falta de notificación en dicho plazo, la ABE considerará que las autoridades competentes no las cumplen. Las notificaciones se presentarán remitiendo el modelo que se encuentra disponible en el sitio web de la ABE con la referencia «EBA/GL/2025/02». Las notificaciones serán presentadas por personas debidamente facultadas para comunicar el cumplimiento en nombre de las respectivas autoridades competentes. Cualquier cambio en la situación de cumplimiento de las directrices deberá notificarse igualmente a la ABE.

4. Las notificaciones se publicarán en el sitio web de la ABE, tal como contempla el artículo 16, apartado 3.

[1] Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010, por el que se crea una Autoridad Europea de Supervisión (Autoridad Bancaria Europea), se modifica la Decisión n.º 716/2009/CE y se deroga la Decisión 2009/78/CE de la Comisión (DO L 331 de 15.12.2010, p. 12).

2. Destinatarios

5. Las presentes directrices se dirigen a las entidades y autoridades competentes a que se refiere el artículo 4, apartado 2, inciso vii), del Reglamento (UE) n.º 1093/2010 y a los proveedores de servicios de pago, tal como se definen en el artículo 1, apartado 1, de la Directiva (UE) 2015/2366[2].

3. Aplicación

Fecha de aplicación

6. Estas directrices se aplicarán a más tardar el 20.05.2025.

4. Modificaciones

7. Las directrices EBA/GL/2019/04 se modifican en los siguientes términos:

8. El objeto, tal como se establece en los apartados 5 y 6, se sustituye por el siguiente:

   «Las presentes directrices se basan en el mandato de elaborar directrices en virtud del artículo 95, apartado 3, de la Directiva (UE) 2015/2366 y abarcan aspectos de la gestión de las relaciones con los usuarios de servicios de pagos».

   Las presentes directrices complementan las medidas de gestión de riesgos en virtud del Reglamento sobre la resiliencia operativa digital (DORA) y las normas técnicas de regulación conexas que los proveedores de servicios de pago a que se refiere el apartado 5 deben adoptar, de conformidad con el artículo 95, apartado 1, de la DSP2, para gestionar los riesgos operativos y de seguridad relacionados con los servicios de pago que prestan.

9. Se suprime el ámbito de aplicación establecido en los apartados 7 y 8.

   «Estas Directrices especifican los requisitos para la creación, la aplicación y el seguimiento de las medidas de seguridad que deben adoptar los PSP (proveedores de servicios de pago) conforme a lo dispuesto en el artículo 95, apartado 1, de la Directiva (UE)

[2] Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE (DO L 337 de 23.12.2015, pp. 35–127)

2015/2366 para gestionar los riesgos operativos y de seguridad relacionados con los servicios de pago que prestan.»

10. Los destinatarios que figuran en el apartado 9 se sustituyen por los siguientes:

«Estas Directrices se dirigen a las autoridades competentes definidas en el artículo 4, apartado 2, inciso vii), del Reglamento (UE) n.º 1093/2010 y a las entidades financieras definidas en el artículo 4, apartado 1, del Reglamento (UE) n.º 1093/2010, que son proveedores de servicios de pago definidos en el artículo 1, apartado 1, letras a), b) y d), de la Directiva (UE) 2015/2366, incluidas las personas físicas o jurídicas que se benefician de una exención en virtud del artículo 32 o 33 de la Directiva (UE) 2015/2366 y las personas jurídicas exentas en virtud del artículo 9 de la Directiva 2009/110/CE[3].»

11. Se suprimen las definiciones que figuran en el apartado 10.

12. Se suprimen los párrafos 1 a 91, que corresponden a las secciones 3.1 a 3.7.

[3] Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE (DO L 267 de 10.10.2009, pp. 7-17).