EBA/GL/2017/10

18/12/2017

Directrices

sobre la notificación de incidentes graves de conformidad con la Directiva (UE) 2015/2366 (PSD2)

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) nº 1093/2010[1]. De conformidad con el artículo 16, apartado 3, del Reglamento (UE) nº 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) nº 1093/2010 a las que sean de aplicación las directrices deberían cumplirlas incorporándolas a sus prácticas de la forma más apropiada (modificando, por ejemplo, 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) nº 1093/2010, las autoridades competentes deberán notificar a la ABE, a más tardar el 19/02/2018, 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 a compliance@eba.europa.eu, con la referencia «EBA/GL/2017/10». 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 y como contempla el artículo 16, apartado 3.

[1] Reglamento (UE) nº 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 nº 716/2009/CE y se deroga la Decisión nº 2009/78/CE de la Comisión, (DO L 331 de 15.12.2010, p. 12).

2. Objeto, ámbito de aplicación y definiciones

Objeto

5. Las presentes Directrices se derivan del mandato otorgado a la ABE en virtud del artículo 96, apartado 3, de la 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, 2013/36/CE y el Reglamento (UE) n.º 1093/2010 y se deroga la Directiva 2007/64/CE (PSD2).

6. En particular, las presentes Directrices especifican los criterios que han de ser empleados para la clasificación de los incidentes operativos o de seguridad graves por parte de los proveedores de servicios de pago, así como el formato y los procedimientos que deben seguir para comunicar tales incidentes a la autoridad competente del Estado miembro de origen, como se establece en el artículo 96, apartado 1, de la mencionada Directiva.

7. Además, estas Directrices contemplan la forma en la que estas autoridades competentes deben evaluar la importancia del incidente y los detalles de los informes de incidentes que, de conformidad con el artículo 96, apartado 2, de dicha Directiva, compartirán con otras autoridades nacionales.

8. Además, estas Directrices también se ocupan de la comunicación a la ABE y al BCE de los detalles relevantes de los incidentes notificados, con el fin de promover un enfoque común y coherente.

Ámbito de aplicación

9. Las presentes Directrices se aplican en relación con la clasificación y la notificación de los incidentes operativos o de seguridad graves, de conformidad con el artículo 96 de la Directiva (UE) 2015/2366.

10. Estas Directrices se aplican a todos los incidentes incluidos en la definición de «incidente operativo o de seguridad grave», que abarca eventos tanto internos como externos que podrían ser maliciosos o accidentales.

11. Las presentes Directrices se aplican también cuando el incidente operativo o de seguridad grave se origina fuera de la Unión (por ejemplo, cuando un incidente se origina en la empresa matriz o en una filial establecida fuera de la Unión) y afecta a los servicios de pago prestados por un proveedor de servicios de pago radicado en la Unión bien de manera directa (la empresa afectada no perteneciente a la Unión presta un servicio relacionado con el pago) o indirecta (la

capacidad del proveedor de servicios de pago para seguir realizando su actividad de pago se ve comprometida de alguna otra manera como resultado del incidente).

Destinatarios

12. El primer conjunto de directrices (sección 4) se dirige a los proveedores de servicios de pago definidos en el artículo 4, apartado 11, de la Directiva (UE) 2015/2366 y contemplados en el artículo 4, apartado 1, del Reglamento (UE) nº 1093/2010.

13. El segundo y el tercer conjunto de directrices (secciones 5 y 6) se dirigen a las autoridades competentes definidas en el artículo 4, apartado 2, letra i), del Reglamento (UE) nº 1093/2010.

Definiciones

14. A menos que se indique lo contrario, los términos utilizados y definidos en la Directiva (UE) 2015/2366 tienen idéntico significado en las Directrices. Además, a los efectos de las presentes Directrices, se entenderá por:

Incidente operativo o de seguridad	Un evento particular o una serie de eventos vinculados no planificados por el proveedor de servicios de pago que tengan o puedan tener un impacto negativo en la integridad, la disponibilidad, la confidencialidad, la autenticidad y/o la continuidad de los servicios relacionados con el pago.
Integridad	Propiedad de salvaguardar la exactitud y la integridad de los activos (incluidos los datos).
Disponibilidad	Propiedad de garantizar la disponibilidad y la capacidad de utilizar los servicios relacionados con el pago por parte de los usuarios de servicios de pago.
Confidencialidad	Propiedad de que la información no se ponga a disposición de terceros, entidades o procesos no autorizados, ni se divulgue a dichas personas, entidades o procesos.
Autenticidad	Propiedad de que una fuente sea lo que afirma ser.
Continuidad	Propiedad de que los procesos, las tareas y los activos de una organización necesarios para la prestación de servicios relacionados con el pago sean plenamente accesibles y se ejecuten a niveles predefinidos aceptables.
Servicios relacionados con el pago	Toda actividad empresarial en virtud del artículo 4, apartado 3, de la PSD2 y todas las tareas técnicas de apoyo necesarias para la correcta prestación de servicios de pago.

3. Aplicación

Fecha de aplicación

15. Las presentes Directrices serán de aplicación a partir del 13 de enero de 2018.

4. Directrices dirigidas a los proveedores de servicios de pago sobre la notificación de incidentes operativos o de seguridad graves a la autoridad competente de su Estado miembro de origen

Directriz 1: Clasificación como incidente grave

1.1. Los proveedores de servicios de pago deben clasificar como graves aquellos incidentes operativos o de seguridad que cumplan

a. uno o más criterios del «nivel de impacto superior», o

b. tres o más criterios del «nivel de impacto inferior»

según lo establecido en la Directriz 1.4 y como resultado de la evaluación establecida en estas Directrices.

1.2. Los proveedores de servicios de pago deben evaluar un incidente operativo o de seguridad de acuerdo con los siguientes criterios y sus indicadores correspondientes:

i. Operaciones afectadas

Los proveedores de servicios de pago deben determinar el valor total de las operaciones afectadas, así como el número de pagos comprometidos como porcentaje del nivel habitual de operaciones de pago realizadas con los servicios de pago afectados.

ii. Usuarios de servicios de pago afectados

Los proveedores de servicios de pago deben determinar el número de usuarios de servicios de pago afectados tanto en términos absolutos como en porcentaje del número total de usuarios de servicios de pago.

iii. Tiempo de inactividad del servicio

Los proveedores de servicios de pago deben determinar el período de tiempo durante el que se prevé que el servicio no estará disponible para el usuario del servicio de pago o durante el cual el proveedor de servicios de pago no podrá procesar la orden de pago, entendida en el sentido del artículo 4, apartado 13, de la PSD2.

iv. Impacto económico

Los proveedores de servicios de pago deben determinar de manera integral los costes monetarios asociados al incidente y tener en cuenta tanto la cifra absoluta como, cuando proceda, la importancia relativa de estos costes en relación con el tamaño del proveedor de servicios de pago (es decir, del capital de nivel 1 (T1) del proveedor de servicios de pago).

v. Elevación interna a alto nivel

Los proveedores de servicios de pago deben determinar si este incidente se ha elevado o probablemente se eleve a niveles ejecutivos superiores.

vi. Otros proveedores de servicios de pago o infraestructuras relevantes potencialmente afectados

Los proveedores de servicios de pago deben determinar las implicaciones sistémicas que probablemente tendrá el incidente, es decir, la posibilidad de que traspase al proveedor de servicios de pago inicialmente afectado y afecte también a otros proveedores de servicios de pago, infraestructuras de los mercados financieros y/o esquemas de pago con tarjeta.

vii. Incidencia sobre la reputación

Los proveedores de servicios de pago deben determinar en qué medida el incidente puede socavar la confianza de los usuarios en el propio proveedor de servicios de pago y, en general, en el servicio correspondiente o en el mercado en su conjunto.

1.3. Los proveedores de servicios de pago deben calcular el valor de los indicadores de acuerdo con la siguiente metodología:

i. Operaciones afectadas

Como regla general, los proveedores de servicios de pago deben entender como «operaciones afectadas» todas las operaciones nacionales y transfronterizas que se han visto o se verán probablemente afectadas de manera directa o indirecta por el incidente y, en particular, aquellas operaciones que no pudieron iniciarse o procesarse, aquellas que sufrieron modificaciones en el contenido del mensaje de pago y aquellas que se ordenaron de manera fraudulenta (con independencia de que los fondos se hayan recuperado o no).

Además, los proveedores de servicios de pago deben entender el nivel habitual de las operaciones de pago como el promedio anual diario de las operaciones de pago nacionales y transfronterizas realizadas con los mismos servicios de pago afectados por el incidente, tomando el año anterior como período de referencia para los cálculos. Si los proveedores de servicios de pago consideran que esta cifra no es representativa (por ejemplo, debido a la estacionalidad), deben utilizar otra métrica más representativa y comunicar a la autoridad competente la justificación de su elección en el campo correspondiente de la plantilla (véase el Anexo 1).

ii. Usuarios de servicios de pago afectados

Los proveedores de servicios de pago deben entender como «usuarios de servicios de pago afectados» a todos los clientes (nacionales o extranjeros, consumidores o empresas) que tienen un contrato con el proveedor de servicios de pago afectado que les permite acceder al servicio de pago afectado y que han sufrido o probablemente sufrirán las consecuencias del incidente. Los proveedores de servicios de pago deben recurrir a estimaciones basadas en su actividad anterior para determinar el número de usuarios de servicios de pago que pueden haber estado utilizando el servicio de pago durante el incidente.

En el caso de grupos, cada proveedor de servicios de pago debe considerar únicamente a sus propios usuarios de servicios de pago. Un proveedor de servicios de pago que ofrezca servicios operativos a terceros deberá considerar solamente a sus propios usuarios de servicios de pago (si los hubiera) y los proveedores de servicios de pago que reciban estos servicios operativos deben evaluar el incidente en relación con sus propios usuarios de servicios de pago.

Por otra parte, los proveedores de servicios de pago deben tomar como número total de usuarios de servicios de pago la cifra agregada de los usuarios de servicios de pago nacionales y transfronterizos vinculados contractualmente en el momento del incidente (o, de manera alternativa, la cifra más reciente disponible) y con acceso al servicio de pago afectado, con independencia de su tamaño o de si se consideran usuarios de servicios de pago activos o pasivos.

iii. Tiempo de inactividad del servicio

Los proveedores de servicios de pago deben considerar el período de tiempo durante el que cualquier tarea, proceso o canal relacionado con la prestación de servicios de pago está o probablemente estará inactivo y, por lo tanto, impide (i) la iniciación o la ejecución de un servicio de pago o (ii) el acceso a una cuenta de pago. Los proveedores de servicios de pago deben contar el tiempo de inactividad del servicio desde el momento en que comienza la inactividad y deben considerar tanto los intervalos de tiempo durante los que están operativos para prestar el servicio, como las horas de cierre y los periodos de mantenimiento, cuando proceda y sea relevante. Si los proveedores de servicios de pago no pueden determinar cuándo se inició la inactividad del servicio, deberán contar excepcionalmente el tiempo de inactividad del servicio desde el momento en el que se detecta la inactividad.

iv. Impacto económico

Los proveedores de servicios de pago deben considerar tanto los costes que puedan estar directamente relacionados con el incidente como los que están indirectamente relacionados con el mismo. Entre otras cuestiones, los proveedores de servicios de pago deben tener en cuenta los fondos o activos expropiados, los costes de sustitución de *hardware* o *software*, otros costes periciales o de reparación, los costes derivados del incumplimiento de obligaciones contractuales, las sanciones, las responsabilidades externas y la pérdida de ingresos. Por lo que respecta a los costes indirectos, los proveedores de servicios de pago deben considerar solo los que ya son conocidos o es muy probable que se materialicen.

v. *Elevación interna a alto nivel*

Los proveedores de servicios de pago deben considerar si, como consecuencia de su impacto en los servicios relacionados con el pago, el Director de Sistemas de Información (o cargo similar) ha sido o será probablemente informado sobre el incidente al margen de cualquier procedimiento de notificación periódica y de manera continua durante toda la duración del incidente. Además, los proveedores de servicios de pago deben considerar si, como resultado del impacto del incidente sobre los servicios relacionados con el pago, se ha activado o es probable que se active un modo de crisis.

vi. *Otros proveedores de servicios de pago o infraestructuras relevantes potencialmente afectados*

Los proveedores de servicios de pago deben evaluar el impacto del incidente sobre el mercado financiero, entendido como las infraestructuras de los mercados financieros y/o los esquemas de pago con tarjeta que los respaldan, así como otros proveedores de servicios de pago. En particular, los proveedores de servicios de pago deben evaluar si el incidente se ha reproducido o es probable que se reproduzca en otros proveedores de servicios de pago, si ha afectado o probablemente afectará al buen funcionamiento de las infraestructuras de los mercados financieros y si ha comprometido o probablemente comprometerá el buen funcionamiento del sistema financiero en su conjunto. Los proveedores de servicios de pago deben tener en cuenta diversos aspectos, como por ejemplo si el componente/*software* afectado es propietario o está disponible para el público en general, si la red comprometida es interna o externa y si el proveedor de servicios de pago ha dejado o es probable que deje de cumplir sus obligaciones en las infraestructuras de los mercados financieros de las que es miembro.

vii. *Incidencia sobre la reputación*

Los proveedores de servicios de pago deben considerar el nivel de visibilidad que, a su leal saber y entender, el incidente ha alcanzado o probablemente alcanzará en el mercado. En particular, deben considerar la probabilidad de que el incidente cause perjuicios a la sociedad como un buen indicador de su potencial para afectar a su reputación. Los proveedores de servicios de pago deben tener en cuenta (i) si el incidente ha afectado a un proceso visible y, por lo tanto, es probable que reciba o ya haya recibido cobertura de los medios de comunicación (considerando no solo los medios tradicionales, como periódicos, sino también blogs, redes sociales, etc.), (ii) si no se han cumplido o probablemente no se cumplirán las obligaciones normativas, (iii) si se han infringido, o probablemente se infringirán, las sanciones o (iv) si el mismo tipo de incidente ha ocurrido anteriormente.

1.4. Los proveedores de servicios de pago deben evaluar un incidente determinando, para cada criterio individual, si los umbrales correspondientes de la Tabla 1 se alcanzan o es probable que se alcancen antes de que se resuelva el incidente.

Tabla 1: Umbrales

Criterios	Nivel de impacto inferior	Nivel de impacto superior
Operaciones afectadas	> 10 % del nivel habitual de operaciones del proveedor de servicios de pago (en términos de número de operaciones) **y** > 100.000 euros	> 25 % del nivel habitual de operaciones del proveedor de servicios de pago (en términos de número de operaciones) **o** > 5 millones de euros
Usuarios de servicios de pago afectados	> 5.000 **y** > 10 % de los usuarios de servicios de pago del proveedor de servicios de pago	> 50.000 **o** > 25 % de los usuarios de servicios de pago del proveedor de servicios de pago
Tiempo de inactividad del servicio	> 2 horas	No aplicable
Impacto económico	No aplicable	> Máx. (0,1 % de capital de nivel 1, * 200 000 euros) **o** > 5 millones de euros
Elevación interna a alto nivel	Sí	Sí, y es probable que se active el *modo de crisis* (o equivalente)
Otros proveedores de servicios de pago o infraestructuras relevantes potencialmente afectados	Sí	No aplicable
Incidencia sobre la reputación	Sí	No aplicable

*Capital de nivel 1 (T1) como se define en el artículo 25 del Reglamento (UE) nº 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y las empresas de inversión, y por el que se modifica el Reglamento (UE) nº 648/2012.

1.5. Los proveedores de servicios de pago deben recurrir a estimaciones si carecen de datos reales que apoyen sus consideraciones acerca de si un umbral determinado se alcanza o es probable que se alcance antes de que se resuelva el incidente (por ejemplo, esto podría suceder durante la fase de investigación inicial).

1.6. Los proveedores de servicios de pago deben llevar a cabo esta evaluación de manera continua durante todo el periodo de duración del incidente, para identificar cualquier posible cambio de estado, ya sea a una situación peor (de no grave a grave) o a una situación mejor (de grave a no grave).

Directriz 2: Proceso de notificación

2.1. Los proveedores de servicios de pago deben recopilar toda la información pertinente, elaborar un informe del incidente utilizando la plantilla que figura en el anexo 1 y presentarlo a la autoridad competente del Estado miembro de origen. Los proveedores de servicios de pago deben cumplimentar la plantilla siguiendo las instrucciones que figuran en el anexo 1.

2.2. Los proveedores de servicios de pago deben utilizar la misma plantilla para informar a la autoridad competente durante toda la duración del incidente (es decir, para los informes

inicial, intermedios y final, como se describe en los puntos 2.7 a 2.21). Los proveedores de servicios de pago deben cumplimentar la plantilla progresivamente, en la medida de lo posible, según dispongan de más información en el curso de sus investigaciones internas.

2.3. Los proveedores de servicios de pago deben presentar también a la autoridad competente del Estado miembro de origen, si procede, una copia de la información facilitada (o que se facilitará) a sus usuarios, tal como se establece en el artículo 96, apartado 1, párrafo segundo, de la PSD2, en cuanto esté disponible.

2.4. Los proveedores de servicios de pago deben proporcionar a la autoridad competente del Estado miembro de origen, si está disponible y se considera pertinente para la autoridad competente, cualquier información adicional adjuntando documentación complementaria a la plantilla normalizada en forma de uno o varios anexos.

2.5. Los proveedores de servicios de pago deben dar seguimiento a cualquier solicitud de la autoridad competente del Estado miembro de origen de información adicional o de aclaraciones sobre la documentación ya presentada.

2.6. Los proveedores de servicios de pago deben preservar en todo momento la confidencialidad y la integridad de la información intercambiada con la autoridad competente del Estado miembro de origen y autenticarse adecuadamente ante dicha autoridad.

Informe inicial

2.7. Los proveedores de servicios de pago deben presentar un informe inicial a la autoridad competente del Estado miembro de origen cuando se detecta un incidente operativo o de seguridad grave.

2.8. Los proveedores de servicios de pago deben enviar el informe inicial a la autoridad competente en un plazo de 4 horas desde el momento en que se detectó el incidente operativo o de seguridad grave o, si se sabe que los canales de notificación de la autoridad competente no están disponibles u operativos en ese momento, tan pronto como vuelvan a estar disponibles u operativos.

2.9. Los proveedores de servicios de pago también deben presentar un informe inicial a la autoridad competente del Estado miembro de origen cuando un incidente que anteriormente no era grave se convierta en un incidente grave. En este caso concreto, los proveedores de servicios de pago deben enviar el informe inicial a la autoridad competente inmediatamente después de que se haya identificado el cambio de estado o, si se sabe que los canales de notificación de la autoridad competente no están disponibles u operativos en ese momento, tan pronto como vuelvan a estar disponibles u operativos.

2.10. Los proveedores de servicios de pago deben incluir información básica en sus informes iniciales (es decir, la sección A de la plantilla) a fin de presentar las características más relevantes del incidente y sus consecuencias previstas sobre la base de la información

disponible inmediatamente después de su detección o reclasificación. Los proveedores de servicios de pago deben recurrir a estimaciones cuando no dispongan de datos reales. También deben incluir en su informe inicial la fecha de la próxima actualización, que debe ser lo antes posible y en ningún caso superar los 3 días hábiles.

Informe intermedio

2.11. Los proveedores de servicios de pago deben presentar informes intermedios cada vez que consideren que hay una novedad relevante y, como mínimo, en la fecha de la próxima actualización indicada en el informe anterior (ya sea el informe inicial o el informe intermedio anterior).

2.12. Los proveedores de servicios de pago deben presentar a la autoridad competente un primer informe intermedio con una descripción más detallada del incidente y sus consecuencias (sección B de la plantilla). Asimismo, deben elaborar informes intermedios adicionales actualizando la información ya proporcionada en las secciones A y B de la plantilla. Dichas actualizaciones deben producirse, al menos, cuando los proveedores de servicios de pago tengan conocimiento de nueva información relevante o de cambios importantes desde la notificación anterior (por ejemplo, si el incidente ha empeorado o ha mejorado, se han identificado nuevas causas o se han adoptado acciones para solucionar el problema). En cualquier caso, los proveedores de servicios de pago deberán elaborar un informe intermedio a petición de la autoridad competente del Estado miembro de origen.

2.13. Al igual que en el caso de los informes iniciales, cuando no dispongan de datos reales, los proveedores de servicios de pago deben utilizar estimaciones.

2.14. Por otro lado, los proveedores de servicios de pago deben incluir en cada informe la fecha de la próxima actualización, que deberá ser lo antes posible y en ningún caso superar los 3 días hábiles. En caso de que el proveedor de servicios de pago no pueda cumplir la fecha estimada para la próxima actualización, deberá ponerse en contacto con la autoridad competente para explicar las razones del retraso, proponer una nueva fecha de presentación razonable (no superior a 3 días hábiles) y enviar un nuevo informe intermedio actualizando exclusivamente la información relativa a la fecha estimada de la próxima actualización.

2.15. Los proveedores de servicios de pago deben enviar el último informe intermedio cuando se recupere el nivel habitual de actividad y se vuelva a la normalidad, informando a la autoridad competente de esta circunstancia. Los proveedores de servicios de pago deben considerar que la actividad vuelve a la normalidad cuando la actividad o las operaciones se restablecen al mismo nivel de servicio o en las mismas condiciones definidos por el proveedor de servicios de pago o establecidos externamente por un Acuerdo de Nivel de Servicio (SLA) en cuanto a tiempo de procesamiento, capacidad, requisitos de seguridad, etc., y ya no estén activadas las medidas de contingencia.

2.16. En caso de que la actividad vuelva a la normalidad antes de que transcurran 4 horas desde la detección del incidente, los proveedores de servicios de pago deberían presentar tanto el

informe inicial como el último informe intermedio simultáneamente (es decir, cumplimentar las secciones A y B de la plantilla) en el mencionado plazo de 4 horas.

Informe final

2.17. Los proveedores de servicios de pago deben enviar un informe final cuando se haya efectuado el análisis de la causa de fondo (independientemente de si ya se han implementado medidas de mitigación o de si se ha identificado la causa de fondo final) y haya cifras reales disponibles para reemplazar cualquier estimación.

2.18. Los proveedores de servicios de pago deben entregar el informe final a la autoridad competente dentro de un plazo máximo de 2 semanas desde que se considere que la actividad ha vuelto a la normalidad. Los proveedores de servicios de pago que necesiten prorrogar este plazo (por ejemplo, por no disponerse aún de cifras reales sobre el impacto) deben ponerse en contacto con la autoridad competente antes de que haya finalizado el plazo y proporcionar una justificación adecuada del retraso, así como una nueva fecha estimada de presentación del informe final.

2.19. En caso de que los proveedores de servicios de pago puedan proporcionar toda la información requerida en el informe final (es decir, la sección C de la plantilla) dentro del plazo de 4 horas desde que se detectó el incidente, deben presentar en su informe inicial la información relativa a los informes inicial, último intermedio y final.

2.20. Los proveedores de servicios de pago deben tratar de incluir en sus informes finales información completa, es decir, (i) cifras reales sobre el impacto en lugar de estimaciones (así como cualquier otra actualización necesaria en las secciones A y B de la plantilla) y (ii) la sección C de la plantilla, que incluye la causa de fondo, si ya se conoce, y un resumen de las medidas adoptadas o previstas para eliminar el problema e impedir que se repita en el futuro.

2.21. Los proveedores de servicios de pago también deben enviar un informe final cuando, como resultado de la evaluación continua del incidente, identifiquen que un incidente ya notificado ha dejado de cumplir los criterios para ser considerado grave y no se espera que los cumpla antes de que se resuelva el incidente. En este caso, los proveedores de servicios de pago deben enviar el informe final tan pronto como se detecte esta circunstancia y, en cualquier caso, como muy tarde en la fecha estimada del próximo informe. En esta situación concreta, en lugar de rellenar la sección C de la plantilla, los proveedores de servicios de pago deben marcar la casilla «Incidente reclasificado como no grave» y explicar las razones que justifican esta reclasificación.

Directriz 3: Notificación delegada y consolidada

3.1. Cuando la autoridad competente lo permita, los proveedores de servicios de pago que deseen delegar en terceros las obligaciones de notificación previstas en la PSD2 deben informar a la autoridad competente del Estado miembro de origen y velar por el cumplimiento de las siguientes condiciones:

a. El contrato formal entre el proveedor de servicios de pago y el tercero o, en su caso, los acuerdos internos existentes dentro de un grupo, que contemplan la notificación delegada definen inequívocamente la asignación de responsabilidades de todas las partes. En particular, establecen de manera clara que, con independencia de la posible delegación de las obligaciones de notificación, el proveedor de servicios de pago afectado sigue siendo plenamente responsable tanto de cumplir con los requisitos establecidos en el artículo 96 de la PSD2 como del contenido de la información proporcionada a la autoridad competente del Estado miembro de origen.

b. La delegación cumple los requisitos para la externalización de funciones operativas importantes, tal como se establece en

   i. el artículo 19, apartado 6, de la PSD2 en relación con las entidades de pago y las entidades de dinero electrónico, aplicable *mutatis mutandis* de conformidad con el artículo 3 de la Directiva 2009/110/CE (DDE); o

   ii. las Directrices del CEBS sobre externalización en relación con las entidades de crédito.

c. La información se presenta por adelantado a la autoridad competente del Estado miembro de origen y, en todo caso, respetando los plazos y procedimientos establecidos por la autoridad competente, cuando proceda.

d. Se garantiza debidamente la confidencialidad de los datos sensibles y la calidad, la coherencia, la integridad y la fiabilidad de la información que debe proporcionarse a la autoridad competente.

3.2. Los proveedores de servicios de pago que deseen permitir que el tercero designado cumpla las obligaciones de notificación de forma consolidada (es decir, presentando un solo informe referido a varios proveedores de servicios de pago afectados por el mismo incidente operativo o de seguridad grave) deben informar a la autoridad competente del Estado miembro de origen, incluir la información de contacto indicada en el campo «PSP afectado» de la plantilla y asegurarse de que se cumplen las siguientes condiciones:

a. Que se incluye esta disposición en el contrato que contempla los informes delegados.

b. Que se supedita la elaboración del informe consolidado a que el incidente esté causado por una interrupción de los servicios proporcionados por el tercero.

c. Que la información consolidada se limita a los proveedores de servicios de pago establecidos en el mismo Estado miembro.

d. Que el tercero evalúa la importancia relativa del incidente para cada proveedor de servicios de pago afectado e incluye en el informe consolidado únicamente a aquellos proveedores de servicios de pago para los que el incidente esté clasificado como grave. Además, debe asegurarse de que, en caso de duda, un proveedor de servicios de pago esté incluido en el informe consolidado, siempre que no haya pruebas que indiquen que no debería incluirse.

e. Que, cuando en la plantilla figuren campos en los que no sea posible una respuesta común (por ejemplo, la sección B 2, B 4 o C 3), el tercero o bien (i) los cumplimenta individualmente para cada proveedor de servicios de pago afectado, especificando la identidad de cada proveedor de servicios de pago al que se refiere la información, o (ii) utiliza rangos, en aquellos campos en los que sea posible, que representen los valores mínimos y máximos observados o estimados para los distintos proveedores de servicios de pago.

f. Que el tercero los mantenga informados en todo momento de toda la información relevante sobre el incidente y de todas las interacciones que el tercero pueda tener con la autoridad competente, así como de su contenido, pero solamente en la medida en que esto sea posible sin quebrantar la confidencialidad de la información relativa a otros proveedores de servicios de pago.

3.3. Los proveedores de servicios de pago no deben delegar sus obligaciones de notificación antes de informar a la autoridad competente del Estado miembro de origen o tras haber sido informados de que el contrato de externalización no cumple los requisitos mencionados en la letra b) de la Directriz 3.1.

3.4. Los proveedores de servicios de pago que deseen retirar la delegación de sus obligaciones de notificación deben comunicar esta decisión a la autoridad competente del Estado miembro de origen, de conformidad con los plazos y procedimientos establecidos por esta última. Los proveedores de servicios de pago deben informar asimismo a la autoridad competente del Estado miembro de origen de cualquier evolución importante que afecte al tercero designado y a su capacidad para cumplir las obligaciones en materia de notificación.

3.5. Los proveedores de servicios de pago tienen el deber material de cumplir con sus obligaciones de notificación sin recurrir a asistencia externa cuando el tercero designado no informe a la autoridad competente del Estado miembro de origen de un incidente operativo o de seguridad grave de conformidad con el artículo 96 de la PSD2 y con las presentes Directrices. Además, los proveedores de servicios de pago deben asegurarse de que un incidente no se notifique dos veces, una vez por parte de dicho proveedor de servicios de pago y, otra, por el tercero.

Directriz 4: Política operativa y de seguridad

4.1. Los proveedores de servicios de pago deben asegurarse de que su política operativa y de seguridad general define claramente todas las responsabilidades en relación con la notificación de incidentes conforme a la PSD2, así como los procesos implementados para cumplir con los requisitos definidos en las presentes Directrices.

5. Directrices dirigidas a las autoridades competentes sobre los criterios para evaluar la importancia del incidente y los detalles de los informes de incidentes que deben compartirse con otras autoridades nacionales

Directriz 5: Evaluación de la importancia del incidente

5.1. Las autoridades competentes del Estado miembro de origen deben evaluar la importancia de un incidente operativo o de seguridad grave para otras autoridades nacionales, tomando como base su propia opinión experta y utilizando los siguientes criterios como indicadores principales de la importancia de dicho incidente:

a. Las causas del incidente están dentro del ámbito regulador de la otra autoridad nacional (es decir, su ámbito de competencia).
b. Las consecuencias del incidente tienen impacto sobre los objetivos de otra autoridad nacional (por ejemplo, salvaguardar la estabilidad financiera).
c. El incidente afecta, o podría afectar, a gran escala a los usuarios de servicios de pago.
d. Es probable que el incidente reciba o haya recibido una amplia cobertura mediática.

5.2. Las autoridades competentes del Estado miembro de origen deben llevar a cabo esta evaluación de forma continua durante todo el tiempo que dure el incidente, a fin de identificar cualquier posible cambio que pueda hacer que un incidente que no se consideraba importante pase a serlo.

Directriz 6: Información que se debe compartir

6.1. Sin perjuicio de cualquier otra obligación legal de compartir información relacionada con incidentes con otras autoridades nacionales, las autoridades competentes deben proporcionar información sobre los incidentes operativos o de seguridad graves a las autoridades nacionales identificadas siguiendo la Directriz 5.1 (es decir, «Otras autoridades nacionales pertinentes»), como mínimo, en el momento de recibir el informe inicial (o, alternativamente, el informe que motivó la comunicación de la información) y cuando se les notifica que la actividad ha vuelto a la normalidad (es decir, el último informe intermedio).

6.2. Las autoridades competentes deben presentar a otras autoridades nacionales pertinentes la información necesaria para transmitir una idea clara de lo ocurrido y de las posibles

consecuencias. Para ello, deben proporcionar, como mínimo, la información facilitada por el proveedor de servicios de pago en los siguientes campos de la plantilla (ya sea en el informe inicial o en el informe intermedio):

- fecha y hora de detección del incidente;
- fecha y hora de inicio del incidente;
- fecha y hora en que el incidente fue restaurado o se espera que se restaure;
- breve descripción del incidente (incluidas las partes no sensibles de la descripción detallada);
- breve descripción de las medidas adoptadas o que se prevé adoptar para recuperarse del incidente;
- descripción de en qué medida este incidente podría afectar a otros PSP o infraestructuras;
- descripción de la cobertura mediática (si la hubiere);
- causa del incidente.

6.3. Las autoridades competentes deben llevar a cabo la anonimización apropiada, según sea necesario, y excluir toda información que pudiera estar sujeta a restricciones de confidencialidad o de propiedad intelectual antes de compartir cualquier información relacionada con los incidentes con otras autoridades nacionales pertinentes. Sin embargo, las autoridades competentes deben proporcionar a otras autoridades nacionales pertinentes el nombre y la dirección del proveedor de servicios de pago que presenta la información cuando dichas autoridades nacionales puedan garantizar que la información será tratada confidencialmente.

6.4. Las autoridades competentes deben preservar en todo momento la confidencialidad y la integridad de la información almacenada e intercambiada con otras autoridades nacionales pertinentes y también autenticarse adecuadamente ante dichas autoridades. En particular, las autoridades competentes deben tratar toda la información recibida en virtud de las presentes Directrices de conformidad con las obligaciones de secreto profesional establecidas en la PSD2, sin perjuicio del Derecho de la Unión y de los requisitos nacionales que sean de aplicación.

6. Directrices dirigidas a las autoridades competentes sobre los criterios para evaluar los detalles relevantes de los informes de incidentes que deben comunicarse a la ABE y al BCE y sobre el formato y los procedimientos para su comunicación

Directriz 7: Información que se debe comunicar

7.1. Las autoridades competentes deben proporcionar siempre a la ABE y al BCE todos los informes recibidos de (o en nombre de) proveedores de servicios de pago afectados por un incidente operativo o de seguridad grave (es decir, informes iniciales, intermedios y finales).

Directriz 8: Comunicación

8.1. Las autoridades competentes deben preservar en todo momento la confidencialidad y la integridad de la información almacenada e intercambiada con la ABE y el BCE y también autenticarse adecuadamente ante la ABE y el BCE. En particular, las autoridades competentes deben tratar toda la información recibida en virtud de las presentes Directrices de conformidad con las obligaciones de secreto profesional establecidas en la PSD2, sin perjuicio del Derecho de la Unión y de los requisitos nacionales que sean de aplicación.

8.2. A fin de evitar retrasos en la transmisión de información relacionada con los incidentes a la ABE/BCE y ayudar a minimizar los riesgos derivados de interrupciones operativas, las autoridades competentes deben poder utilizar medios de comunicación adecuados.

Anexo 1 - Plantillas de notificación para proveedores de servicios de pago

CLASSIFICATION: RESTRICTED

Major Incident Report

☐ Initial report	within 4 hours after detection
☐ Intermediate report	maximum of 3 business days from previous report
☐ Last intermediate report	
☐ Final report	within 2 weeks after closing the incident
☐ Incident reclassified as non-major — Please explain:	

Report date	DD/MM/YYYY	Time	HH:MM
Incident identification number, if applicable (for interim and final reports)			

A - Initial report

A 1 - GENERAL DETAILS					
Type of report					
Type of report	☐ Individual	☐ Consolidated			
Affected payment service provider (PSP)					
PSP name					
PSP unique identification number, if relevant					
PSP authorisation number					
Head of group, if applicable					
Home country					
Country/countries affected by the incident					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)					
Name of the reporting entity					
Unique identification number, if relevant					
Authorisation number, if applicable					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION			
Date and time of detection of the incident	DD/MM/YYYY, HH:MM		
The incident was detected by (1)		If Other, please explain:	
Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)			
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM		

B - Intermediate report

B 1 - GENERAL DETAILS

Please provide a more DETAILED description of the incident. e.g. information on: - What is the specific issue? - How it happened - How did it develop - Was it related to a previous incident? - Consequences (in particular for payment service users) - Background of the incident detection - Areas affected - Actions taken so far - Service providers/ third party affected or involved - Crisis management started (internal and/or external (Central Bank Crisis management)) - PSP internal classification of the incident	
Date and time of beginning of the incident (if already identified)	DD/MM/YYYY, HH:MM
Incident status	☐ Diagnostics ☐ Recovery ☐ Repair ☐ Restoration
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

Overall impact	☐ Integrity ☐ Confidentiality ☐ Continuity ☐ Availability ☐ Authenticity
Transactions affected [2]	Number of transactions affected — ☐ Actual figure ☐ Estimation As a % of regular number of transactions — ☐ Actual figure ☐ Estimation Value of transactions affected in EUR — ☐ Actual figure ☐ Estimation Comments:
Payment service users affected [3]	Number of payment service users affected — ☐ Actual figure ☐ Estimation As a %-of total payment service users — ☐ Actual figure ☐ Estimation
Service downtime[4]	Total service downtime DD:HH:MM — ☐ Actual figure ☐ Estimation
Economic impact [5]	Direct costs in EUR — ☐ Actual figure ☐ Estimation Indirect costs in EUR — ☐ Actual figure ☐ Estimation
High level of internal escalation	☐ YES ☐ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe
Other PSPs or relevant infrastructures potentially affected	☐ YES ☐ NO Describe how this incident could affect other PSPs and/or infrastructures
Reputational impact	☐ YES ☐ NO Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.)

B 3 - INCIDENT DESCRIPTION

Type of Incident	☐ Operational ☐ Security
Cause of incident	☐ Under investigation ☐ External attack ☐ Internal attack Type of attack: ☐ Distributed/Denial of Service (D/DoS) ☐ Infection of internal systems ☐ Targeted intrusion ☐ Other If Other, specify ☐ External events ☐ Human error ☐ Process failure ☐ System failure ☐ Other If Other, specify
Was the incident affecting you directly, or indirectly through a service provider?	☐ Directly ☐ Indirectly If indirectly, please provide the service provider's name

B 4 - INCIDENT IMPACT

Building(s) affected (Address), if applicable	
Commercial channels affected	☐ Branches ☐ Telephone banking ☐ Point of sale ☐ E-banking ☐ Mobile banking ☐ Other ☐ ATMs If Other, specify:
Payment services affected	☐ Cash placement on a payment account ☐ Credit transfers ☐ Money remittance ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiation services ☐ Operations required for operating a payment account ☐ Card payments ☐ Account information services ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other If Other, specify:
Functional areas affected	☐ Authentication/authorisation ☐ Clearing ☐ Indirect settlement ☐ Communication ☐ Direct settlement ☐ Other If Other, specify:
Systems and components affected	☐ Application/software ☐ Hardware ☐ Database ☐ Network/infrastructure ☐ Other If Other, specify:
Staff affected	☐ YES ☐ NO Describe how the incident could affect the staff of the PSP/service provider (e.g. staff not being able to reach the office to support customers, etc.)

B 5 - INCIDENT MITIGATION

Which actions/measures have been taken so far or are planned to recover from the incident?	
Has the Business Continuity Plan and/or Disaster Recovery Plan been activated? If so, when? If so, please describe	☐ YES ☐ NO DD/MM/YYYY, HH:MM
Has the PSP cancelled or weakened some controls because of the incident? If so, please explain	☐ YES ☐ NO

C - Final report	
If no intermediate report has been sent, please also complete section B	
C 1 - GENERAL DETAILS	
Please update the information from the intermediate report (summary): - additional actions/measures taken to recover from the incident - final remediation actions taken - root cause analysis - lessons learnt - addittional actions - any other relevant information	
Date and time of closing the incident	DD/MM/YYYY, HH:MM
If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place?	☐ YES ☐ NO
If so, please explain	
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW-UP	
What was the root cause (if already known)? (possible to attach a file with detailed information)	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	
C 3 - ADDITIONAL INFORMATION	
Has the incident been shared with other PSPs for information purposes?	☐ YES ☐ NO
If so, please provide details	
Has any legal action been taken against the PSP?	☐ YES ☐ NO
If so, please provide details	

Notes:

(1) Pull-down menu: payment service user; internal organisation; external organisation; none of the above

(2) Pull-down menu: > 10% of regular level of transactions and > EUR 100,000; > 25% of regular level of transactions or > EUR 5 milion; none of the above

(3) Pull-down menu: > 5,000 and > 10% payment service users; > 50,000 or > 25% payment service users; none of the above

(4) Pull-down menu: > 2 hours; < 2 hours

(5) Pull-down menu: > Max (0,1% Tier 1 capital, EUR 200,000) or > EUR 5 million; none of the above

CONSOLIDATED REPORT - LIST OF PSPs		
PSP Name	**PSP Unique Identification Number**	**PSP Authorisation number**

INSTRUCCIONES PARA CUMPLIMENTAR LAS PLANTILLAS

Los proveedores de servicios de pago cumplimentarán la sección correspondiente de la plantilla, dependiendo de la fase de notificación en la que se encuentren: sección A para el informe inicial, sección B para los informes intermedios y sección C para el informe final. Todos los campos son obligatorios, a menos que se indique claramente lo contrario.

Encabezamiento

Informe inicial: esta es la primera notificación que el PSP envía a la autoridad competente del Estado miembro de origen.

Informe intermedio: se trata de una actualización de un informe anterior (inicial o intermedio) sobre el mismo incidente.

Último informe intermedio: informa a la autoridad competente del Estado miembro de origen de que se ha recuperado el nivel habitual de actividad y de que se ha vuelto a la normalidad, por lo que no se presentarán más informes intermedios.

Informe final: es el último informe que el PSP enviará sobre el incidente, ya que (i) ya se ha realizado un análisis de la causa de fondo y es posible reemplazar las estimaciones por cifras reales o (ii) el incidente ya no se considera grave.

Incidente reclasificado como no grave: el incidente ya no cumple los criterios para ser considerado grave y no se espera que los cumpla antes de su resolución. Los PSP deben explicar las razones de este cambio de estado.

Fecha y hora del informe: la fecha y la hora exactas de presentación del informe a la autoridad competente.

Número de identificación del incidente, si procede (para informes intermedios y final): el número de referencia indicado por la autoridad competente en el momento del informe inicial para identificar de forma inequívoca el incidente, si procede (es decir, si la autoridad competente proporciona dicha referencia).

A- Informe inicial

A 1 - Detalles generales

Tipo de informe

Individual: el informe se refiere a un único PSP.

Consolidado: el informe hace referencia a varios PSP que utilizan la opción de notificación consolidada. Los campos de «PSP afectado» deben dejarse en blanco (con la excepción del campo «País/países afectados por el incidente») y se facilitará una lista de los PSP incluidos en el informe rellenando la tabla correspondiente (Informe consolidado - Lista de PSP).

PSP afectado: se refiere al PSP que está sufriendo el incidente.

Nombre del PSP: nombre completo del PSP sujeto al procedimiento de notificación tal y como aparece en el registro nacional oficial aplicable de PSP.

Número de identificación único del PSP, si procede: el número de identificación único pertinente utilizado en cada Estado miembro para identificar al PSP. Deberá proporcionarse si no se cumplimenta el campo «número de autorización del PSP».

Número de autorización del PSP: número de autorización en el Estado miembro de origen.

Cabecera del grupo: en caso de grupos de entidades, tal como se definen en el artículo 4, apartado 40, de la 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, 2013/36/CE y el

Reglamento (UE) nº 1093/2010 y se deroga la Directiva 2007/64/CE, indíquese el nombre de la entidad cabecera del grupo.

País de origen: Estado miembro en el que esté situado el domicilio social del PSP; o si el PSP no tiene, según su Derecho nacional, sede social, el Estado miembro en el que esté situada su administración central.

País/países afectados por el incidente: país o países donde se ha materializado el impacto del incidente (por ejemplo, se ven afectadas varias sucursales de un PSP en diferentes países). Puede ser o no el mismo que el Estado miembro de origen.

Persona de contacto principal: nombre y apellidos de la persona responsable de notificar el incidente o, si lo hace un tercero en nombre del PSP afectado, nombre y apellidos de la persona encargada del departamento de gestión de incidentes, departamento de riesgos o área similar, en el PSP afectado.

Correo electrónico: dirección de correo electrónico a la que se puede dirigir cualquier solicitud de aclaraciones adicionales, si fuera necesario. Puede ser un correo electrónico personal o de empresa.

Teléfono: número de teléfono al que llamar para pedir aclaraciones adicionales, si es necesario. Puede ser un número de teléfono personal o de empresa.

Persona de contacto secundaria: nombre y apellidos de una persona alternativa con la que la autoridad competente podría contactar para preguntar sobre un incidente cuando la persona de contacto principal no esté disponible. Si un tercero notifica el incidente en nombre del PSP afectado, nombre y apellidos de una persona alternativa del departamento de gestión de incidentes, departamento de riesgos o área similar, en el PSP afectado.

Correo electrónico: dirección de correo electrónico de la persona de contacto alternativa a la que se puede dirigir cualquier solicitud de aclaraciones adicionales, si fuera necesario. Puede ser un correo electrónico personal o de empresa.

Teléfono: número de teléfono de la persona de contacto alternativa al que llamar para pedir aclaraciones adicionales, si es necesario. Puede ser un número de teléfono personal o de empresa.

Entidad que presenta la información: esta sección debe completarse si un tercero cumple las obligaciones de notificación en nombre del PSP afectado.

Nombre de la entidad que presenta la información: nombre completo de la entidad que notifica el incidente, tal como aparece en el registro mercantil nacional correspondiente.

Número de identificación único, si procede: el número de identificación único pertinente utilizado en el país en el que se encuentra el tercero para identificar a la entidad que informa del incidente. Se debe proporcionar si no se rellena el campo «Número de autorización».

Número de autorización, si procede: el número de autorización del tercero en el país donde se encuentra, cuando proceda.

Persona de contacto principal: nombre y apellidos de la persona responsable de notificar el incidente.

Correo electrónico: dirección de correo electrónico a la que se puede dirigir cualquier solicitud de aclaraciones adicionales, si fuera necesario. Puede ser un correo electrónico personal o de empresa.

Teléfono: número de teléfono al que llamar para pedir aclaraciones adicionales, si es necesario. Puede ser un número de teléfono personal o de empresa.

Persona de contacto secundaria: nombre y apellidos de una persona alternativa de la entidad que notifica el incidente con la que la autoridad competente podría contactar cuando la persona de contacto principal no esté disponible.

Correo electrónico: dirección de correo electrónico de la persona de contacto alternativa a la que se puede dirigir cualquier solicitud de aclaraciones adicionales, si fuera necesario. Puede ser un correo electrónico personal o de empresa.

Teléfono: número de teléfono de la persona de contacto alternativa al que llamar para pedir aclaraciones adicionales, si es necesario. Puede ser un número de teléfono personal o de empresa.

A 2 - Detección del incidente y clasificación inicial

Fecha y hora de detección del incidente: fecha y hora en que el incidente fue identificado.

El incidente fue detectado por: indicar si el incidente fue detectado por un usuario del servicio de pago, otra persona dentro del PSP (por ejemplo, la función de auditoría interna) o una parte externa (por ejemplo, un proveedor de servicios externo). Si no fuera ninguno de estos, se debe proporcionar una explicación en el campo correspondiente.

Breve descripción general del incidente: explique brevemente los aspectos más relevantes del incidente, indicando las posibles causas, impactos inmediatos, etc.

¿Cuál es la fecha prevista para la próxima actualización?: indique la fecha y hora estimadas para la presentación de la próxima actualización (informe intermedio o final).

B - Informe intermedio

B 1 - Detalles generales

Descripción más detallada del incidente: describa las principales características del incidente, cubriendo como mínimo los puntos presentados en el cuestionario (a qué problema específico se enfrenta el PSP, cómo se inició y se desarrolló, posible conexión con un incidente anterior, consecuencias, especialmente para usuarios de servicios de pago, etc.).

Fecha y hora de inicio del incidente: fecha y hora en que se inició el incidente, si se conoce.

Estado del incidente:

Diagnóstico: se acaban de identificar las características del incidente.

Reparación: los elementos atacados se están reconfigurando.

Recuperación: los elementos que han fallado se están restaurando a su último estado recuperable.

Restauración: el servicio relacionado con el pago se vuelve a prestar.

Fecha y hora en que el incidente fue restaurado o se espera que sea restaurado: indique la fecha y hora en que el incidente se controló o se espera que esté controlado y la actividad volvió o se espera que vuelva a la normalidad.

B 2 - Clasificación del incidente/Información sobre el incidente

Impacto general: indique los aspectos que se han visto afectados por el incidente. Se pueden marcar varias casillas.

Integridad: propiedad de salvaguardar la exactitud y la integridad de los activos (incluidos los datos).

Disponibilidad: propiedad de garantizar la disponibilidad y la capacidad de utilizar los servicios relacionados con el pago por parte de los usuarios de servicios de pago.

Confidencialidad: propiedad de que la información no se ponga a disposición de personas, entidades o procesos no autorizados, ni se divulgue a dichas personas, entidades o procesos.

Autenticidad: propiedad de que una fuente sea lo que afirma ser.

Continuidad: propiedad de que los procesos, las tareas y los activos de una organización necesarios para la prestación de servicios relacionados con el pago sean plenamente accesibles y se ejecuten a niveles predefinidos aceptables.

Operaciones afectadas: Los PSP deben indicar los umbrales que el incidente ha alcanzado o probablemente alcanzará, en su caso, y las cifras correspondientes: número de operaciones afectadas, porcentaje de operaciones afectadas en relación con el número de operaciones de pago realizadas con los mismos servicios de pago que se han visto afectados por el incidente, y el valor total de las operaciones. Los PSP deben proporcionar valores específicos para estas variables, que pueden ser tanto cifras reales como estimaciones. Las entidades que informan en nombre de varios PSP (es decir, notificación consolidada) pueden proporcionar intervalos de valores, que representan los valores inferiores y superiores observados o estimados dentro del grupo de PSP incluidos en el informe, separados por un guion. Como regla general, los PSP deben entender como «operaciones afectadas» todas las operaciones nacionales y transfronterizas que se han visto o se verán probablemente afectadas de manera directa o indirecta por el incidente y, en particular, aquellas operaciones que no pudieron iniciarse o procesarse, aquellas que sufrieron modificaciones en el contenido del mensaje de pago y aquellas que se ordenaron de manera fraudulenta (con independencia de que los fondos se hayan recuperado o no). Además, los PSP deben entender el nivel habitual de las operaciones de pago como el promedio anual diario de las operaciones de pago nacionales y transfronterizas realizadas con los mismos servicios de pago afectados por el incidente, tomando el año anterior como período de referencia para los cálculos. Si los PSP consideran que esta cifra no es representativa (por ejemplo, debido a la estacionalidad), deben utilizar otra métrica más representativa y comunicar a la autoridad competente la justificación de su elección en el campo «Comentarios».

Usuarios de servicios de pago afectados: Los PSP deben indicar los umbrales que el incidente ha alcanzado o probablemente alcanzará, en su caso, y las cifras correspondientes: número total de usuarios de servicios de pago afectados y porcentaje de usuarios de servicios de pago afectados en relación con el número total de usuarios de servicios de pago. Los PSP deben proporcionar valores concretos para estas variables, que pueden ser tanto cifras reales como estimaciones. Las entidades que informan en nombre de varios PSP (es decir, notificación consolidada) pueden proporcionar intervalos de valores, que representan los valores inferiores y superiores observados o estimados dentro del grupo de PSP incluidos en el informe, separados por un guion. Los PSP deben entender como «usuarios de servicios de pago afectados» a todos los clientes (nacionales o extranjeros, consumidores o empresas) que tienen un contrato con el proveedor de servicios de pago afectado que les permite acceder al servicio de pago afectado y que han sufrido o probablemente sufrirán las consecuencias del incidente. Los PSP deben recurrir a estimaciones basadas en su actividad anterior para determinar el número de usuarios de servicios de pago que pueden haber estado utilizando el servicio de pago durante el incidente. En el caso de grupos, cada PSP debe considerar únicamente a sus propios usuarios de servicios de pago. Un PSP que ofrezca servicios operativos a terceros solamente deberá considerar a sus propios usuarios de servicios de pago (si los hubiera) y los PSP que reciban estos servicios operativos también deben evaluar el incidente en relación con sus propios usuarios de servicios de pago. Por otra parte, los PSP deben tomar como número total de usuarios de servicios de pago la cifra agregada de los usuarios de servicios de pago nacionales y transfronterizos vinculados contractualmente en el momento del incidente (o, de manera alternativa, la cifra más reciente disponible) y con acceso al servicio de pago afectado, con independencia de su tamaño o de si se consideran usuarios de servicios de pago activos o pasivos.

Tiempo de inactividad del servicio: Los PSP deben indicar si el incidente ha alcanzado o es probable que alcance el umbral y la cifra correspondiente: tiempo total de inactividad del servicio.

Los PSP deben proporcionar valores concretos para esta variable, que pueden consistir tanto en cifras reales como en estimaciones. Las entidades que informan en nombre de varios PSP (es decir, notificación consolidada) pueden proporcionar un intervalo de valores, que representan el valor inferior y superior observados o estimados dentro del grupo de PSP incluidos en el informe, separados por un guion. Los PSP deben considerar el período de tiempo durante el que cualquier tarea, proceso o canal relacionado con la prestación de servicios de pago está o probablemente estará inactivo y, por lo tanto, impide (i) la iniciación o la ejecución de un servicio de pago o (ii) el acceso a una cuenta de pago. Los PSP deben contar el tiempo de inactividad del servicio desde el momento en que comienza la inactividad y deben considerar tanto los intervalos de tiempo durante los que están operativos para prestar el servicio, como las horas de cierre y los periodos de mantenimiento, cuando proceda y sea relevante. Si los proveedores de servicios de pago no pueden determinar cuándo se inició la inactividad del servicio, deberán contar excepcionalmente el tiempo de inactividad del servicio desde el momento en el que se detecta la inactividad.

Impacto económico: Los PSP deben indicar si el incidente ha alcanzado o es probable que alcance el umbral y las cifras correspondientes: costes directos e indirectos. Los PSP deben proporcionar valores concretos para estas variables, que pueden ser tanto cifras reales como estimaciones. Las entidades que informan en nombre de varios PSP (es decir, notificación consolidada) pueden proporcionar un intervalo de valores, que representan los valores inferiores y superiores observados o estimados dentro del grupo de PSP incluidos en el informe, separados por un guion. Los PSP deben considerar tanto los costes que puedan estar directamente relacionados con el incidente como los que están indirectamente relacionados con el mismo. Entre otras cuestiones, los PSP deben tener en cuenta los fondos o activos expropiados, los costes de sustitución de *hardware* o *software*, otros costes periciales o de reparación, los costes derivados del incumplimiento de obligaciones contractuales, las sanciones, las responsabilidades externas y la pérdida de ingresos. Por lo que respecta a los costes indirectos, los PSP deben considerar solo los que ya son conocidos o que es muy probable que se materialicen.

> **Costes directos:** importe (en euros) del coste directamente imputable al incidente, incluidos los fondos necesarios para rectificarlo (por ejemplo, fondos o activos expropiados, costes de sustitución de *hardware* y *software*, costes derivados del incumplimiento de obligaciones contractuales).
>
> **Costes indirectos:** importe (en euros) del coste indirectamente imputable al incidente (por ejemplo, costes de reparación/indemnización de clientes, pérdida de ingresos como resultado de oportunidades de negocio perdidas, posibles costes legales).

Elevación interna a alto nivel: Los PSP deben considerar si, como consecuencia de su impacto en los servicios relacionados con el pago, el Director de Sistemas de Información (o cargo similar) ha sido o será probablemente informado sobre el incidente al margen de cualquier procedimiento de notificación periódica y de manera continua durante toda la duración del incidente. En el caso de los informes delegados, la elevación a cargos superiores tendría lugar dentro del tercero. Además, los PSP deben considerar si, como resultado del impacto del incidente sobre los servicios relacionados con el pago, se ha activado o es probable que se active un modo de crisis.

Otros PSP o infraestructuras relevantes potencialmente afectados: los proveedores de servicios de pago deben evaluar el impacto del incidente sobre el mercado financiero, entendido como las infraestructuras de los mercados financieros y/o los esquemas de pago con tarjeta que los respaldan, así como otros PSP. En particular, los PSP deben evaluar si el incidente se ha reproducido o es probable que se reproduzca en otros PSP, si ha afectado o probablemente afectará al buen funcionamiento de las infraestructuras de los mercados financieros y si ha comprometido o probablemente comprometerá la solidez del sistema financiero en su conjunto. Los PSP deben tener en cuenta diversos aspectos, como si el componente/*software* afectado es

propietario o está disponible para el público en general, si la red comprometida es interna o externa y si el PSP ha dejado o es probable que deje de cumplir sus obligaciones en las infraestructuras de los mercados financieros de las que es miembro.

Incidencia sobre la reputación: Los PSP deben considerar el nivel de visibilidad que, a su leal saber y entender, el incidente ha alcanzado o probablemente alcanzará en el mercado. En particular, deben considerar la probabilidad de que el incidente cause perjuicios a la sociedad como un buen indicador de su potencial para afectar a su reputación. Los PSP deben tener en cuenta (i)si el incidente ha afectado a un proceso visible y, por lo tanto, es probable que reciba o ya haya recibido cobertura de los medios de comunicación (considerando no solo los medios tradicionales, como periódicos, sino también blogs, redes sociales, etc.), (ii) si no se ha cumplido o probablemente no se cumplirán las obligaciones normativas, (iii) si se han infringido, o probablemente se infringirán, las sanciones o (iv) si el mismo tipo de incidente ha ocurrido anteriormente.

B 3 - Descripción del incidente

Tipo de incidente: indique si, a su leal saber y entender, se trata de un incidente operativo o de seguridad.

Operativo: incidentes derivados de procesos, personas y sistemas inadecuados o fallidos, o eventos de fuerza mayor que afectan a la integridad, la disponibilidad, la confidencialidad, la autenticidad y/o la continuidad de los servicios relacionados con el pago.

Seguridad: acceso, uso, revelación, interrupción, modificación o destrucción no autorizados de los activos del PSP que afectan a la integridad, la disponibilidad, la confidencialidad, la autenticidad y/o la continuidad de los servicios relacionados con el pago. Esto puede ocurrir cuando, entre otros, el PSP sufre ciberataques, el diseño o la aplicación de sus políticas de seguridad resultan inadecuados o la seguridad física no es la apropiada.

Causa del incidente: indique la causa del incidente o, si aún no se sabe, su causa más probable. Se pueden marcar varias casillas.

Bajo investigación: la causa todavía no se ha determinado.

Ataque externo: la causa es de origen externo y el ataque está dirigido intencionadamente al PSP (por ejemplo, ataques de *software* malicioso).

Ataque interno: la causa es de origen interno y el ataque está dirigido intencionadamente al PSP (por ejemplo, fraude interno).

Tipo de ataque:

Denegación de servicio/distribuida (D/DoS): un intento de impedir la disponibilidad de un servicio *on line* sobrecargándolo con tráfico procedente de múltiples fuentes.

Infección de los sistemas internos: actividad dañina que ataca los sistemas informáticos, tratando de robar espacio en el disco duro o tiempo de la CPU, acceder a información privada, corromper datos, robar contactos, etc.

Intrusión dirigida: acto no autorizado de espionaje, intromisión (*snooping*) y robo de información a través del ciberespacio.

Otros: cualquier otro tipo de ataque que el PSP pueda haber sufrido, ya sea directamente o a través de un proveedor de servicios. En particular, se debe marcar esta casilla si ha habido un ataque dirigido contra el proceso de autorización y autenticación. Se deben proporcionar detalles en el campo de texto libre.

Eventos externos: la causa se asocia con eventos que están generalmente fuera del control de la organización (por ejemplo, desastres naturales, asuntos legales, cuestiones comerciales y dependencias del servicio).
Error humano: el incidente fue causado por el error involuntario de una persona, ya sea como parte del procedimiento de pago (por ejemplo, cargar un lote de pagos erróneo en el sistema de pagos) o porque esté relacionado con él de alguna manera (por ejemplo, la electricidad se corta accidentalmente y la actividad de pago queda retenida).
Fallo del proceso: la causa del incidente ha sido una deficiencia en el diseño o la ejecución del proceso de pago, los controles del proceso o los procesos de soporte (por ejemplo, proceso de cambio/migración, pruebas, configuración, capacidad, seguimiento).
Fallo del sistema: la causa del incidente está asociada con un diseño, una ejecución, unos componentes, unas especificaciones, una integración o una complejidad inadecuados de los sistemas que soportan la actividad de pago.
Otros: la causa del incidente no es ninguna de las anteriores. Se deben proporcionar más detalles en el campo de texto libre.

¿El incidente le afectó de directamente, o indirectamente a través de un proveedor de servicios?: un incidente puede estar dirigido directamente a un PSP o afectarlo de manera indirecta, a través de un tercero. En el caso de un impacto indirecto, indique el nombre del proveedor o proveedores de servicios.

B 4 - Impacto del incidente

Edificio(s) afectado(s) (dirección), si procede: si un edificio físico está afectado, indique su dirección.

Canales comerciales afectados: indique el canal o canales de interacción con los usuarios de servicios de pago que se han visto afectados por el incidente. Se pueden marcar varias casillas.

Sucursales: lugar de actividad (distinto de las oficinas centrales) que forma parte de un PSP, no tiene personalidad jurídica y realiza directamente una parte o la totalidad de las operaciones inherentes al negocio de un PSP. Todos los centros de actividad establecidos en el mismo Estado miembro por un mismo PSP que tenga su sede en otro Estado miembro se consideran una única sucursal.
Banca electrónica: el uso de ordenadores para realizar operaciones financieras a través de Internet.
Banca telefónica: el uso de teléfonos para realizar operaciones financieras.
Banca móvil: el uso de una aplicación bancaria específica en un teléfono inteligente o dispositivo similar para realizar operaciones financieras.
Cajeros automáticos: dispositivos electromecánicos que permiten a los usuarios de servicios de pago retirar efectivo de sus cuentas y/o acceder a otros servicios.
Punto de venta: instalación física del comerciante en el que se inicia la operación de pago.
Otros: el canal comercial afectado no es ninguno de los anteriores. Se deben proporcionar detalles en el campo de texto libre.

Servicios de pago afectados: indique los servicios de pago que no funcionan correctamente como resultado del incidente. Se pueden marcar varias casillas.

Ingreso de efectivo en una cuenta de pago: la entrega de dinero en efectivo a un PSP para depositarlo en una cuenta de pago.

Retirada de efectivo de una cuenta de pago: la solicitud recibida por un PSP de su usuario del servicio de pago para proporcionar efectivo y adeudar su cuenta de pago por el importe correspondiente.

Operaciones necesarias para la gestión de una cuenta de pago: las acciones que hay que realizar en una cuenta de pago para activarla, desactivarla o mantenerla (por ejemplo, apertura, bloqueo).

Adquisición de instrumentos de pago: un servicio de pago prestado por un PSP que ha convenido mediante contrato con un beneficiario en aceptar y procesar las operaciones de pago, de modo que se produzca una transferencia de fondos al beneficiario.

Transferencias: un servicio de pago destinado a efectuar un abono en una cuenta de pago de un beneficiario mediante una operación de pago o una serie de operaciones de pago con cargo a una cuenta de pago de un ordenante por el PSP que mantiene la cuenta de pago del ordenante y prestado sobre la base de las instrucciones dadas por el ordenante.

Adeudos domiciliados: un servicio de pago destinado a efectuar un cargo en la cuenta de pago del ordenante, en el que la operación de pago es iniciada por el beneficiario sobre la base del consentimiento dado por el ordenante al beneficiario, al proveedor de servicios de pago del beneficiario o al propio proveedor de servicios de pago del propio ordenante.

Pagos con tarjeta: un servicio de pago basado en la infraestructura y las reglas de negocio de un esquema de pago con tarjeta para realizar una operación de pago mediante cualquier tarjeta o dispositivo de telecomunicación, digital o informático o *software*, siempre que se trate de una operación con tarjeta de débito o crédito. Las operaciones de pago basadas en tarjetas excluyen operaciones basadas en otros tipos de servicios de pago.

Emisión de instrumentos de pago: un servicio de pago en el cual un PSP se compromete mediante contrato a proporcionar a un ordenante un instrumento de pago que permite iniciar y procesar las operaciones de pago del ordenante.

Servicio de envío de dinero: servicio de pago que permite recibir fondos de un ordenante, sin que se cree ninguna cuenta de pago en nombre del ordenante o del beneficiario, con el único fin de transferir una cantidad equivalente a un beneficiario o a otro PSP que actúe por cuenta del beneficiario, y/o recibir fondos por cuenta del beneficiario y ponerlos a disposición de este.

Servicios de iniciación de pagos: servicios de pago que permiten iniciar una orden de pago, a petición del usuario del servicio de pago, respecto de una cuenta de pago abierta con otro PSP.

Servicios de información sobre cuentas: servicios de pago en línea cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago bien en otro PSP, bien en varios PSP.

Otros: el servicio de pago afectado no es ninguno de los anteriores. Se deben proporcionar detalles en el campo de texto libre.

Áreas funcionales afectadas: indique la fase o fases del proceso de pago que se han visto afectadas por el incidente. Se pueden marcar varias casillas.

Autenticación/autorización: procedimientos que permiten al PSP comprobar la identidad del usuario de un servicio de pago o la validez de la utilización de un determinado instrumento de pago, incluida la utilización de credenciales de seguridad personalizadas del usuario y del usuario del servicio de pago (o un tercero que actúa en nombre de dicho usuario) que da su consentimiento para transferir fondos o valores.

Comunicación: flujo de información con fines de identificación, autenticación, notificación e información entre el PSP gestor de cuenta y los proveedores de servicios de iniciación de pagos, proveedores de servicios de información sobre cuentas, ordenantes, beneficiarios y otros PSP.
Compensación: un proceso de transmisión, conciliación y, en algunos casos, confirmación de órdenes de transferencia antes de su liquidación, como, por ejemplo, el neteo de órdenes y el establecimiento de posiciones finales para la liquidación.
Liquidación directa: la finalización de una operación o de la tramitación con el fin de cumplir con las obligaciones de los participantes a través de la transferencia de fondos, cuando esta acción es llevada a cabo por el propio PSP afectado.
Liquidación indirecta: la finalización de una operación o de la tramitación con el fin de cumplir con las obligaciones de los participantes a través de la transferencia de fondos, cuando esta acción es llevada a cabo por otro PSP en nombre del PSP afectado.
Otros: el área funcional afectada no es ninguna de las anteriores. Se deben proporcionar detalles en el campo de texto libre.

Sistemas y componentes afectados: indique qué parte o partes de la infraestructura tecnológica del PSP se han visto afectadas por el incidente. Se pueden marcar varias casillas.

Aplicación/*software*: programas, sistemas operativos, etc. que apoyan la prestación de servicios de pago por parte del PSP.
Base de datos: estructura de datos que almacena la información personal y de pago necesaria para ejecutar las operaciones de pago.
***Hardware*:** equipo de tecnología física que ejecuta los procesos y/o almacena los datos que necesitan los PSP para llevar a cabo su actividad relacionada con el pago.
Red/Infraestructura: redes de telecomunicaciones, públicas o privadas, que permiten el intercambio de datos e información durante el proceso de pago (por ejemplo, Internet).
Otros: el sistema y los componentes afectados no son ninguno de los anteriores. Se deben proporcionar detalles en el campo de texto libre.

Personal afectado: indique si el incidente ha tenido algún efecto en el personal del PSP y, en caso afirmativo, proporcione detalles en el campo de texto libre.

B 5 - Mitigación del incidente

¿Qué acciones/medidas se han adoptado hasta ahora o se prevé adoptar para recuperarse del incidente?: proporcione detalles sobre las medidas que se han adoptado o se prevé adoptar para resolver temporalmente el incidente.
¿Se ha activado el Plan de Continuidad de la Actividad o el Plan de Recuperación en caso de Catástrofes?: indique si se han activado o no y, en caso afirmativo, proporcione los detalles más relevantes de lo ocurrido (es decir, cuándo se activaron y en qué consistieron estos planes).
¿El PSP ha anulado o suavizado algunos controles debido al incidente?: indique si el PSP ha tenido que anular algunos controles (por ejemplo, prescindir del uso del principio de los «cuatro ojos») para resolver el incidente y, en caso afirmativo, detalle las razones que justifican la reducción o anulación de controles.

C- Informe final

C 1 - Detalles generales

Actualización de la información del informe intermedio (resumen): proporcione información adicional sobre las medidas adoptadas para recuperarse del incidente y evitar su repetición, análisis de la causa de fondo, lecciones extraídas, etc.

Fecha y hora de cierre del incidente: indique la fecha y la hora en que el incidente se consideró cerrado.

¿Se han vuelto a restaurar los controles originales?: si el PSP tuvo que anular o suavizar algunos controles debido al incidente, indique si se han vuelto a restaurar y proporcione cualquier información adicional en el campo de texto libre.

C 2 - Análisis de la causa de fondo y seguimiento

¿Cuál fue la causa de fondo (si ya se conoce)?: explique cuál es la causa de fondo del incidente o, si aún no se conoce, las conclusiones preliminares extraídas del análisis de la causa de fondo. Los PSP pueden adjuntar un archivo con información detallada si se considera necesario.

Principales medidas de corrección/medidas adoptadas o previstas para evitar que el incidente vuelva a ocurrir en el futuro, si ya se conocen: sírvase describir las principales medidas que se han adoptado o se prevé adoptar para evitar que el incidente vuelva a repetirse en el futuro.

C 3 – Información adicional

¿Se ha compartido el incidente con otros PSP con fines informativos? proporcione una visión general de los PSP con los que se ha contactado, formal o informalmente, para informarles sobre el incidente, proporcionando detalles de los PSP que han sido informados, la información que se ha compartido y las razones por las que se ha compartido esta información.

¿Se han emprendido acciones legales contra el PSP?: indique si, en el momento de rellenar el informe final, se ha emprendido alguna acción legal contra el PSP (por ejemplo, acción judicial o pérdida de licencia) como resultado del incidente.