EBA/GL/2021/03

10 de junio de 2021

Directrices revisadas

sobre la notificación de incidentes graves de conformidad con la Directiva de servicios de pago (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 de la ABE[1]. De conformidad con el artículo 16, apartado 3, del Reglamento de la ABE, las autoridades competentes y las entidades financieras harán todo lo posible por 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 de la ABE 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 de la ABE, las autoridades competentes deberán notificar a la ABE, a más tardar el [07.11.2021], 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/2021/03». 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. 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, por la que se modifican las Directivas 2002/65/CE, 2009/110/CE, 2013/36/UE 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 PSD2.

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 la PSD2, 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 PSD2.

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).

12. Las presentes Directrices se aplican también a incidentes graves que afectan a funciones externalizadas a terceros por parte de los proveedores de servicios de pago.

Destinatarios

13. 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 PSD2 y contemplados en el artículo 4, apartado 1, del Reglamento (UE) n.º 1093/2010.

14. 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, inciso i), del Reglamento (UE) n.º 1093/2010.

Definiciones

15. Salvo que se indique lo contrario, los términos utilizados y definidos en la PSD2 tendrán el mismo significado en las Directrices. Además, a los efectos de estas Directrices, se entenderá por:

Autenticidad	Propiedad de que una fuente sea lo que afirma ser.
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.
Disponibilidad	Propiedad de garantizar la accesibilidad y la capacidad de utilizar los servicios relacionados con el pago por parte de los usuarios de servicios de pago, conforme a los niveles aceptables previamente definidos por el proveedor de servicios de pago.
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 y/o la autenticidad de los servicios relacionados con el pago.
Integridad	Propiedad de salvaguardar la exactitud y la completitud de los activos (incluidos los datos).
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

16. Las presentes Directrices serán de aplicación a partir del 1 de enero de 2022.

Derogación

17. Quedan derogadas las siguientes Directrices con efectos a partir del 1 de enero de 2022:

Directrices sobre la notificación de incidentes graves de conformidad con la Directiva (UE) 2015/2366 (PSD2) (EBA/GL/2017/10)

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 clasificarán 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 evaluarán 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 determinarán el valor total de las operaciones afectadas, así como el número de pagos comprometidos como porcentaje del nivel habitual de las operaciones de pago realizadas con los servicios de pago afectados.

ii. Usuarios de servicios de pago afectados

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

iii. Violación de la seguridad de las redes o sistemas de información

Los proveedores de servicios de pago determinarán si alguna acción maliciosa ha comprometido la seguridad de las redes o sistemas de información relacionados con la prestación de servicios de pago.

iv. Tiempo de inactividad del servicio

Los proveedores de servicios de pago determinarán 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.

v. Impacto económico

Los proveedores de servicios de pago determinarán de manera integral los costes monetarios asociados al incidente y tendrán 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, con el capital de nivel 1 [T1] del proveedor de servicios de pago).

vi. Elevación interna a alto nivel

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

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

Los proveedores de servicios de pago determinarán 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 o esquemas de pago.

viii. Impacto reputacional

Los proveedores de servicios de pago determinarán 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 calcularán el valor de los indicadores de acuerdo con la siguiente metodología:

i. Operaciones afectadas:

Como regla general, los proveedores de servicios de pago entenderán por «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) o en aquellos casos en los que el incidente impida o dificulte de cualquier otro modo la debida ejecución.

En el caso de incidentes operativos que afectan a la capacidad de iniciar o procesar operaciones, los proveedores de servicios de pago notificarán únicamente aquellos incidentes con una duración superior a una hora. La duración del incidente se calculará desde el momento en el que se produce el incidente hasta el momento en el que se restablecen las actividades/operaciones habituales al nivel de servicio que se prestaba antes del incidente.

Además, los proveedores de servicios de pago entenderán 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), utilizarán otra métrica más representativa y comunicarán a la autoridad competente la justificación de su elección en el campo correspondiente de la plantilla (véase el Anexo).

ii. Usuarios de servicios de pago afectados

Los proveedores de servicios de pago entenderán por «usuarios de servicios de pago afectados» 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 recurrirán a estimaciones basadas en su actividad anterior para determinar el número de usuarios del servicio 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 considerará únicamente a sus propios usuarios de servicios de pago. Un proveedor de servicios de pago que ofrezca servicios operativos a otros PSP considerará solamente a sus propios usuarios de servicios de pago (si los hubiera), y los proveedores de servicios de pago que reciban estos servicios operativos evaluarán el incidente en relación con sus propios usuarios de servicios de pago.

En el caso de incidentes operativos que afecten a la capacidad de iniciar o procesar operaciones, los proveedores de servicios de pago notificarán únicamente aquellos incidentes que afecten a los usuarios de servicios de pago durante más de una hora. La duración del incidente se calculará desde el momento en el que se produce el incidente hasta el momento en el que se restablecen las actividades/operaciones habituales al nivel de servicio que se prestaba antes del incidente.

Por otra parte, los proveedores de servicios de pago tomarán 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. Violación de la seguridad de las redes o sistemas de información

Los proveedores de servicios de pago determinarán si alguna acción maliciosa ha comprometido la disponibilidad, autenticidad, integridad o confidencialidad de las redes o los sistemas de información (incluidos los datos) relacionados con la prestación de servicios de pago.

iv. Tiempo de inactividad del servicio

Los proveedores de servicios de pago considerarán el período de tiempo 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 contarán el tiempo de inactividad del servicio desde el momento en que comienza la inactividad y considerarán 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, contarán excepcionalmente el tiempo de inactividad del servicio desde el momento en el que se detecta la inactividad.

v. Impacto económico

Los proveedores de servicios de pago considerarán 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 tendrán 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 las obligaciones contractuales, las sanciones, las responsabilidades externas y las pérdidas de ingresos. Por lo que respecta a los costes indirectos, los proveedores de servicios de pago considerarán solo los que ya son conocidos o es muy probable que se materialicen.

vi. *Elevación interna a alto nivel*

Los proveedores de servicios de pago considerarán si, como consecuencia de su impacto en los servicios relacionados con el pago, el órgano de dirección, tal como se define en las Directrices de la ABE sobre gestión de riesgos de TIC y de seguridad, ha sido o será probablemente informado, tal como contempla la Directriz 60, apartado d), de las Directrices de la ABE sobre gestión de riesgos de TIC y de seguridad, acerca del 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 considerarán 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.

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

Los proveedores de servicios de pago evaluarán el impacto del incidente sobre el mercado financiero, entendido como las infraestructuras de los mercados financieros o los esquemas de pago que lo respaldan y el resto de proveedores de servicios de pago. En particular, los proveedores de servicios de pago evaluarán 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 tendrán 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 o 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.

viii. *Impacto reputacional*

Los proveedores de servicios de pago considerarán el nivel de visibilidad que, a su leal saber y entender, el incidente ha alcanzado o probablemente alcanzará en el mercado. En particular, considerarán 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 tendrán en cuenta i) si los usuarios de servicios de pago u otros proveedores de servicios de pago se han quejado del impacto negativo del incidente, ii) si el incidente ha afectado a un proceso visible relacionado con el servicio de pago y, por lo tanto, es probable que reciba o ya ha recibido cobertura mediática (considerando no solo los medios tradicionales, como periódicos, sino también blogs, redes sociales, etc.), iii) si no se han cumplido o probablemente no se cumplirán las obligaciones contractuales, lo que ha dado o probablemente dará lugar al inicio de acciones legales contra el proveedor de servicios de pago, iv) si no se han cumplido las obligaciones normativas, lo que ha provocado la imposición de sanciones o medidas supervisoras que se han publicado o probablemente se harán públicas, y v) si el mismo tipo de incidente ha ocurrido anteriormente.

1.4. Los proveedores de servicios de pago evaluarán 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 las operaciones del proveedor de servicios de pago (en términos de número de operaciones) **y** duración del incidente > 1 hora* **o** > 500.000 EUR **y** duración del incidente > 1 hora*	> 25 % del nivel habitual de las operaciones del proveedor de servicios de pago (en términos de número de operaciones) **o** > 15.000.000 EUR
Usuarios de servicios de pago afectados	> 5.000 **y** duración del incidente > 1 hora* **o** > 10 % de los usuarios de servicios de pago del proveedor de servicios de pago **y**	> 50.000 **o** > 25 % de los usuarios de servicios de pago del proveedor de servicios de pago

	duración del incidente > 1 hora*	
Tiempo de inactividad del servicio	> 2 horas	No aplicable
Violación de la seguridad de las redes o sistemas de información	Sí	No aplicable
Impacto económico	No aplicable	> Máx. (0,1 % de capital de nivel 1**, 200.000 EUR) **o** > 5.000.000 EUR
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
Impacto reputacional	Sí	No aplicable

* El umbral relativo a la duración del incidente por un período superior a una hora es aplicable solo en el caso de incidentes operativos que afectan a la capacidad del proveedor de servicios de pago de iniciar o procesar operaciones.

**Capital de nivel 1 (T1) como se define en el artículo 25 del Reglamento (UE) n.º 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) n.º 648/2012.

1.5. Los proveedores de servicios de pago recurrirán 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 llevarán a cabo esta evaluación de manera continua durante todo el período 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). Toda reclasificación de un incidente de grave a no grave se comunicará sin demoras indebidas a la autoridad competente, tal como contempla el requisito de la Directriz 2.21.

Directriz 2: Proceso de notificación

2.1. Los proveedores de servicios de pago recopilarán toda la información pertinente, elaborarán un informe del incidente utilizando la plantilla que figura en el anexo y lo presentarán a la autoridad competente del Estado miembro de origen. Los proveedores de servicios de pago rellenarán todos los campos de la plantilla siguiendo las instrucciones que figuran en el anexo.

2.2. Los proveedores de servicios de pago usarán la misma plantilla al presentar los informes inicial, intermedios y final relativos al mismo incidente. Por lo tanto, los proveedores de

servicios de pago rellenarán una única plantilla progresivamente y actualizarán, cuando proceda, la información facilitada en informes anteriores.

2.3. Los proveedores de servicios de pago presentarán 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 contempla en el artículo 96, apartado 1, párrafo segundo, de la PSD2, en cuanto esté disponible.

2.4. Los proveedores de servicios de pago, previa solicitud de la autoridad competente del Estado miembro de origen, facilitarán cualquier documentación adicional que complemente la información presentada en la plantilla estándar. Los proveedores de servicios de pago darán seguimiento a cualquier solicitud de la autoridad competente del Estado miembro de origen de información adicional o de aclaraciones sobre la documentación ya presentada.

2.5. Los proveedores de servicios de pago reflejarán en la plantilla, de conformidad con la Directriz 2.1, la información adicional incluida en los documentos que faciliten a la autoridad competente, ya sea por iniciativa del proveedor de servicios de pago o previa solicitud de la autoridad competente tal como contempla la Directriz 2.4.

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

Informe inicial

2.7. Los proveedores de servicios de pago presentarán un informe inicial a la autoridad competente del Estado miembro de origen cuando un incidente operativo o de seguridad se clasifique como grave. Las autoridades competentes acusarán recibo del informe inicial sin demoras indebidas y asignarán un código de referencia único que identifique de manera inequívoca el incidente. Los proveedores de servicios de pago indicarán este código de referencia cuando presenten una actualización del informe inicial o de los informes intermedio y final relativos al mismo incidente, a menos que los informes intermedio y final se presenten conjuntamente con el informe inicial.

2.8. Los proveedores de servicios de pago enviarán el informe inicial a la autoridad competente en el plazo de cuatro horas desde el momento en que el incidente operativo o de seguridad se clasifique como grave. Si se sabe que los canales de notificación de la autoridad competente no están disponibles u operativos en ese momento, los proveedores de servicios de pago enviarán el informe inicial tan pronto como vuelvan a estar disponibles/operativos.

2.9. Los proveedores de servicios de pago clasificarán el incidente conforme a las Directrices 1.1 y 1.4 de manera oportuna tras haber detectado el incidente, pero no más tarde de 24 horas a partir de la detección del mismo, y sin demoras indebidas después de que el proveedor de servicios de pago disponga de la información necesaria para la clasificación del incidente. Si

se necesitara un plazo mayor para clasificar el incidente, los proveedores de servicios de pago expondrán los motivos en el informe inicial presentado a la autoridad competente.

2.10. Los proveedores de servicios de pago también presentarán 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 enviarán 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/operativos.

2.11. Los proveedores de servicios de pago facilitarán 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 clasificación como incidente grave. Los proveedores de servicios de pago recurrirán a estimaciones cuando no dispongan de datos reales.

Informe intermedio

2.12. Los proveedores de servicios de pago presentarán el informe intermedio cuando se hayan recuperado las actividades habituales y se haya vuelto a la normalidad, informando a la autoridad competente de esta circunstancia. Los proveedores de servicios de pago considerarán que la actividad vuelve a la normalidad cuando la actividad o las operaciones se restablezcan al mismo nivel de servicio o de condiciones definido por el proveedor de servicios de pago o establecido externamente por un Acuerdo de Nivel de Servicio (tiempo de procesamiento, capacidad, requisitos de seguridad, etc.) y cuando ya no estén en vigor medidas contingentes. El informe intermedio incluirá una descripción más detallada del incidente y sus consecuencias (sección B de la plantilla).

2.13. Si todavía no se han recuperado las actividades habituales, los proveedores de servicios de pago presentarán un informe intermedio a la autoridad competente en el plazo de tres días hábiles desde la presentación del informe inicial.

2.14. Los proveedores de servicios de pago actualizarán la información ya proporcionada en las secciones A y B de la plantilla cuando tengan conocimiento 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). Esto incluye el caso en el que el incidente no se haya resuelto en el plazo de tres días hábiles, lo que exigiría la presentación de un informe intermedio adicional por parte de los proveedores de servicios de pago. En cualquier caso, los proveedores de servicios de pago presentarán un informe intermedio adicional a petición de la autoridad competente del Estado miembro de origen.

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

2.16. En caso de que la actividad vuelva a la normalidad antes de que transcurran cuatro horas desde que se hubiera clasificado el incidente como grave, los proveedores de servicios de pago tratarán de presentar tanto el informe inicial como el informe intermedio simultáneamente (es decir, cumplimentar las secciones A y B de la plantilla) en el plazo de cuatro horas.

Informe final

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

2.18. Los proveedores de servicios de pago entregarán el informe final a la autoridad competente dentro de un plazo máximo de 20 días hábiles 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 o por no haber identificado aún la causa raíz) se pondrán en contacto con la autoridad competente antes de que haya finalizado el plazo y proporcionarán 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 cuatro horas desde que el incidente se clasificó como grave, tratarán de presentar conjuntamente la información relativa a los informes inicial, intermedio y final.

2.20. Los proveedores de servicios de pago incluirán en su informe final 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 raíz, 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 enviarán 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 enviarán el informe final tan pronto como se detecte esta circunstancia y, en cualquier caso, dentro del plazo establecido para la presentación del próximo informe. En esta situación concreta, en lugar de rellenar la sección C de la plantilla, los proveedores de servicios de pago marcarán la casilla «Incidente reclasificado como no grave» y explicarán 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 informarán a la autoridad competente del Estado miembro de origen y velarán 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; o

ii. las directrices de la ABE sobre externalización (EBA/GL/2019/02) en relación con todos los proveedores de servicios de pago.

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) informarán a la autoridad competente del Estado miembro de origen, incluirán la información de contacto indicada en el campo «PSP afectado» de la plantilla y se asegurarán de que se cumplen las siguientes condiciones:

a. Que se incluye esta disposición en el contrato que contempla la notificación delegada.

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 se facilita una lista de todos los proveedores de servicios de pago afectados por el incidente.

e. 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 está clasificado como grave. Asimismo, se asegurarán 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.

f. Que, cuando en la plantilla figuren campos en los que no sea posible una respuesta común (por ejemplo, las secciones B 2, B 4 o C 3 de la plantilla), 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 los valores acumulados observados o estimados para los proveedores de servicios de pago.

g. Que el tercero mantiene al proveedor de servicios de pago informado 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 delegarán 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 comunicarán 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 informarán 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 cumplirán todas 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. Los proveedores de servicios de pago también se asegurarán 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.

3.6. Los proveedores de servicios de pago se asegurarán de que, si el incidente está causado por una interrupción de los servicios proporcionados por un proveedor de servicios técnicos (o una infraestructura) que afecta a varios PSP, la notificación delegada haga referencia a la información individual del proveedor de servicios de pago (excepto en el caso de una notificación consolidada).

Directriz 4: Política operativa y de seguridad

4.1. Los proveedores de servicios de pago se asegurarán de que su política operativa y de seguridad general defina claramente todas las responsabilidades en relación con la notificación de incidentes conforme a la PSD2, así como los procesos implementados con el fin de 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 evaluarán 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 ha recibido una amplia cobertura mediática.

5.2. Las autoridades competentes del Estado miembro de origen llevarán 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 proporcionarán información sobre los incidentes operativos o de seguridad graves a las autoridades nacionales pertinentes identificadas siguiendo la Directriz 5.1, 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 informe intermedio).

6.2. Las autoridades competentes presentarán a las autoridades nacionales pertinentes la información necesaria para transmitir una idea clara de lo ocurrido y de las posibles consecuencias. Para ello, proporcionarán, 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 clasificación del incidente como grave.
- Fecha y hora de detección del incidente.
- Fecha y hora de inicio del incidente.
- Fecha y hora en que el incidente fue resuelto o se espera que se resuelva.
- 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 proveedores de servicios de pago o infraestructuras.
- Descripción de la cobertura mediática (si la hubiera).
- Causa del incidente.

6.3. Las autoridades competentes llevarán a cabo la anonimización apropiada, según sea necesario, y excluirán toda información que pudiera estar sujeta a restricciones de confidencialidad o de propiedad intelectual antes de compartir cualquier información relacionada con los incidentes con las autoridades nacionales pertinentes. Sin embargo, las autoridades competentes proporcionarán a las 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 preservarán en todo momento la confidencialidad y la integridad de la información almacenada e intercambiada y también se autenticarán adecuadamente ante las autoridades nacionales pertinentes. En particular, las autoridades competentes tratarán 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 compartir con la ABE y el BCE y sobre el formato y los procedimientos para su comunicación

Directriz 7: Información que se debe compartir

7.1. Las autoridades competentes proporcionarán 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 utilizando un archivo estándar disponible en el sitio web de la ABE.

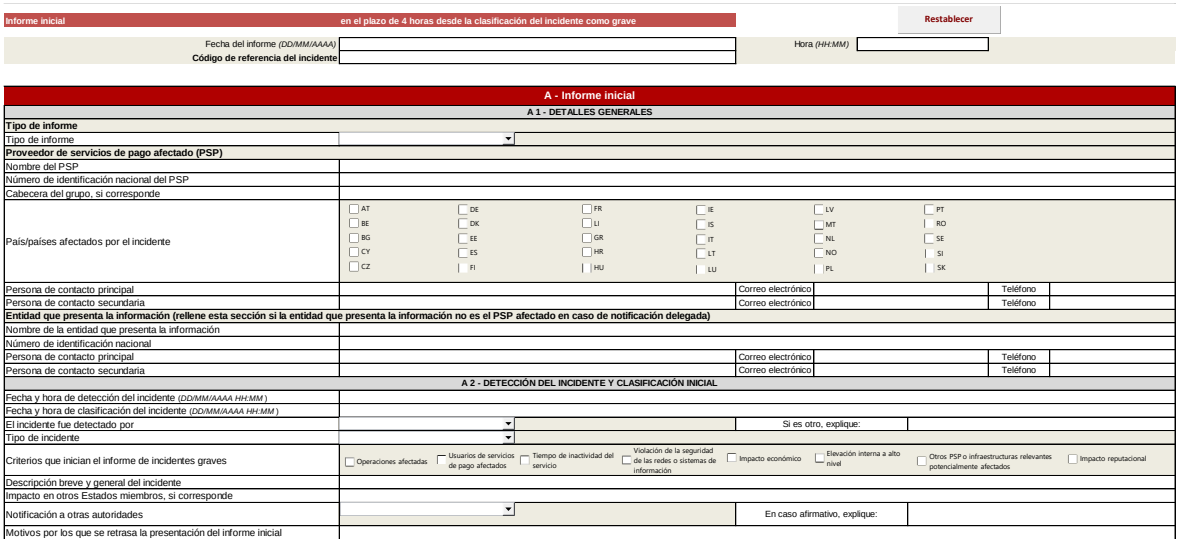
Directriz 8: Comunicación

8.1. Las autoridades competentes preservarán en todo momento la confidencialidad y la integridad de la información almacenada e intercambiada y también se autenticarán adecuadamente ante la ABE y el BCE. En particular, las autoridades competentes tratarán 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 podrán utilizar medios de comunicación adecuados.

Anexo - Plantilla de notificación para proveedores de servicios de pago

Informe inicial



Informe inicial	en el plazo de 4 horas desde la clasificación del incidente como grave		Restablecer
Fecha del informe *(DD/MM/AAAA)*		Hora *(HH:MM)*	
Código de referencia del incidente			

A - Informe inicial					
A 1 - DETALLES GENERALES					
Tipo de informe					
Tipo de informe					
Proveedor de servicios de pago afectado (PSP)					
Nombre del PSP					
Número de identificación nacional del PSP					
Cabecera del grupo, si corresponde					
País/países afectados por el incidente	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ	☐ DE ☐ DK ☐ EE ☐ ES ☐ FI	☐ FR ☐ LI ☐ GR ☐ HR ☐ HU	☐ IE ☐ IS ☐ IT ☐ LT ☐ LU	☐ LV ☐ MT ☐ NL ☐ NO ☐ PL	☐ PT ☐ RO ☐ SE ☐ SI ☐ SK
Persona de contacto principal		Correo electrónico		Teléfono	
Persona de contacto secundaria		Correo electrónico		Teléfono	
Entidad que presenta la información (rellene esta sección si la entidad que presenta la información no es el PSP afectado en caso de notificación delegada)					
Nombre de la entidad que presenta la información					
Número de identificación nacional					
Persona de contacto principal		Correo electrónico		Teléfono	
Persona de contacto secundaria		Correo electrónico		Teléfono	
A 2 - DETECCIÓN DEL INCIDENTE Y CLASIFICACIÓN INICIAL					
Fecha y hora de detección del incidente *(DD/MM/AAAA HH:MM)*					
Fecha y hora de clasificación del incidente *(DD/MM/AAAA HH:MM)*					
El incidente fue detectado por		Si es otro, explique:			
Tipo de incidente					
Criterios que inician el informe de incidentes graves	☐ Operaciones afectadas ☐ Usuarios de servicios de pago afectados ☐ Tiempo de inactividad del servicio ☐ Violación de la seguridad de las redes o sistemas de información ☐ Impacto económico ☐ Elevación interna a alto nivel ☐ Otros PSP o infraestructuras relevantes potencialmente afectados ☐ Impacto reputacional				
Descripción breve y general del incidente					
Impacto en otros Estados miembros, si corresponde					
Notificación a otras autoridades		En caso afirmativo, explique:			
Motivos por los que se retrasa la presentación del informe inicial					

Informe intermedio

Informe de incidentes graves

Informe intermedio	en el plazo máximo de 3 días hábiles desde la presentación del informe inicial	Restablecer selecciones

Fecha del informe *(DD/MM/AAAA)* | Hora *(HH:MM)*

Código de referencia del incidente

B - Informe intermedio

B 1 - DETALLES GENERALES

Proporcione una descripción más detallada del incidente:

¿Cuál es el problema específico?	
¿Cómo se inició el incidente?	
¿Cómo se desarrolló el incidente?	
¿Cuáles son las consecuencias (en concreto para los usuarios del servicio de pago)?	
¿Se comunicó el incidente a los usuarios del servicio de pago?	En caso afirmativo, explique:
¿Estaba relacionado con un incidente o incidentes anteriores?	En caso afirmativo, explique:
¿Se vieron afectados o involucrados otros prestadores de servicios/terceros?	En caso afirmativo, explique:
¿Se inició una gestión de crisis (interna y/o externa)?	En caso afirmativo, explique:
Fecha y hora de inicio del incidente (si ya se ha identificado) *(DD/MM/AAAA HH:MM)*	
Fecha y hora en que el incidente fue restaurado o se espera que se restaure *(DD/MM/AAAA HH:MM)*	
Áreas funcionales afectadas	☐ Autenticación/autorización ☐ Liquidación directa ☐ Comunicación ☐ Liquidación indirecta ☐ Compensación ☐ Otros — Si es Otro, especifique:
Cambios realizados en informes anteriores	

B 2 - CLASIFICACIÓN DEL INCIDENTE/INFORMACIÓN SOBRE EL INCIDENTE

Operaciones afectadas [2]	Nivel de impacto Número de operaciones afectadas En % del número habitual de operaciones Importe de las operaciones afectadas en EUR Duración del incidente (aplicable solo para incidentes operativos) Observaciones
Usuarios de servicios de pago afectados [3]	Nivel de impacto Número de usuarios de servicios de pago afectados En % del total de usuarios de servicios de pago
Violación de la seguridad de las redes y sistemas de información	Describa cómo las redes o sistemas de información se han visto afectados
Tiempo de inactividad del servicio	Tiempo total de inactividad del servicio: Días: Horas: Minutos:
Impacto económico	Nivel de impacto Costes directos en EUR Costes indirectos en EUR
Elevación interna a alto nivel	Describa el nivel de elevación interna del incidente a cargos superiores, indicando si se ha activado o es posible que se active un modo de crisis (o equivalente) y, en caso afirmativo, descríbalo
Otros PSP o infraestructuras relevantes potencialmente afectados	Describa en qué medida este incidente podría afectar a otros PSP o infraestructuras
Incidencia sobre la reputación	Describa en qué medida el incidente podría afectar a la reputación del PSP (por ejemplo, cobertura mediática, publicación de acciones legales o infracciones normativas, etc.).

B 3 - DESCRIPCIÓN DEL INCIDENTE

Tipo de incidente	
Causa del incidente	☐ Bajo investigación ☐ Acción maliciosa ☐ Fallo del proceso ☐ Fallo del sistema ☐ Errores humanos ☐ Eventos externos ☐ Otros — Si es Otro, especifique:
¿El incidente le afectó directamente, o indirectamente a través de un proveedor de servicios?	Si es indirectamente, proporcione el nombre del proveedor de servicios:

B 4 - IMPACTO DEL INCIDENTE

Impacto general	☐ Integridad	☐ Confidencialidad	
	☐ Disponibilidad	☐ Autenticidad	
Canales comerciales afectados	☐ Sucursales	☐ Banca telefónica	☐ Punto de venta
	☐ Banca electrónica	☐ Banca móvil	☐ Otros
	☐ Comercio electrónico	☐ Cajeros automáticos	
	Si es Otro, especifique:		
Servicios de pago afectados	☐ Ingreso de efectivo en una cuenta de pago	☐ Transferencias	☐ Servicio de envío
	☐ Retirada de efectivo de una cuenta de pago	☐ Adeudos domiciliados	☐ Servicios de
	☐ Operaciones necesarias para operar una cuenta de pago	☐ Pagos con tarjeta	☐ Servicios de información sobre cuentas
	☐ Adquisición de instrumentos de pago	☐ Emisión de instrumentos de pago	

B 5 - MITIGACIÓN DEL INCIDENTE

¿Qué acciones/medidas se han adoptado hasta ahora o se prevé adoptar para recuperarse del incidente?	
¿Se ha activado el Plan de Continuidad de la Actividad o el Plan de Recuperación en caso de Catástrofes?	
En caso afirmativo, ¿cuándo? *(DD/MM/AAAA HH:MM)*	
En caso afirmativo, describa	

Informe final

Informe de incidentes graves

Seleccione el tipo de informe:

en el plazo de 20 días hábiles tras la presentación del informe intermedio

Describa:
(aplicable para incidentes reclasificados como no graves)

Restablecer selecciones desplegables

Fecha del informe *(DD/MM/AAAA)* | Hora *(HH:MM)*

Código de referencia del incidente

C - Informe final

Si no se ha enviado ningún informe intermedio, rellénese también la sección B

C 1 - DETALLES GENERALES

Actualización de la información del informe inicial y del informe o los informes intermedios

Cambios realizados en informes anteriores	
Cualquier otra información pertinente	
¿Están todos los controles originales en vigor?	
En caso negativo, especifique qué controles y el período adicional necesario para restaurarlos	

C 2 - ANÁLISIS DE LA CAUSA DE FONDO Y SEGUIMIENTO

¿Cuál fue la causa de fondo (si ya se conoce)?

☐ Acción maliciosa ☐ Fallo del proceso ☐ Fallo del sistema ☐ Error humano ☐ Evento externo ☐ Otros

Se ruega especificar:

Acción maliciosa	Fallo del proceso	Fallo del sistema	Error humano	Evento externo
Código malicioso	Control y seguimiento deficientes	Fallo del hardware	Involuntario	Fallo de un proveedor/prestador de servicios técnicos
Recogida de información	Problemas de comunicación	Fallo de red	Inacción	Fuerza mayor
Intrusiones	Operaciones incorrectas	Problemas con la aplicación/software	Insuficiencia de recursos	Otros
Ataque de denegación de servicio/distribuida (D/DoS)	Gestión inadecuada del cambio	Fallo de aplicación/software	Otros	
Acciones internas deliberadas	Insuficiencia de procedimientos y documentación internos	Daños físicos		
Daños físicos externos deliberados	Problemas de recuperación	Otros		
Seguridad del contenido informático	Otros			
Acciones				
Otros				

Si es Otro, especifique:

Otra información pertinente sobre la causa de fondo	
Principales medidas de corrección/medidas adoptadas o previstas para evitar que el incidente vuelva a ocurrir en el futuro, si ya se conocen	

C 3 - INFORMACIÓN ADICIONAL

¿Se ha compartido el incidente con otros PSP con fines informativos?	En caso afirmativo, proporcione los detalles:
¿Se han emprendido acciones legales contra el PSP?	En caso afirmativo, proporcione los detalles:
Evaluación de la eficacia de la medida adoptada	Proporcione detalles:

INSTRUCCIONES PARA CUMPLIMENTAR LA PLANTILLA

Los proveedores de servicios de pago (PSP) 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. Los PSP usarán la misma plantilla cuando presenten los informes inicial, intermedio y final relativos al mismo incidente. Todos los campos son obligatorios, a menos que se indique claramente lo contrario.

Encabezamiento

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

Informe intermedio: incluye una descripción más detallada del incidente y sus consecuencias. Es una actualización del informe inicial (y, si procede, de un informe intermedio anterior) sobre el mismo incidente.

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

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 clasificación.

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

Código de referencia del incidente (aplicable para informes intermedios y final, así como para actualizaciones del informe inicial): el código de referencia emitido por la autoridad competente en el momento del informe inicial para identificar de forma inequívoca el incidente. Cada autoridad competente incluirá como prefijo el código ISO de dos dígitos[2] de su Estado miembro correspondiente.

A - Informe inicial

A 1 - Datos generales

Tipo de informe:

Individual: el informe se refiere a un único PSP.

Consolidado: el informe se refiere a varios PSP en el mismo Estado miembro afectados por el mismo incidente operativo o de seguridad grave, que utilizan la opción de notificación consolidada. Los campos del apartado «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 nacional del PSP: el número de identificación nacional único utilizado por la autoridad competente del Estado miembro de origen en su registro nacional para identificar al PSP inequívocamente.

Cabecera del grupo: en el caso de grupos de entidades, tal como se definen en el artículo 4, apartado 40, de la PSD2, indique el nombre de la entidad cabecera.

País/países afectados por el incidente: país o países en los que se ha materializado el impacto del incidente (por ejemplo, se ven afectadas varias sucursales del PSP radicadas en distintos

[2] Consúltense los códigos de países alfa-2 en virtud de la norma ISO-3166 en https://www.iso.org/iso-3166-country-codes.html

países), con independencia de la gravedad del incidente en el otro país/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 fuera 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 fuera 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, si procede.

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 nacional: el número de identificación nacional único utilizado en el país donde está radicado el tercero para identificar inequívocamente a la entidad que informa del incidente. Si el tercero que realiza la notificación es un PSP, el número de identificación nacional debe ser el número de identificación nacional único del PSP utilizado por la autoridad competente del Estado miembro de origen en su registro nacional.

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 fuera necesario. Puede ser un número de teléfono personal o de empresa.

Persona de contacto secundaria: nombre y apellido de una persona alternativa en 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 fuera 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 por primera vez.

Fecha y hora de clasificación del incidente: fecha y hora en que el incidente operativo o de seguridad se clasificó como grave.

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

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

> **Operativo:** incidente derivado de la intervención humana, de procesos inadecuados o defectuosos, de fallos en los sistemas o de eventos de fuerza mayor que afectan a la integridad, la disponibilidad, la confidencialidad o la autenticidad de los servicios relacionados con el pago.
>
> **De seguridad:** acceso, uso, revelación, interrupción, modificación o destrucción no autorizados de los activos del PSP que afectan a la integridad, la disponibilidad, la confidencialidad o la autenticidad de los servicios relacionados con el pago. Esto puede ocurrir, entre otros casos, cuando el PSP sufre una violación de la seguridad de las redes o sistemas de información.

Criterios que motivan el informe de incidentes graves: indique qué criterios han motivado la notificación del incidente grave. Se pueden seleccionar varias opciones entre los criterios: operaciones afectadas, usuarios del servicio de pago afectados, tiempo de inactividad del servicio, violación de la seguridad de las redes o sistemas de información, impacto económico, elevación interna a alto nivel, otros PSP o infraestructuras relevantes potencialmente afectados, o impacto reputacional.

Descripción breve y general del incidente: explique brevemente los aspectos más relevantes del incidente, indicando las posibles causas, impactos inmediatos, etc.

Impacto en otros Estados miembros de la UE, si corresponde: explique brevemente el impacto que el incidente tuvo en otro Estado miembro de la UE (por ejemplo, en usuarios de servicios de pago, PSP o infraestructuras de pagos). Si fuera posible dentro de los plazos aplicables a la notificación, facilite una traducción al inglés.

Notificación a otras autoridades: indique si el incidente ha sido notificado o será notificado a otras autoridades conforme a distintos marcos de comunicación de incidentes, si se conoce en el momento de presentar la notificación. En caso afirmativo, especifique las autoridades pertinentes.

Motivos por los que se retrasa la presentación del informe inicial: explique los motivos por los que necesitó más de 24 horas para clasificar el incidente.

B Informe intermedio

B 1 – Datos generales

Descripción más detallada del incidente: describa las principales características del incidente, indicando al menos la información sobre el problema específico y sus antecedentes, la descripción de cómo se inició y desarrolló el incidente, así como las consecuencias, en particular para los usuarios del servicio de pago, etc. Facilite también información sobre la comunicación con los usuarios del servicio de pago, si procede.

¿Estaba relacionado con un incidente o incidentes anteriores?: indique si el incidente estaba relacionado o no con incidentes anteriores, si se dispone de esta información. Si el incidente se ha relacionado con incidentes anteriores, especifique cuáles.

¿Se vieron afectados o involucrados otros proveedores de servicios/terceros?: indique si el incidente ha afectado o involucrado a otros proveedores de servicios o terceros, si se dispone de esta información. Si el incidente ha afectado o involucrado a otros proveedores de servicios o terceros, facilite una lista de los mismos junto con información adicional.

¿Se inició una gestión de crisis (interna o externa)?: indique si se inició o no una gestión de crisis (interna o externa). Si se inició dicha gestión de crisis, facilite información adicional.

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

Fecha y hora en que el incidente fue resuelto o se espera que sea resuelto: 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.

Áreas funcionales afectadas: indique la fase o fases del proceso de pago que se han visto afectadas por el incidente, como autenticación o autorización, comunicación, compensación, liquidación directa, liquidación indirecta y otras.

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 las 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.

Comunicación: flujo de información con fines de identificación, autenticación, notificación e información entre los PSP que prestan servicio en las cuentas 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 la 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.

Otra: el área funcional afectada no es ninguna de las anteriores. Se deben proporcionar más detalles en el campo de texto libre.

Cambios realizados respecto a informes anteriores: indique los cambios realizados en la información proporcionada en informes anteriores relativos al mismo incidente (por ejemplo, el informe inicial o, si procede, un informe intermedio).

B 2 – Clasificación del incidente/Información sobre el incidente

Operaciones afectadas: Los PSP indicarán los umbrales que, en su caso, el incidente ha alcanzado o probablemente alcanzará 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 proporcionarán valores concretos para estas variables, que pueden ser cifras reales o estimaciones. Como regla general, los PSP entenderán por «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 entenderán 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), utilizarán otra métrica más representativa y comunicarán a la autoridad competente la justificación de su elección

en el campo «Comentarios». En los casos en los que las operaciones de pago con monedas distintas al euro se vean afectadas por el incidente, a la hora de calcular los umbrales y de notificar el valor de las operaciones afectadas, los PSP convertirán a euros el importe de las operaciones en una moneda distinta al euro utilizando el tipo de cambio diario de referencia del BCE del día previo a la notificación del incidente.

Usuarios de servicios de pago afectados: Los PSP indicarán los umbrales que, en su caso, el incidente ha alcanzado o probablemente alcanzará, 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 proporcionarán valores concretos para estas variables, que pueden ser cifras reales o estimaciones. Los PSP entenderán por «usuarios de servicios de pago afectados» todos los clientes (nacionales o extranjeros, consumidores o empresas) que tienen un contrato con el PSP afectado que les permite acceder al servicio de pago afectado y que han sufrido o probablemente sufrirán las consecuencias del incidente. Los PSP recurrirán 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 considerará únicamente sus propios usuarios de servicios de pago. Un PSP que ofrezca servicios operativos a otros PSP solamente considerará sus propios usuarios de servicios de pago (si los hubiera), y los PSP que reciban estos servicios operativos también evaluarán el incidente en relación con sus propios usuarios de servicios de pago. Por otra parte, los PSP tomarán 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.

Violación de la seguridad de las redes o sistemas de información: Los PSP determinarán si alguna acción maliciosa ha comprometido la disponibilidad, autenticidad, integridad o confidencialidad de las redes o los sistemas de información (incluidos los datos) relacionados con la prestación de servicios de pago.

Tiempo de inactividad del servicio: Los PSP indicarán si el incidente ha alcanzado o es probable que alcance el umbral, y la cifra correspondiente: tiempo total de inactividad del servicio. Los PSP proporcionarán valores concretos para esta variable, que pueden consistir en cifras reales o en estimaciones. Los PSP considerarán 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 contarán el tiempo de inactividad del servicio desde el momento en que comienza la inactividad y considerarán 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. Excepcionalmente, si los proveedores de servicios de pago no pueden determinar cuándo se inició la inactividad del servicio, contarán el tiempo de inactividad del servicio desde el momento en el que se detecta la inactividad.

Impacto económico: Los PSP indicarán si el incidente ha alcanzado o es probable que alcance el umbral, y las cifras correspondientes: costes directos e indirectos. Los PSP proporcionarán valores concretos para estas variables, que pueden ser cifras reales o estimaciones. Los PSP considerarán 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 tendrán 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 las obligaciones contractuales, las sanciones, las responsabilidades externas y la pérdida de ingresos. Por lo que respecta a los costes indirectos, los PSP considerarán solo los que ya son conocidos o que es muy probable que se materialicen. En los casos de costes en monedas distintas al euro, a la hora de calcular los umbrales y de notificar el valor del impacto

económico, los PSP convertirán a euros el importe de los costes en una moneda distinta al euro utilizando el tipo de cambio diario de referencia del BCE del día previo a la presentación del informe del incidente.

Costes directos: importe (en euros) del coste directamente imputable al incidente, incluidos los costes para corregir el incidente (por ejemplo, fondos o activos expropiados, costes de sustitución de *hardware* y *software*, costes derivados del incumplimiento de las obligaciones contractuales).

Costes indirectos: importe (en euros) del coste indirectamente imputable al incidente (por ejemplo, costes de reparación/indemnización de clientes, posibles costes legales).

Elevación interna a alto nivel: Los PSP considerarán si, como consecuencia del impacto del incidente en los servicios relacionados con el pago, el órgano de dirección, tal como se define en las Directrices de la ABE sobre gestión de riesgos de TIC y de seguridad, ha sido o probablemente será informado, conforme a la Directriz 60, apartado d), de las Directrices de la ABE sobre gestión de riesgos de TIC y de seguridad, 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 considerarán 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 PSP evaluarán el impacto del incidente sobre el mercado financiero, entendido como las infraestructuras de los mercados financieros o los esquemas de pago que lo respaldan, así como otros PSP. En particular, los PSP evaluarán 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 tendrán 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 o 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.

Impacto reputacional: Los PSP considerarán el nivel de visibilidad que, a su leal saber y entender, el incidente ha alcanzado o probablemente alcanzará en el mercado. En particular, los PSP considerarán 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 tendrán en cuenta i) si los usuarios de servicios de pago u otros PSP se han quejado del impacto negativo del incidente, ii) si el incidente ha afectado a un proceso visible relacionado con el servicio de pago y, por lo tanto, es probable que reciba o ya ha recibido cobertura mediática (considerando no solo los medios tradicionales, como periódicos, sino también blogs, redes sociales, etc.; no obstante, por cobertura mediática en este contexto no solo se entienden unos pocos comentarios negativos de seguidores, sino que debe existir un informe válido o una cantidad importante de alertas/comentarios negativos), iii) si no se han cumplido o probablemente no se cumplirán las obligaciones contractuales, lo que ha dado o probablemente dará lugar al inicio de acciones legales contra el proveedor de servicios de pago, iv) si no se han cumplido las obligaciones normativas, lo que ha provocado la imposición de sanciones o medidas supervisoras que se han publicado o probablemente se harán públicas, o v) si el mismo tipo de incidente ha ocurrido anteriormente.

B 3 – Descripción del incidente

Tipo de incidente: operativo o de seguridad. Se facilita información adicional en el campo correspondiente del informe inicial.

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: marque la casilla cuando la causa siga siendo desconocida.

Acción maliciosa: acciones que están dirigidas intencionadamente al PSP. Esto abarca código malicioso, obtención de información, intrusiones, ataque de denegación de servicio/distribuido (D/DoS), acciones internas deliberadas, daños físicos externos deliberados, compromiso de la información, acciones fraudulentas y otras. Para más información, consulte la sección C2 de esta plantilla.

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, monitorización).

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, redes, infraestructuras y bases de datos que soportan la actividad de pago.

Errores humanos: el incidente fue causado por el error involuntario de una persona, ya sea como parte del procedimiento de pago (por ejemplo, cargar un fichero 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).

Eventos externos: la causa se asocia con eventos que están generalmente fuera del control directo de la organización (por ejemplo, desastres naturales, un fallo de un proveedor de servicios técnicos).

Otra: 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 directamente, o indirectamente a través de un proveedor de servicios?: indique si el incidente estaba directamente dirigido al PSP o le afecta de manera indirecta a través de un tercero, si se dispone de esta información. En el caso de un impacto indirecto, indique el nombre del proveedor o proveedores de servicios.

B 4 – Impacto del incidente

Impacto general: indique qué aspectos se han visto afectados por el incidente operativo o de seguridad. Se pueden marcar varias casillas.

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

Disponibilidad: propiedad de garantizar la accesibilidad y la capacidad de utilizar los servicios relacionados con el pago por parte de los usuarios de servicios de pago, conforme a los niveles aceptables previamente definidos.

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.

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

Sucursales: centro de actividad (distinto de la administración central) 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 administración central en otro Estado miembro se considerarán 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: dispositivo electromecánico que permite a los usuarios de servicios de pago retirar efectivo de sus cuentas o acceder a otros servicios.

Punto de venta: instalación física del comerciante en el que se inicia la operación de pago.
Comercio electrónico: la operación de pago se inicia en un punto de venta virtual (por ejemplo, en el caso de pagos iniciados a través de Internet utilizando transferencias, tarjetas de pago, transferencia de dinero electrónico entre cuentas de dinero electrónico).
Otro: el canal comercial afectado no es ninguno de los anteriores. Se deben proporcionar más 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 gestionar de una cuenta de pago: las acciones necesarias 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 parte del 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 PSP del beneficiario o al propio PSP del 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, dispositivo 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: un 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: un servicio de pago que permite 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: un servicio 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.

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 de Desastres?: 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).

C – Informe final

C 1 – Datos generales

Actualización de la información del informe inicial y del informe o los informes intermedios (resumen): proporcione información adicional sobre el incidente, incluidos los cambios específicos realizados respecto a la información facilitada en el informe intermedio. Incluya también cualquier otra información pertinente.

¿Se han restaurado todos los controles originales?: indique si el PSP tuvo que anular o suavizar algunos controles en algún momento durante el incidente. En caso afirmativo, indique si se han vuelto a restaurar todos los controles y, de no ser así, explique en el campo de texto libre qué controles no se han restaurado y el período adicional necesario para restaurarlos.

C 2 – Análisis de la causa raíz y seguimiento

¿Cuál fue la causa raíz (si ya se conoce)?: indique la causa raíz del incidente o, si aún no se conoce, su causa más probable. Se pueden marcar varias casillas. (Recuerde que la causa raíz debe diferenciarse del impacto del incidente).

Acción maliciosa: acciones internas o externas que están dirigidas intencionadamente al PSP. Se pueden clasificar en las categorías siguientes:

Código malicioso: por ejemplo, un virus, gusano, troyano, programas espía.

Obtención de información: por ejemplo, escaneo de redes, *sniffing*, ingeniería social.

Intrusiones: por ejemplo, compromiso de cuenta con privilegios, compromiso de cuenta sin privilegios, compromiso de aplicaciones, bot.

Ataque de denegación de servicio/distribuido (D/DoS): un intento de impedir la disponibilidad de un servicio en línea sobrecargándolo con tráfico procedente de múltiples fuentes.

Acciones internas deliberadas: por ejemplo, sabotaje, robo.

Daños físicos externos deliberados: por ejemplo, sabotaje, ataque físico a instalaciones/centros de datos.

Compromiso de la información: acceso no autorizado a información, modificación no autorizada de información.

Acciones fraudulentas: uso no autorizado de recursos, derechos de autor, suplantación, *phishing*.

Otra (se ruega especificar): la causa del incidente no es ninguna de las anteriores. Se deben proporcionar más detalles en el campo de texto libre.

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, monitorización). Se pueden clasificar en las categorías siguientes:

Control y monitorización deficientes: por ejemplo, en relación con la operativa del proceso, fechas de vencimiento de certificados, fechas de vencimiento de licencias, fechas de vencimiento de parches de seguridad, valores de contadores máximos definidos, niveles de capacidad de almacenamiento de las bases de datos, gestión de los derechos del usuario, principio de control dual.

Problemas de comunicación: por ejemplo, entre los participantes en el mercado o dentro de la organización.

Incorrecta operativa del proceso: por ejemplo, falta de intercambio de certificados, caché llena.

Inadecuada Gestión del cambio: por ejemplo, errores de configuración no identificados, de implementación (incluidas actualizaciones), problemas de mantenimiento, errores inesperados.

Insuficiencia de procedimientos internos y documentación: por ejemplo, falta de transparencia en cuanto a las funcionalidades, procesos y aparición de un fallo, ausencia de documentación.

Problemas de recuperación: por ejemplo, gestión de contingencias, redundancia inadecuada.

Otro (se ruega especificar): la causa del incidente no es ninguna de las anteriores. Se deben proporcionar más detalles en el campo de texto libre.

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, redes, infraestructuras y bases de datos que soportan la actividad de pago. Se pueden clasificar en las categorías siguientes:

Fallo del *hardware*: fallo del equipo de tecnología física que ejecuta los procesos o almacena los datos que los PSP necesitan para realizar su actividad relacionada con el pago (por ejemplo, fallo de unidades de disco duro, centros de datos, otra infraestructura).

Fallo de red: fallo en las redes de telecomunicaciones, públicas o privadas, que permiten el intercambio de datos e información (por ejemplo, a través de Internet) durante el proceso de pago.

Problemas con la base de datos: estructuración de los datos que almacenan la información personal y relacionada con el pago necesaria para ejecutar las operaciones de pago.

Fallo de aplicación/*software*: fallos en programas, sistemas operativos, etc., que soportan la prestación de servicios de pago por parte del PSP (por ejemplo, mal funcionamiento, funciones desconocidas).

Daños físicos: por ejemplo, daños involuntarios causados por unas condiciones inadecuadas, obras de construcción.

Otro (se ruega especificar): la causa del incidente no es ninguna de las anteriores. Se deben proporcionar más detalles en el campo de texto libre.

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 fichero 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). Se pueden clasificar en las categorías siguientes:

Involuntario: por ejemplo, errores, omisiones, falta de experiencia y conocimiento.

Inacción: por ejemplo, debido a falta de competencias, conocimientos, experiencia o concienciación.

Insuficiencia de recursos: por ejemplo, falta de personal, disponibilidad del personal.

Otro (se ruega especificar): la causa del incidente no es ninguna de las anteriores. Se deben proporcionar más detalles en el campo de texto libre.

Evento externo: la causa se asocia con eventos generalmente fuera del control de la organización. Se pueden clasificar en las categorías siguientes:

Fallo de un proveedor/proveedor de servicios técnicos: por ejemplo, fallo de alimentación eléctrica, problemas de conexión a Internet, problemas jurídicos, problemas empresariales, dependencias del servicio.

Fuerza mayor: por ejemplo, fallo de alimentación eléctrica, incendio, catástrofes naturales tales como terremotos, inundaciones, precipitaciones intensas, fuerte viento.

Otro (se ruega especificar): la causa del incidente no es ninguna de las anteriores. Se deben proporcionar más detalles en el campo de texto libre.

Otra: la causa del incidente no es ninguna de las anteriores. Se deben proporcionar más detalles en el campo de texto libre.

Otra información pertinente sobre la causa raíz: facilite todos los detalles adicionales sobre la causa raíz, incluidas las conclusiones preliminares extraídas del análisis de la causa raíz.

Principales acciones correctivas/medidas adoptadas o previstas para evitar que el incidente vuelva a ocurrir en el futuro, si ya se conocen: describa 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.

Evaluación de la eficacia de la medida adoptada: incluya, cuando proceda, una autoevaluación de la eficacia de las medidas adoptadas durante el período de duración del incidente, incluidas las lecciones aprendidas del incidente.