►B

REGLAMENTO DELEGADO (UE) 2018/389 DE LA COMISIÓN

de 27 de noviembre de 2017

por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros

(Texto pertinente a efectos del EEE)

(DO L 69 de 13.3.2018, p. 23)

Rectificado por:

►C1 Rectificación, DO L 88 de 24.3.2020, p. 11 (2018/389)

▼B

REGLAMENTO DELEGADO (UE) 2018/389 DE LA COMISIÓN

de 27 de noviembre de 2017

por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros

(Texto pertinente a efectos del EEE)

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto

El presente Reglamento establece los requisitos que deben cumplir los proveedores de servicios de pago a efectos de la aplicación de medidas de seguridad que les permitan hacer lo siguiente:

a) aplicar el procedimiento de autenticación reforzada de clientes, de conformidad con el artículo 97 de la Directiva (UE) 2015/2366;

b) eximir de la aplicación de los requisitos de seguridad de la autenticación reforzada de clientes, bajo determinadas condiciones limitadas y basadas en el nivel de riesgo, el importe de la operación de pago y la frecuencia con que se repite, y el canal de pago empleado para la ejecución de dicha operación;

c) proteger la confidencialidad y la integridad de las credenciales de seguridad personalizadas del usuario de servicios de pago;

d) establecer estándares abiertos comunes y seguros para la comunicación entre los proveedores de servicios de pago gestores de cuenta, los proveedores de servicios de iniciación de pagos, los proveedores de servicios de información sobre cuentas, los ordenantes, los beneficiarios y otros proveedores de servicios de pago en relación con la provisión y la utilización de servicios de pago en aplicación del título IV de la Directiva (UE) 2015/2366.

Artículo 2

Requisitos generales de autenticación

1. Los proveedores de servicios de pago dispondrán de mecanismos de supervisión de las operaciones que les permitan detectar operaciones de pago no autorizadas o fraudulentas a efectos de la aplicación de las medidas de seguridad a que se hace referencia en el artículo 1, letras a) y b).

Dichos mecanismos se basarán en el análisis de las operaciones de pago teniendo en cuenta los elementos que caractericen al usuario de servicios de pago en el contexto de un uso normal de las credenciales de seguridad personalizadas.

▼B

2. Los proveedores de servicios de pago garantizarán que los mecanismos de supervisión de las operaciones tengan en cuenta, como mínimo, todos los factores basados en el riesgo siguientes:

a) listas de elementos de autenticación comprometidos o sustraídos;

b) el importe de cada operación de pago;

c) supuestos de fraude conocidos en la prestación de servicios de pago;

d) señales de infecciones por programas informáticos maliciosos en cualquier sesión del procedimiento de autenticación;

e) en caso de que el dispositivo o el programa informático de acceso sea facilitado por el proveedor de servicios de pago, un registro de la utilización del dispositivo o el programa informático de acceso facilitado al usuario de los servicios de pago y de su uso anormal.

Artículo 3

Revisión de las medidas de seguridad

1. La aplicación de las medidas de seguridad a que se refiere el artículo 1 deberá documentarse, probarse periódicamente, evaluarse y auditarse de conformidad con el marco jurídico aplicable al proveedor de servicios de pago por auditores con experiencia en el ámbito de la seguridad y los pagos informáticos y funcionalmente independientes, ya pertenezcan al organigrama del propio proveedor de servicios de pago o sean externos a él.

2. El período entre las auditorías a que se refiere el apartado 1 se determinará teniendo en cuenta el correspondiente marco aplicable al proveedor de servicios de pago en materia de contabilidad y de auditoría legal.

No obstante, los proveedores de servicios de pago que se acojan a la exención a que se refiere el artículo 18 estarán sujetos, como mínimo con una periodicidad anual, a una auditoría de la metodología, el modelo y los índices de fraude notificados. El auditor que lleve a cabo dicha auditoría poseerá conocimientos técnicos en el ámbito de la seguridad y los pagos informáticos y será funcionalmente independiente, ya pertenezca al organigrama del propio proveedor de servicios de pago o sea externo a él. Durante el primer año de uso de la exención prevista en el artículo 18 y al menos cada tres años en lo sucesivo, o con mayor frecuencia si así lo solicita la autoridad competente, esta auditoría será llevada a cabo por un auditor externo cualificado e independiente.

3. Esta auditoría presentará una evaluación de la conformidad de las medidas de seguridad adoptadas por el proveedor de servicios de pago con los requisitos establecidos en el presente Reglamento, y un informe al respecto.

El informe completo deberá ponerse a disposición de las autoridades competentes, a petición de estas.

▼B

CAPÍTULO II

MEDIDAS DE SEGURIDAD PARA LA APLICACIÓN DE LA AUTENTICACIÓN REFORZADA DE CLIENTES

Artículo 4

Código de autenticación

1. Cuando los proveedores de servicios de pago apliquen la autenticación reforzada de clientes, de conformidad con el artículo 97, apartado 1, de la Directiva (UE) 2015/2366, la autenticación se basará en dos o más elementos categorizados como conocimiento, posesión e inherencia y tendrá como resultado la generación de un código de autenticación.

El código de autenticación únicamente será aceptado por el proveedor de servicios de pago una sola vez cuando el ordenante lo use para acceder a su cuenta de pago en línea, para iniciar una operación de pago electrónico o para llevar a cabo cualquier acción a través de un canal remoto que pueda entrañar un riesgo de fraude en el pago u otros abusos.

2. A efectos del apartado 1, los proveedores de servicios de pago adoptarán medidas de seguridad que garanticen el cumplimiento de todos los requisitos siguientes:

a) que la divulgación del código de autenticación no permita derivar información alguna sobre ninguno de los elementos a que se refiere el apartado 1;

b) que no sea posible crear un nuevo código de autenticación basado en el conocimiento de cualquier otro código de autenticación generado anteriormente;

c) que el código de autenticación no pueda ser falsificado.

3. Los proveedores de servicios de pago garantizarán que la autenticación mediante la generación de un código de autenticación implique todas las medidas siguientes:

a) cuando la autenticación para el acceso remoto, los pagos remotos electrónicos y cualesquiera otras acciones a través de un canal remoto que puedan entrañar un riesgo de fraude en el pago u otros abusos no haya logrado generar un código de autenticación a efectos de lo dispuesto en el apartado 1, no será posible determinar cuál de los elementos mencionados en dicho apartado era incorrecto;

b) el número de intentos fallidos de autenticación que pueden tener lugar consecutivamente, alcanzado el cual las acciones a que se hace referencia en el artículo 97, apartado 1, de la Directiva (UE) 2015/2366 se bloquearán temporal o permanentemente, no excederá de cinco dentro de un período de tiempo determinado;

c) las sesiones de comunicación estarán protegidas contra la captación de los datos de autenticación transmitidos durante esta y contra la manipulación por personas no autorizadas, de conformidad con los requisitos establecidos en el capítulo V;

▼B

d) el tiempo máximo sin actividad del ordenante después de que este haya procedido a su autenticación para acceder a su cuenta de pago en línea no excederá de cinco minutos.

4. En caso de que el bloqueo a que se refiere el apartado 3, letra b), sea temporal, la duración de dicho bloqueo y el número de reintentos se determinarán en función de las características del servicio prestado al ordenante y de todos los riesgos pertinentes conexos, teniendo en cuenta, como mínimo, los factores a que se refiere el artículo 2, apartado 2.

Deberá alertarse al ordenante antes de hacer permanente el bloqueo.

En caso de que el bloqueo se haya hecho permanente, deberá establecerse un procedimiento seguro que permita al ordenante recuperar el uso de los instrumentos de pago electrónico bloqueados.

Artículo 5

Vinculación dinámica

1. Cuando los proveedores de servicios de pago apliquen la autenticación reforzada de clientes, de conformidad con el artículo 97, apartado 2, de la Directiva (UE) 2015/2366, además de cumplir los requisitos del artículo 4 del presente Reglamento también deberán adoptar medidas de seguridad que reúnan todos los requisitos siguientes:

a) que el ordenante sea informado del importe de la operación de pago y del beneficiario;

b) que el código de autenticación generado sea específico para el importe y el beneficiario de la operación de pago aceptados por el ordenante al iniciar la operación;

c) que el código de autenticación aceptado por el proveedor de servicios de pago se corresponda con el importe específico original de la operación de pago y con la identidad del beneficiario aceptados por el ordenante;

d) que cualquier cambio del importe o del beneficiario suponga la invalidación del código de autenticación generado.

▼C1

2. A efectos del apartado 1, los proveedores de servicios de pago deberán adoptar medidas de seguridad que garanticen la confidencialidad, autenticidad e integridad de todos los siguientes elementos:

▼B

a) el importe de la operación y el beneficiario, en todas las fases de la autenticación;

b) la información que se muestre al ordenante en todas las fases de la autenticación, incluidas la generación, la transmisión y la utilización del código de autenticación.

3. A efectos del apartado 1, letra b), y en los casos en que los proveedores de servicios de pago apliquen la autenticación reforzada de clientes, de conformidad con el artículo 97, apartado 2, de la Directiva (UE) 2015/2366, se aplicarán los siguientes requisitos al código de autenticación:

▼B

a) en relación con una operación de pago con tarjeta para la que el ordenante haya dado su consentimiento respecto del importe exacto de los fondos que han de bloquearse, con arreglo al artículo 75, apartado 1, de la citada Directiva, el código de autenticación será específico para el importe que el ordenante haya aprobado al iniciarse la operación y a cuyo bloqueo haya dado su consentimiento;

b) en relación con las operaciones de pago para las que el ordenante haya dado su consentimiento respecto de la ejecución de un lote de operaciones remotas electrónicas a uno o varios beneficiarios, el código de autenticación será específico para el importe total del lote de operaciones de pago y para los beneficiarios específicos.

Artículo 6

Requisitos de los elementos categorizados como conocimiento

1. Los proveedores de servicios de pago adoptarán medidas para mitigar el riesgo de que los elementos de autenticación reforzada de clientes categorizados como conocimiento se revelen o se divulguen a terceros no autorizados.

2. La utilización de dichos elementos por el ordenante estará sujeta a medidas de mitigación para evitar su divulgación a terceros no autorizados.

Artículo 7

Requisitos de los elementos categorizados como posesión

1. Los proveedores de servicios de pago adoptarán medidas para mitigar el riesgo de que los elementos de autenticación reforzada de clientes categorizados como posesión sean utilizados por terceros no autorizados.

2. La utilización de dichos elementos por el ordenante estará sujeta a medidas destinadas a evitar la replicación de los elementos.

Artículo 8

Requisitos aplicables a los dispositivos y programas informáticos vinculados a los elementos categorizados como inherencia

1. Los proveedores de servicios de pago adoptarán medidas para mitigar el riesgo de que los elementos de autenticación categorizados como inherencia y leídos por dispositivos y programas informáticos de acceso facilitados al ordenante se revelen a terceros no autorizados. Como mínimo, los proveedores de servicios de pago velarán por que esos dispositivos y programas informáticos de acceso permitan una muy baja probabilidad de que un tercero no autorizado sea autenticado como ordenante.

2. La utilización por el ordenante de dichos elementos estará sujeta a medidas que velen por que los dispositivos y los programas informáticos garantizan la resistencia contra un uso no autorizado de los elementos producido a través del acceso a los dispositivos y los programas informáticos.

▼B

Artículo 9

Independencia de los elementos

1. Los proveedores de servicios de pago se asegurarán de que el uso de los elementos de autenticación reforzada de clientes a que se hace referencia en los artículos 6, 7 y 8 esté sujeto a medidas que garanticen que, en términos de tecnología, algoritmos y parámetros, el quebrantamiento de uno de los elementos no compromete la fiabilidad de los demás.

2. Los proveedores de servicios de pago adoptarán medidas de seguridad, cuando alguno de los elementos de autenticación reforzada de clientes o el propio código de autenticación se utilicen a través de un dispositivo polivalente, a fin de mitigar el riesgo que se derivaría de que dicho dispositivo se viera comprometido.

3. A efectos del apartado 2, las medidas de mitigación incluirán todos los elementos siguientes:

a) el uso de entornos separados de ejecución segura a través de los programas informáticos instalados en los dispositivos polivalentes;

b) mecanismos para garantizar que ni el ordenante ni ningún tercero hayan modificado los programas informáticos o el dispositivo;

c) cuando se hayan producido modificaciones, mecanismos para mitigar las consecuencias de aquellas.

CAPÍTULO III

EXENCIONES DE LA AUTENTICACIÓN REFORZADA DE CLIENTES

Artículo 10

Información de cuentas de pago

1. Los proveedores de servicios de pago tendrán la posibilidad de no aplicar la autenticación reforzada de clientes, siempre que se cumplan los requisitos establecidos en el artículo 2 y en el apartado 2 del presente artículo, cuando un usuario de servicios de pago esté limitado a acceder a uno de los siguientes elementos en línea o a ambos sin divulgar datos de pago sensibles:

a) el saldo de una o varias cuentas de pago designadas;

b) las operaciones de pago ejecutadas en los 90 últimos días a través de una o varias cuentas de pago designadas.

2. A efectos del apartado 1, los proveedores de servicios de pago no estarán exentos de la aplicación de la autenticación reforzada de clientes cuando se cumpla alguna de las siguientes condiciones:

▼B

a) que el usuario de servicios de pago esté accediendo en línea a la información especificada en el apartado 1 por primera vez;

b) que hayan transcurrido más de 90 días desde la última vez que el usuario de servicios de pago accediera en línea a la información especificada en el apartado 1, letra b), y se aplicara la autenticación reforzada de clientes.

Artículo 11

Pagos sin contacto en el punto de venta

Los proveedores de servicios de pago tendrán la posibilidad de no aplicar la autenticación reforzada de clientes, siempre que se cumplan los requisitos establecidos en el artículo 2, cuando el ordenante inicie una operación de pago electrónico sin contacto en la que se cumplan las condiciones siguientes:

a) que el importe de la operación de pago electrónico sin contacto no exceda de 50 EUR, y

b) que el importe acumulado de las operaciones previas de pago electrónico sin contacto iniciadas por medio de un instrumento de pago con una funcionalidad sin contacto desde la fecha de la última aplicación de la autenticación reforzada de clientes no exceda de 150 EUR, o

c) que el número de operaciones de pago electrónico sin contacto consecutivas iniciadas por medio de un instrumento de pago que ofrezca una funcionalidad sin contacto desde la fecha de la última aplicación de la autenticación reforzada de clientes no exceda de cinco.

Artículo 12

Terminales no atendidas para tarifas de transporte o pagos de aparcamiento

Los proveedores de servicios de pago tendrán la posibilidad de no aplicar la autenticación reforzada de clientes, siempre que se cumplan los requisitos establecidos en el artículo 2, cuando el ordenante inicie una operación de pago electrónico en una terminal de pago no atendida con el fin de abonar una tarifa de transporte o un pago de aparcamiento.

Artículo 13

Beneficiarios de confianza

1. Los proveedores de servicios de pago aplicarán la autenticación reforzada de clientes cuando el ordenante cree o modifique una lista de beneficiarios de confianza a través del proveedor de servicios de pago gestor de la cuenta del ordenante.

2. Los proveedores de servicios de pago tendrán la posibilidad de no aplicar la autenticación reforzada de clientes, siempre que se cumplan los requisitos de autenticación general, cuando el ordenante inicie una operación de pago y el beneficiario esté incluido en una lista de beneficiarios de confianza previamente creada por el ordenante.

▼B

Artículo 14

Operaciones frecuentes

▼C1

1. Los proveedores de servicios de pago aplicarán la autenticación reforzada de clientes cuando el ordenante cree, modifique o inicie por primera vez una serie de operaciones frecuentes con el mismo importe y el mismo beneficiario..

▼B

2. Los proveedores de servicios de pago tendrán la posibilidad de no aplicar la autenticación reforzada de clientes, siempre que se cumplan los requisitos de autenticación general, para la iniciación de todas las operaciones de pago subsiguientes incluidas en la serie de operaciones de pago a que se refiere el apartado 1.

Artículo 15

Transferencias de créditos entre cuentas mantenidas por la misma persona física o jurídica

Los proveedores de servicios de pago tendrán la posibilidad de no aplicar la autenticación reforzada de clientes, siempre que se cumplan los requisitos establecidos en el artículo 2, cuando el ordenante inicie una transferencia de créditos en circunstancias en las que el ordenante y el beneficiario sean la misma persona física o jurídica y ambas cuentas de pago sean mantenidas por el mismo proveedor de servicios de pago gestor de cuenta.

Artículo 16

Operaciones de escasa cuantía

Los proveedores de servicios de pago tendrán la posibilidad de no aplicar la autenticación reforzada de clientes cuando el ordenante inicie una operación remota de pago electrónico, si se cumplen las siguientes condiciones:

a) que el importe de la operación remota de pago electrónico no exceda de 30 EUR, y

b) que el importe acumulado de las operaciones remotas de pago electrónico previas iniciadas por el ordenante desde la última aplicación de la autenticación reforzada de clientes no exceda de 100 EUR, o

c) que el número de las operaciones remotas de pago electrónico previas iniciadas por el ordenante desde la última aplicación de la autenticación reforzada de clientes no exceda de cinco operaciones remotas de pago electrónico individuales consecutivas.

Artículo 17

Procesos y protocolos de pago corporativo seguro

Los proveedores de servicios de pago tendrán la posibilidad de no aplicar la autenticación reforzada de clientes para personas jurídicas que inicien operaciones de pago electrónico mediante el uso de procesos o protocolos de pago que solo estén disponibles para los ordenantes que no sean

▼B

consumidores, cuando las autoridades competentes estén convencidas de que dichos procesos o protocolos garantizan unos niveles de seguridad al menos equivalentes a los previstos por la Directiva (UE) 2015/2366.

Artículo 18

Análisis del riesgo de la operación

1. Los proveedores de servicios de pago tendrán la posibilidad de no aplicar la autenticación reforzada de clientes cuando el ordenante inicie una operación remota de pago electrónico cuyo nivel de riesgo el proveedor de servicios de pago haya identificado como bajo según los mecanismos de supervisión de las operaciones a que se hace referencia en el artículo 2 y en el apartado 2, letra c), del presente artículo.

2. Se considerará que el nivel de riesgo de las operaciones de pago electrónico mencionadas en el apartado 1 es bajo cuando se cumplan todas las condiciones siguientes:

a) que el índice de fraude para ese tipo de operaciones, señalado por el proveedor de servicios de pago y calculado con arreglo al artículo 19, sea equivalente o inferior al índice de fraude de referencia especificado en el cuadro que figura en el anexo para los «pagos remotos electrónicos con tarjeta» y las «transferencias de créditos remotas electrónicas», respectivamente;

b) que el importe de la operación no supere el valor umbral de exención (en lo sucesivo, «VUE») pertinente, que se especifica en el cuadro que figura en el anexo;

c) que los proveedores de servicios de pago no hayan detectado, como consecuencia de la realización de un análisis del riesgo en tiempo real, ninguno de los elementos siguientes:

   i) gastos o pautas de comportamiento anormales en el ordenante,

   ii) información inusual sobre el dispositivo o programa informático de acceso del ordenante,

   iii) infecciones por programas informáticos maliciosos en cualquier sesión del procedimiento de autenticación,

   iv) supuestos conocidos de fraude en la prestación de servicios de pago,

   v) una ubicación anormal del ordenante,

   vi) una ubicación de alto riesgo del beneficiario.

3. Los proveedores de servicios de pago que tengan intención de eximir operaciones remotas de pago electrónico de la autenticación reforzada de clientes por entender que implican un bajo nivel de riesgo deberán tener en cuenta, como mínimo, los siguientes factores basados en el riesgo:

a) las pautas de gasto anteriores del usuario de servicios de pago en concreto;

b) el historial de operaciones de pago de cada usuario de servicios de pago del proveedor de que se trate;

▼B

c) la ubicación del ordenante y del beneficiario en el momento de la operación de pago en los casos en que el dispositivo o el programa informático de acceso sea facilitado por el proveedor de servicios de pago;

d) la identificación de pautas de pago anormales del usuario de servicios de pago en relación con su historial de operaciones de pago.

La evaluación realizada por el proveedor de servicios de pago combinará todos los citados factores basados en el riesgo en una puntuación de riesgo para cada operación específica, con el fin de determinar si un pago concreto debe permitirse sin la autenticación reforzada de clientes.

Artículo 19

Cálculo de los índices de fraude

1. Para cada tipo de operación a que se hace referencia en el cuadro que figura en el anexo, el proveedor de servicios de pago garantizará que el índice de fraude global que cubre tanto las operaciones de pago autenticadas mediante la autenticación reforzada de clientes como las ejecutadas con arreglo a alguna de las exenciones contempladas en los artículos 13 a 18 es equivalente o inferior al índice de fraude de referencia indicado en el cuadro que figura en el anexo para el mismo tipo de operación de pago.

El índice de fraude global para cada tipo de operación se calculará como el valor total de las operaciones remotas no autorizadas o fraudulentas, independientemente de que se hayan recuperado o no los fondos, dividido entre el valor total de todas las operaciones remotas del mismo tipo, tanto autenticadas mediante la aplicación de la autenticación reforzada de clientes como ejecutadas con arreglo a alguna de las exenciones contempladas en los artículos 13 a 18 sobre una base rotatoria trimestral (90 días).

2. La revisión de auditoría a que se refiere el artículo 3, apartado 2, evaluará el cálculo de los índices de fraude y las cifras resultantes y garantizará que sean completos y exactos.

3. La metodología y cualquier modelo usados por el proveedor de servicios de pago para calcular los índices de fraude, así como los propios índices de fraude, estarán debidamente documentados y serán plenamente accesibles a las autoridades competentes y a la ABE, a petición de estas y previa notificación a la autoridad o autoridades competentes pertinentes.

Artículo 20

Cese de las exenciones basadas en el análisis del riesgo de la operación

1. Los proveedores de servicios de pago que se acojan a la exención a que se hace referencia en el artículo 18 informarán inmediatamente a las autoridades competentes cuando uno de sus índices de fraude supervisados sea, para cualquier tipo de operación de pago indicado en el cuadro que figura en el anexo, superior al índice de fraude de referencia aplicable y proporcionarán a las autoridades competentes una descripción de las medidas que tengan previsto adoptar para restablecer la conformidad de su índice de fraude supervisado con los índices de fraude de referencia aplicables.

▼B

2. Los proveedores de servicios de pago dejarán inmediatamente de hacer uso de la exención a que se refiere el artículo 18 para cualquier tipo de operaciones de pago indicado en el cuadro que figura en el anexo en el umbral de exención específico, cuando su índice de fraude supervisado supere durante dos trimestres consecutivos el índice de fraude de referencia aplicable al instrumento de pago o tipo de operación de pago correspondiente a ese umbral de exención.

3. Tras el cese de la exención a que se refiere el artículo 18, de conformidad con lo dispuesto en el apartado 2 del presente artículo, los proveedores de servicios de pago no reanudarán el uso de esa exención hasta que su índice de fraude calculado sea igual o menor que los índices de fraude de referencia aplicables a ese tipo de operación de pago correspondiente a dicho umbral de exención durante un trimestre.

4. Cuando los proveedores de servicios de pago tengan la intención de reanudar el uso de la exención a que se refiere el artículo 18, lo comunicarán a las autoridades competentes en un plazo razonable y, antes de hacer efectiva la reanudación, facilitarán pruebas de que se ha vuelto a la conformidad de su índice de fraude supervisado con el índice de fraude de referencia aplicable para dicho umbral de exención de conformidad con el apartado 3 del presente artículo.

Artículo 21

Supervisión

1. Con el fin de hacer uso de las exenciones establecidas en los artículos 10 a 18, los proveedores de servicios de pago registrarán y supervisarán los siguientes datos para cada tipo de operaciones de pago, desglosando las operaciones remotas y no remotas de pago y con una frecuencia al menos trimestral:

a) el valor total de las operaciones de pago no autorizadas o fraudulentas de conformidad con lo dispuesto en el artículo 64, apartado 2, de la Directiva (UE) 2015/2366, el valor total de todas las operaciones de pago y el índice de fraude resultante, incluido un desglose de las operaciones de pago iniciadas por medio de una autenticación reforzada de clientes y las iniciadas al amparo de cada una de las exenciones;

b) el valor medio de las operaciones, incluido un desglose de las operaciones de pago iniciadas por medio de una autenticación reforzada de clientes y las iniciadas al amparo de cada una de las exenciones;

c) el número de operaciones de pago en que se ha aplicado cada una de las exenciones y su porcentaje con respecto al número total de operaciones de pago.

2. Los proveedores de servicios de pago pondrán los resultados de la supervisión realizada de conformidad con el apartado 1 a disposición de las autoridades competentes y de la ABE, a petición de estas y previa notificación a la autoridad o autoridades competentes pertinentes.

▼B

CAPÍTULO IV

CONFIDENCIALIDAD E INTEGRIDAD DE LAS CREDENCIALES DE SEGURIDAD PERSONALIZADAS DE LOS USUARIOS DE SERVICIOS DE PAGO

Artículo 22

Requisitos generales

1. Los proveedores de servicios de pago garantizarán la confidencialidad y la integridad de las credenciales de seguridad personalizadas del usuario de servicios de pago, incluidos los códigos de autenticación, durante todas las fases de su autenticación.

2. A efectos del apartado 1, los proveedores de servicios de pago velarán por el cumplimiento de todos los requisitos siguientes:

a) que las credenciales de seguridad personalizadas se enmascaren cuando se muestren y no sean legibles en su totalidad cuando sean introducidas por el usuario de servicios de pago durante la autenticación;

b) que las credenciales de seguridad personalizadas en formato de datos, así como los materiales criptográficos relacionados con el cifrado de las credenciales de seguridad personalizadas, no sean almacenados en formato de texto común;

c) que el material criptográfico secreto quede protegido de una divulgación no autorizada.

3. Los proveedores de servicios de pago documentarán exhaustivamente el proceso relacionado con la gestión del material criptográfico utilizado para cifrar o hacer ilegibles las credenciales de seguridad personalizadas.

4. Los proveedores de servicios de pago velarán por que el tratamiento y el encaminamiento de las credenciales de seguridad personalizadas y de los códigos de autenticación generados de conformidad con el capítulo II tengan lugar en entornos seguros en consonancia con estándares firmes y ampliamente reconocidos del sector.

Artículo 23

Creación y transmisión de credenciales

Los proveedores de servicios de pago garantizarán que la creación de credenciales de seguridad personalizadas se lleva a cabo en un entorno seguro.

Antes de la entrega de las credenciales de seguridad personalizadas y de los dispositivos y los programas informáticos de autenticación al ordenante, los proveedores de servicios de pago mitigarán los riesgos de su uso no autorizado en caso de extravío, robo o reproducción.

Artículo 24

Asociación con el usuario de servicios de pago

1. Los proveedores de servicios de pago velarán por que solo el usuario de servicios de pago correspondiente esté asociado, de manera segura, con las credenciales de seguridad personalizadas y los dispositivos y programas informáticos de autenticación.

▼B

2. A efectos del apartado 1, los proveedores de servicios de pago velarán por el cumplimiento de todos los requisitos siguientes:

a) que la asociación de la identidad del usuario de servicios de pago con las credenciales de seguridad personalizadas y los dispositivos y programas informáticos de autenticación se lleva a cabo en entornos seguros bajo la responsabilidad del proveedor de servicios de pago, incluidos al menos los locales del proveedor de servicios de pago, el entorno de internet facilitado por el proveedor de servicios de pago u otros sitios web seguros similares utilizados por el proveedor de servicios de pago y sus servicios de cajeros automáticos, y toma en consideración los riesgos asociados con los dispositivos y componentes subyacentes utilizados durante el proceso de asociación que no estén bajo la responsabilidad del proveedor de servicios de pago;

b) que la asociación por medio de un canal remoto de la identidad del usuario del servicio de pago con las credenciales de seguridad personalizadas y con los dispositivos o programas informáticos de autenticación se realiza a través de la autenticación reforzada de clientes.

Artículo 25

Entrega de credenciales y de dispositivos y programas informáticos de autenticación

1. Los proveedores de servicios de pago garantizarán que la entrega al usuario de servicios de pago de credenciales de seguridad personalizadas y de dispositivos y programas informáticos de autenticación se lleva a cabo de una forma segura que aborde los riesgos relacionados con su uso no autorizado debido a su extravío, robo o reproducción.

2. A efectos del apartado 1, los proveedores de servicios de pago aplicarán, como mínimo, todas las medidas siguientes:

a) mecanismos de entrega seguros y eficaces que garanticen que las credenciales de seguridad personalizadas y los dispositivos y programas informáticos de autenticación se entregan al legítimo usuario de servicios de pago;

b) mecanismos que permitan al proveedor de servicios de pago comprobar la autenticidad de los programas informáticos de autenticación entregados al usuario de servicios de pago a través de internet;

c) medidas que garanticen que, cuando la entrega de credenciales de seguridad personalizadas se ejecute fuera de los locales del proveedor de servicios de pago o a través de un canal remoto:

   i) ningún tercero no autorizado pueda obtener más de una característica de las credenciales de seguridad personalizadas o los dispositivos o programas informáticos de autenticación cuando se entreguen a través del mismo canal,

   ii) las credenciales de seguridad personalizadas o los dispositivos o programas informáticos de autenticación entregados requieran activación antes de su utilización;

▼B

d) medidas que garanticen que, en los casos en que las credenciales de seguridad personalizadas o los dispositivos o programas informáticos de autenticación deban activarse antes de su primera utilización, la activación tenga lugar en un entorno seguro de conformidad con los procedimientos de asociación a que se refiere el artículo 24.

Artículo 26

Renovación de credenciales personalizadas de seguridad

Los proveedores de servicios de pago garantizarán que la renovación o la reactivación de las credenciales de seguridad personalizadas respetan los procedimientos para la creación, la asociación y la entrega de las credenciales y los dispositivos de autenticación de conformidad con lo dispuesto en los artículos 23, 24 y 25.

Artículo 27

Destrucción, desactivación y revocación

Los proveedores de servicios de pago garantizarán que disponen de procesos efectivos para la aplicación de cada una de las medidas de seguridad siguientes:

a) la destrucción, la desactivación o la revocación seguras de las credenciales de seguridad personalizadas y los dispositivos y programas informáticos de autenticación;

b) que, cuando el proveedor de servicios de pago distribuya dispositivos y programas informáticos de autenticación reutilizables, la reutilización segura de un dispositivo o programa se decida, documente y ejecute antes de ponerlo a disposición de otro usuario de servicios de pago;

c) la desactivación o revocación de información relativa a las credenciales de seguridad personalizadas almacenadas en los sistemas y bases de datos del proveedor de servicios de pago y, en su caso, en registros públicos.

CAPÍTULO V

ESTÁNDARES DE COMUNICACIÓN ABIERTOS COMUNES Y SEGUROS

Sección 1

Requisitos generales de comunicación

Artículo 28

Requisitos de identificación

1. Los proveedores de servicios de pago garantizarán la identificación segura en las comunicaciones entre el dispositivo del ordenante y los dispositivos de aceptación del beneficiario para los pagos electrónicos, en particular, pero no exclusivamente, las terminales de pago.

2. Los proveedores de servicios de pago garantizarán que los riesgos de desviaciones de comunicación a terceros no autorizados en las aplicaciones móviles y otras interfaces de usuarios de servicios de pago que ofrezcan servicios de pago electrónico se mitigan de forma eficaz.

▼B

Artículo 29

Trazabilidad

1. Los proveedores de servicios de pago dispondrán de procesos que garanticen la trazabilidad de todas las operaciones de pago y otras interacciones con el usuario de los servicios de pago, con los demás proveedores de servicios de pago y con otras entidades, incluidos los comerciantes, en el contexto de la prestación de servicios de pago, de forma que quede garantizado el conocimiento posterior de todas las circunstancias relevantes para la operación electrónica en todas sus fases.

2. A efectos del apartado 1, los proveedores de servicios de pago garantizarán que toda sesión de comunicación con el usuario de los servicios de pago, con los demás proveedores de servicios de pago y con otras entidades, incluidos los comerciantes, se fundamenta en todos los elementos siguientes:

a) un identificador único de la sesión;

b) mecanismos de seguridad para el registro detallado de la operación, incluidos el número de operación, marcas de tiempo y todos los datos pertinentes de la operación;

c) marcas de tiempo que deben basarse en un sistema unificado de referencia temporal y sincronizarse con arreglo a una señal temporal oficial.

Sección 2

Requisitos específicos para los estándares de comunicación abiertos comunes y seguros

Artículo 30

Obligaciones generales para las interfaces de acceso

1. Los proveedores de servicios de pago gestores de cuenta que ofrezcan a un ordenante una cuenta de pago accesible en línea deberán contar con al menos una interfaz que cumpla todos los requisitos siguientes:

a) que los proveedores de servicios de información sobre cuentas, los proveedores de servicios de iniciación de pagos y los proveedores de servicios de pago que emitan instrumentos de pago basados en tarjetas puedan identificarse ante el proveedor de servicios de pago gestor de cuenta;

b) que los proveedores de servicios de información sobre cuentas puedan comunicarse de forma segura para solicitar y recibir información sobre una o más cuentas de pago designadas y las operaciones de pago asociadas a ellas;

c) que los proveedores de servicios de iniciación de pagos puedan comunicarse de forma segura para iniciar una orden de pago a partir de la cuenta de pago del ordenante y recibir toda la información sobre la iniciación de la operación de pago y toda la información accesible a los proveedores de servicios de pago gestores de cuenta relativa a la ejecución de la operación de pago.

▼B

2. A efectos de la autenticación del usuario de servicios de pago, la interfaz a que se refiere el apartado 1 debe permitir a los proveedores de servicios de información sobre cuentas y los proveedores de servicios de iniciación de pagos servirse de todos los procedimientos de autenticación facilitados al usuario del servicio de pago por el proveedor de servicios de pago gestor de cuenta.

La interfaz deberá cumplir como mínimo todos los requisitos siguientes:

a) que un proveedor de servicios de iniciación de pagos o un proveedor de servicios de información sobre cuentas pueda dar instrucciones al proveedor de servicios de pago gestor de cuenta para iniciar una autenticación basada en el consentimiento del usuario de servicios de pago;

b) que las sesiones de comunicación entre el proveedor de servicios de pago gestor de cuenta, el proveedor de servicios de información sobre cuentas, el proveedor de servicios de iniciación de pagos y cualquier usuario de servicios de pago de que se trate se establezcan y mantengan durante todo el proceso de autenticación;

c) que la integridad y la confidencialidad de las credenciales de seguridad personalizadas y de los códigos de autenticación transmitidos por el proveedor de servicios de iniciación de pagos o el proveedor de servicios de información sobre cuentas, o a través de ellos, estén garantizadas.

3. Los proveedores de servicios de pago gestores de cuenta garantizarán que sus interfaces sigan estándares de comunicación emitidos por organizaciones de normalización internacionales o europeas.

Los proveedores de servicios de pago gestores de cuenta se asegurarán también de que las especificaciones técnicas de cualquiera de las interfaces se documentan especificando un conjunto de rutinas, protocolos y herramientas que necesitan los proveedores de servicios de iniciación de pagos, los proveedores de servicios de información sobre cuentas y los proveedores de servicios de pago que emitan instrumentos de pago basados en tarjetas para permitir la interoperabilidad de sus programas informáticos y aplicaciones con los sistemas de los proveedores de servicios de pago gestores de cuenta.

No menos de seis meses antes de la fecha de aplicación a que se refiere el artículo 38, apartado 2, o antes de la fecha prevista para la aparición en el mercado de la interfaz de acceso cuando dicha aparición tenga lugar después de la fecha indicada en el artículo 38, apartado 2, los proveedores de servicios de pago gestores de cuenta deberán, como mínimo, previa solicitud de los proveedores autorizados de servicios de iniciación de pagos, de servicios de información sobre cuentas y de servicios de pago que emitan instrumentos de pago basados en tarjetas, o de los proveedores de servicios de pago que hayan presentado a sus autoridades competentes la solicitud de autorización pertinente, poner la documentación a disposición de estos de forma gratuita y dar acceso público en su sitio web a un resumen de esa documentación.

▼B

4. Además de lo dispuesto en el apartado 3, los proveedores de servicios de pago gestores de cuenta se asegurarán de que, salvo en situaciones de emergencia, cualquier modificación de las especificaciones técnicas de su interfaz se ponga a disposición de los proveedores autorizados de servicios de iniciación de pagos, de servicios de información sobre cuentas y de servicios de pago que emitan instrumentos de pago basados en tarjetas, o de los proveedores de servicios de pago que hayan presentado a sus autoridades competentes una solicitud de autorización pertinente, tan pronto como sea posible y en un plazo no inferior a tres meses antes de que se aplique la modificación.

Los proveedores de servicios de pago documentarán las situaciones de emergencia en las que se hayan introducido modificaciones y pondrán la documentación a disposición de las autoridades competentes previa solicitud.

5. Los proveedores de servicios de pago gestores de cuenta pondrán una instalación de prueba para pruebas funcionales y de conexión, que incluya asistencia, a disposición de los proveedores autorizados de servicios de iniciación de pagos, de servicios de pago que emitan instrumentos de pago basados en tarjetas o de servicios de información sobre cuentas, o de los proveedores de servicios de pago que hayan solicitado la autorización pertinente, con objeto de permitirles poner a prueba los programas informáticos y aplicaciones utilizados para ofrecer servicios de pago a los usuarios. Esta instalación de prueba debe estar disponible a más tardar seis meses antes de la fecha de aplicación a que se refiere el artículo 38, apartado 2, o antes de la fecha prevista para la aparición en el mercado de la interfaz de acceso cuando esta tenga lugar después de la fecha a que se hace referencia en el artículo 38, apartado 2.

Sin embargo, no se compartirá información sensible a través de la instalación de prueba.

6. Las autoridades competentes velarán por que los proveedores de servicios de pago gestores de cuenta cumplan en todo momento las obligaciones previstas en estos estándares en lo que respecta a la interfaz o las interfaces que pongan en marcha. En caso de que un proveedor de servicios de pago gestor de cuenta no cumpla con los requisitos fijados para las interfaces en los presentes estándares, las autoridades competentes velarán por que la prestación de servicios de iniciación de pagos y servicios de información sobre cuentas no se impida o distorsione en la medida en que los proveedores respectivos de esos servicios cumplan las condiciones establecidas en el artículo 33, apartado 5.

Artículo 31

Opciones de las interfaces de acceso

Los proveedores de servicios de pago gestores de cuenta pondrán en funcionamiento la interfaz o interfaces a que se refiere el artículo 30 mediante una interfaz específica o autorizando el uso por los proveedores de servicios de pago a que se refiere el artículo 30, apartado 1, de las interfaces utilizadas para la autenticación de los usuarios de servicios de pago del proveedor de servicios de pago gestor de cuenta en cuestión o para la comunicación con dichos usuarios.

▼B

Artículo 32

Obligaciones relativas a las interfaces específicas

1. En cumplimiento de lo dispuesto en los artículos 30 y 31, los proveedores de servicios de pago gestores de cuenta que hayan puesto en marcha una interfaz específica velarán por que dicha interfaz específica ofrezca en todo momento el mismo nivel de disponibilidad y de rendimiento, incluida la asistencia, que las interfaces puestas a disposición del usuario de servicios de pago para acceder directamente a su cuenta de pago en línea.

2. Los proveedores de servicios de pago gestores de cuenta que hayan puesto en marcha una interfaz específica definirán indicadores clave de rendimiento y objetivos de nivel de servicio transparentes y al menos tan estrictos, en términos tanto de disponibilidad como de los datos facilitados de conformidad con el artículo 36, como los establecidos para la interfaz utilizada por sus usuarios de servicios de pago. Las autoridades competentes supervisarán las interfaces, los indicadores y los objetivos y los someterán a pruebas de resistencia.

3. Los proveedores de servicios de pago gestores de cuenta que hayan establecido una interfaz específica se asegurarán de que esta no cree obstáculos a la prestación de servicios de iniciación de pagos y servicios de información sobre cuentas. Estos obstáculos pueden incluir, entre otras cosas, impedir el uso por los proveedores de servicios de pago a que se refiere el artículo 30, apartado 1, de las credenciales expedidas por los proveedores de servicios de pago gestores de cuenta a sus clientes; imponer la redirección hacia la autenticación u otras funciones del proveedor de servicios de pago gestor de cuenta; exigir autorizaciones y registros adicionales, además de los previstos en los artículos 11, 14 y 15 de la Directiva (UE) 2015/2366; o exigir controles adicionales del consentimiento dado por los usuarios de los servicios de pago a los proveedores de servicios de iniciación de pagos y servicios de información sobre cuentas.

4. A efectos de los apartados 1 y 2, los proveedores de servicios de pago gestores de cuenta supervisarán la disponibilidad y el rendimiento de la interfaz específica. Los proveedores de servicios de pago gestores de cuenta publicarán en su sitio web las estadísticas trimestrales sobre la disponibilidad y el rendimiento de la interfaz específica y de la interfaz utilizada por sus usuarios de servicios de pago.

Artículo 33

Medidas de contingencia para las interfaces específicas

1. Los proveedores de servicios de pago gestores de cuenta incluirán, en la concepción de la interfaz específica, una estrategia y planes para medidas de contingencia en caso de que la interfaz no rinda conforme a lo que exige el artículo 32, que la interfaz no esté disponible por motivos imprevistos o que el sistema se averíe. Podrá presumirse que la interfaz no está disponible por motivos imprevistos o que el sistema está averiado cuando no se dé respuesta, en un período de treinta segundos, a cinco solicitudes consecutivas de acceso a la información destinada a la provisión de servicios de iniciación de pago o servicios de información sobre cuentas.

▼B

2. Las medidas de contingencia incluirán planes de comunicación para informar a los proveedores de servicios de pago que hagan uso de la interfaz específica sobre las medidas para restablecer el sistema y una descripción de las opciones alternativas inmediatamente disponibles a las que los proveedores de servicios de pago pueden acceder durante ese tiempo.

3. Tanto el proveedor de servicios de pago gestor de cuenta como los proveedores de servicios de pago a que se refiere el artículo 30, apartado 1, notificarán sin demora los problemas con interfaces específicas descritos en el apartado 1 a sus respectivas autoridades nacionales competentes.

4. Como parte de un mecanismo de contingencia, los proveedores de servicios de pago a que se refiere el artículo 30, apartado 1, estarán autorizados a hacer uso de las interfaces a disposición de los usuarios de servicios de pago para la autenticación y comunicación con su proveedor de servicios de pago gestor de cuenta, hasta que la interfaz específica vuelva a alcanzar el nivel de disponibilidad y rendimiento que exige el artículo 32.

5. A tal fin, los proveedores de servicios de pago gestores de cuenta garantizarán que los proveedores de servicios de pago a que se refiere el artículo 30, apartado 1, puedan ser identificados y servirse de los procedimientos de autenticación facilitados por el proveedor de servicios de pago gestor de cuenta al usuario de servicios de pago. Cuando los proveedores de servicios de pago a que se refiere el artículo 30, apartado 1, hagan uso de la interfaz contemplada en el apartado 4, deberán:

a) adoptar las medidas necesarias para garantizar que no acceden a datos, los almacenan o los tratan para fines distintos de la prestación del servicio solicitado por el usuario del servicio de pago;

b) seguir cumpliendo las obligaciones derivadas del artículo 66, apartado 3, y del artículo 67, apartado 2, de la Directiva (UE) 2015/2366, respectivamente;

c) registrar los datos a los que se acceda a través de la interfaz gestionada por el proveedor de servicios de pago gestor de cuenta para los usuarios de servicios de pago y facilitar, previa petición y sin demora indebida, los archivos de registro a su autoridad nacional competente;

d) justificar debidamente a su autoridad nacional competente, previa petición y sin demora indebida, la utilización de la interfaz puesta a disposición de los usuarios de servicios de pago para acceder directamente a su cuenta de pago en línea;

e) informar al proveedor de servicios de pago gestor de cuenta en consecuencia.

6. Las autoridades competentes, tras consultar a la ABE a fin de garantizar una aplicación coherente de las siguientes condiciones, eximirán a los proveedores de servicios de pago gestores de cuenta que hayan optado por una interfaz específica de la obligación de crear el mecanismo de contingencia descrito en el apartado 4 cuando la interfaz cumpla todas las condiciones siguientes:

a) ajustarse a todas las obligaciones para las interfaces específicas según lo establecido en el artículo 32;

▼B

b) haberse concebido y probado de conformidad con el artículo 30, apartado 5, a satisfacción de los proveedores de servicios de pago a los que se hace referencia en dicho apartado;

c) haber sido utilizada de manera generalizada durante al menos tres meses por los proveedores de servicios de pago para ofrecer servicios de información sobre cuentas y servicios de iniciación de pagos y para confirmar la disponibilidad de fondos para los pagos con tarjeta;

d) que cualquier problema relacionado con la interfaz específica haya sido resuelto sin demora indebida.

7. Las autoridades competentes revocarán la exención a que se refiere el apartado 6 cuando los proveedores de servicios de pago gestores de cuenta no cumplan las condiciones a) y d) durante más de dos semanas naturales consecutivas. Las autoridades competentes informarán a la ABE de esta revocación y velarán por que el proveedor de servicios de pago gestor de cuenta establezca, en el plazo más breve posible y a más tardar en el plazo de dos meses, el mecanismo de contingencia previsto en el apartado 4.

Artículo 34

Certificados

1. A efectos de identificación, como se indica en el artículo 30, apartado 1, letra a), los proveedores de servicios de pago se servirán de los certificados cualificados de sello electrónico a que se refiere el artículo 3, punto 30, del Reglamento (UE) n.º 910/2014 o de autenticación de sitio web a que se hace referencia en el artículo 3, punto 39, de dicho Reglamento.

2. A efectos del presente Reglamento, el número de registro al que van referidos los registros oficiales de conformidad con lo dispuesto en la letra c) del anexo III o en la letra c) del anexo IV del Reglamento (UE) n.º 910/2014 será el número de autorización del proveedor de servicios de pago que emita instrumentos de pago basados en tarjetas, el proveedor de servicios de información sobre cuentas o el proveedor de servicios de iniciación de pagos, incluidos los proveedores de servicios de pago gestores de cuenta que prestan tales servicios, disponible en el registro público del Estado miembro de origen de conformidad con el artículo 14 de la Directiva (UE) 2015/2366 o que resulte de las notificaciones de cada autorización concedida con arreglo al artículo 8 de la Directiva 2013/36/UE del Parlamento Europeo y del Consejo [1] de conformidad con el artículo 20 de dicha Directiva.

3. A efectos del presente Reglamento, los certificados cualificados de sello electrónico o de autenticación de sitio web a que se refiere el apartado 1 incluirán, en una lengua habitual en el campo de las finanzas internacionales, atributos específicos adicionales en relación con todos los aspectos siguientes:

[1] Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE (DO L 176 de 27.6.2013, p. 338).

▼B

a) el papel del proveedor de servicios de pago, que podrá ser uno o varios de los siguientes:

i) gestor de cuenta,

ii) proveedor de servicios de iniciación de pagos,

iii) proveedor de información sobre cuentas,

iv) emisor de instrumentos de pago basados en tarjetas;

b) el nombre de las autoridades competentes en el lugar en que esté registrado el proveedor de servicios de pago.

4. Los atributos a que se refiere el apartado 3 no afectarán a la interoperabilidad y reconocimiento de los certificados cualificados de sello electrónico o autenticación de sitio web.

Artículo 35

Seguridad de las sesiones de comunicación

1. Los proveedores de servicios de pago gestores de cuenta, los proveedores de servicios de pago que emitan instrumentos de pago basados en tarjetas, los proveedores de servicios de información sobre cuentas y los proveedores de servicios de iniciación de pagos velarán por que, en el intercambio de datos a través de internet, se aplique un cifrado seguro entre las partes durante toda la sesión de comunicación respectiva, a fin de proteger la confidencialidad y la integridad de los datos, utilizando técnicas de cifrado reforzadas y ampliamente reconocidas.

2. Los proveedores de servicios de pago que emitan instrumentos de pago basados en tarjetas, los proveedores de servicios de información sobre cuentas y los proveedores de servicios de iniciación de pagos deberán reducir al mínimo tiempo posible la duración de las sesiones de acceso ofrecidas por los proveedores de servicios de pago gestores de cuenta y poner término activo a estas sesiones tan pronto como se haya completado la acción solicitada.

3. A la hora de mantener las sesiones paralelas de red con el proveedor de servicios de pago gestor de cuenta, los proveedores de servicios de información sobre cuentas y los proveedores de servicios de iniciación de pagos se asegurarán de que estas sesiones están ligadas de forma segura a las sesiones pertinentes establecidas con el usuario o los usuarios de los servicios de pago a fin de evitar la posibilidad de que pueda desviarse el encaminamiento de cualquier mensaje o la información comunicada entre ellos.

4. Los proveedores de servicios de información sobre cuentas, los proveedores de servicios de iniciación de pagos y los proveedores de servicios de pago que emitan instrumentos de pago basados en tarjetas con el proveedor de servicios de pago gestor de cuenta incluirán referencias inequívocas a todos los puntos siguientes:

a) el usuario o los usuarios de servicios de pago y la correspondiente sesión de comunicación, a fin de distinguir las distintas solicitudes del mismo usuario o los mismos usuarios de servicios de pago;

b) para los servicios de iniciación de pagos, la operación de pago iniciada con una identificación única;

▼B

c) para la confirmación de la disponibilidad de fondos, la solicitud con una identificación única relacionada con la cantidad necesaria para la ejecución de la operación de pago con tarjeta.

5. Los proveedores de servicios de pago gestores de cuenta, los proveedores de servicios de información sobre cuentas, los proveedores de servicios de iniciación de pagos y los proveedores de servicios de pago que emitan instrumentos de pago basados en tarjetas garantizarán que, cuando comuniquen credenciales de seguridad personalizadas y códigos de autenticación, estos no sean legibles, ni directa ni indirectamente, por ningún miembro del personal en ningún momento.

En caso de pérdida de confidencialidad de las credenciales de seguridad personalizadas de su ámbito de competencia, esos proveedores informarán sin demora indebida al usuario de servicios de pago vinculado a ellas y al emisor de las credenciales de seguridad personalizadas.

Artículo 36

Intercambios de datos

1. Los proveedores de servicios de pago gestores de cuenta deberán cumplir todos los requisitos siguientes:

a) facilitar a los proveedores de servicios de información sobre cuentas la misma información de las cuentas de pago designadas y las operaciones de pago asociadas a ellas que se haya puesto a disposición del usuario de servicios de pago al solicitar directamente el acceso a la información sobre la cuenta, siempre que la información no incluya datos de pago sensibles;

b) facilitar, inmediatamente después de la recepción de la orden de pago, a los proveedores de servicios de iniciación de pagos la misma información sobre la iniciación y la ejecución de la operación de pago facilitada al usuario del servicio de pago o puesta a su disposición cuando este último haya iniciado directamente la operación;

c) facilitar inmediatamente a los proveedores de servicios de pago, previa petición, una confirmación, con un simple «sí» o «no», de si el importe necesario para la ejecución de una operación de pago está disponible en la cuenta de pago del ordenante.

2. En caso de un suceso inesperado o de un error durante el proceso de identificación, autenticación o intercambio de los datos, el proveedor de servicios de pago gestor de cuenta enviará un mensaje de notificación al proveedor de servicios de iniciación de pagos o al proveedor de servicios de información sobre cuentas y al proveedor de servicios de pago que emita instrumentos de pago basados en tarjetas, en el que explique las razones del suceso inesperado o del error.

Cuando el proveedor de servicios de pago gestor de cuenta ofrezca una interfaz específica con arreglo al artículo 32, la interfaz proporcionará mensajes de notificación relativos a sucesos inesperados o errores, que cualquier proveedor de servicios de pago que detecte el suceso o error deberá comunicar a los demás proveedores de servicios de pago que participen en la sesión de comunicación.

▼B

3. Los proveedores de servicios de información sobre cuentas tendrán en funcionamiento mecanismos apropiados y eficaces que impidan el acceso a información distinta de la de las cuentas de pago designadas y las operaciones de pago correspondientes, de conformidad con el consentimiento expreso del usuario.

4. Los proveedores de servicios de iniciación de pagos facilitarán a los proveedores de servicios de pago gestores de cuenta la misma información que se requiera al usuario de servicios de pago cuando se inicie la operación de pago directamente.

5. Los proveedores de servicios de información sobre cuentas podrán acceder a la información de las cuentas de pago designadas y las operaciones de pago correspondientes que posean los proveedores de servicios de pago gestores de cuenta a efectos de realizar el servicio de información sobre cuentas en cualquiera de las siguientes circunstancias:

a) siempre que el usuario de servicios de pago solicite activamente dicha información;

b) cuando el usuario de servicios de pago no solicite activamente esa información, no más de cuatro veces en un período de 24 horas, salvo que se acuerde una mayor frecuencia entre el proveedor de servicios de información sobre cuentas y los proveedores de servicios de pago gestores de cuenta, con el consentimiento del usuario de servicios de pago.

CAPÍTULO VI

DISPOSICIONES FINALES

Artículo 37

Revisión

Sin perjuicio de lo dispuesto en el artículo 98, apartado 5, de la Directiva (UE) 2015/2366, la ABE revisará, a más tardar el 14 de marzo de 2021 , los índices de fraude a que se hace referencia en el anexo del presente Reglamento, así como las exenciones concedidas de conformidad con el artículo 33, apartado 6, en lo que se refiere a las interfaces específicas, y presentará, si procede, proyectos de actualizaciones a la Comisión de conformidad con el artículo 10 del Reglamento (UE) n.º 1093/2010.

Artículo 38

Entrada en vigor

1. El presente Reglamento entrará en vigor el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

2. El presente Reglamento será de aplicación a partir del 14 de septiembre de 2019.

3. No obstante, los apartados 3 y 5 del artículo 30 serán de aplicación a partir del 14 de marzo de 2019.

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

▼B

ANEXO

	Índice de fraude de referencia (%) para:	
VUE	Pagos remotos electrónicos con tarjeta	Transferencias de créditos remotas electrónicas
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015