BANCO DE ESPAÑA
Eurosistema

Dirección General de Operaciones, Mercados y Sistemas de Pago

Aplicación Técnica nº 10/2021

TARGET2-Banco de España – Requisitos relativos a la gestión de la seguridad de la información y a la gestión de la continuidad operativa.

Departamento de Sistemas de Pago

Con motivo de la adopción por parte del Banco Central Europeo de la Orientación BCE/2021/30, de 20 de julio, por la que se modifica la Orientación BCE/2012/27 sobre el sistema automatizado transeuropeo de transferencia urgente para la liquidación bruta en tiempo real (TARGET2), es necesario aprobar una nueva aplicación técnica para recoger los requisitos relativos a la gestión de la seguridad de la información y a la gestión de la continuidad operativa a los que se refiere la Cláusula 35.ª (*Requisitos de seguridad y procedimientos de control*) de las cláusulas generales relativas a las condiciones uniformes para la apertura y el funcionamiento de una cuenta del módulo de pagos en TARGET2-Banco de España, aprobadas mediante resolución de la Comisión Ejecutiva del Banco de España de 20 de julio de 2007, tras su reciente modificación por la resolución de la Comisión Ejecutiva del Banco de España de 13 de octubre de 2021 (publicada en el BOE de 21 de octubre de 2021).

Como se indica en dicha Cláusula 35.ª, el Banco de España puede imponer medidas de reparación a los participantes cuyo nivel de cumplimiento de estos requisitos se haya evaluado como leve o grave; medidas de reparación que incluyen, entre otras, penalizaciones económicas, así como la suspensión o terminación de la participación en TARGET2-Banco de España, en los términos indicados en dicha Cláusula 35.ª

Estos requisitos, y las correspondientes medidas de reparación, resultarán también de aplicación respecto de los sistemas vinculados, en los términos previstos en los correspondientes acuerdos bilaterales suscritos con el Banco de España de conformidad con lo establecido en el artículo 13 de la Orientación BCE/2012/27 antes mencionada respecto de su operativa en el módulo de pagos.

1. Gestión de la seguridad de la información

Estos requisitos son aplicables a todos los participantes, a menos que demuestren que no les es aplicable un requisito específico. Al establecer el ámbito de aplicación de los requisitos dentro de sus infraestructuras, los participantes identificarán los elementos que formen parte de la cadena de las operaciones de pago (COP). En concreto, la COP comienza en un punto de entrada, es decir, un sistema que interviene en la creación de operaciones (por ejemplo, puestos de trabajo, aplicaciones de «interfaz» y de «motor», soporte intermedio), y termina en el sistema responsable de enviar el mensaje a SWIFT (por ejemplo, SWIFT VPN Box) o a Internet (siendo este último aplicable al acceso basado en Internet).

a) Requisito 1.1: Política de seguridad de la información

La dirección establecerá una política clara en consonancia con los objetivos de negocio y demostrará su apoyo y compromiso con la seguridad de la información mediante la elaboración, la aprobación y el mantenimiento de una política de seguridad de la información destinada a gestionar la seguridad de la información y la ciberresiliencia en toda la organización respecto a la identificación, la evaluación y el tratamiento de los riesgos de ciberseguridad y seguridad de la información. La política contendrá al menos las secciones siguientes: objetivos, ámbito de aplicación (incluidos ámbitos como la organización, los recursos humanos, la gestión de activos, etc.), principios y reparto de responsabilidades.

b) Requisito 1.2: Organización interna

Se establecerá un marco de seguridad de la información para aplicar la política de seguridad de la información dentro de la organización. La dirección coordinará y revisará el establecimiento del marco de seguridad de la información para garantizar la aplicación de la política de seguridad de la información (conforme al requisito 1.1) en toda la organización, incluidos la asignación de recursos suficientes y el reparto de responsabilidades en materia de seguridad a tal fin.

c) Requisito 1.3: Terceros

La seguridad de las instalaciones de tratamiento de la información y de la información de la organización no debe verse mermada por la introducción de uno o varios terceros o de los productos o servicios que estos proporcionan, o por la dependencia de estos. Se controlará el acceso de terceros a las instalaciones de tratamiento de la información de la organización. Cuando sea preciso que terceros o productos de terceros accedan a las instalaciones de tratamiento de la información de la organización, se llevará a cabo una evaluación de riesgos para determinar las implicaciones para la seguridad y los requisitos de control. Los controles se acordarán y determinarán de acuerdo con cada tercero pertinente.

d) Requisito 1.4: Gestión de activos

Todos los activos de información, los procesos de negocio y los sistemas de información subyacentes, tales como los sistemas operativos, las infraestructuras, las aplicaciones de negocio, los productos disponibles, los servicios y las aplicaciones desarrolladas por el usuario, en el ámbito de la cadena de las operaciones de pago se contabilizarán y tendrán un propietario designado. Se asignará la responsabilidad del mantenimiento y el funcionamiento de los controles adecuados en los procesos operativos y los componentes informáticos relacionados para salvaguardar los activos de información. Nota: el propietario puede delegar la realización de controles específicos, según proceda, pero sigue siendo responsable de la adecuada protección de los activos.

e) Requisito 1.5: Clasificación de los activos de información

Los activos de información se clasificarán en función de su importancia para la correcta prestación del servicio por parte del participante. La clasificación indicará la necesidad, las prioridades y el grado de protección requeridos al tratar el activo de información en los procesos de negocio pertinentes y tendrá en cuenta también los componentes informáticos subyacentes. Se utilizará un sistema de clasificación de activos de información aprobado por la dirección para determinar un conjunto adecuado de controles de protección a lo largo del ciclo de vida de los activos de información (incluida la retirada y destrucción de los activos de información) y para comunicar la necesidad de medidas de tratamiento especiales.

f) Requisito 1.6: Seguridad de los recursos humanos

Las responsabilidades en materia de seguridad se abordarán antes de la contratación del personal mediante descripciones de los puestos de trabajo adecuadas y en las condiciones laborales. Todos los candidatos a un empleo, los contratistas y los usuarios terceros serán sometidos a un examen adecuado, especialmente en el caso de los puestos sensibles. Los empleados, contratistas y usuarios terceros de las instalaciones de tratamiento de la información firmarán un contrato relativo a sus funciones y responsabilidades en materia de seguridad. Se garantizará un nivel adecuado de conocimiento de todos los empleados, contratistas y usuarios terceros, y se les proporcionará educación y formación sobre los procedimientos de seguridad y el uso correcto de las instalaciones de tratamiento de la información para minimizar los posibles riesgos para la seguridad. Se establecerá un procedimiento disciplinario formal para tratar las violaciones de la seguridad por parte de los empleados. Se establecerán responsabilidades para garantizar que se gestiona la salida o traslado de un empleado, contratista o tercero dentro de la organización, así como la devolución de todo el equipo y la supresión de todos los derechos de acceso.

g) Requisito 1.7: Seguridad física y ambiental

Las instalaciones de tratamiento de la información esencial o sensible estarán alojadas en zonas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad y controles de entrada adecuados. Estarán físicamente protegidas contra el acceso no autorizado, los daños y las interferencias. El acceso debe concederse únicamente a las personas a las que les sea aplicable el requisito 1.6. Se establecerán procedimientos y normas para proteger los soportes físicos que contengan activos de información cuando se encuentren en tránsito.

Los equipos estarán protegidos de las amenazas físicas y medioambientales. Es necesario proteger los equipos (incluidos los equipos utilizados fuera de las instalaciones) y establecer protección para evitar la retirada de bienes, a fin de reducir el riesgo de acceso no autorizado a la información y para prevenir la pérdida o deterioro de equipos o información. Pueden ser necesarias medidas especiales para protegerse de las amenazas físicas y salvaguardar las instalaciones de apoyo, tales como las infraestructuras de suministro eléctrico y de cableado.

h) Requisito 1.8: Gestión de las operaciones

Se establecerán responsabilidades y procedimientos para la gestión y el funcionamiento de las instalaciones de tratamiento de la información que abarquen todos los sistemas subyacentes de la cadena de las operaciones de pago de extremo a extremo.

Por lo que se refiere a los procedimientos operativos, incluida la administración técnica de los sistemas informáticos, se llevará a cabo, cuando proceda, la separación de funciones para reducir el riesgo de un mal uso del sistema de manera negligente o deliberada. Cuando no pueda llevarse a cabo la separación de funciones por razones objetivas documentadas, se llevarán a cabo controles compensatorios tras un análisis formal de los riesgos. Se establecerán controles para prevenir y detectar la introducción de códigos maliciosos en los sistemas de la cadena de las operaciones de pago. También se establecerán controles (incluida la concienciación de los usuarios) para prevenir, detectar y eliminar códigos malintencionados. Solo se utilizará el código móvil de fuentes fiables (por ejemplo, componentes de Microsoft COM firmados y Java Applets). Se controlará estrictamente la configuración del navegador (por ejemplo, el uso de extensiones y plugins).

La dirección aplicará políticas de salvaguarda y recuperación de los datos. Dichas políticas incluirán un plan del proceso de restauración que se probará con regularidad al menos una vez al año.

Se controlarán los sistemas que sean esenciales para la seguridad de los pagos y se registrarán los acontecimientos relacionados con la seguridad de la información. Los registros del operador se utilizarán para garantizar que se detectan problemas en el sistema de información. Los registros del operador se revisarán periódicamente por muestreo, atendiendo a la criticidad de las operaciones. Se supervisará el sistema para comprobar la eficacia de los controles que se consideren esenciales para la seguridad de los pagos y para verificar la conformidad con un modelo de política de acceso.

Los intercambios de información entre organizaciones se basarán en una política formal de intercambio, se llevarán a cabo de conformidad con los acuerdos de intercambio entre las partes implicadas y se ajustarán a la legislación pertinente. Los componentes de software de terceros empleados en el intercambio de información con TARGET2 (como los programas informáticos recibidos de una Oficina de Servicios en el escenario 2 de la sección del ámbito de aplicación del acuerdo de autocertificación de TARGET2) deberán utilizarse con arreglo a un acuerdo formal con el tercero.

i) Requisito 1.9: Control de acceso

El acceso a los activos de la información se justificará atendiendo a los requisitos de negocio (necesidad de conocer[1]) y de acuerdo con el marco establecido de políticas corporativas (incluida la política de seguridad de la información). Se establecerán normas claras de control de acceso basadas en el principio de mínimo privilegio[2] para reflejar

1 El principio de necesidad de conocer se refiere a la identificación de la información a la que una persona necesita acceder para desempeñar sus funciones.

2 El principio de mínimo privilegio hace referencia a la adaptación del perfil de acceso de un sujeto a un sistema informático para que se ajuste a la función empresarial correspondiente.

fielmente las necesidades de los procesos de negocio e informáticos correspondientes. Cuando proceda (por ejemplo, para la gestión de copias de seguridad), el control de acceso lógico debe estar en consonancia con el control de acceso físico, a menos que existan controles compensatorios adecuados (por ejemplo, cifrado, anonimización de datos personales).

Se establecerán procedimientos formales y documentados para controlar la asignación de derechos de acceso a los sistemas y servicios de información que se encuentren dentro del ámbito de aplicación de la cadena de las operaciones de pago. Los procedimientos abarcarán todas las fases del ciclo de vida del acceso de los usuarios, desde el registro inicial de nuevos usuarios hasta la baja definitiva de los usuarios que ya no requieran acceso.

Se prestará especial atención, cuando proceda, a la asignación de derechos de acceso de tal importancia que el abuso de dichos derechos pueda tener graves repercusiones negativas en las operaciones del participante (por ejemplo, derechos de acceso que permitan la administración del sistema, la anulación de los controles del sistema, el acceso directo a los datos de negocio).

Se establecerán controles adecuados para identificar, autenticar y autorizar a los usuarios en puntos específicos de la red de la organización, por ejemplo, para el acceso local y remoto a los sistemas de la cadena de las operaciones de pago. Las cuentas personales no se compartirán para garantizar la asunción de responsabilidades.

En el caso de las contraseñas, las normas se establecerán y aplicarán mediante controles específicos para garantizar que las contraseñas no se puedan adivinar fácilmente, por ejemplo, normas de complejidad y validez temporal limitada. Se establecerá un protocolo seguro de recuperación o restablecimiento de contraseña.

Se elaborará y aplicará una política sobre el uso de controles criptográficos para proteger la confidencialidad, autenticidad e integridad de la información. Se establecerá una política de gestión de claves para apoyar el uso de controles criptográficos.

Habrá una política de visualización de información confidencial en pantalla o impresa (por ejemplo, una pantalla clara, una política de escritorio clara) para reducir el riesgo de acceso no autorizado.

Cuando se trabaje a distancia, se tendrán en cuenta los riesgos de trabajar en un entorno desprotegido y se aplicarán los controles técnicos y organizativos adecuados.

j) Requisito 1.10: Adquisición, desarrollo y mantenimiento de los sistemas de información

Los requisitos de seguridad se determinarán y acordarán antes del desarrollo o la implantación de los sistemas de información.

Se incorporarán controles adecuados en las aplicaciones, incluidas las desarrolladas por el usuario, para garantizar un tratamiento correcto. Estos controles abarcarán la validación de

los datos de entrada, el procesamiento interno y los datos de salida. Pueden ser necesarios controles adicionales para los sistemas que procesan información sensible, valiosa o esencial, o que repercuten en ella. Dichos controles se determinarán en función de los requisitos de seguridad y la evaluación de riesgos de acuerdo con las políticas establecidas (por ejemplo, política de seguridad de la información, política de control criptográfico).

Los requisitos operativos de los nuevos sistemas se establecerán, documentarán y probarán antes de su aceptación y utilización. Por lo que se refiere a la seguridad de la red, deben aplicarse controles adecuados, incluida la segmentación y la gestión segura, teniendo en consideración el carácter esencial de los flujos de datos y el nivel de riesgo de las zonas de red de la organización. Se llevarán a cabo controles específicos para proteger la información sensible que circule a través de redes públicas.

Se controlará el acceso a los archivos del sistema y al código fuente del programa, y los proyectos informáticos y las actividades de apoyo se llevarán a cabo de manera segura. Se procurará evitar la exposición de datos sensibles en entornos de prueba. Se controlarán estrictamente los entornos de proyectos y de apoyo. Se controlará estrictamente el despliegue de los cambios en producción. Se llevará a cabo una evaluación del riesgo de los principales cambios que se vayan a introducir en producción.

También se llevarán a cabo actividades periódicas de pruebas de seguridad de los sistemas en producción de acuerdo con un plan predefinido basado en los resultados de una evaluación de riesgos, y las pruebas de seguridad incluirán, como mínimo, evaluaciones de la vulnerabilidad. Se evaluarán todas las deficiencias detectadas durante las actividades de las pruebas de seguridad y se prepararán y supervisarán oportunamente planes de acción para subsanar cualquier deficiencia detectada.

k) Requisito 1.11: Seguridad de la información en las relaciones con proveedores[3]

Para garantizar la protección de los sistemas de información internos del participante a los que puedan acceder los proveedores, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del proveedor deberán documentarse y acordarse formalmente con el proveedor.

l) Requisito 1.12: Gestión de los incidentes de seguridad de la información y mejoras

Para garantizar un enfoque coherente y eficaz de la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre incidentes y deficiencias en materia de seguridad, se establecerán y probarán funciones, responsabilidades y procedimientos a nivel técnico y empresarial a fin de asegurar una recuperación rápida, eficaz, ordenada y segura de los incidentes de seguridad de la información, incluidos los escenarios relacionados con una causa relacionada con el ciberespacio (por ejemplo, un fraude llevado

[3] En el contexto de este procedimiento, se entenderá por proveedor cualquier tercero (y su personal) que tenga un contrato (acuerdo) con la entidad para prestar un servicio y que, en virtud del acuerdo de servicios, el tercero (y su personal) tenga acceso, ya sea a distancia o in situ, a la información o a los sistemas de información o a las instalaciones de procesamiento de la información de la entidad en cuestión o asociados al ámbito enmarcado en el procedimiento de autocertificación de TARGET2.

a cabo por un agresor externo o por uno interno). El personal que participe en estos procedimientos recibirá la formación adecuada.

m) Requisito 1.13: Revisión de la conformidad técnica

Los sistemas de información internos de los participantes (por ejemplo, los sistemas internos, las redes internas y la conectividad a la red externa) se evaluarán periódicamente para comprobar el cumplimiento del marco de políticas establecido por la organización (por ejemplo, política de seguridad de la información, política de control criptográfico).

n) Requisito 1.14: Virtualización

Las máquinas virtuales invitadas cumplirán todos los controles de seguridad establecidos para el hardware y los sistemas físicos (por ejemplo, refuerzo, registro). Los controles relativos a los hipervisores deberán incluir: refuerzo del hipervisor y del sistema operativo de alojamiento, corrección de errores periódica, separación estricta de diferentes entornos (por ejemplo, producción y desarrollo). La gestión centralizada, el registro y el seguimiento, así como la gestión de los derechos de acceso, en particular para las cuentas con elevados privilegios, se llevarán a cabo atendiendo a una evaluación de riesgos. Las máquinas virtuales invitadas gestionadas por el mismo hipervisor tendrán un perfil de riesgo similar.

o) Requisito 1.15: Computación en la nube

El uso de soluciones en la nube públicas o híbridas en la cadena de las operaciones de pago debe basarse en una evaluación formal del riesgo, teniendo en cuenta los controles técnicos y las cláusulas contractuales relacionadas con la solución en la nube.

Si se utilizan soluciones en la nube híbridas, se entiende que el nivel de criticidad del sistema global será el más alto de los sistemas conectados. Todos los componentes de las soluciones híbridas que se encuentren en las instalaciones deberán estar separados de los demás sistemas instalados en ellas.

2. Gestión de la continuidad operativa (aplicable solo a los participantes críticos)

Los siguientes requisitos (2.1 a 2.6) se refieren a la gestión de la continuidad operativa. Todos los participantes en TARGET2 clasificados por el Eurosistema como críticos para el correcto funcionamiento del sistema TARGET2 deberán contar con una estrategia de continuidad operativa que contemple los elementos siguientes:

a) Requisito 2.1: Se elaborarán planes de continuidad operativa y se establecerán procedimientos para su mantenimiento.

b) Requisito 2.2: Se dispondrá de un emplazamiento operativo alternativo.

c) Requisito 2.3: El perfil de riesgo del emplazamiento alternativo debe ser diferente del emplazamiento principal, a fin de evitar que ambos emplazamientos se vean afectados al mismo tiempo por el mismo suceso. Por ejemplo, el emplazamiento

alternativo debe estar en una red eléctrica y un circuito central de telecomunicaciones diferentes de los de la sede principal de la empresa.

d) **Requisito 2.4**: En el caso de que se produzca una interrupción operativa grave que impida el acceso al emplazamiento principal o que el personal esencial no esté disponible, el participante crítico deberá poder reanudar las operaciones normales desde el emplazamiento alternativo, donde debe ser posible cerrar correctamente el día hábil y abrir el siguiente o los siguientes días hábiles.

e) **Requisito 2.5**: Deberán establecerse procedimientos para garantizar que el tratamiento de las operaciones se reanude desde el emplazamiento alternativo en un plazo razonable tras la interrupción inicial del servicio y que sea proporcional a la importancia de la actividad que se haya visto interrumpida.

f) **Requisito 2.6**: Se debe probar al menos una vez al año la capacidad para hacer frente a las interrupciones operativas y el personal esencial debe recibir una formación adecuada. El período máximo entre pruebas no será superior a un año.

Entrada en vigor

Esta Aplicación Técnica entrará en vigor el día 21 de noviembre de 2021.

Para consultas relacionadas con operativa, pueden dirigirse a la dirección de correo electrónico target2@bde.es, o al teléfono 91 338 5840.

Para cuestiones administrativas, a la dirección de correo target2.registro@bde.es, o a los teléfonos 91 338 5582 ó 91 338 7044.

Juan Ayuso
Director General de Operaciones,
Mercados y Sistemas de Pago