SISTEMA NACIONAL DE COMPENSACIÓN ELECTRÓNICA

INSTRUCCIONES OPERATIVAS COMUNES DEL SERVICIO DE CENTRALIZACIÓN DE INTERCAMBIOS

INSTRUCCIÓN SNCE/CE/01/059
MODIFICACIÓN DE LA INSTRUCCIÓN SNCE/CE/01/001

Asunto: Actualización de las modalidades de conexión al SNCE e incorporación del nuevo Marco de control de ciberseguridad del SNCE

El Consejo de Administración de Iberpay, en su reunión de diciembre de 2019, aprobó las Líneas Estratégicas de la compañía para el periodo 2020-2021. Dentro de estas Líneas Estratégicas se definieron dos iniciativas concretas orientadas a revisar los requisitos de acceso al SNCE, tanto técnicos como de ciberseguridad, y que tienen por objetivos: mejorar la resiliencia del SNCE, adecuarlos a las prácticas habituales de otras cámaras europeas y facilitar la incorporación de entidades de tamaño muy reducido.

En este sentido, se establecen nuevas modalidades de conexión para las entidades que estén conectadas directamente al Centro Común de Procesos del SNCE, o vayan a estarlo, en función de su criticidad y riesgo operativo en el sistema, así como su nivel de actividad, tanto en el SNCE en general, entendiendo como tal el valor agregado de su nivel de actividad en el conjunto de los subsistemas en los que participa la entidad, según se define en el artículo 8.3.1. del Reglamento del SNCE, como en el Subsistema de Transferencias SEPA Inmediatas en particular. Estas modalidades de conexión se incluyen en un nuevo Anexo 20 de las presentes Instrucciones Operativas Comunes.

Adicionalmente, se persigue reforzar la ciberseguridad en el SNCE, bajo una perspectiva integral, incluyendo los procesos y los sistemas relevantes en las entidades que estén conectadas directamente al Centro Común de Procesos del SNCE (CICLOM). Para ello, se establecen nuevos requisitos de ciberseguridad que las entidades deben satisfacer según lo definido en la versión vigente en cada momento del Marco de control de ciberseguridad en el SNCE, así como los requerimientos de gobernanza establecidos en su Modelo de Gobierno, recogido en el nuevo Anexo 21 de las presentes Instrucciones Operativas Comunes, donde se establecen los mecanismos de evaluación y reporte exigibles a las entidades obligadas.

Por último, se hacen algunas correcciones y actualizaciones menores en algunos textos de la instrucción.

En virtud de lo expuesto, la Sociedad Española de Sistemas de Pago, S.A, a propuesta del Comité Técnico Asesor del SNCE y una vez concluido el trámite de aprobación de su normativa por parte de Banco de España (establecido en la Circular 1/2007, de 26 de enero), ha dispuesto la publicación de la presente instrucción.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

ENTRADA EN VIGOR

La presente instrucción entrará en vigor en la fecha de su publicación.

Se acompañan, las hojas modificadas de la Instrucción SNCE/CE/01/001, en las que se incorporan las modificaciones introducidas por la presente instrucción, así como la incorporación de los Anexos 20 y 21 correspondientes a: i) los Requisitos de conexión al Centro Común de Procesos del SNCE y ii) el Modelo de gobierno para el Marco de control de ciberseguridad en el SNCE, respectivamente.

En Madrid, a 31 de julio de 2020

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

SISTEMA NACIONAL DE COMPENSACIÓN ELECTRÓNICA

INSTRUCCIONES OPERATIVAS COMUNES

ÍNDICE

INTRODUCCIÓN 12

CAPITULO I – CENTROS DE PROCESO 15

1. CENTROS DE PROCESOS 15

1.1 Centro Común de Procesos del SNCE 15

1.2 De las Entidades con conexión técnica directa al Centro Común de Procesos del SNCE 16

1.2.1. Centro Principal de las entidades 17

1.2.2. Centro de Respaldo de las entidades 18

2. MECANISMOS DE INTERCAMBIO DE INFORMACIÓN. OPCIONES DE REDES DE INTERCAMBIO 19

2.1. Intercambio de ficheros 19

2.2. Servicios web 19

2.3 Seguridad en los intercambios del SNCE 20

2.3.1. Seguridad en las redes de comunicaciones 20

2.3.2. Seguridad extremo a extremo mediante la firma electrónica de ficheros 20

2.3.3. Requisitos de ciberseguridad en el SNCE 22

CAPITULO II - OTROS ASPECTOS TECNICOS 24

1. TABLAS DE ENTIDADES PARTICIPANTES EN LOS SUBSISTEMAS DEL SNCE Y FICHERO DEL CALENDARIO DE DÍAS INHÁBILES DE INTERCAMBIO Y DE LIQUIDACIÓN 24

1.1 Objeto 24

1.2 Contenido de las tablas de entidades 24

1.2.1. Tablas de entidades 24

1.2.2. Fichero de Calendario de días inhábiles 25

ANEXO 17: MODIFICACIÓN JURÍDICA SUSTANCIAL DE UNA ENTIDAD MIEMBRO DEL SNCE COMO ENTIDAD PARTICIPANTE DIRECTO

Modelo 1 Modelo de escrito a dirigir a Iberpay por cambio en la situación societaria de un miembro del SNCE.
Modelo 2 Contrato de adhesión al SNCE.
Modelo 3 Modelo de autorización al Banco de España para el asiento en la cuenta del módulo de pagos de Target2.
Modelo 4 Modelo de escrito de garantía.
Modelo 5 Identificación de las personas representante y suplente de una entidad ante el SNCE

ANEXO 18: MODIFICACIÓN JURÍDICA SUSTANCIAL DE UNA ENTIDAD MIEMBRO DEL SNCE COMO ENTIDAD REPRESENTADA

Modelo 1 Modelo de escrito a dirigir a Iberpay por cambio en la situación societaria de un miembro del SNCE.
Modelo 2 Contrato de adhesión al SNCE.
Modelo 3 Sin contenido
Modelo 4 Identificación de las personas representante y suplente de una entidad ante el SNCE

ANEXO 19: TABLA DE ENTIDADES ADHERIDAS AL SUBSISTEMA DE TRANSFERENCIAS SEPA INMEDIATAS

Modelo 1: Con presentación y recepción de operaciones a través de Redsys
Modelo 2: Con presentación y recepción de operaciones directamente a través de CICLOM

ANEXO 20: REQUISITOS DE CONEXIÓN AL CENTRO COMÚN DE PROCESOS DEL SNCE

ANEXO 21: MODELO DE GOBIERNO PARA EL MARCO DE CONTROL DE CIBERSEGURIDAD EN EL SNCE

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

- Excepcionalmente, el intercambio de aquellas Transferencias SEPA Inmediatas, cuyos importes se incluyan dentro del saldo operacional neto total integrado del SNCE para su asiento en las cuentas del módulo de pagos en TARGET2 mediante el procedimiento de liquidación ASI4, podrá llevarse a cabo a través de la conexión técnica de la plataforma de procesamiento online, cuyo gestor técnico en la actualidad es Redsys, con la plataforma CICLOM.

  Ambas plataformas residen en el Centro Común de Procesos del SNCE, en el que se lleva a cabo el intercambio de información relativo a estas transferencias entre las entidades miembros y el resto de la operativa relacionada con la compensación y liquidación de las operaciones
- El envío y la recepción de operaciones entre las entidades del SNCE y el resto de las entidades adheridas a otros sistemas de pagos con los que Iberpay haya alcanzado acuerdos de interoperabilidad (Pasarelas de Interoperabilidad) o con los que mantenga Pasarelas de Pago, así como el resto de las funciones las lleva a cabo igualmente el Centro Común de Procesos del SNCE.

En los escenarios de indisponibilidad de alguna de estas infraestructuras técnicas que impidan el normal funcionamiento de un centro, el procesamiento completo del SNCE se realizará desde otro de los centros de proceso, de manera automática y totalmente transparente para las entidades. Los centros de procesos podrán estar gestionados por terceros, con los cuales se celebrarán los correspondientes contratos de subcontratación, para lo cual los gestores técnicos del Sistema están amplia y expresamente autorizados.

1.2 De las Entidades con conexión técnica directa al Centro Común de Procesos del SNCE

Los centros de proceso de las entidades, debe cumplir las especificaciones y requisitos establecidos por Iberpay como gestor del SNCE y haber cubierto satisfactoriamente el plan de pruebas que tenga definido en cada momento.

Los requisitos que deben de cumplir los centros de proceso de las entidades son los siguientes:

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

- Disponer de al menos dos centros de proceso físicos o en cloud ubicados dentro del Espacio Económico Europeo.
- Tener redundancia a nivel de centros de proceso, siendo al menos dos de ellos independientes entre sí en cuanto a recursos (alimentación, comunicaciones, seguridad, etc.) y con una separación geográfica suficiente para evitar verse afectado ante desastres naturales o atentados terroristas de ámbito comarcal. En el caso de servidores en cloud, cuando no se pueda garantizar la separación geográfica, se deberá contar con un servicio de recuperación de desastres.
- Disponer de las capacidades de proceso adecuadas para realizar las funciones de envío y recepción de operaciones y de información relacionada con el SNCE.
- Tener configurados los accesos a las redes de comunicación del SNCE y, en el caso de las conexiones con alguna de las redes privadas, disponer de capacidad de alojamiento en los centros de proceso para instalar los equipos de comunicaciones del proveedor.
- Haber realizado los procesos de certificación que los gestores técnicos del Sistema establezcan en cada momento, que aseguren la capacitación técnica de las entidades mantenida en el tiempo.

1.2.1. Centro Principal de las entidades

a) Definición

Es el centro de proceso que una entidad utiliza para su participación en el SNCE, conectado a las redes de comunicación del SNCE, mediante enlaces o direcciones, cuyos detalles técnicos se han comunicado a los gestores técnicos del Sistema, y que es utilizado habitualmente en todas las funciones efectuadas para el envío y recepción de operaciones y de información relacionada con el SNCE.

Un mismo centro de proceso, puede ser utilizado por una o más entidades, aunque cada una de ellas deberá contar con enlaces diferenciados.

Una entidad puede tener más de un centro principal

1.2.2. Centro de Respaldo de las entidades

Es el centro de proceso que una entidad utiliza para su participación cuando, por cualquier causa, no puede disponer de su Centro Principal.

Por lo tanto, un Centro de Respaldo es un centro de proceso de backup, distinto al Centro Principal y conectado a las mismas redes de comunicación que el centro principal mediante direcciones también distintas a las de éste.

Un mismo centro de proceso puede ser utilizado como Centro de Respaldo por una o más entidades, aunque cada una de ellas debe contar con enlaces diferenciados. Asimismo, el Centro Principal de una entidad puede también ser Centro de Respaldo de otra u otras entidades.

Una entidad puede tener más de un centro de respaldo.

Respecto al funcionamiento del centro de respaldo, cuando se produzca una situación que ocasione la indisponibilidad del Centro Principal de una entidad durante un periodo que ésta prevea superior al necesario para poner en marcha su Centro de Respaldo, la entidad transferirá su operativa en el SNCE a este último centro, en la forma que se establece en el apartado siguiente.

Producida la situación de indisponibilidad en el Centro Principal, la entidad comunicará a los gestores técnicos del Sistema la puesta en servicio del Centro de Respaldo, mediante un correo electrónico remitido por el representante de la entidad en el SNCE dirigido a los gestores técnicos del Sistema, indicando el momento en que éste va a estar operativo para envío y recepción de operaciones.

Cuando la entidad que haya sufrido la indisponibilidad comunique al SNCE que su Centro Principal está de nuevo disponible, deberán darse los pasos necesarios para volver a la situación normal de utilización del Centro Principal.

2. MECANISMOS DE INTERCAMBIO DE INFORMACIÓN. OPCIONES DE REDES DE INTERCAMBIO

El tipo de transmisión de la información representativa de las operaciones, así como de las imágenes de los documentos, en su caso, desde el centro de proceso de las entidades participantes presentadoras al Centro Común de Procesos del SNCE, dependerá del formato de los datos intercambiados (ficheros o servicios web) en función de cada subsistema.

2.1. Intercambio de ficheros

El intercambio de ficheros se podrá efectuar mediante alguno de los siguientes mecanismos:

- Software de transferencia de ficheros EDITRAN a través de las redes de comunicación del SNCE, o
- Protocolo de transferencia segura de ficheros sFTP a través de las redes de comunicación del SNCE para el subsistema de transferencias SEPA inmediatas, o
- Servicio de transferencia de ficheros FileAct sobre red SWIFT Net y SWIFT Net Bulk Payments, utilizando el Grupo Cerrado de Usuarios (CUG) de Iberpay.

2.2. Servicios web

En el caso de los subsistemas y servicios en tiempo real, como el Subsistema de Transferencias SEPA Inmediatas del SNCE, se utilizarán servicios web sobre las redes de comunicación del SNCE.

Los requisitos y el procedimiento para la conexión de una entidad al Centro Común de Procesos del SNCE se encuentran recogidos en el Anexo 20 de las presentes Instrucciones Operativas Comunes.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

2.3 Seguridad en los intercambios del SNCE

2.3.1. Seguridad en las redes de comunicaciones

Las redes de comunicaciones del SNCE incorporan sus propios elementos de seguridad, proporcionando amplias garantías de integridad sobre los datos que diariamente intercambian las entidades participantes en los distintos subsistemas del SNCE en los que participan.

Por lo tanto, no requiere el intercambio de claves criptográficas, salvo en los intercambios de operaciones a través del subsistema de Transferencias SEPA Inmediatas, en el caso de aquellas entidades que utilicen la plataforma de procesamiento online de un proveedor que contemple el uso de estas u otras claves como un requisito necesario.

2.3.2. Seguridad extremo a extremo mediante la firma electrónica de ficheros

Adicionalmente a la seguridad de las redes de comunicaciones, el SNCE incorpora una serie de medidas de ciberseguridad complementarias y enfocadas a garantizar, de extremo a extremo, la integridad de los datos de las operaciones intercambiadas, basadas en la firma electrónica.

La incorporación de la firma electrónica, tras la generación un fichero que contenga operaciones, garantiza la autenticidad de la información contenida en el fichero firmado, al poder detectar una posible manipulación del mismo en caso de que el resultado del proceso de verificación de la firma electrónica en el momento de su recepción no sea el esperado.

a) Definición y objetivo

Se establece el uso de un procedimiento estándar de firma electrónica que se incorpora a los ficheros de operaciones del subsistema de Transferencias SEPA, tanto en los generados por las entidades con conexión directa al Centro Común de Procesos del SNCE, como en los generados por el propio Centro Común de Procesos del SNCE.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

- Proceso fallido en el Centro Común de Procesos del SNCE: el fichero de operaciones no puede procesarse y es rechazado. Ese rechazo se informa a la entidad correspondiente a través del fichero de validación indicando el motivo del rechazo: certificado revocado, firma no correcta o fichero manipulado.

  Tal y como se indica en el apartado anterior, este fichero de validación enviado desde el Centro Común de Procesos del SNCE hacia la entidad, no es objeto de firma electrónica.

  Una vez resuelto el problema que había provocado el proceso fallido de verificación de la firma electrónica, la entidad vuelve a enviar el fichero, debidamente firmado, al Centro. Común de Procesos del SNCE.

- Proceso fallido en la entidad: el fichero de operaciones no puede procesarse. Se informa inmediatamente a Iberpay sobre el error detectado a través de correo electrónico y/o llamada al departamento de operaciones de Iberpay. Adicionalmente, la entidad solicitará a Iberpay el reenvío del fichero a, siguiendo lo descrito en el apartado 2.6 sobre procedimiento de reenvío de ficheros del Capítulo II.

2.3.3. Requisitos de ciberseguridad en el SNCE

Las entidades con conexión directa al Centro Común de Procesos del SNCE deben cumplir unos mínimos controles de ciberseguridad con objeto de fortalecer la comunicación y cooperación entre los participantes del SNCE en materia de ciberseguridad, asegurando la ciberresiliencia del sistema en su conjunto. Asimismo, a través de estos controles, se asegura la protección de los puntos de entrada y salida al sistema, evitando la propagación de incidentes.

Por este motivo, las entidades con conexión directa al Centro Común de Procesos del SNCE deberán satisfacer los requisitos de ciberseguridad que se recojan en la versión vigente en cada momento del *Marco de Control de Ciberseguridad del SNCE*, así como los requerimientos de gobernanza establecidos en su modelo de gobierno, recogido en el Anexo 21 de las presentes Instrucciones Operativas Comunes, donde se establecen los mecanismos de evaluación y reporte exigibles a las entidades obligadas.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

- Formulario de datos estáticos. Autorización de adeudos sistemas vinculados (TARGET2 form collection of Static Data – Debit mandate for AS Settlement)-Mod. 2002 (Modelo 11).

- Modelo de escrito de garantía (Modelo 12).

- Formulario de datos estáticos – Autorización de adeudos sistemas vinculados (TARGET2 form for collection of Static Data – Sub Account for dedicated liquidity) mod 1014 (Modelo 16).

Estos cuatro últimos modelos, se cumplimentarán sólo una vez, cuando la entidad se dé de alta en el SNCE. La entidad los cumplimentará por triplicado, remitiendo dos a Iberpay, que a su vez hará seguir uno a Banco de España. El tercer ejemplar quedará en poder de la propia entidad.

En cuanto a requisitos técnicos, las entidades que deseen adherirse como Participante Directo deberán cumplir con los requerimientos establecidos en el Capítulo I de las presentes Instrucciones Operativas Comunes, así como con los requisitos y el procedimiento de conexión definidos en el Anexo 20 de las presentes Instrucciones Operativas Comunes.

Asimismo, los Participantes Directos deberán satisfacer los requisitos de ciberseguridad que se recojan en la versión vigente en cada momento del *Marco de Control de Ciberseguridad del SNCE*, así como los requerimientos de gobernanza establecidos en su modelo de gobierno, recogido en el Anexo 21 de las presentes Instrucciones Operativas Comunes, donde se establecen los mecanismos de evaluación y reporte exigibles a las entidades obligadas.

Como medida previa al alta en el SNCE, las entidades deberán haber superado todas las fases de las pruebas de incorporación al subsistema correspondiente, establecidas por los gestores técnicos del Sistema en el correspondiente plan de pruebas, que será debidamente dado a conocer mediante comunicación del SNCE.

Los Participantes Directos asumen solidariamente la responsabilidad derivada de las operaciones intercambiadas en los subsistemas por las entidades a las que representan.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

Para la incorporación de entidades como Participantes Directos a los distintos subsistemas de intercambio, se establece un calendario, con suficiente antelación, con objeto de organizar a las entidades en ventanas y establecer periodos de prueba entre ellas. No obstante, previo acuerdo del CTA podrán establecerse otras fechas de incorporación.

La solicitud de incorporación deberá estar en poder de Iberpay con un plazo mínimo de dos meses de antelación a la fecha en la que la entidad desee incorporarse al correspondiente subsistema, que habrá de ser una de las previstas en el calendario definido a tal efecto.

Iberpay informará tanto a la entidad solicitante como al resto de entidades, la fecha de entrada en vigor de la incorporación. Esta comunicación se realizará como mínimo con quince días naturales de antelación a la fecha prevista de incorporación.

De conformidad con lo especificado en las instrucciones operativas, todos los documentos y operaciones que, emitidos por las propias entidades o por sus clientes debidamente autorizados por ellas, que sean susceptibles de tratamiento en el subsistema correspondiente, deberán estar normalizados.

Complementariamente, Iberpay podrá solicitar a la entidad interesada en participar en el SNCE, cualquier información adicional que considere razonable para preservar al máximo el correcto funcionamiento del SNCE.

2.2 Como entidad representada

La entidad que desee participar como Entidad Representada deberá cumplimentar y presentar la siguiente documentación (Anexo 9):

- Carta de solicitud de incorporación al SNCE (Modelo 1).

- Solicitud de incorporación a un subsistema nacional (Modelo 2).

- Solicitud de adhesión al subsistema de Transferencias SEPA, cuando proceda (Modelo 3).

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

- Carta de comunicación de aceptación en la representación por el Participante Directo que la representante (Modelo 9).

Las entidades representadas podrán participar enviando y recibiendo operaciones a través de su Participante Directo o hacerlo mediante conexión técnica directa con el Centro Común de Procesos del SNCE, bien bajo la modalidad de Gestión de Representada o en el subsistema de Transferencias SEPA Inmediatas. En cualquiera de estas situaciones, la liquidación la seguirá llevando a cabo su Participante Directo representante.

Para ello, además de los requisitos anteriores, las entidades representadas con conexión directa al Centro Común de Procesos del SNCE para la presentación y recepción técnica directa de operaciones, deberán cumplir con los requerimientos establecidos en el Capítulo I de las presentes Instrucciones Operativas Comunes, así como con los requisitos y el procedimiento de conexión definidos en el Anexo 20 de las presentes Instrucciones Operativas Comunes.

Asimismo, las entidades con conexión directa al Centro Común de Procesos del SNCE deberán satisfacer los requisitos de ciberseguridad que se recojan en la versión vigente en cada momento del *Marco de Control de Ciberseguridad del SNCE*, así como los requerimientos de gobernanza establecidos en su modelo de gobierno, recogido en el Anexo 21 de las presentes Instrucciones Operativas Comunes, donde se establecen los mecanismos de evaluación y reporte exigibles a las entidades obligadas.

Como medida previa al alta en el SNCE, deberán haber superado todas las fases de pruebas de incorporación al subsistema correspondiente establecidas por los gestores técnicos del Sistema en el plan de pruebas.

En el caso de darse de alta en el Servicio de Gestión de Representada la entidad deberá suscribir el “Acuerdo de Prestación del Servicio de Gestión de Representadas del SNCE” disponible en la web de Iberpay dentro del apartado de “Más Servicios”. En el caso del Subsistema de Transferencias SEPA Inmediatas deberá indicarlo en el modelo de adhesión al citado subsistema.

Para la incorporación de entidades como representadas a los distintos subsistemas se establece, como referencia, el primer día hábil de cada mes.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

Para la incorporación de entidades como representadas con conexión directa al Centro Común de Procesos del SNCE para cualquier de sus subsistemas se establece, como referencia, el mismo calendario que para los Participantes Directos.

Iberpay informará tanto a la entidad solicitante como al resto de entidades, la fecha de entrada en vigor de la incorporación. Esta comunicación se realizará como mínimo con quince días naturales de antelación a la fecha prevista de incorporación.

La solicitud de incorporación deberá estar en poder de Iberpay con un plazo mínimo de treinta días naturales de antelación a la fecha en la que la entidad desee incorporarse al correspondiente subsistema, y de dos meses para las entidades representadas con conexión directa al Centro Común de Procesos del SNCE.

Existe la posibilidad de que entidades adheridas al subsistema de Transferencias SEPA Inmediatas puedan participar en la Pasarela Iberpay-RT1 con EBA Clearing, como BICs accesibles de un Participante Directo en la misma.
Los BICs accesibles son entidades representadas que no llevan a cabo la presentación y recepción técnica directa de operaciones, haciéndolo por su cuenta el Participante Directo que las representa en la pasarela, asumiendo la liquidación de sus operaciones que estará garantizada por la previa provisión de fondos llevada a cabo por aquél. Estas entidades requieren simplemente la identificación con su BIC por su Participante Directo representante en su propio documento de adhesión.

De conformidad con lo especificado en las instrucciones operativas, todos los documentos y operaciones que, emitidos por las propias entidades o por sus clientes debidamente autorizados por ellas, que sean susceptibles de tratamiento en el subsistema correspondiente, deberán estar normalizados.

Complementariamente, Iberpay podrá solicitar a la entidad interesada en participar en el SNCE, cualquier información adicional que considere razonable para preservar al máximo el correcto funcionamiento del SNCE.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

- Sexto ciclo: de 19:30:00 h a 21:30:00 h del día D con ajuste en TARGET2 a las 21:45:00 del día hábil D+1.

- Séptimo ciclo: de 21:30:00 h del día D a 01:00:00 h del día D+1 con ajuste en TARGET2 a las 01:15:00 h del día hábil D+1.

- Octavo ciclo: de 1:00:00 h a 07:00:00 h del día D+1 con ajuste en TARGET2 a las 07:15:00 h del día hábil D+1.

c) Transferencias SEPA inmediatas enviadas y recibidas a través de la Pasarela Iberpay-RT1.

Provisión de fondos entre Participantes Directos en la Pasarela y Participantes Directos en RT1 (con liquidación en ASI2). Se establecen cuatro ciclos de liquidación por ajustes de liquidez:

- Primer ciclo: de 7:00:00 h a 10:00:00 h del día D con asiento en cuenta en TARGET2 a las 10:15:00 h del día hábil D.

- Segundo ciclo: de 10:00:00 h a 13:00:00 h del día D con asiento en cuenta en TARGET2 a las 13:15:00 h del día hábil D.

- Tercer ciclo: de 13:00:00 h a 16:00:00 h del día D con asiento en cuenta en TARGET2 a las 16:15:00 h del día hábil D.

- Cuarto ciclo: de 16:00:00 h del día D a 7:00:00 h del día D+1 con asiento en cuenta en TARGET2 a las 7:15:00 h del día hábil D+1.

Aunque el último ciclo diario de ajuste de liquidez de un día D se lleva a cabo a las 16:15 h, los Participantes Directos en el servicio RT1 podrán seguir haciendo ajustes de liquidez en ASI6 real-time durante cuatro horarios adicionales, sin que puedan hacerse entre los Participantes Directos en la Pasarela y los Participantes Directos en RT1.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

directamente en las cuentas en el módulo de pagos de TARGET2 de los Participantes Directos que se encuentren en esta situación.

1.5. Operaciones del Subsistema de Transferencias SEPA Inmediatas cuya liquidación requiere de una provisión previa de fondos mediante la utilización del procedimiento de liquidación en TARGET2 ASI6 real-time

1.5.1. Operaciones intercambiadas entre entidades adheridas al Subsistema.

Tanto el asiento en las cuentas de los clientes ordenantes y beneficiarios, como en las cuentas de posición de los Participantes Directos en este subsistema, se lleva a cabo por el importe bruto de cada operación en tiempo real de manera continua en régimen de 24x7.

El modelo de liquidación ASI6 real-time en TARGET2, además del asiento en las cuentas de posición de los Participantes Directos, permite llevar a cabo ajustes de liquidez de los fondos previamente aportados por los Participantes Directos que así lo requieran, en la cuenta técnica específica mantenida por el Banco de España en TARGET2-BE por cuenta del SNCE y gestionada por Iberpay.

Estos ajustes de liquidez permiten reponer fondos desde la cuenta en el módulo de pagos de TARGET2 del Participante Directo hacia la cuenta técnica, siempre que el saldo de su cuenta de posición descienda por debajo del umbral inferior fijado para la entidad, o bien devolver el exceso de liquidez en el caso de que dicho saldo supere el umbral superior igualmente establecido previamente.
Adicionalmente, la entidad puede solicitar un ajuste excepcional de reposición de fondos a través de la funcionalidad diseñada a al efecto en el Sistema de Información del SNCE.

Estos ajustes solo pueden realizarse si la plataforma TARGET2 está abierta para permitir estos movimientos de fondos.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

En los escenarios de indisponibilidad de alguna de estas infraestructuras técnicas que impidan el normal funcionamiento de un centro, el procesamiento completo del SNCE se realizará desde el otro centro de proceso, de manera automática y totalmente transparente para las entidades.

b) Indisponibilidad en las redes de comunicación:

Los gestores técnicos del Sistema gestionan las redes de comunicaciones del SNCE utilizadas habitualmente por las entidades financieras para los intercambios con el Centro Común de Procesos del SNCE, así como los accesos de este Centro Común a la red SWIFT, en su caso.

Tanto las entidades financieras como los gestores técnicos del Sistema disponen de doble acceso a las redes de comunicaciones del SNCE, por lo que, si en algún momento se produce una incidencia grave con pérdida de conectividad en el acceso principal, entra en funcionamiento automáticamente el acceso de respaldo. Los gestores técnicos del Sistema gestionarán con el proveedor de la red la recuperación de la conectividad a través de la línea principal tan pronto como sea posible.

Si la incidencia inhabilita tanto el acceso principal a las redes de comunicaciones del SNCE como el de respaldo de una entidad financiera, se podrá utilizar el servicio FileAct de la red SWIFT para los intercambios con el Centro Común de Procesos del SNCE, siempre y cuando la entidad tenga previamente configurada y probada su conexión a través de esta red.

c) Indisponibilidad de los edificios de en los que se encuentren alojadas las oficinas desde las que se opera el Sistema:

En el caso de que se produzca un acontecimiento externo anormal que afecte al edificio donde se encuentran las oficinas que operen el Sistema, esta circunstancia no tiene repercusión sobre el normal funcionamiento del SNCE. Según lo previsto en el SGCN, la operación funcional del servicio se realizará desde el Centro Alternativo de Operaciones.

Atendiendo a las circunstancias y según la gravedad de la incidencia, Iberpay informará a las entidades participantes, mediante correo electrónico dirigido al responsable del SNCE y a través del Sistema de Información, de los detalles de la incidencia, la situación actual, el impacto

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

2.1.3 Procedimiento de envío de ficheros al servicio

La entidad hará llegar a Iberpay las operaciones a presentar en el SNCE utilizando alguno de los canales de envío para los que la entidad se haya previamente certificado, pudiendo ser los siguientes:

a) Entorno de pruebas de la entidad: si la situación de contingencia se ha producido en su entorno de producción, la entidad podrá utilizar su entorno de pruebas para enviar las operaciones al servicio.

b) Servicio FileAct de SWIFT: si la situación de contingencia impide la conexión a las redes de comunicaciones del SNCE, la entidad podrá utilizar el servicio de transferencia de ficheros FileAct sobre la red SWIFT.

c) Mecanismos seguros de transferencias de ficheros por Internet:

- Upload / download de ficheros a través del Sistema de Información del SNCE.
- Secure File Transfer Protocol (sFTP)
- Correo electrónico con fichero adjunto

d) Soporte físico (etiquetado y precintado):

- CD o DVD
- Pen drive USB
- Disco duro externo USB

Adicionalmente, la entidad enviará a Iberpay un correo electrónico, a la dirección indicada anteriormente, con los siguientes datos de control para verificar los ficheros de operaciones recibidos:

- Subsistema;
- Tipo de Fichero;
- Nombre del fichero;
- Total de Operaciones; y - Total de Importes.

Una vez contrastados los datos, Iberpay comunicará a la entidad la correcta recepción de los ficheros y el inicio de su procesamiento.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

b) Pruebas periódicas.

Iberpay establecerá un Plan de Pruebas periódicas para la verificación, mantenimiento y mejora del servicio.

Todos los Participantes Directos o entidades representadas con presentación y recepción directa de operaciones en el SNCE, participarán en estas pruebas periódicas al menos una vez al año.

Durante la realización de estas pruebas, las entidades podrán certificarse en otros canales adicionales para el envío y recepción de sus ficheros de operaciones, distintos a los ya certificados.

2.2 Otras situaciones de contingencia en las entidades

Además de las situaciones que pudieran requerir la activación del servicio de intercambio de operaciones para entidades en contingencia, pueden darse otro tipo de situaciones en las que es suficiente con solicitar la ampliación de los plazos de devolución, el recurso a los procedimientos de excepción para el intercambio físico de documentos e imágenes o la utilización del segundo ciclo de intercambio para los subsistemas que así lo tengan previsto.

En estos casos, la entidad cumplimentará y enviará a Iberpay el modelo de Notificación de Situaciones Extraordinarias (Anexo 11) mediante correo electrónico a la dirección snce@iberpay.es o al fax 91.571.19.08, aceptándose por el resto de las entidades salvo buen fin, siendo asumidos los perjuicios derivados de este recurso por la entidad solicitante.

3. MEDIDAS DE CONTINUIDAD OPERATIVA APLICABLES AL SNCE COMO SISTEMA VINCULADO PARTICIPANTE EN TARGET2

En el caso de que se produzcan incidencias que afecten a las comunicaciones entre el SNCE, como Sistema Vinculado, y TARGET2-BdE, o problemas que afecten al normal funcionamiento de la plataforma TARGET2, se seguirán los procedimientos de contingencia y medidas de continuidad operativa recogidos en la correspondiente Aplicación Técnica del Banco de España y en el Convenio firmado entre Iberpay y TARGET2-BdE.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

ANEXO 20: REQUISITOS PARA LA CONEXIÓN DE ENTIDADES AL CENTRO COMÚN DE PROCESOS DEL SNCE

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

ÍNDICE

0. INTRODUCCIÓN 2

1. COMUNICACIONES EN EL SNCE 3

1.1 MECANISMOS DE INTERCAMBIO DE INFORMACIÓN EN EL SNCE 3
1.2 REDES DE COMUNICACIÓN DEL SNCE 3
1.3 MODELO DE CONEXIÓN A LAS REDES DE COMUNICACIÓN 3
1.4 REQUISITOS DE CONEXIÓN POR GRUPO DE ENTIDADES 4

2. PROCEDIMIENTO DE CONEXIÓN PARA LAS ENTIDADES 5

© Sociedad Española de Sistemas de Pago, S.A. (iberpay)

0. INTRODUCCIÓN

El presente anexo constituye, junto con el Capítulo I de las Instrucciones Operativas Comunes, el conjunto de requisitos técnicos y procedimientos para la adhesión de una entidad con conexión directa al Centro Común de Procesos del SNCE a cualquiera de sus subsistemas.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

1. COMUNICACIONES EN EL SNCE

1.1 MECANISMOS DE INTERCAMBIO DE INFORMACIÓN EN EL SNCE

Los mecanismos de intercambio de información desde el centro de proceso de las entidades, que se conectan directamente con el Centro Común de Procesos del SNCE, y este último, dependerá del formato de los datos intercambiados (ficheros o servicios web) y de cada subsistema, pudiendo ser::

— Software de transferencia de ficheros EDITRAN;

— Protocolo de transferencia segura de ficheros sFTP;

— Servicios web; y

— Mensajería de SWIFT Net.

1.2 REDES DE COMUNICACIÓN DEL SNCE

Los citados mecanismos de intercambio de información con el Centro Común de Procesos del SNCE se llevan a cabos a través de las siguientes redes de comunicación del SNCE:

— Red privada principal del SNCE;

— Red privada backup del SNCE con un segundo proveedor, diferente al de la red principal;

— Conexión segura por redes públicas; y

— Red de comunicación SWIFT en el caso en el que se utilice SWIFT Net para el intercambio de ficheros.

1.3 MODELO DE CONEXIÓN A LAS REDES DE COMUNICACIÓN

Se ha establecido un modelo de conexión a las redes de comunicación para las entidades conectadas directamente al Centro Común de Procesos del SNCE que tiene en cuenta la criticidad y el riesgo operativo de cada entidad en función de:

— Su nivel de actividad en el SNCE, entendiendo como tal el valor agregado de su nivel de actividad en el conjunto de los subsistemas en los que participa la entidad, según se define en el artículo 8.3.1. del Reglamento del SNCE; y

— Su nivel de actividad en el subsistema de Transferencias SEPA Inmediatas del SNCE.

Con este criterio se han definido los siguientes grupos de entidades en función de su criticidad para el correcto funcionamiento del SNCE en su conjunto:

— Grupo 1: Entidades con un nivel de actividad en el SNCE o en el subsistema de Transferencias SEPA Inmediatas del SNCE mayor al 6%.

— Grupo 2: Entidades con un nivel de actividad en el SNCE o en el subsistema de Transferencias SEPA Inmediatas del SNCE entre el 1 y 6% y que no cumplan las condiciones para pertenecer al Grupo 1.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

— Grupo 3: Entidades con un nivel de actividad en el SNCE y en el subsistema de Transferencias SEPA Inmediatas del SNCE inferior al 1%.

Adicionalmente se deben de tener en cuenta las siguientes consideraciones:

— En el caso de compartición de líneas de comunicación entre entidades, se considerará la suma de los niveles de actividad individuales de estas entidades, entendiendo como tales, los valores agregados de los niveles de actividad de todos y cada uno de los subsistemas en los que participan las entidades, según se define en el artículo 8.3.1. del Reglamento del SNCE.

— En el caso de nuevas incorporaciones al SNCE, las entidades adheridas entrarán inicialmente en el Grupo 3.

— Con carácter anual se revisará la evolución del nivel de actividad considerado de las entidades, por si fuera necesaria una actualización de sus modalidades de conexión.

— Estos requisitos marcan el mínimo a cumplir por las entidades en cada grupo, pudiendo cada entidad optar por implantar una modalidad de conexión de un grupo superior.

— En su caso, se revisarán y analizarán bilateralmente situaciones particulares de las entidades.

— En el caso de las entidades que actualmente utilizan conexiones a través de SWIFT Net en los subsistemas tradicionales (Transferencias en D y D+1, Adeudos SEPA, Cheques, etc.), se permitirá mantener esta conexión como única conexión o como conexión backup en su caso, ya que por defecto dispone de doble proveedor de comunicaciones.

1.4 REQUISITOS DE CONEXIÓN POR GRUPO DE ENTIDADES

Los requisitos de conexión en función del grupo en el que se catalogue a cada entidad son los siguientes:

— Grupo 1: Conexión principal a través de la red privada principal del SNCE y conexión backup a través de la red privada backup del SNCE.

— Grupo 2: Conexión principal a través de la red privada principal del SNCE y conexión backup a elegir entre la red privada backup del SNCE y la conexión segura por redes públicas.

— Grupo 3: Se requiere al menos una conexión a elegir entre la red privada principal del SNCE y la conexión segura por redes públicas.

En cuanto a la conexión SWIFT Net, que puede ser utilizada para los subsistemas con intercambio de ficheros, se considera una opción válida para cualquier grupo de entidades, tanto como conexión principal como conexión backup.

© Sociedad Española de Sistemas de Pago, S.A. (iberpay)

2. PROCEDIMIENTO DE CONEXIÓN PARA LAS ENTIDADES

Para proceder a utilizar cualquiera de los mecanismos y redes de comunicación con el SNCE, las entidades deberán:

- Solicitar preeviamente el mecanismo de envío y recepción de operaciones seleccionado y ser planificada y probada su implantación en coordinación con los gestores técnicos del Sistema, siguiendo, en cualquier caso, lo establecido en la normativa y procedimiento de adhesión al o a los subsistemas implicados;
- Tener en cuenta que esta funcionalidad podrá ser solicitada y utilizada por subsistema, siendo de aplicación a todas sus operaciones.
- Solicitar la red o redes de comunicación del SNCE seleccionadas siempre y cuando cumpla con los requisitos de conexión para las entidades.
- Mantener cada mecanismo y red de comunicación durante un periodo de tiempo razonable.
- Asumir los gastos propios del mecanismo y las redes de comuniación elegidas.
- En el caso de elección de la red SWIFT Net, asumir los gastos propios de Swift y solicitar su adhesión al Grupo Cerrado de Usuarios (CUG) de Iberpay con carácter previo a las pruebas (CUG de test) y a la puesta en funcionamiento (CUG live).

La interconexión entre los centros de proceso de los gestores técnicos del Sistema y los centros de procesos de las entidades conectadas directamente al Centro Común de Procesos del SNCE, permiten llevar a cabo la presentación y recepción de operaciones en los horarios establecidos, así como la distribución de informes y lanzamiento de consultas, en su caso, relativos a la presentación y recepción de operaciones, a los procesos de liquidación y asiento en cuenta, datos estadísticos, etc.

La publicación de los aspectos funcionales y técnicos necesarios para la instalación de los mecanismos de envío y recepción de operaciones y normativa sobre su funcionamiento, así como las sucesivas modificaciones a los mismos, se realizará mediante instrucciones operativas o comunicaciones del SNCE dirigidas a las entidades desde Iberpay. Asimismo, las entidades disponen de Manuales de Operación, Especificaciones Funcionales y Técnicas de cada subsistema en los que se recogen los requerimientos técnicos aplicables en cada momento. Esta documentación complementaria será también de obligado cumplimiento y aplicación para las entidades.

Las entidades vendrán obligadas a prestar cuanta colaboración les sea requerida en la realización de las pruebas necesarias y en los plazos que se fijen para la puesta en funcionamiento de nuevas versiones de los mecanismos de envío y recepción de operaciones que hayan de efectuarse.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

ANEXO 21: MODELO DE GOBIERNO PARA EL MARCO DE CONTROL DE CIBERSEGURIDAD DEL SNCE

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

INDICE

1. INTRODUCCIÓN AL MARCO DE CONTROL DE CIBERSEGURIDAD DEL SNCE 2
2. PROCESO DE DEFINICIÓN DEL MARCO DE CONTROL 4
3. COMPOSICIÓN DEL MARCO DE CONTROL 5
4. ALCANCE DEL MARCO DE CONTROL 7
5. ACTUALIZACIÓN Y MANTENIMIENTO DEL MARCO DE CONTROL 9
6. MODELO DE GOBIERNO 10
6.1 ROLES Y RESPONSABILIDADES 10
6.1.1 Iberpay 10
6.1.2 Entidades 11
6.1.3 Grupo de Ciberseguridad del SNCE 12
6.2 CUMPLIMIENTO DEL MARCO DE CONTROL. EVALUACIÓN 12
6.3 FASES DEL PROCESO Y PLAZOS ESTABLECIDOS 14
6.4 REPORTE Y VISIBILIDAD DE LOS RESULTADOS DE EVALUACIÓN 15
6.5 SEGUIMIENTO 15
7. ANEXO I - DEFINICIONES DEL MARCO DE CONTROL DE CIBERSEGURIDAD 16
8. ANEXO II - RELACIÓN DE LOS DOCUMENTOS ENTREGADOS Y DESTINATARIO 18
9. ANEXO III - RIESGOS INCLUIDOS EN EL MARCO DE CONTROL 19
10. ANEXO IV - RELACIÓN ENTRE PRINCIPIOS Y OBJETIVOS DE CONTROL 21
11. ANEXO V - ALINEAMIENTO A ESTÁNDARES Y OTROS MARCOS 22

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

1. INTRODUCCIÓN AL MARCO DE CONTROL DE CIBERSEGURIDAD DEL SNCE

El Sistema Nacional de Compensación Electrónica (SNCE) gestionado por Iberpay a través de la plataforma CICLOM, constituye el mecanismo normativo, operativo y técnico que soporta el sistema de pagos al por menor español y realiza el intercambio, compensación y liquidación interbancaria de las transacciones. Estas transacciones comprenden principalmente transferencias, adeudos, cheques y efectos, cada una de ellas a través de módulos específicos o subsistemas dentro del SNCE.

Actualmente, ya sea como Participantes Directos o como Entidades Representadas, en el SNCE participan la totalidad de los bancos, cajas de ahorros y cooperativas de crédito establecidos en España, lo que lo convierte en un claro objetivo de delincuencia organizada, grupos de activismo o atacantes con el fin de comprometer el sistema financiero.

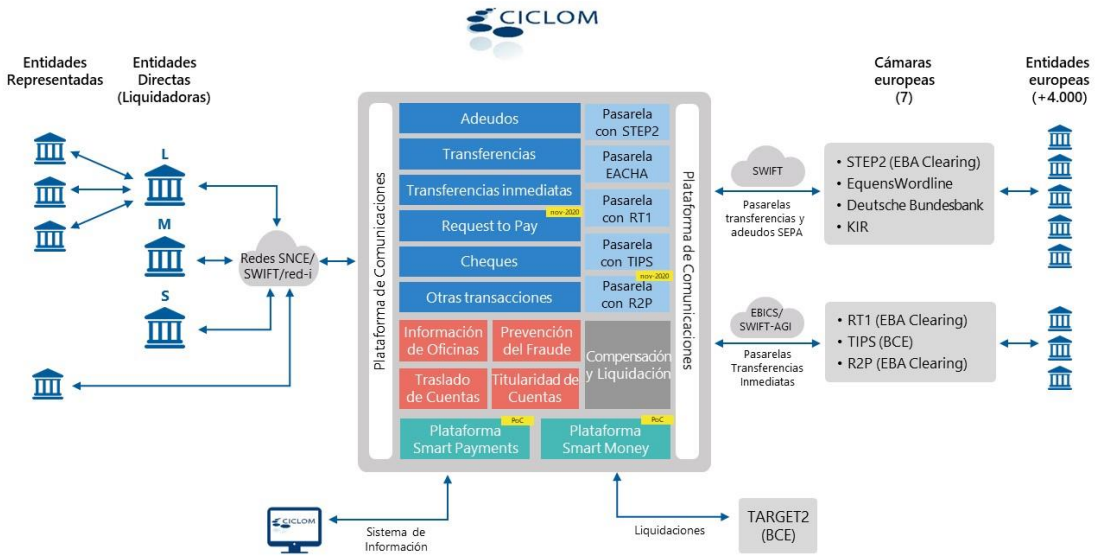


Figura 1. Esquema general de la plataforma CICLOM

En este contexto, el compromiso de alguno de los participantes en el SNCE podría comprometer al resto y, por tanto, al sistema financiero español. Por este motivo se define el presente Marco de Control de Ciberseguridad para el SNCE que pretende:

- Fortalecer la comunicación y cooperación entre los participantes del SNCE en materia de ciberseguridad.
- Definir una línea base de referencia de controles de ciberseguridad exigible a los participantes del sistema actuales o futuros.
- Asegurar la ciberresiliencia del sistema en su conjunto.
- Asegurar la protección de los puntos de entrada y salida al sistema, evitando la propagación de incidentes.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

- Fortalecer el protocolo de respuesta a incidentes en el caso de compromiso de algunos de los participantes y que pudiera poner en riesgo al resto.
- Definir un ciclo de mejora continua que permita la adaptación del Marco de Control ante nuevas amenazas y/o lecciones aprendidas.
- Alcanzar un gobierno efectivo en materia de ciberseguridad para el SNCE basado en la mejora e iteración continua, fortaleciendo la relación entre Iberpay como gestor del sistema y las distintas Entidades participantes.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

2. PROCESO DE DEFINICIÓN DEL MARCO DE CONTROL

El Marco ha sido construido en base al entendimiento de la arquitectura y la infraestructura desplegada por las Entidades para la comunicación con el SNCE. Para ello, Iberpay ha distribuido un cuestionario a las Entidades integrantes, lo que ha permitido obtener un mayor conocimiento sobre los activos y procesos involucrados en la comunicación y el procesamiento de la información que se intercambia con el SNCE.

Como resultado de este análisis, se constata que la arquitectura tecnológica presente en las Entidades conectadas al SNCE, con independencia de los subsistemas a los que se conectan, presenta una arquitectura similar a la siguiente, diferenciando entre transferencias SEPA inmediatas y el resto de los subsistemas basados en intercambio de ficheros:

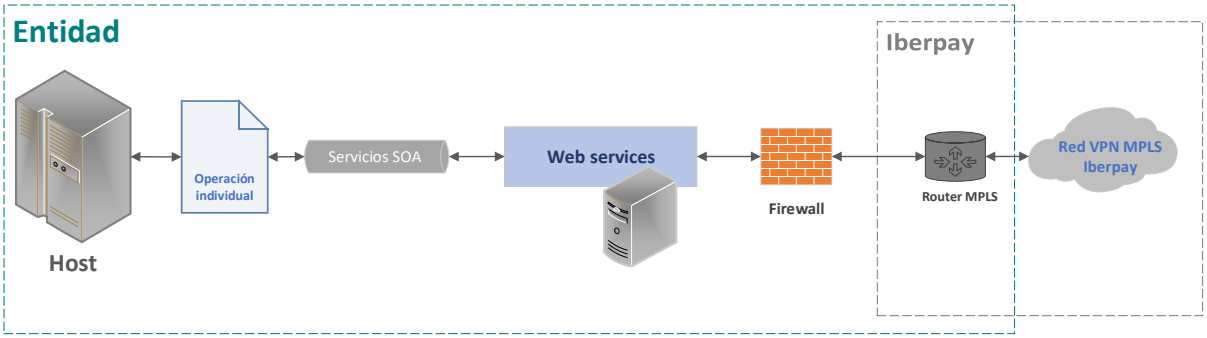


Figura 2. Diagrama genérico para la conexión al subsistema de Transferencias SEPA Inmediatas

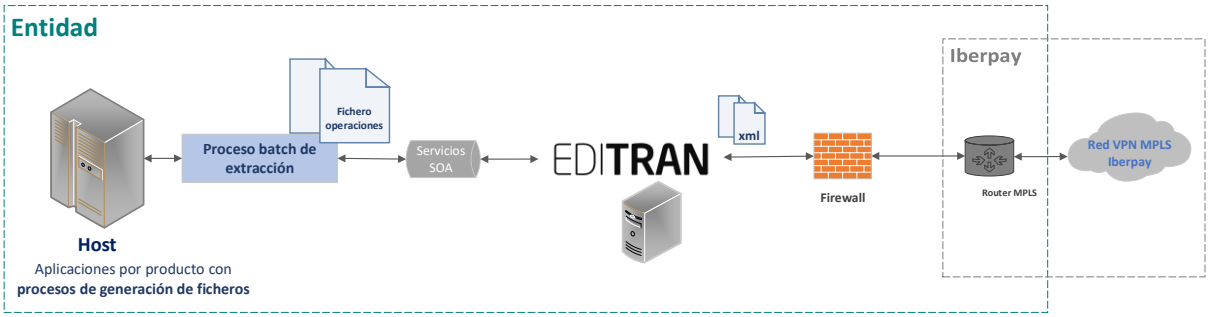


Figura 3. Diagrama genérico para la conexión al resto de subsistemas

Una vez conocidos estos activos y procesos se han identificado los principales riesgos[1] asociados y se han establecido los objetivos de control y controles necesarios para mitigarlos hasta un nivel aceptable.

Finalmente, se han considerado tendencias y buenas prácticas del sector financiero y de pagos en materia de seguridad para construir un marco completo, razonable y adaptado a los riesgos identificados.

[1] En el Anexo III - Riesgos incluidos en el Marco de Control se incluye el listado de riesgos sobre los que se construye el Marco de Control

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

3. COMPOSICIÓN DEL MARCO DE CONTROL

El Marco de Control definido se estructura conforme a los elementos presentados en el siguiente gráfico. En el mismo se incluye la volumetría de cada uno de los niveles en los que está estructurado:

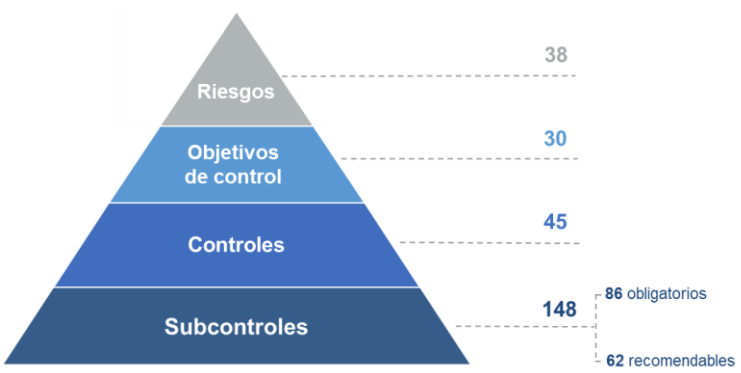


Figura 4. Lógica de construcción del Marco de Control

Los controles definidos dan cobertura a una suma de procesos, tecnología, políticas, gobierno, alineamiento con el negocio, concienciación y otros elementos necesarios para gestionar, de manera efectiva, la ciberseguridad de la Entidad respecto a los sistemas que interactúan con el SNCE.

A su vez, el Marco de Control se divide en 5 grandes principios focalizados en aquellos aspectos relevantes según la arquitectura e infraestructura local de las Entidades que se conectan con el SNCE:

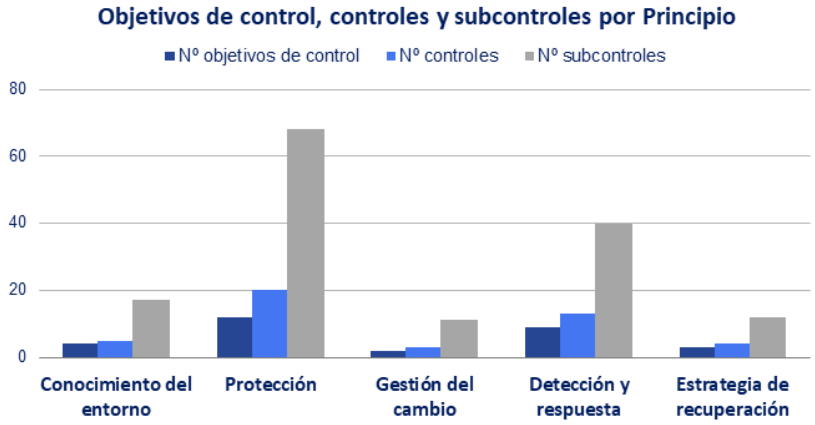


Figura 5. Principios del Marco de Control [2]

Los controles incluidos en el Marco de Control se encuentran en gran medida alineados con estándares y modelos conocidos de la Industria. Se proporciona, junto con el Marco

[2] En la tabla incluida en el Anexo IV – Relación entre principios y objetivos de control se recoge la relación entre estos 5 principios y los Objetivos de control abordados en el Marco de Control.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

de Control, la relación entre los controles del Marco y otros estándares, facilitando así su asimilación por parte de las Entidades[3] .

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

3 En el Anexo IV – Relación entre principios y objetivos de control se puede consultar más información al respecto.

4. ALCANCE DEL MARCO DE CONTROL

El Marco de Control evalúa la protección del SNCE desde el entorno local de las Entidades, por tanto, el alcance depende de la arquitectura concreta de cada Entidad participante. Dentro de este alcance se deben tener en cuenta las personas, los procesos, los sistemas y tecnologías que intervienen en la generación, procesamiento e intercambio de información con el SNCE:

- **Personas** dentro del alcance: los empleados y colaboradores de las Entidades que se ven afectadas de forma directa o indirecta por los controles incluidos en el Marco:
  - Responsable de la Seguridad de la Información de la Entidad.
  - Equipos dedicados a la monitorización de los sistemas, a la gestión de incidentes, al tratamiento de vulnerabilidades y demás actividades de control relacionadas directamente con la seguridad del sistema.
  - Operadores y administradores de los sistemas que se conectan al SNCE.
- **Procesos**: conjunto de actividades que se encargan de generar, de transformar (por ejemplo, de agrupar las transacciones en ficheros o su posterior conversión a XML), de intercambiar la información con Iberpay a través de los canales seguros establecidos. Adicionalmente, se incluyen aquellos procesos de soporte a la actividad que están relacionados con el SNCE, por ejemplo, proceso de gestión de incidentes, gestión de perfilado, entre otros.
- **Tecnología**: conjunto de servidores, aplicaciones, bases de datos y componentes de red que intervienen en la generación, procesamiento e intercambio de información con el SNCE. Algunos ejemplos de los elementos previamente mencionados son los siguientes:
  - Servidores: web, aplicación, base de datos, autenticación, proxy, protocolos de red, servidores de nombre de dominio, etc.
  - Aplicaciones: internas / externas, compradas / adaptadas, etc.
  - Componentes de red: firewalls, switches, routers, puntos de acceso wireless, appliances de red y de seguridad, etc. utilizados para proteger la red interna del exterior y para segmentar las redes y equipos utilizados para el SNCE de los del resto de la Entidad.

Sobre estos elementos, se requiere aplicar configuraciones y bastionado de seguridad adecuadas al riesgo, además de otros controles que les sean de aplicación.

Se incluyen aquellos elementos utilizados tanto para el subsistema de Transferencias SEPA Inmediatas como para el resto de los subsistemas en los que participe la Entidad (Adeudos, Transferencias SEPA, Cheques, Traspasos, Efectos, etc.).

Dado que en la mayoría de las Entidades la generación y transformación de la información que se intercambia con el SNCE tiene lugar en un entorno Host de propósito general, esto es, compartido con otros procesos de las entidades, para este caso concreto, se debe

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

limitar el alcance de los controles a aquellos procesos dedicados al SNCE y configuraciones o parámetros generales que puedan afectar a esta parte (como por ejemplo configuraciones en RACF, aplicaciones específicas, interfaces de entrada y salida de información para el SNCE, etc.)

El Marco de Control está dirigido a las entidades que participen en el SNCE como Participantes Directos, así como para todas aquellas Entidades Representadas con conexión técnica directa.

Así mismo, será de obligado cumplimiento para toda nueva entidad que desee incorporarse en el SNCE en las modalidades comentadas anteriormente.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

5. ACTUALIZACIÓN Y MANTENIMIENTO DEL MARCO DE CONTROL

El Marco de Control se ha planteado con un enfoque de mejora continua, de forma que en cada ciclo de evaluación se revisen y se actualicen los riesgos, objetivos de control y controles, con el fin de mejorar su adaptación al esquema del SNCE y las tendencias de la industria.

Para ello, se tendrán en cuenta tanto los resultados obtenidos de la revisión de las Entidades como sus comentarios respecto al Marco de Control que surjan en el seno del Grupo de Ciberseguridad del SNCE en cada iteración del proceso[4] .



Figura 6. Enfoque de mejora continua del Marco de Control

El Marco de Control está sujeto a revisión anual y, en su caso, actualización si fuera necesario, así como en función de situaciones excepcionales que motiven un cambio sobre los controles definidos, como puede ser un cambio en la infraestructura de las Entidades que se conectan al SNCE.

En las revisiones del Marco de Control, algunos controles inicialmente calificados como de cumplimiento recomendable, podrían pasar a ser obligatorios si así se determina siguiendo los procesos definidos de actualización.

[4] El detalle de este proceso se encuentra en el apartado 6.3 Fases del proceso y plazos establecidos.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

6. MODELO DE GOBIERNO

El Modelo de Gobierno pretende facilitar la colaboración y comunicación entre Iberpay como gestora del SNCE y los integrantes del sistema para la adopción del Marco de Control de Ciberseguridad del SNCE y servir como guía que contenga la información necesaria para que las Entidades puedan cumplir con sus obligaciones al respecto.

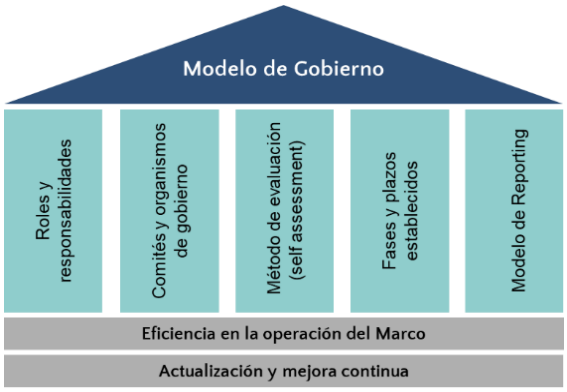


Figura 7. Bases sobre las que se construye el Modelo de Gobierno

Se determinan por tanto en el Modelo de Gobierno las personas, los procesos, los tiempos y las herramientas necesarias para hacer posible el manejo y la gestión del Marco de una forma ágil y eficiente.

6.1 ROLES Y RESPONSABILIDADES

En este apartado se definen las funciones y obligaciones en cuanto al Marco de Control por parte de Iberpay, las Entidades que se conectan al SNCE - y a las que va dirigido este Marco de Control-, y el Grupo de Ciberseguridad del SNCE, como órgano de coordinación con las Entidades participantes en el SNCE, en lo que a seguridad del sistema se refiere.

6.1.1 Iberpay

Responsable de la gestión del SNCE y responsable de la seguridad, continuidad y ciberresiliencia del mismo.

Es responsabilidad de Iberpay:

- La definición del Marco de Control, partiendo de la identificación de los ciber riesgos para el SNCE y definiendo los objetivos de control y los controles necesarios para mitigarlos hasta un nivel aceptable.
- Promover y fomentar entre las Entidades el cumplimiento del Marco de Control, comunicando todos aquellos aspectos necesarios con relación al mismo, definidos en su Modelo de Gobierno.
- Realizar un seguimiento continuo sobre la participación e involucración de las Entidades en relación con el cumplimiento del Marco de Control.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

- Fomentar el diálogo y aportación de sugerencias por parte de las Entidades con relación al Marco de Control, incorporando aquellos aspectos de mejora que contribuyan a la reducción de ciber riesgos del SNCE.
- Establecer la forma en la que las Entidades deben evaluarse frente al Marco de Control, definiendo así mismo las fechas y plazos para dichas evaluaciones. A estos efectos, Iberpay facilitará modelos de reporte y criterios de evaluación para facilitar la respuesta por parte de las Entidades.
- Tratar los resultados de las evaluaciones de las Entidades de forma confidencial y habilitar un canal de comunicación seguro con ellas para su intercambio.
- Diseñar un modelo de seguimiento interno que ayude a identificar la situación sectorial y posibles riesgos o desviaciones sobre el rendimiento esperado (número de entidades adheridas, existencia de entidades no proactivas o que no responden en tiempo y forma, adaptación al Marco de Control para cada una de las entidades, etc.).
- Informar, en el modo y forma que corresponda, a los diferentes grupos de interés del SNCE (Entidades, Comité Técnico Asesor, Grupo de Ciberseguridad, Consejo de Administración y Banco de España) del estado de cumplimiento del Marco de Control por parte del conjunto de las entidades.

6.1.2 Entidades

Participantes Directos conectados al SNCE y corresponsables del mantenimiento de la seguridad continuidad y ciberresiliencia del Sistema.

Es responsabilidad de las Entidades:

- Cumplir con los objetivos y controles del Marco de Control para minimizar los ciber riesgos del SNCE, fomentando la adopción del Marco de Control en los procesos corporativos de la Entidad.
- Definir internamente los procesos, los recursos, el personal encargado y los interlocutores que se verán involucrados en el gobierno y gestión del Marco de Control por parte de la Entidad.
- Designar un punto de contacto único que actúe como punto central de coordinación y comunicación para la gestión del Marco de Control por parte de la Entidad.
- Participar en los grupos u órganos de gobierno que establezca Iberpay para el seguimiento del Marco de Control.
- Reportar a Iberpay los resultados de las evaluaciones de cumplimiento, conforme a los formatos y plazos establecidos por Iberpay.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

- Definir las acciones necesarias para la adopción de los controles no implementados, realizando un seguimiento periódico para garantizar los plazos acordados para su implantación.
- Reportar a Iberpay en caso de acometer algún cambio relevante en la infraestructura de la Entidad que pudiera afectar al SNCE o tuviese impacto en el alcance del Marco de Control.
- Participar en el proceso de mejora continua del Marco de Control proporcionando opinión sobre el contenido y forma de gestión de éste.

6.1.3 Grupo de Ciberseguridad del SNCE

Órgano representativo de las Entidades participantes, asesor en materia de ciberseguridad y promotor de iniciativas de mejora para la seguridad, continuidad y ciberresiliencia en el SNCE.

Es responsabilidad del Grupo de Ciberseguridad del SNCE:

- Ser el centro de debate en relación con las actividades derivadas de la aplicación del Marco de Control de Seguridad del SNCE y su buen funcionamiento (metodología de evaluación, criterios de evaluación, periodicidad de las evaluaciones, seguimiento de la situación general de cumplimiento de todos los participantes).
- Analizar la conveniencia de los objetivos de control y los riesgos identificados en el Marco de Control y su alineamiento con la realidad presente en las Entidades a las que representan, aportando las sugerencias para la evolución del Marco de Control.
- Coordinar, vigilar e impulsar la adopción y el cumplimiento del Marco de Control por parte de las Entidades a las que representan.

6.2 CUMPLIMIENTO DEL MARCO DE CONTROL. EVALUACIÓN

Cada Entidad debe realizar un ejercicio de evaluación respecto al cumplimiento de los controles contenidos en el Marco de Control. Iberpay pone a disposición de las Entidades el formulario de evaluación, el cual contiene los siguientes campos:

Campos de información del contexto de los controles:

- **Principio**: Determina a cuál de los 5 principios detallados anteriormente pertenece el subcontrol (Conocimiento del Entorno, Protección, Gestión del Cambio, Detección y Respuesta o Estrategia de Recuperación.
- **Objetivo de Control**: Indica a alto nivel el aspecto que se persigue cubrir con esa familia de controles.
- **ID de Control**: Identificador único de control.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

- **Descripción del Control**: Para cada Objetivo de Control indica con un mayor nivel de detalle los aspectos a evaluar.
- **ID Subcontrol**: Identificador único de subcontrol.
- **Subcontrol**: Punto de control único que la Entidad debe evaluar si se encuentra implantado y con qué nivel de madurez.
- **Recomendable / Obligatorio**: Indica si se trata de un control obligatorio o recomendable.
- **Priorización**: Toma los valores A, B, C o D en función de la prioridad que se debe dar al cumplimiento del control, siendo "A" el más prioritario y "D" el menos, tratándose estos de controles recomendables. La Entidad deberá tener en cuenta este orden a la hora de priorizar su aplicación.
- **Evidencia tipo**: Ejemplo de evidencia que la Entidad podría utilizar para apoyar su respuesta. No será necesario que la Entidad aporte la evidencia a Iberpay, se trata de un campo orientativo.

Campos que cumplimentar por las Entidades:

- **Implantado**: Se debe marcar Sí o No en función de si la Entidad ha implementado el subcontrol.
- **Nivel de cumplimiento**: Representa la madurez del control implementado por la Entidad. Se debe marcar un valor entre el 1 y el 4 de acuerdo con la siguiente lógica.

Valor	Definición
1	El control está implementado, documentado, operando de forma efectiva y optimizado (se siguen mejores prácticas, se automatiza lo máximo posible y se busca una mejora continua del control).
2	El control está implementado, documentado y operando de forma efectiva de manera general, aunque hay posibles mejoras.
3	Existen controles similares, pero no estandarizados en toda la Entidad, se necesitan mejoras.
4	Control inexistente. Los riesgos no se encuentran mitigados de forma eficaz.

- **Fortalezas**: Campo donde se debe explicar el motivo que ha llevado a la Entidad a elegir un nivel alto de cumplimiento y los aspectos positivos sobre cómo se ha implementado el subcontrol.
- **Debilidades**: Campo donde se debe explicar el motivo que ha llevado a la Entidad a elegir un nivel bajo de cumplimiento y se deben incluir las necesidades de mejora. En este campo, se espera que la Entidad indique las

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

acciones planificadas y en marcha para solventar las debilidades detectadas. Sobre estas acciones se hará un seguimiento activo para confirmar que se están solventando en tiempo y forma.

Mecanismo de evaluación:

Se contempla la evaluación de madurez del Marco de Control a través de la realización de ejercicios de autoevaluación por parte de las propias Entidades, validados por roles competentes dentro de la Entidad (CISO, CTO, CIO, etc.), siguiendo las instrucciones detalladas anteriormente.

En el proceso de evaluación se deberán responder a todos los controles de carácter obligatorio y opcionalmente a los controles recomendables.

6.3 FASES DEL PROCESO Y PLAZOS ESTABLECIDOS



Figura 8. Representación de las fases del proceso de evaluación y actualización

Las fases del proceso de evaluación están claramente diferenciadas y son las siguientes:

- A partir de la fecha en la que se libere la versión del Marco de Control a las Entidades, éstas cuentan con un periodo de adecuación en el que pueden acometer los cambios o mejoras que consideren sobre sus sistemas o procesos relacionados con el SNCE.
- Pasado este periodo, las Entidades deben completar el cuestionario de autoevaluación y enviar sus respuestas a Iberpay dentro del plazo establecido para ello.
- Iberpay procesará los cuestionarios recibidos y presentará, tras su análisis, el informe con los resultados agregados obtenidos de la evaluación de cada una de las Entidades.
- Previo al siguiente ejercicio de evaluación, dado que se trata de un proceso iterativo y orientado a la mejora continua, se establece un periodo de consulta

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

en el que las Entidades dan su opinión sobre el contenido y formato del Marco de Control y proponen mejoras.

- En base al nivel de adaptación sectorial y a las propuestas realizadas, se liberará una nueva versión del Marco de Control adecuada y sobre el que las Entidades deberán repetir el proceso anteriormente descrito.

6.4 REPORTE Y VISIBILIDAD DE LOS RESULTADOS DE EVALUACIÓN

Envío del cuestionario de autoevaluación: Las Entidades deberán remitir a Iberpay la respuesta de su evaluación a través de correo electrónico a la dirección seguridad@iberpay.es cifrado con las claves PGP previamente intercambiadas entre Iberpay y cada Entidad.

El cuestionario se debe remitir en el mismo formato que se ha recibido de Iberpay (Excel) tras haber cubierto las columnas que se indican en el apartado 6.2 Cumplimiento del Marco de Control. Evaluación.

Reporte de los resultados: Una vez recibidas todas las respuestas, Iberpay procederá a su análisis y a la elaboración de un reporte de resultados por Entidad que compartirá de forma individual con cada una de las ellas a través del mismo canal por el que se ha recibido.

Adicionalmente, se mostrará a cada Entidad de forma anonimizada la situación del resto de Entidades evaluadas y la posición de la Entidad frente a estas, sirviendo de comparativa anónima para que la Entidad pueda conocer su situación respecto al sector.

Iberpay facilitará, de la misma forma, la información extraída de la evaluación de las Entidades a Banco de España como figura reguladora.

6.5 SEGUIMIENTO

En caso de que el resultado de alguna Entidad esté significativamente por debajo del nivel de cumplimiento medio, Iberpay realizará junto con la Entidad el seguimiento de los aspectos detectados de mayor criticidad. Para ello, se tomarán como referencia y se hará seguimiento de las acciones de mejora definidas por la Entidad en el campo “Debilidades” (tal como se ha explicado en el Apartado 6.2 Cumplimiento del Marco de Control - evaluación).

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

7. ANEXO I - DEFINICIONES DEL MARCO DE CONTROL DE CIBERSEGURIDAD

Listado de definiciones relacionadas con el Marco de Control, enumeradas según su orden de aparición en el documento:

- **Participante Directo**: Entidad de crédito miembro del SNCE que participa en al menos un Subsistema presentando y recibiendo siempre por sí misma Operaciones y, en su caso, en representación, en nombre y por cuenta de una o más Entidades Representadas con las que así lo haya acordado, asumiendo en cualquier caso las obligaciones de pago derivadas de la Liquidación, tanto de sus propias Operaciones como de las correspondientes a las Entidades Representadas a las que represente incluyendo las de provisión previa de fondos para aquellas Operaciones que así lo requieran así como las obligaciones de garantía referidas en el Reglamento del SNCE. El Banco de España también podrá ser Participante Directo.
- **Entidad Representada:** Es toda entidad que participa en el SNCE a través de un Participante Directo con el que ha suscrito un acuerdo de representación en virtud del cual éste asume solidariamente las obligaciones de pago derivadas de la liquidación de las operaciones de la entidad representada, incluyendo las de provisión previa de fondos para aquellas Operaciones que así lo requieran. Podrá presentar y recibir técnicamente operaciones de forma directa previo acuerdo con Iberpay y con el Participante Directo que la represente.
- **Subsistema**: Cada uno de los procedimientos de Intercambio, Compensación y Liquidación de Operaciones referido a un tipo de instrumento de pago o de información procesados en el SNCE.
- **Subsistema de transferencias SEPA inmediatas**: Subsistema del SNCE a través del cual se envían y reciben órdenes de transferencias SEPA individuales en tiempo real adaptadas al estándar definido por el EPC y cuyos importes se abonan al beneficiario de forma inmediata.
- **Priorización**: Indica la prioridad que se debe dar al cumplimiento del subcontrol, siendo A el más prioritario y D, el menos, por tratarse de un control recomendable. La Entidad debe tener en cuenta este orden a la hora de priorizar su aplicación.

  El criterio empleado para establecer la priorización de los subcontroles es el siguiente:

  - **A**: Proteger los sistemas y redes y estar preparado para responder a una brecha o ataque.
  - **B**: Securizar las aplicaciones, los procesos definidos en las aplicaciones y los servidores en los que se alojan.
  - **C**: Monitorizar y controlar el acceso a los sistemas.
  - **D**: Controles recomendables

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

- **CSP 2020** (Customer Security Programme): Publicado por SWIFT, tiene como objetivo mejorar el intercambio de información en toda la comunidad y proporcionar un marco de control de seguridad para los clientes adheridos a la red SWIFT.
- **ENSI C4V**: modelo de construcción de capacidades de ciberseguridad para sistemas de control industrial publicado por INCIBE-CERT. Pensado para poder evaluar de forma independiente la Disponibilidad, Confidencialidad e Integridad de la información en sistemas de control industrial (SCI).
- **ISO 27002 (2013):** estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional. Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.
- **NIST CSF v1.1**: Publicado por NIST (National Institute of Standards and Technology), ofrece un marco normativo que sirve como guía sobre seguridad de la información para que las organizaciones del sector privado de Estados Unidos puedan evaluar y mejorar su capacidad de prevenir, detectar y responder a los ciberataques.
- **PCI DSS 3.2**: (Payment Card Industry Data Security Standard) estándar desarrollado por el comité denominado PCI SSC (Payment Card Industry Security Standards Council) como una guía para ayudar a las organizaciones que procesan, almacenan y/o transmiten datos de titulares de tarjeta a proteger dichos datos, con el fin de evitar fraudes que involucran tarjetas de pago débito y crédito.

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

8. ANEXO II - RELACIÓN DE LOS DOCUMENTOS ENTREGADOS Y DESTINATARIO

Descripción	Iberpay	Entidad
Marco de Control de Ciberseguridad SNCE v1.0: Incluye los riesgos, objetivos de control, controles y subcontroles que componen el Marco de Control de Ciberseguridad.	x	x
Marco de Control de Ciberseguridad del SNCE - Formato Word v1.0: mismo contenido que el Marco de Control pero en formato Word.	x	x
Cuestionario Marco de Control de Ciberseguridad SNCE v1.0: Cuestionario de autoevaluación para las Entidades sobre el Marco de Control de Ciberseguridad.	x	x
Modelo de Gobierno - Marco de Control de Ciberseguridad SNCE v1.0: Describe los principales aspectos de organización en relación al Marco de Control.	x	x

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

9. ANEXO III - RIESGOS INCLUIDOS EN EL MARCO DE CONTROL

Dominio de riesgo	Inventario de riesgos
Estrategia	Gestión de activos no adecuada
	Nivel de exposición no identificado
Arquitectura/ Infraestructura no adecuados	Inventario de procesos, activos y sistemas deficiente
	No identificación de procesos y datos críticos
	Segmentación e independencia de equipos no adecuada
Organización y Gobierno de TI	Roles y responsabilidades no formalizadas en relación a los activos del SNCE
Gestión del personal	Personal mal capacitado y no formado
	Personal u operadores de sistemas no preparados
Financiación y Costes	Ausencia de recursos específicos para la gestión de SNCE
Incidentes/Incidencias y problemas	Ausencia de planes de gestión de incidentes específicos sobre el SNCE
Disponibilidad TIC	Ausencia de planes de Continuidad y Contingencia
	Ausencia de planes de prueba
Seguridad TIC (ciber riesgos)	Acceso no autorizado
	Acceso físico no autorizado
	Compromiso de las credenciales de usuario
	Reutilización de credenciales
	Abuso de privilegios de acceso
	Ausencia de segregación de funciones
	Compromiso del sistema de autenticación
	Ruptura de contraseñas
	Robo de contraseñas
	Ejecución de código malicioso
	Exposición a ataques basados en Internet
	Explotación de la configuración insegura del sistema
	Explotación de vulnerabilidades de seguridad conocidas
Seguridad TIC (ciber riesgos)	Vulnerabilidades de seguridad desconocidas o configuraciones erróneas de seguridad
	Exposición por prácticas de seguridad deficientes
	Anomalías no detectadas o actividad sospechosa
	Falta de trazabilidad
	Tráfico de sistema no autenticado
	Compromiso de las copias de seguridad
	Eliminación de registros y pruebas forenses
Gestión del cambio TIC	Modelo de gobierno del cambio ineficiente

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

Dominio de riesgo	Inventario de riesgos
	Ausencia de metodología de gestión de cambios
	Cambios no autorizados en el sistema
Integridad del Dato TIC	Pérdida de la integridad de la información
Outsourcing TIC	Ausencia de control en terceros
	Entornos Cloud no controlados

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

10. ANEXO IV - RELACIÓN ENTRE PRINCIPIOS Y OBJETIVOS DE CONTROL

Principio	Objetivo de Control
Conocimiento del entorno	Gestión de activos
	Identificación de funciones en materia de seguridad de la información
	Identificación de intercambios de información
	Análisis de riesgo
	Gobierno de la seguridad
Protección	Seguridad en las comunicaciones
	Seguridad en el acceso lógico
	Seguridad en las credenciales de acceso
	Gestión de las cuentas de administración
	Seguridad en el acceso remoto
	Seguridad en el acceso físico
	Formación y awareness
	Configuración de seguridad en los sistemas
	Actualizaciones de seguridad
	Protección de la plataforma de virtualización
	Seguridad en servicios externalizados
Gestión del cambio	Seguridad en los desarrollos
	Segregación de funciones y entornos en el proceso de desarrollo
Detección y respuesta	Auditoría de seguridad
	Monitorización y supervisión
	Detección y prevención de intrusiones
	Monitorización de las cuentas de administración
	Identificación de vulnerabilidades
	Gestión y corrección de las vulnerabilidades identificadas
	Gestión de incidentes de seguridad
	Protección antimalware
	Realización de ejercicios de ciberseguridad y pruebas
Estrategia de recuperación	Definición de la estrategia de continuidad para el SNCE
	Realización de pruebas sobre la estrategia de continuidad
	Recuperación de la información

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)

11. ANEXO V - ALINEAMIENTO A ESTÁNDARES Y OTROS MARCOS

Entendimiento a partir del cuestionario cumplimentado por las Entidades

Identificación de riesgos aplicables al SNCE

ÁREA / PRINCIPIO	CSP SWIFT 2020	ENSI C4V	ISO 27002 (2013)	NIST CSF v1.1	PCI DSS 3.2
Conocimiento del entorno	24%	71%	53%	82%	53%
Protección	94%	60%	53%	50%	49%
Gestión del cambio	0%	73%	91%	45%	91%
Detección y respuesta	80%	68%	58%	53%	48%
Estrategia de recuperación	0%	67%	83%	92%	17%
Del total de subcontroles del Framework	68%	65%	59%	57%	49%

© Sociedad Española de Sistemas de Pago, S.A. (Iberpay)