DECISIÓN n.º 2/2020 DEL COMITÉ MIXTO ESTABLECIDO POR EL ACUERDO ENTRE LA UNIÓN EUROPEA Y LA CONFEDERACIÓN SUIZA RELATIVO A LA VINCULACIÓN DE SUS REGÍMENES DE COMERCIO DE DERECHOS DE EMISIÓN DE GASES DE EFECTO INVERNADERO

de 5 de noviembre de 2020

por la que se modifican los anexos I y II del Acuerdo y se adoptan Normas Técnicas de Enlace (NTE) [2021/1034]

EL COMITÉ MIXTO,

Visto el Acuerdo entre la Unión Europea y la Confederación Suiza relativo a la vinculación de sus regímenes de comercio de derechos de emisión de gases de efecto invernadero ([1]) (en lo sucesivo, «Acuerdo»), y en particular su artículo 3, apartado 7, y su artículo 13, apartado 2,

Considerando lo siguiente:

(1) La Decisión n.º 2/2019 del Comité Mixto, de 5 de diciembre de 2019 ([2]), modificó los anexos I y II del Acuerdo, cumpliendo así las condiciones para la vinculación establecidas en el Acuerdo.

(2) Tras la adopción de la Decisión n.º 2/2019 del Comité Mixto y de conformidad con el artículo 21, apartado 3, del Acuerdo, las Partes intercambiaron sus instrumentos de ratificación o aprobación, al considerar cumplidas todas las condiciones para la vinculación establecidas en el Acuerdo.

(3) De conformidad con el artículo 21, apartado 4, del Acuerdo, este entró en vigor el 1 de enero de 2020.

(4) El anexo I del Acuerdo debe modificarse de conformidad con el artículo 13, apartado 2, del Acuerdo, teniendo en cuenta los progresos realizados en el establecimiento del enlace entre los registros, a fin de garantizar una transición fluida para el tratamiento de los operadores de aeronaves asignados por primera vez a Suiza.

(5) A fin de tener en cuenta la evolución reciente y permitir una mayor flexibilidad en el establecimiento del enlace entre los registros requerido por el Acuerdo, es necesario modificar el anexo II del Acuerdo, de conformidad con el artículo 13, apartado 2, de dicho Acuerdo, a fin de prever la posibilidad de utilizar un conjunto de tecnologías más amplio y equivalente para establecer dicho enlace.

(6) De conformidad con el artículo 3, apartado 7, del Acuerdo, el administrador del Registro suizo y el administrador central del Registro de la Unión deben elaborar Normas Técnicas de Enlace (NTE), sobre la base de los principios dispuestos en el anexo II del Acuerdo. Las NTE deben describir los requisitos detallados para el establecimiento de una conexión sólida y segura entre el Diario de Transacciones Suplementario de Suiza (DTSS) y el Diario de Transacciones de la Unión Europea (DTUE). Las NTE deben surtir efecto una vez sean adoptadas mediante decisión del Comité Mixto.

(7) De conformidad con el artículo 13, apartado 1, del Acuerdo, el Comité Mixto debe acordar unas directrices técnicas para garantizar la correcta aplicación del Acuerdo, incluido el establecimiento de una conexión sólida y segura entre el DTSS y el DTUE. La elaboración de las directrices técnicas puede encomendarse a un grupo de trabajo constituido de conformidad con el artículo 12, apartado 5, del Acuerdo. El grupo de trabajo debe como mínimo incluir entre sus miembros al administrador del Registro suizo y al administrador central del Registro de la Unión y debe asistir al Comité Mixto en las funciones que le asigna el artículo 13 del Acuerdo.

(8) Teniendo en cuenta el carácter técnico de las directrices y la necesidad de adaptarlas a la evolución actual, las directrices técnicas elaboradas por el administrador del Registro suizo y el administrador central del Registro de la Unión deben someterse al Comité Mixto a título informativo o, cuando proceda, para su aprobación.

([1]) DO L 322 de 7.12.2017, p. 3.

([2]) Decisión n.º 2/2019 del Comité Mixto establecido por el Acuerdo entre la Unión Europea y la Confederación Suiza Relativo a la vinculación de sus regímenes de comercio de derechos de emisión de gases de efecto invernadero, de 5 de diciembre de 2019, por la que se modifican los anexos I y II del Acuerdo entre la Unión Europea y la Confederación Suiza relativo a la vinculación de sus regímenes de comercio de derechos de emisión de gases de efecto invernadero (DO L 314 de 29.9.2020, p. 68).

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

En el anexo I, parte B, punto 17, el párrafo segundo se sustituye por el texto siguiente:

«Los operadores de aeronaves asignados a Suiza por primera vez después de la entrada en vigor del presente Acuerdo serán gestionados por Suiza a partir del 30 de abril del año de asignación y una vez que esté operativo el acoplamiento provisional de los registros.».

Artículo 2

En el anexo II del Acuerdo, el párrafo cuarto se sustituye por el texto siguiente:

«Las NTE dispondrán que las comunicaciones entre el DTSS y el DTUE consistan en intercambios seguros de mensajes de servicio web basados en las tecnologías siguientes (*) o equivalentes:

— servicios web que utilicen un Protocolo Simple de Acceso a Objetos (SOAP, por sus siglas en inglés),

— Red Privada Virtual (VPN, por sus siglas en inglés) basada en un soporte físico,

— Lenguaje Extensible de Marcado (XML, por sus siglas en inglés),

— firma digital, y

— protocolos de sincronización de la red.

_____

(*) Se trata de las tecnologías que se usan en la actualidad para establecer una conexión entre el Registro de la Unión y el Diario Internacional de Transacciones, así como entre el Registro suizo y el Diario Internacional de Transacciones.».

Artículo 3

Se adoptan las Normas Técnicas de Enlace (NTE) adjuntas a la presente Decisión.

Artículo 4

Se constituye un grupo de trabajo, de conformidad con el artículo 12, apartado 5, del Acuerdo. Dicho grupo de trabajo ayudará al Comité Mixto a garantizar la correcta aplicación del Acuerdo, incluida la elaboración de directrices técnicas para la aplicación de las NTE.

El grupo de trabajo incluirá entre sus miembros, como mínimo, al administrador del Registro suizo y al administrador central del Registro de la Unión.

Artículo 5

Esta Decisión entrará en vigor el día de su adopción.

Hecho en Bruselas, el 5 de noviembre de 2020.

Por el Comité Mixto,	El Presidente,	Secretaria por Suiza
Secretaria por la Unión Europea	Beatriz YORDI	Caroline BAUMANN
Maja-Alexandra DITTEL		

ANEXO

Normas técnicas de enlace (NTE), de conformidad con al Artículo 3, apartado 7, del Acuerdo entre la UNIÓN EUROPEA Y LA CONFEDERACIÓN SUIZA RELATIVO A LA VINCULACIÓN DE SUS REGÍMENES DE COMERCIO DE DERECHOS DE EMISIÓN DE GASES DE EFECTO INVERNADERO.

Normas para una solución provisional

(1) Glosario

Cuadro 1-1

Siglas y definiciones de actividades

Acrónimo/Término	Definición
Derecho de emisión	Derecho a emitir una tonelada equivalente de dióxido de carbono durante un período específico, válido únicamente a efectos del cumplimiento de los requisitos del RCDE UE o del RCDE de Suiza
CH	Confederación Suiza
CHU	Derechos de emisión generales de Suiza (el término «CHU2» se utiliza como abreviatura de los derechos CHU en el segundo período de compromiso)
CHUA	Derecho de emisión de Suiza en el sector de la aviación
POC	Procedimientos Operativos Comunes elaborados conjuntamente por las Partes del Acuerdo para establecer el enlace entre el RCDE UE y el RCDE de Suiza
RCE	Registro de comercio de emisiones
RCDE	Régimen de comercio de derechos de emisión
UE	Unión Europea
EUA	Derecho de emisión general de la UE
EUAA	Derecho de emisión de la UE en el sector de la aviación
RCUE	Registro consolidado de la Unión Europea
DTUE	Diario de Transacciones de la Unión Europea
Registro	Sistema de contabilidad de los derechos de emisión expedidos en el marco del RCDE, que permite el rastreo de la titularidad de los derechos de emisión depositados en cuentas electrónicas.
DTSS	Diario de Transacciones Suplementario de Suiza
Transacción	Proceso de inscripción en el registro que implica la transferencia de un derecho de una cuenta a otra.
Sistema de registro de transacciones	El diario de transacciones contiene un registro de cada transacción propuesta enviada de un registro al otro.

Cuadro 1-2

Siglas y definiciones técnicas

Acrónimo	Definición
Criptografía asimétrica	Utiliza claves públicas y privadas para cifrar y descifrar datos.
Autoridad de certificación (AC)	Entidad que emite certificados digitales.

Acrónimo	Definición
Clave criptográfica	Información que determina el resultado funcional de un algoritmo criptográfico.
Descodificación	Proceso inverso en el proceso de cifrado.
Firma digital	Técnica matemática empleada para validar la autenticidad e integridad de un mensaje, programa informático o documento digital.
Cifrado	Proceso de conversión de información o datos en un código, en particular para impedir el acceso no autorizado.
Ingesta de datos	Proceso de ingesta de datos.
Cortafuegos	Dispositivos o programas informáticos para garantizar la seguridad de la red, que supervisan y controlan el tráfico de entrada y salida en la red sobre la base de normas predefinidas.
Seguimiento de la señal de presencia	Señal periódica, generada y supervisada por equipos o programas informáticos, que indica que la operación es normal o permite la sincronización con otras partes de un sistema de proceso de datos.
IPsec	IP SECurity. Serie de protocolos de red que autentifican y encriptan los paquetes de datos a fin de permitir una comunicación encriptada y segura entre dos ordenadores en una red IP (Protocolo de internet).
Prueba de penetración	Puesta a prueba de un sistema informático, una red informática o una aplicación web para detectar fallas de seguridad que un atacante podría aprovechar.
Proceso de conciliación	Proceso para garantizar la concordancia de dos series de registros.
VPN	Red privada virtual
XML	Lenguaje Extensible de Marcado. Lenguaje informático que permite a los diseñadores crear etiquetas personalizadas y definir, transmitir, validar e interpretar los datos entre diferentes aplicaciones y entre diferentes organizaciones.

(2) **Introducción**

El Acuerdo entre la Unión Europea y la Confederación Suiza relativo a la vinculación de sus regímenes de comercio de derechos de emisión de gases de efecto invernadero, de 23 de noviembre de 2017 (en lo sucesivo, «el Acuerdo»), prevé el reconocimiento mutuo de los derechos de emisión que pueden utilizarse para el cumplimiento del régimen de comercio de derechos de emisión de la Unión Europea («RCDE UE») o del régimen de comercio de derechos de emisión de Suiza («RCDE de Suiza»). A fin de que el enlace entre el RCDE UE y el RCDE de Suiza sea operativo, es preciso establecer, entre el Diario de Transacciones de la Unión Europea (DTUE) del Registro de la Unión y el Diario de Transacciones Suplementario de Suiza (DTSS) del Registro suizo, un enlace directo que permita la transferencia entre ambos registros de los derechos de emisión expedidos en el marco de cualquiera de los dos RCDE (artículo 3, apartado 2, del Acuerdo). Para que el enlace entre el RCDE UE y el RCDE de Suiza sea operativo, debía aplicarse una solución provisional en mayo de 2020 o lo antes posible a partir de esa fecha. Las Partes debían cooperar con objeto de sustituir la solución provisional por un enlace permanente entre los registros lo antes posible (anexo II del Acuerdo).

De conformidad con el artículo 3, apartado 7, del Acuerdo, el administrador del Registro suizo y el administrador central del Registro de la Unión tienen que elaborar Normas Técnicas de Enlace (NTE), sobre la base de los principios dispuestos en el anexo II del Acuerdo, en las que se describan los requisitos detallados para el establecimiento de una conexión sólida y segura entre el DTSS y el DTUE. Las NTE diseñadas por los administradores surtirán efecto una vez sean adoptadas mediante decisión del Comité Mixto.

El Comité Mixto debe aprobar las NTE, tal como figuran en el presente documento, mediante la Decisión n.º 2/2020. De conformidad con la presente Decisión, el Comité Mixto solicitará al administrador del Registro suizo y al administrador central del Registro de la Unión que elaboren nuevas directrices técnicas para que el enlace sea operativo y garanticen que estas se vayan adaptando constantemente al progreso técnico y a los nuevos requisitos de seguridad y protección del enlace, así como a su funcionamiento eficaz y eficiente.

2.1. *Ámbito de aplicación*

El presente documento representa el entendimiento común entre las Partes en el Acuerdo con relación al establecimiento de las bases técnicas del enlace entre los registros del RCDE UE y el RCDE de Suiza. Aunque sienta las bases de las especificaciones técnicas en términos de requisitos de arquitectura, servicio y seguridad, se necesitarán directrices más detalladas para que el enlace sea operativo.

Para un correcto funcionamiento del enlace, será preciso establecer los procesos y procedimientos oportunos. De conformidad con el artículo 3, apartado 6, del Acuerdo, estos aspectos se describen detalladamente en un documento separado sobre los procedimientos operativos comunes (POC), que debe adoptarse por separado mediante decisión del Comité Mixto.

2.2. *Destinatarios*

Los destinatarios del presente documento son el administrador del Registro suizo y el Administrador Central del Registro de la Unión.

3. **Disposiciones generales**

3.1. *Arquitectura del enlace de comunicación*

El propósito de esta sección es describir la arquitectura general para la puesta en funcionamiento del enlace entre el RCDE UE y el RCDE de Suiza y los distintos componentes implicados.

Dado que la seguridad es un elemento clave para la definición de la arquitectura del enlace entre registros, se han adoptado todas las medidas necesarias para disponer de una arquitectura sólida. Aunque el enlace permanente entre los registros previsto se basará en servicios web, en la solución provisional se utilizará más bien un mecanismo de intercambio de archivos.

La solución técnica es la siguiente:

— un protocolo seguro de transferencia de mensajes para el intercambio de mensajes;

— mensajes XML;

— firma digital y cifrado XML;

— una red segura de transporte de datos que utilice un *router* VPN o equivalente.

3.1.1. Intercambio de mensajes

La comunicación entre el Registro de la Unión y el Registro suizo se basará en un mecanismo de intercambio de mensajes a través de canales seguros. Cada extremo contará con su propio archivo de mensajes recibidos.

Ambas Partes mantendrán un diario de los mensajes recibidos, así como de los detalles relativos al tratamiento.

Deberán comunicarse, en forma de alertas, los errores o estados inesperados, y los equipos de apoyo deberán mantener un contacto personal.

Los errores y contingencias se tratarán de acuerdo con los procedimientos operativos establecidos en el proceso de gestión de incidentes del POC.

3.1.2. Mensaje XML — Nivel de descripción superior

Los mensajes XML contendrán uno de los siguientes elementos:

— una o varias solicitudes de transacción o una o varias respuestas a transacciones;

— una operación/respuesta enmarcada en el proceso de conciliación;

— un mensaje de prueba.

Cada mensaje contendrá un encabezamiento con los siguientes elementos:

— RCDE de origen;

— número de secuencia.

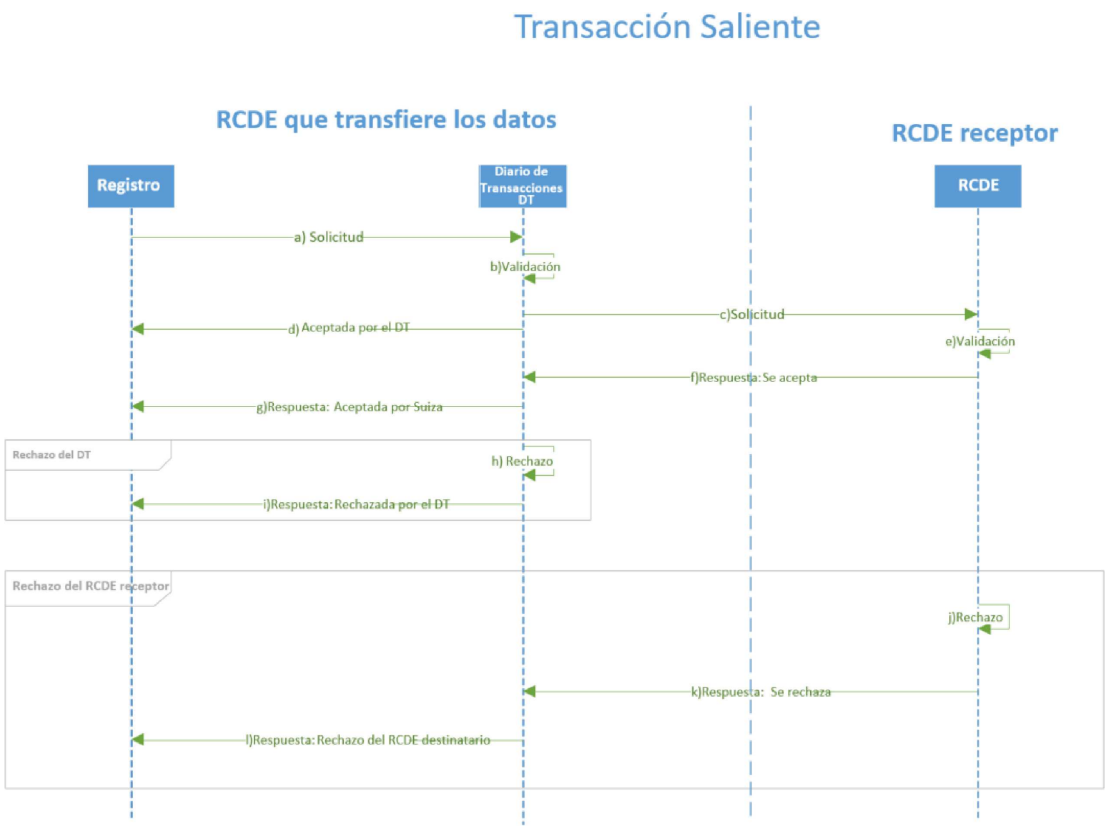
3.1.3. Períodos de ingesta

La solución provisional se basa en períodos de ingesta predefinidos, seguidos de un conjunto de eventos designados. Las solicitudes de transacción recibidas a través del enlace solo se introducirán a intervalos predefinidos. Los períodos de ingesta incluyen una validación técnica para las transacciones entrantes y salientes. Además, las conciliaciones podrán efectuarse diariamente y se podrán activar manualmente.

Los cambios de frecuencia o de calendario de cualquiera de estos eventos se tratarán siguiendo los procedimientos operativos establecidos en el proceso de ejecución de las solicitudes de los COP.

3.1.4. Flujo de mensajes de transacción

Transacciones salientes



Esta sección refleja el punto de vista del RCDE que transfiere los datos. El diagrama de secuencia anterior describe todos los flujos específicos de las transacciones salientes.

Flujo principal en el caso de una «Transacción Normal» (las etapas se indican en el diagrama anterior):

a) en el RCDE que transfiere los datos, una vez transcurridos todos los plazos de la actividad (24 horas, si procede), la solicitud de transacción se envía del registro al diario de transacciones;

b) el diario de transacciones valida la solicitud de transacción;

c) la solicitud de transacción se envía al RCDE destinatario;

d) la respuesta de aceptación se envía al registro del RCDE de origen;

e) el RCDE destinatario valida la solicitud de transacción;

f) el RCDE destinatario devuelve la respuesta de aceptación al RCDE de origen;

g) el diario de transacciones envía la respuesta de aceptación al registro.

Flujo alternativo en el caso de «denegación de inscripción en el diario de transacciones» [las etapas se indican en el diagrama anterior, a partir igualmente de la letra a)]:

a) en el RCDE de origen, una vez transcurridos todos los plazos de la actividad (24 horas, si procede), la solicitud de transacción se envía del registro al diario de transacciones.

A continuación:

b) el diario de transacciones no valida la solicitud;

c) el mensaje de denegación se envía al registro de origen.

Flujo alternativo en el caso de «denegación del RCDE» [las etapas se indican en el diagrama anterior, a partir de la letra a)]:

a) en el RCDE de origen, una vez transcurridos todos los plazos de la actividad (24 horas, si procede), la solicitud de transacción se envía del registro al diario de transacciones;

b) el diario de transacciones valida la transacción;

c) la solicitud de transacción se envía al RCDE destinatario;

d) el mensaje de aceptación se envía al registro del RCDE de origen.

A continuación:

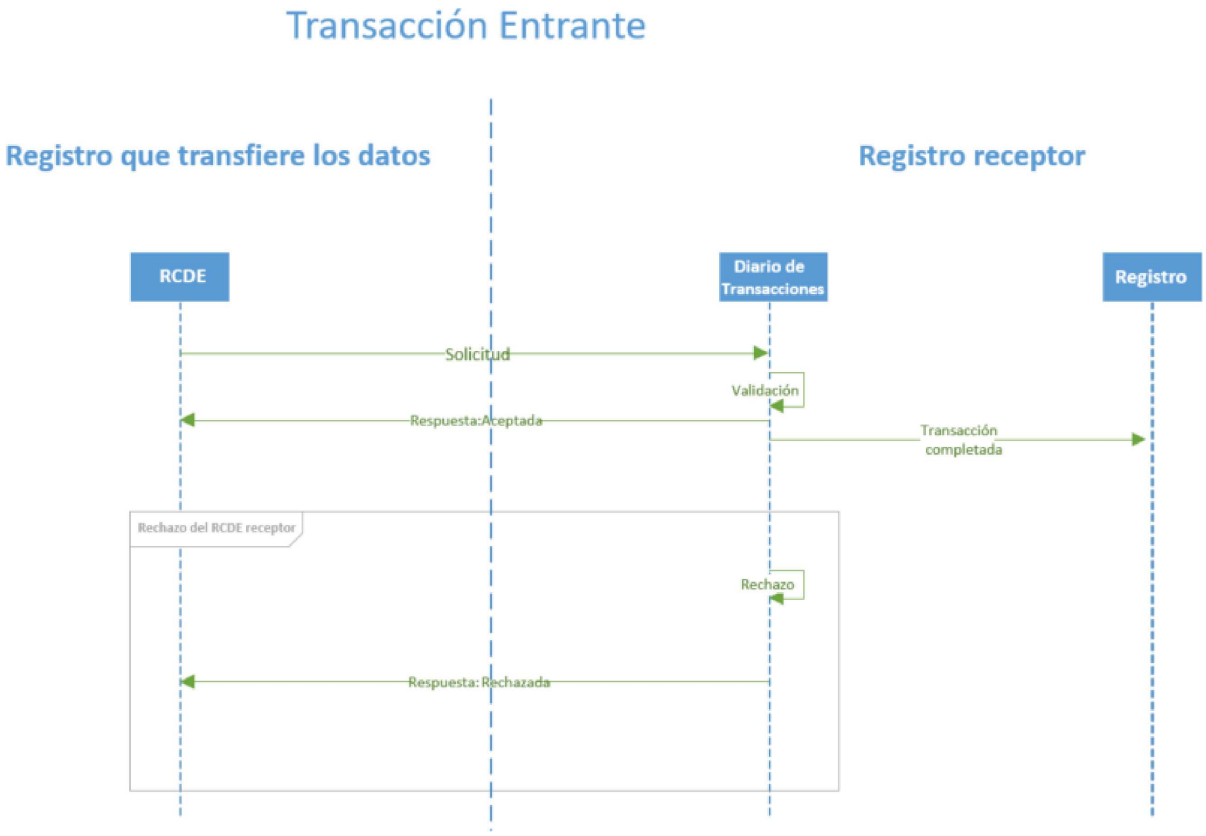
e) el diario de transacciones del RCDE que recibe los datos no valida la transacción;

f) el RCDE que recibe los datos envía la respuesta de denegación al diario de transacciones del RCDE que transfiere los datos;

g) el diario de transacciones envía la denegación al registro.

Transacciones entrantes

Esta sección refleja el punto de vista del RCDE que recibe los datos. El flujo específico se representa en el siguiente diagrama de secuencia:



El diagrama ilustra lo siguiente:

1. Cuando el diario de transacciones del RCDE que recibe los datos valida la solicitud, envía un mensaje de aceptación al RCDE que transfiere los datos y un mensaje de «transacción completada» al registro del RCDE que recibe los datos.
2. Cuando una solicitud entrante es rechazada en el diario de transacciones que recibe los datos, la solicitud de transacción no se envía al registro original del RCDE que recibe los datos.

Protocolo

El ciclo de mensajes de transacción solo incluye dos mensajes:

— Propuesta de transacción RCDE que transfiere datos RCDE que recibe datos

— Respuesta de transacción RCDE que transfiere datos RCDE que recibe datos: bien aceptación, bien denegación (incluida la razón de la denegación):

  — aceptación: transacción completada;

  — denegación: transacción finalizada.

Estado de la transacción

— Las transacciones del RCDE que transfiere los datos adquirirán el estado «proposed» (propuesta) en el momento de enviarse la solicitud.

— Las transacciones del RCDE que recibe los datos adquirirán el estado «proposed» (propuesta) en el momento de recibirse la solicitud y durante el tratamiento de la misma.

— Las transacciones del RCDE que recibe los datos adquirirán el estado «completed/terminated» (completado/finalizado) en el momento de procesarse la propuesta. A continuación, el RCDE que recibe los datos enviará el mensaje de aceptación o denegación correspondiente.

— Las transacciones del RCDE que transfiere los datos adquirirán el estado «completed/terminated» (completado/finalizado) en el momento de recibirse y procesarse la aceptación o denegación.

— En el RCDE que transfiere los datos, el estado de las transacciones seguirá siendo «proposed» mientras no se reciba respuesta.

— El RCDE que recibe los datos asignará el estado «terminated» (finalizado) a cualquier transacción que se mantenga en estado «proposed» durante más de treinta minutos.

Los incidentes relacionados con las transacciones se tratarán de acuerdo con los procedimientos operativos establecidos en el proceso de gestión de incidentes de los POC.

3.2. *Seguridad de la transferencia de datos*

Los datos en tránsito estarán protegidos por cuatro niveles de seguridad:

1) control de acceso a la red: cortafuegos y capa de interconexión de redes;

2) cifrado en el nivel «transporte»: una red segura de transporte de datos que utilice un router VPN o equivalente.

3) cifrado en el nivel «sesión»: protocolo seguro de transferencia para el intercambio de mensajes;

4) cifrado en el nivel «aplicación»: firma XML y cifrado XML del contenido.

3.2.1. Cortafuegos e interconexión de redes

El enlace se establece por medio de una red protegida por un cortafuegos basado en un soporte físico. El cortafuegos se configura según unas reglas en virtud de las cuales únicamente los clientes «registrados» pueden conectarse al servidor VPN.

3.2.2. Red privada virtual (VPN)

Todas las comunicaciones entre las Partes se protegerán mediante una tecnología de transporte de datos segura. En el caso de una red privada virtual (VPN), la infraestructura debe basarse en equipos informáticos o virtuales. Las tecnologías VPN proporcionan la capacidad de «túnel» a través de una red como internet desde un punto a otro, protegiendo todas las comunicaciones. Antes de la creación del túnel VPN, se expide un certificado digital a un cliente potencial, lo que le permite aportar pruebas de la identidad durante la negociación de la conexión. Cada Parte es responsable de la instalación del certificado en su extremo de la VPN. Utilizando certificados digitales, cada servidor VPN accederá a una autoridad central para negociar credenciales de autenticación. El cifrado se negocia durante el proceso de creación del túnel, garantizando la protección de todas las comunicaciones a través del túnel.

Los extremos VPN del cliente se configurarán para mantener el túnel VPN con carácter permanente, a fin de permitir una comunicación fiable, bidireccional e instantánea entre las Partes en todo momento.

Cualquier otra solución equivalente deberá ajustarse a los principios antes mencionados.

3.2.3. Aplicación de IPsec

Si se utiliza una solución VPN, el uso del protocolo IPsec para la instalación de la infraestructura VPN entre emplazamientos permitirá la autenticación, la integridad y el cifrado de los datos entre emplazamientos. Las configuraciones VPN IPsec garantizan una autenticación adecuada entre dos extremos de la conexión VPN. Las Partes identificarán y autenticarán al cliente remoto a través de la conexión IPSec utilizando certificados digitales facilitados por una autoridad de certificación reconocida por el otro extremo.

La conexión IPsec también garantiza la integridad de los datos de todas las comunicaciones que se transmiten a través del túnel VPN. Los paquetes de datos se someten a un proceso de comprobación aleatoria y firma utilizando la información de autenticación establecida por la VPN. La confidencialidad de los datos se garantiza asimismo mediante el cifrado IPSec.

3.2.4. Protocolo seguro de transferencia para el intercambio de mensajes

La solución provisional se basa en múltiples capas de cifrado para intercambiar datos de forma segura entre las Partes. Ambos sistemas y sus distintos entornos están interconectados a nivel de red mediante túneles VPN o redes seguras de transporte de datos equivalentes. En el nivel «aplicación», los ficheros se transfieren utilizando un protocolo seguro de transferencia para el intercambio de mensajes en el nivel «sesión».

3.2.5. Firma y cifrado XML

En los ficheros XML, la firma y el cifrado tienen lugar a dos niveles. Cada solicitud de transacción, respuesta de transacción y mensaje de conciliación se firma individualmente por vía electrónica.

En una segunda etapa, cada subelemento del elemento «mensaje» se cifra individualmente.

Además, en una tercera etapa y para garantizar la integridad y la no denegación del mensaje completo, el mensaje del elemento raíz se firma digitalmente. Esto da lugar a un elevado nivel de protección de los datos integrados XML. La aplicación técnica cumple las normas del Consorcio World Wide Web.

Para descifrar y verificar el mensaje, el proceso es el mismo pero en orden inverso.

3.2.6. Claves criptográficas

Se utilizará una criptografía de clave pública para el cifrado y la firma.

Para el caso específico de IPSec, se utilizará un certificado digital emitido por una autoridad de certificación (AC) que goce de la confianza de ambas Partes. Esta AC verifica la identidad del titular del certificado y emite certificados que se utilizan para reconocer formalmente una organización y establecer canales seguros de comunicación de datos entre las Partes.

Se utilizan claves criptográficas para firmar y cifrar los canales de comunicación y los ficheros de datos. Las Partes intercambian digitalmente los certificados públicos utilizando canales seguros y verificados fuera de banda. Este procedimiento forma parte integrante del proceso de gestión de la seguridad de la información de los POC.

3.3. *Lista de funciones en el marco del enlace*

El enlace especifica el sistema de transmisión para una serie de funciones que aplican los procesos de actividad derivados del Acuerdo. El enlace incluye también las especificaciones relativas al proceso de conciliación y a los mensajes de prueba que permitirán realizar un seguimiento de la señal de presencia.

3.3.1. Transacciones de actividad

Desde el punto de vista de la actividad, el enlace contempla cuatro (4) tipos de solicitudes de transacción:

— Transferencias externas:

  — tras la entrada en vigor de la vinculación de los RCDE, los derechos de la UE y de Suiza se convierten en fungibles y, por lo tanto, pueden transferirse plenamente entre las Partes;

— una transferencia en el marco del enlace implicará la existencia de una cuenta de origen de la transferencia en uno de los RCDE y una cuenta destinataria de la transferencia en el otro RCDE;

— la transferencia podrá incluir cualquier cantidad de los cuatro (4) tipos de derechos de emisión:

— derechos de emisión generales de Suiza (CHU);

— derechos de emisión de Suiza en el sector de la aviación (CHUA);

— derechos de emisión generales de la UE (EUA);

— derechos de emisión de la UE en el sector de la aviación (EUAA).

— Asignación internacional:

los operadores de aeronaves cubiertos por un RCDE con obligaciones respecto al otro RCDE, y que tengan derecho a recibir derechos de emisión gratuitos en el marco de este segundo RCDE, recibirán gratuitamente derechos de emisión de la aviación en el marco del segundo RCDE mediante la transacción «asignación internacional».

— Anulación de la asignación internacional:

esta transacción se llevará a cabo en el caso de que se anulen íntegramente los derechos de emisión asignados gratuitamente a una cuenta de haberes de un operador de aeronaves en el marco del otro RCDE.

— Restitución de la asignación excedentaria:

similar a la anulación, pero aplicable en los casos en que la asignación no debe anularse en su totalidad, y solo los derechos asignados en exceso deben ser devueltos al RCDE en cuyo marco se hubieran asignado.

3.3.2. Protocolo de conciliación

Las conciliaciones se efectuarán únicamente después del cierre de los períodos de ingesta, validación y tratamiento de los mensajes.

Las conciliaciones son parte integrante de las medidas de seguridad y de coherencia de la vinculación. Ambas Partes acordarán el calendario exacto de la conciliación antes de fijar ningún horario. Puede programarse diariamente una conciliación si así lo acuerdan ambas Partes. No obstante, una vez realizada la ingesta, se efectuará al menos una conciliación programada.

En cualquier caso, cada Parte podrá iniciar conciliaciones manuales.

Los cambios en el calendario y la frecuencia de la conciliación programada se tratarán de conformidad con los procedimientos operativos establecidos en el proceso de ejecución de las solicitudes de los COP.

3.3.3. Mensaje de prueba

Se ha previsto un mensaje de prueba para comprobar la comunicación de extremo a extremo. El mensaje contendrá datos que lo identificarán como prueba y en el otro extremo se generará una respuesta en el momento de la recepción.

3.4. *Normas aplicables a los servicios web*

Los servicios web no se utilizarán en la solución provisional. No obstante, cabe señalar que la forma y el formato de los mensajes XML se mantendrán en gran medida sin cambios. Con la introducción, en el futuro, del enlace permanente entre los registros, los servicios web deben permitir el intercambio instantáneo de mensajes XML.

3.5. *Definición específica de los servicios web*

Esta sección no es aplicable a la solución provisional. Como se ha indicado en la sección anterior, los servicios web solo se utilizarán en el futuro enlace permanente entre los registros.

3.6. *Requisitos relativos al registro de datos*

A fin de abordar la necesidad de ambas Partes de mantener la exactitud y coherencia de la información, y con el fin de disponer de herramientas para eliminar las incoherencias, ambas Partes conservarán cuatro (4) tipos de registros de datos:

— diarios de transacciones;

— registros de conciliaciones;

— archivo de mensajes;

— registros de auditoría interna.

Todos los datos de estos registros se conservarán al menos durante tres (3) meses a efectos de resolución de problemas y su posterior retención dependerá de la legislación aplicable en cada extremo a efectos de auditoría. Los ficheros de registro de más de tres (3) meses de antigüedad pueden archivarse en un lugar seguro dentro de un sistema informático independiente, siempre y cuando se puedan recuperar o se pueda acceder a ellos en un plazo razonable.

Registros de transacciones

Los diarios de transacciones se ejecutan en los subsistemas DTUE y DTSS.

Más concretamente, los diarios de transacciones llevarán un registro de cada una de las transacciones propuestas al otro RCDE. Cada registro contiene todos los campos del contenido de la transacción y el posterior resultado de esta (la respuesta del RCDE que recibe la solicitud). Los registros de transacciones también llevarán un registro de las transacciones entrantes, así como de la respuesta enviada al RCDE de origen.

Registros de conciliaciones

El registro de conciliaciones indicará cada uno de los mensajes de conciliación intercambiados entre las Partes, incluido el identificador de la conciliación, la marca de tiempo y el resultado de la conciliación: estado de conciliación «Pass» (Correcto) o «Discrepancies» (Discrepancias). En la solución provisional, los mensajes de conciliación forman parte integrante de los mensajes intercambiados.

Ambas Partes registrarán cada solicitud y su respuesta en el registro de conciliaciones. Aunque la información contenida en el registro de conciliaciones no se comparte directamente como parte de la propia reconciliación, puede ser necesario acceder a esta información para resolver incoherencias.

Archivo de mensajes

Ambas Partes están obligadas a archivar una copia de los datos intercambiados (archivos XML), enviados y recibidos, así como la indicación de si estos o los mensajes XML tenían o no el formato correcto.

El principal objetivo del archivo es la auditoría, ya que permite disponer de pruebas de lo que se envió a la otra Parte y se recibió de ella. En este sentido, junto con los ficheros, deben archivarse también los certificados correspondientes.

Estos ficheros proporcionarán también información adicional para la resolución de problemas.

Registros de auditoría interna

Cada Parte definirá y utilizará dichos registros de forma individual.

3.7. *Requisitos operativos*

El intercambio de datos entre los dos sistemas no es totalmente autónomo en el contexto de la solución provisional, lo que significa que se requieren operadores y procedimientos para que el enlace sea operativo.

4. **Disposiciones sobre disponibilidad**

4.1. *Diseño que garantice la disponibilidad de las comunicaciones*

La arquitectura de la solución provisional consiste fundamentalmente en una infraestructura de TIC y en un programa informático que permite la comunicación entre el RCDE de Suiza y el RCDE de la UE. Garantizar unos niveles elevados de disponibilidad, integridad y confidencialidad de este flujo de datos constituye, por lo tanto, un aspecto esencial que ha de tenerse en cuenta al diseñar la solución provisional y el enlace permanente entre los registros. Al tratarse de un proyecto en el que la infraestructura de TIC, el programa informático a la medida y los procesos desempeñan un papel integral, estos tres elementos deben tenerse en cuenta para diseñar un sistema resiliente.

Resiliencia de la infraestructura TIC

En el capítulo de disposiciones generales del presente documento se detallan los elementos «arquitectónicos». En lo que se refiere a la infraestructura de TIC, el enlace provisional establece una red VPN resiliente (o equivalente) que crea túneles de comunicación seguros para el intercambio seguro de mensajes. Los demás elementos de la infraestructura están configurados en alta disponibilidad o cuentan con mecanismos alternativos de solución de fallos.

Resiliencia de los programas informáticos a medida

Los módulos de programas informáticos a medida mejoran la resiliencia al reintentar restablecer la comunicación durante un determinado período de tiempo con el otro extremo si, por alguna razón, este no está disponible.

Resiliencia de los servicios

En la solución provisional, los intercambios de datos entre las Partes se producen en franjas horarias predefinidas a lo largo de todo el año. Algunas de las etapas requeridas para los intercambios de datos preprogramados requieren una intervención manual por parte de los operadores de sistema o los administradores de los registros. Teniendo en cuenta este aspecto y con el fin de aumentar la disponibilidad y el éxito de los intercambios:

— los procedimientos operativos incluirán espacios temporales importantes para cada etapa;

— los módulos de programas informáticos de la solución provisional ejecutarán una comunicación asíncrona;

— el proceso automático de conciliación detectará si han surgido problemas en la ingesta de ficheros de datos en cada extremo;

— los procesos de seguimiento (infraestructura de TIC y módulos de programas informáticos a medida) se tendrán en cuenta en los procedimientos de gestión de incidentes y los activarán (tal como se definen en el documento sobre los procedimientos operativos comunes). Los procedimientos que tienen por objeto reducir el tiempo necesario para restablecer el funcionamiento normal tras los incidentes son esenciales para garantizar un alto índice de disponibilidad.

4.2. *Inicialización, comunicación, reactivación y plan de pruebas*

Todos los elementos que intervienen en la arquitectura de la solución provisional se someterán a pruebas individuales y colectivas con el fin de verificar que la infraestructura de TIC y los sistemas de información de la plataforma están listos para funcionar. Estas pruebas operativas son un prerrequisito obligatorio cada vez que la solución provisional deba pasar del estado de suspended» («suspendido») al estado «operational» («operativo»).

La activación del estado operativo del enlace exige la ejecución satisfactoria de un plan de prueba predefinido. Este plan confirmará que cada registro ha realizado primero un conjunto de pruebas internas, seguidas por la validación de la conectividad de extremo a extremo, antes de comenzar el envío de las transacciones de producción entre ambas Partes.

El plan de pruebas debe mencionar la estrategia global de prueba y los detalles relativos a la infraestructura de prueba. En particular, para cada elemento de cada bloque de prueba deberá incluir:

— los criterios y las herramientas de prueba;

— las funciones asignadas para realizar la prueba;

— los resultados esperados (positivos y negativos)

— el calendario de pruebas;

— el registro de los requisitos relativos a los resultados de las pruebas;

— la documentación relativa a la resolución de problemas;

— las disposiciones relativas a la activación de los niveles sucesivos de intervención.

El proceso correspondiente a las pruebas de activación del estado operativo podría subdividirse en cuatro (4) bloques o fases conceptuales:

4.2.1. Pruebas de la infraestructura interna de TIC

Se espera que estas pruebas sean realizadas o verificadas por ambas Partes en su respectivo extremo.

Cada elemento de la infraestructura de TIC en cada extremo se someterá a prueba individualmente. Esto incluye todos y cada uno de los componentes de la infraestructura. Estas pruebas podrán realizarse de forma automática o manual, pero deberán verificar que todos los elementos de la infraestructura estén operativos.

4.2.2. Pruebas de comunicación

Cada una de las Partes deberá iniciar separadamente las pruebas, pero estas deberán concluirse en cooperación con el otro extremo.

Una vez que los distintos elementos estén operativos, deberán someterse a prueba los canales de comunicación entre ambos registros. A tal fin, cada una de las Partes verificará que el acceso a internet funciona, que se han establecido los túneles VPN (o de una red de transporte segura equivalente) y se dispone de una conectividad IP entre emplazamientos. Deberían seguidamente confirmarse en el otro extremo la accesibilidad de los elementos de infraestructura locales y distantes y la conectividad IP.

4.2.3. Pruebas del sistema completo (de extremo a extremo)

Está previsto que estas pruebas se lleven a cabo en cada extremo y que los resultados se comuniquen a la otra Parte.

Una vez que se hayan sometido a prueba los canales de comunicación y los distintos componentes de los dos registros, se preparará en cada extremo una serie de transacciones y conciliaciones simuladas, representativas del conjunto de funciones que se vayan a ejecutar en el marco del enlace.

4.2.4. Pruebas de seguridad

Está previsto que ambas Partes realicen o activen estas pruebas en cada extremo y según las instrucciones que figuran en las secciones 5.4, «Directrices para las pruebas de seguridad», y 5.5, «Disposiciones relativas a la evaluación del riesgo».

Solo puede considerarse operativo el enlace provisional después de que las cuatro fases/bloques hayan dado lugar a un resultado previsible.

Recursos para la realización de pruebas

Cada Parte contará con recursos de prueba específicos (equipos y programas informáticos de infraestructura de TIC específicos) y desarrollará las funciones de prueba en su respectivo sistema con el fin de respaldar la validación continua y manual de la plataforma. Los administradores del registro pueden ejecutar en cualquier momento procedimientos manuales de forma individual o cooperativa. La activación del estado operativo es un proceso manual en sí mismo.

También se prevé que la plataforma realice controles automáticos a intervalos regulares. Estos controles pretenden incrementar la disponibilidad de la plataforma mediante la detección temprana de posibles problemas a nivel de la infraestructura. Este plan de seguimiento de la plataforma se compone de dos elementos:

— supervisión de las infraestructuras de TIC: en ambos extremos, la infraestructura será supervisada por los proveedores de servicios de infraestructura de TIC. Las pruebas automáticas cubrirán los diferentes elementos de la infraestructura y la disponibilidad de los canales de comunicación.

— Supervisión de las aplicaciones: los módulos de programas informáticos de la vinculación provisional implementarán la supervisión de la comunicación a nivel de aplicación (manualmente y/o a intervalos regulares) para probar la disponibilidad de extremo a extremo de la vinculación simulando algunas de las transacciones previstas en la vinculación.

4.3. *Entornos de prueba/validación*

La arquitectura del Registro de la Unión y del Registro suizo incluirá los tres entornos siguientes:

— Producción (PROD): este entorno contiene los datos reales y procesa transacciones reales;

— Validación (aceptación — ACC): este entorno contiene datos representativos, ficticios o anonimizados. Es el entorno en el que los operadores de sistema de ambas Partes validan las nuevas versiones;

— Prueba (TEST): este entorno contiene datos representativos, ficticios o anonimizados. Este entorno está limitado a los administradores de los registros y está destinado a ser utilizado para realizar pruebas de integración por ambas Partes.

Con la excepción de la VPN (o red equivalente), los tres entornos son completamente independientes entre sí, lo que significa que los equipos, los programas informáticos, las bases de datos, los entornos virtuales, las direcciones IP y los puertos se instalan y funcionan de manera independiente.

Existe una configuración VPN para dos entornos diferentes, uno para el entorno PROD y otro independiente para los entornos ACC y TEST.

5. **Disposiciones sobre confidencialidad e integridad**

Los mecanismos y procedimientos de seguridad permiten que dos personas compartan una misma función (principio de doble control) para las operaciones llevadas a cabo en relación con el enlace entre el Registro de la Unión y el Registro suizo. Este principio del doble control se aplicará siempre que sea necesario. No obstante, no debe aplicarse a todas las acciones efectuadas por los administradores de los registros.

En el plan de gestión de la seguridad, que también incluye los procesos relacionados con el tratamiento de los incidentes de seguridad tras una eventual vulneración de la seguridad, se contemplan y se abordan los requisitos de seguridad. La parte operativa de estos procesos se describe en los POC.

5.1. *Infraestructura para las pruebas de seguridad*

Cada Parte se compromete a establecer una infraestructura de pruebas de seguridad (utilizando el conjunto común de equipos y programas informáticos utilizado para detectar vulnerabilidades en las fases de desarrollo y explotación):

— separada del entorno de producción;

— en la que la seguridad sea analizada por un equipo independiente de los equipos encargados del desarrollo y de la explotación del sistema.

Cada Parte se compromete a realizar análisis estáticos y dinámicos.

En el caso de los análisis dinámicos (como la prueba de penetración), ambas Partes se comprometen a limitar normalmente las evaluaciones a los entornos de prueba y validación (tal como se definen en la sección 4.3, «Entornos de prueba/validación»). Las excepciones a esta política están sujetas a la aprobación de ambas Partes.

Antes de ser desplegado en el entorno de producción, cada módulo de programa informático del enlace (tal como se define en la sección 3.1, «Arquitectura de enlace de comunicación») se someterá a una prueba de seguridad.

La infraestructura de pruebas debe estar separada de la infraestructura de producción, tanto a nivel de red como de infraestructura, Las pruebas de seguridad necesarias para verificar el cumplimiento de los requisitos de seguridad se llevan a cabo en la infraestructura de pruebas.

5.2. *Disposiciones relativas a la suspensión y la reactivación del enlace*

Si se sospecha que la seguridad del Registro suizo, el DTSS, el Registro de la Unión o el DTUE se ha visto comprometida, ambas Partes se informarán de ello de manera inmediata y suspenderán el enlace entre el DTSS y el DTUE.

Los procedimientos para el intercambio de información, la decisión de suspensión y la decisión de reactivación forman parte del proceso de ejecución de las solicitudes de los COP.

Suspensión

La suspensión del enlace entre los registros de conformidad con el anexo II del Acuerdo podrá producirse por las razones siguientes:

— razones administrativas previstas (por ejemplo, mantenimiento);

— razones de seguridad imprevistas (o fallo de la infraestructura informática).

En caso de emergencia, cada Parte informará a la otra Parte y suspenderá unilateralmente el enlace entre los registros.

Si se decide suspender el enlace entre los registros, cada Parte se asegurará de que el enlace se interrumpe en el nivel de la red (mediante el bloqueo de las conexiones entrantes y salientes, en su totalidad o en parte).

La decisión de suspender el enlace de los registros, prevista o no, se tomará de acuerdo con el procedimiento de gestión de cambios o el procedimiento de gestión de incidentes de seguridad de los POC.

Reactivación de la comunicación

La decisión de reactivar la comunicación se tomará conforme se detalla en los POC y, en cualquier caso, no antes de que se hayan completado con éxito los procedimientos de verificación de la seguridad, tal como se especifica en las secciones 5.4, «Directrices para las pruebas de seguridad» y 4.2, «Plan de inicialización, de comunicación, de reactivación y de prueba».

5.3. *Disposiciones relativas a las vulneraciones de la seguridad*

Una vulneración de la seguridad se considera un incidente de seguridad que podría afectar a la confidencialidad e integridad de información sensible y/o a la disponibilidad del sistema que la trata.

La información sensible está incluida en la Lista de Información Sensible y puede ser procesada en el sistema o en cualquier parte relacionada con este.

A menos que se indique lo contrario, la información directamente relacionada con la vulneración de la seguridad se considerará sensible, llevará la indicación «ETS CRITICAL» (crítico RCDE) y se tratará de conformidad con las instrucciones de tratamiento.

Toda vulneración de la seguridad se tratará de conformidad con el capítulo relativo a la gestión de incidentes de seguridad de los POC.

5.4. *Directrices para las pruebas de seguridad*

5.4.1. Programas informáticos

Las pruebas de seguridad, incluidas las pruebas de penetración, si procede, se efectuarán al menos en todas las nuevas versiones importantes de los programas informáticos, de conformidad con los requisitos de seguridad establecidos en las NTE a fin de evaluar la seguridad de la vinculación y los riesgos correspondientes.

Si no se ha producido ninguna versión importante en los últimos doce meses, deberá efectuarse una prueba de seguridad en el sistema vigente teniendo en cuenta la evolución de las amenazas informáticas registrada en los últimos doce meses.

Las pruebas de seguridad del enlace entre los registros deberán realizarse en el entorno de validación y, si fuera necesario, en el entorno de producción, de forma coordinada y con el mutuo acuerdo de las Partes.

Las pruebas de aplicación de internet respetarán las normas abiertas internacionales, como las establecidas por el Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP por sus siglas en inglés).

5.4.2. Infraestructuras

Las infraestructuras que respalden el sistema de producción deberán verificarse con regularidad para detectar las vulnerabilidades (al menos una vez al mes), y las vulnerabilidades detectadas deberán ser solucionadas. Las pruebas se realizan con arreglo al método señalado en la sección 5.4.1, a través de una base de datos de vulnerabilidad actualizada.

5.5. *Disposiciones relativas a la evaluación del riesgo*

Si es preciso realizar pruebas de penetración, estas deben incluirse en las pruebas de seguridad.

Cada Parte podrá contratar a una empresa especializada para la realización de pruebas de seguridad, siempre que dicha empresa:

— posea la competencia y experiencia necesarias en relación con tales pruebas de seguridad;

— no rinda cuentas directamente al desarrollador responsable o a su contratista y no participe en el desarrollo del programa informático del enlace, ni sea un subcontratista del desarrollador;

— haya firmado un acuerdo de no divulgación en el que se comprometa a respetar la confidencialidad de los resultados y a tratarlos como nivel «ETS CRITICAL» (crítico RCDE), de acuerdo con las instrucciones de tratamiento.