2024/1873

5.7.2024

DECISIÓN (UE) 2024/1873 DEL CONSEJO

de 24 de junio de 2024

relativa a la posición que debe adoptarse, en nombre de la Unión Europea, en el 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, por lo que respecta a la modificación del anexo II del Acuerdo y de los procedimientos operativos comunes y las normas técnicas de enlace

(Texto pertinente a efectos del EEE)

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 192, apartado 1, en relación con su artículo 218, apartado 9,

Vista la propuesta de la Comisión Europea,

Considerando lo siguiente:

(1) 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») fue firmado el 23 de noviembre de 2017 de conformidad con la Decisión (UE) 2017/2240 del Consejo ([2]).

(2) El Acuerdo fue celebrado mediante la Decisión (UE) 2018/219 del Consejo ([3]) y entró en vigor el 1 de enero de 2020.

(3) De acuerdo con el artículo 12, apartado 3, del Acuerdo, el Comité Mixto puede adoptar decisiones que, en el momento de su entrada en vigor, serán vinculantes para las Partes.

(4) El artículo 13, apartado 2, del Acuerdo establece que el Comité Mixto puede modificar los anexos del Acuerdo.

(5) El artículo 3, apartados 6 y 7, establece que los procedimientos operativos comunes y las normas técnicas de enlace han de surtir efecto una vez sean adoptados mediante decisión del Comité Mixto. Mediante las Decisiones n.º 1/2020 ([4]) y n.º 2/2020 ([5]), el Comité Mixto adoptó los procedimientos operativos comunes y las normas técnicas de enlace, respectivamente.

(6) Procede modificar el anexo II del Acuerdo para reflejar la evolución del enlace entre los registros del Régimen de comercio de derechos de emisión de la UE y el Régimen de comercio de derechos de emisión de Suiza y para racionalizar las disposiciones del anexo II a la luz del progreso tecnológico. Para garantizar la coherencia de los procedimientos operativos comunes y las normas técnicas de enlace con el anexo II, también deben modificarse dichos documentos.

([1]) DO L 322 de 7.12.2017, p. 3.
([2]) Decisión (UE) 2017/2240 del Consejo, de 10 de noviembre de 2017, relativa a la firma, en nombre de la Unión, y a la aplicación provisional 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 322 de 7.12.2017, p. 1).
([3]) Decisión (UE) 2018/219 del Consejo, de 23 de enero de 2018, relativa a la celebración 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 43 de 16.2.2018, p. 1).
([4]) Decisión n.º 1/2020 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, sobre la adopción de procedimientos operativos comunes (POC) [2021/1033] (DO L 226 de 25.6.2021, p. 2).
([5]) 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] (DO L 226 de 25.6.2021, p. 16).

(7) El Comité Mixto, durante su séptima reunión, o antes mediante procedimiento escrito de conformidad con el artículo 8, apartado 4, del reglamento interno del Comité Mixto ([6]), ha de adoptar una decisión por lo que respecta a la modificación del anexo II del Acuerdo y a la modificación de los procedimientos operativos comunes y las normas técnicas de enlace.

(8) Procede establecer la posición que debe adoptarse, en nombre de la Unión, en el Comité Mixto, por lo que respecta a la modificación del anexo II del Acuerdo y a la modificación de los procedimientos operativos comunes y las normas técnicas de enlace, habida cuenta de que la decisión será vinculante para la Unión.

(9) Por lo tanto, la posición de la Unión en el Comité Mixto debe basarse en el proyecto de Decisión adjunto.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

La posición que debe adoptarse, en nombre de la Unión, durante la séptima reunión del Comité Mixto, o antes mediante procedimiento escrito con arreglo al artículo 8, apartado 4, del reglamento interno del Comité Mixto, se basará en el proyecto de Decisión del Comité Mixto adjunto a la presente Decisión.

Artículo 2

La presente Decisión entrará en vigor el día de su adopción.

Hecho en Luxemburgo, el 24 de junio de 2024.

Por el Consejo

El Presidente

D. CLARINVAL

([6]) Decisión n.º 1/2019 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 25 de enero de 2019, relativa a la adopción de su reglamento interno y Decisión (UE) 2018/1279 del Consejo, de 18 de septiembre de 2018, relativa a la posición que debe adoptarse en nombre de la Unión Europea en el seno 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 en relación con la adopción de su reglamento interno (DO L 239 de 24.9.2018, p. 8).

DECISIÓN N.º1/2024 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 …

por lo que respecta a la modificación del anexo II del Acuerdo y de los procedimientos operativos comunes y las normas técnicas de enlace

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 9 y su artículo 13, apartado 2,

Considerando lo siguiente:

(1) La Decisión n.º 2/2019 del Comité Mixto ([2]) estableció una solución provisional para hacer operativo el vínculo entre el RCDE UE y el RCDE de Suiza.

(2) En su tercera reunión, el Comité Mixto convino en la necesidad de efectuar un análisis de los costes y beneficios derivados del establecimiento de un enlace permanente entre el Registro de la Unión y el Registro suizo.

(3) En su quinta reunión, el Comité Mixto mostró su acuerdo con el informe presentado por el grupo de trabajo creado por las Decisiones 1/2020 ([3]) y 2/2020 ([4]) del Comité Mixto. En dicho informe, el grupo de trabajo analizó y recomendó un enfoque para aplicar el enlace permanente entre el Registro de la Unión y el Registro suizo.

(4) Para reflejar los requisitos técnicos del enlace permanente entre el Registro de la Unión y el Registro suizo, y para racionalizar las disposiciones del anexo II del Acuerdo a la luz del progreso tecnológico, debe modificarse el anexo II del Acuerdo.

(5) Para garantizar la coherencia de los procedimientos operativos comunes y las normas técnicas de enlace con el anexo II del Acuerdo, también deben modificarse dichos documentos.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

1. El anexo II del Acuerdo se sustituye por el texto que figura en el anexo I de la presente Decisión.

2. Los procedimientos operativos comunes a que se refiere el artículo 3, apartado 6, del Acuerdo figuran en el anexo II de la presente Decisión. Sustituyen a los procedimientos operativos comunes que figuran en el anexo de la Decisión n.º 1/2020.

3. Las normas técnicas de enlace a que se refiere el artículo 3, apartado 7, del Acuerdo figuran en el anexo III de la presente Decisión. Sustituyen a las normas técnicas de enlace que figuran en el anexo de la Decisión n.º 2/2020

([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 [2020/1359] (DO L 314 de 29.9.2020, p. 68).

([3]) Decisión n.º 1/2020 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 sobre la adopción de procedimientos operativos comunes (POC) [2021/1033] (DO L 226 de 25.6.2021, p. 2).

([4]) 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] (DO L 226 de 25.6.2021, p. 16).

Artículo 2

La presente Decisión entrará en vigor el día de su adopción.

Hecho en …, el

Por el Comité Mixto

La Secretaria / El Secretario por la Unión Europea	*La Presidenta / El Presidente*	*La Secretaria / El Secretario por Suiza*

ANEXO I

«ANEXO II

NORMAS TÉCNICAS DE ENLACE

A fin de hacer operativo el enlace entre el RCDE UE y el RCDE de Suiza, se aplicó una solución provisional en 2020. A partir de 2023, el enlace entre los registros de los dos sistemas de comercio de derechos de emisión se irá transformando gradualmente en un enlace permanente entre los registros, cuya aplicación está prevista a más tardar en 2024, para permitir el funcionamiento de los mercados vinculados con respecto a los beneficios de la liquidez del mercado y la ejecución de las transacciones entre los dos sistemas vinculados, de manera equivalente a un único mercado compuesto por dos sistemas y que permita a los participantes en el mercado actuar como si estuvieran en un único mercado, sujeto únicamente a las disposiciones reglamentarias individuales de las Partes.

Las normas técnicas de enlace (NTE) especificarán:

— la arquitectura del enlace de comunicación,

— las comunicaciones entre el DTSS y el DTUE.

— la seguridad de la transferencia de datos,

— la lista de funciones (transacciones, conciliación, etc.),

— la definición de la capa de transporte,

— los requisitos de registro de datos,

— los mecanismos operativos (servicio de asistencia, ayuda, etc.),

— el plan de activación de la comunicación y el procedimiento de ensayo,

— el procedimiento de verificación de la seguridad.

Las NTE especificarán que los administradores adoptarán todas las medidas razonables para garantizar que el DTSS, el DTUE y el enlace estén en funcionamiento veinticuatro horas al día, siete días a la semana, y que se reduzcan al mínimo las interrupciones en la actividad del DTSS, del DTUE y del enlace.

Las NTE establecerán requisitos adicionales de seguridad para el Registro de Suiza, el DTSS, el Registro de la Unión y el DTUE y estarán documentadas en un “plan de gestión de la seguridad”. En concreto, las NTE especificarán que:

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

— en caso de vulneración de la seguridad, las Partes se comprometerán a intercambiarse inmediatamente la información. En la medida en que se disponga de los detalles técnicos, el administrador del Registro de Suiza y el administrador central de la Unión compartirán un informe en el que se describa el incidente (fecha, causa, repercusión, soluciones) en el plazo de veinticuatro horas tras determinarse que un incidente de seguridad supone una vulneración de la seguridad.

El procedimiento de verificación de la seguridad dispuesto en las NTE se completará antes de establecer el enlace de comunicación entre el DTSS y el DTUE y cuando se requiera una nueva versión o revisión del DTSS o del DTUE.

Las NTE dispondrán dos entornos de ensayo además del entorno productivo: un entorno de ensayo para desarrolladores y un entorno de aceptación.

Las Partes acreditarán, a través del administrador del Registro de Suiza y del administrador central de la Unión, que se ha efectuado una evaluación independiente de la seguridad de sus sistemas en los últimos doce meses de conformidad con los requisitos de seguridad dispuestos en las NTE. Toda actualización importante de los programas informáticos se someterá a una prueba de verificación de la seguridad, y en concreto a ensayos de penetración, de conformidad con los requisitos de seguridad dispuestos en las NTE. Los ensayos de penetración no serán realizados por el desarrollador de los programas informáticos ni por un subcontratista de este.».

ANEXO II

PROCEDIMIENTOS OPERATIVOS COMUNES (POC) DE CONFORMIDAD CON EL ARTÍCULO 3, APARTADO 6, 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

Procedimientos para el enlace permanente entre los registros

Índice

1. GLOSARIO . . . 9
2. INTRODUCCIÓN . . . 9
2.1. Ámbito de aplicación . . . 10
2.2. Destinatarios . . . 10
3. ENFOQUE Y NORMAS . . . 10
4. GESTIÓN DE INCIDENTES . . . 11
4.1. Detección y registro de incidentes . . . 11
4.2. Clasificación y apoyo inicial . . . 11
4.3. Investigación y diagnóstico . . . 12
4.4. Resolución y reanudación del servicio . . . 12
4.5. Cierre de incidentes . . . 12
5. GESTIÓN DE PROBLEMAS . . . 13
5.1. Identificación y registro del problema . . . 13
5.2. Priorización de problemas . . . 13
5.3. Investigación y diagnóstico de problemas . . . 13
5.4. Resolución . . . 13
5.5. Cierre del problema . . . 13
6. EJECUCIÓN DE SOLICITUDES . . . 13
6.1. Inicio de solicitudes . . . 13
6.2. Registro y análisis de solicitudes . . . 14
6.3. Aprobación de solicitudes . . . 14
6.4. Ejecución de solicitudes . . . 14
6.5. Transferencia de solicitudes . . . 14
6.6. Revisión de la ejecución de solicitudes . . . 14
6.7. Cierre de solicitudes . . . 14
7. GESTIÓN DE CAMBIOS . . . 14
7.1. Solicitud de cambio . . . 15
7.2. Evaluación y planificación de cambios . . . 15
7.3. Aprobación del cambio . . . 15
7.4. Ejecución del cambio . . . 15
8. GESTIÓN DE VERSIONES . . . 15
8.1. Planificación de la versión . . . 15
8.2. Paquete de medidas de desarrollo y comprobación de la versión . . . 16
8.3. Preparación del despliegue . . . 16

8.4. Reversión de la versión . . . 16
8.5. Revisión y cierre de la versión . . . 16
9. GESTIÓN DE INCIDENTES DE SEGURIDAD . . . 17
9.1. Categorización de incidentes de seguridad de la información . . . 17
9.2. Tratamiento de incidentes de seguridad de la información . . . 17
9.3. Identificación de incidentes de seguridad . . . 17
9.4. Análisis de incidentes de seguridad . . . 17
9.5. Evaluación de la gravedad de los incidentes de seguridad, activación de los niveles sucesivos de intervención y presentación de informes . . . 17
9.6. Informes de respuesta en materia de seguridad . . . 18
9.7. Seguimiento, desarrollo de las capacidades y mejora continua . . . 18
10. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN . . . 18
10.1. Identificación de la información sensible . . . 18
10.2. Niveles de confidencialidad de los recursos de información . . . 18
10.3. Asignación del titular de los recursos de información . . . 18
10.4. Registro de información sensible . . . 19
10.5. Tratamiento de la información sensible . . . 19
10.6. Gestión del acceso . . . 19
10.7. Gestión de certificados o claves . . . 19

1. GLOSARIO

Cuadro 1-1: Acrónimos y definiciones

Acrónimo/Término	Definición
Autoridad de certificación (AC)	Entidad que emite certificados digitales
CH	Confederación Suiza
RCDE	Régimen de comercio de derechos de emisión
UE	Unión Europea
IMT	Equipo encargado de la gestión de incidentes
Recurso de información	Información útil para una empresa u organización
TI	Tecnologías de la información
ITIL	Biblioteca de infraestructura de tecnologías de la información
GSTI	Gestión de Servicios de TI
NTE	Normas Técnicas de Enlace
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.
SDC	Solicitud de cambio
LIS	Lista de información sensible
SR	Solicitud de servicio
Wiki	Sitio web que permite a los usuarios intercambiar información y conocimientos mediante la adición o adaptación de contenidos directamente a través de un navegador web.

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, «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 hacer operativo el enlace entre el RCDE UE y el RCDE de Suiza, se establecerá, 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 permitirá 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 hacer operativo el enlace entre el RCDE UE y el RCDE de Suiza, se aplicó una solución provisional en 2020. A partir de 2023, el enlace entre los registros de los dos sistemas de comercio de derechos de emisión se irá transformando gradualmente en un enlace permanente entre los registros, cuya aplicación está prevista a más tardar en 2024, para permitir el funcionamiento de los mercados vinculados con respecto a los beneficios de la liquidez del mercado y la ejecución de las transacciones entre los dos sistemas vinculados, de manera equivalente a un único mercado compuesto por dos sistemas y que permita a los participantes en el mercado actuar como si estuvieran en un único mercado, sujeto únicamente a las disposiciones reglamentarias individuales de las Partes (anexo II del Acuerdo).

De conformidad con el artículo 3, apartado 6, del Acuerdo, el administrador del Registro suizo y el administrador central de la Unión determinarán los procedimientos operativos comunes (POC) sobre cuestiones técnicas o de otra índole necesarias para el funcionamiento del enlace, teniendo en cuenta las prioridades de la legislación nacional. Los POC diseñados por los administradores surtirán efecto una vez sean adoptados mediante decisión del Comité Mixto.

Los POC fueron adoptados por el Comité Mixto mediante la Decisión n.º 1/2020. El Comité Mixto aprobará los POC actualizados, tal como figuran en el presente documento, mediante la Decisión n.º 1/2024. De conformidad con la presente Decisión y con las solicitudes del Comité Mixto, el administrador del Registro suizo y el administrador central de la Unión han elaborado, y actualizarán, directrices técnicas adicionales para hacer operativo el enlace y garantizar que estas se vayan adaptando constantemente al progreso técnico y a los nuevos requisitos relativos a la seguridad y la 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 procesales del enlace entre los registros del RCDE UE y el RCDE de Suiza. Aunque establece los requisitos generales de procedimiento en términos operativos, serán necesarias otras directrices técnicas para hacer operativo el enlace.

Para su correcto funcionamiento, el enlace exigirá especificaciones técnicas que permitan hacerlo más operativo. De conformidad con el artículo 3, apartado 7, del Acuerdo, estos asuntos se detallan en el documento de Normas Técnicas de Enlace (NTE), que se adoptará por separado mediante decisión del Comité Mixto.

El objetivo de los POC es garantizar que los servicios informáticos relacionados con el funcionamiento del enlace entre los registros del RCDE UE y del RCDE de Suiza se prestan de manera eficaz y eficiente, especialmente para satisfacer las solicitudes de servicio, remediar los fallos de los servicios y resolver problemas, así como para llevar a cabo tareas operativas rutinarias con arreglo a normas internacionales para la gestión de servicios de TI.

Para el enlace permanente entre los registros, solo serán necesarios los siguientes POC, que forman parte del presente documento:

— gestión de incidentes,

— gestión de problemas,

— ejecución de solicitudes,

— gestión de cambios,

— gestión de versiones,

— gestión de incidentes de seguridad,

— gestión de la seguridad de la información.

2.2. Destinatarios

Los destinatarios de estos POC son los equipos de apoyo a los registros de la UE y de Suiza.

3. ENFOQUE Y NORMAS

El principio siguiente se aplica a todos los POC:

— La UE y la CH acuerdan definir los POC sobre la base de la ITIL (Biblioteca de Infraestructura de Tecnologías de la Información, versión 4). Las prácticas extraídas de esta norma se reutilizan y adaptan a las exigencias específicas relacionadas con el enlace permanente entre los registros.

— La comunicación y la coordinación necesarias para el tratamiento de los POC entre las dos Partes se realizan a través de los servicios de asistencia de los registros de la CH y la UE. Las tareas se asignan siempre en una Parte.

— En caso de desacuerdo sobre la tramitación de un POC, se procederá a su análisis y resolución entre los dos servicios de asistencia. Si no se llega a un acuerdo, la búsqueda de una solución conjunta se transfiere al nivel siguiente.

Niveles de intervención	UE	CH
Primer nivel	Servicio de asistencia de la UE	Servicio de asistencia de la CH
Segundo nivel	Gestor de operaciones de la UE	Gestor de aplicación del Registro de la CH
Tercer nivel	Comité Mixto (que puede delegar esta responsabilidad con arreglo al artículo 12, apartado 5, del Acuerdo)	
Cuarto nivel	Comité Mixto, si se ha delegado el tercer nivel	

— Cada Parte podrá determinar los procedimientos para el funcionamiento de su propio sistema de registro, teniendo en cuenta los requisitos e interfaces relacionados con estos POC.

— Se utiliza una herramienta de gestión de servicios de TI (GSTI) para apoyar a los POC, en particular la gestión de incidentes, la gestión de problemas y la ejecución de solicitudes, y la comunicación entre ambas Partes.

— Además, se permite el intercambio de información por correo electrónico.

— Ambas Partes garantizan que se cumplen los requisitos de seguridad de la información de acuerdo con las instrucciones de tratamiento.

4. GESTIÓN DE INCIDENTES

El objetivo del proceso de gestión de incidentes es recuperar lo antes posible un nivel de servicio normal de los servicios de TI tras un incidente y limitar al máximo la interrupción de las actividades.

La gestión de incidentes también debe llevar un registro de incidentes a efectos de notificación e integrarse con otros procesos para impulsar una mejora continua.

Desde una perspectiva global, la gestión de incidentes comprende las siguientes actividades:

— detección y registro de incidentes,

— clasificación y apoyo inicial,

— investigación y diagnóstico,

— resolución y reanudación del servicio,

— cierre de incidentes.

A lo largo de todo el ciclo de vida de un incidente, el proceso de gestión de incidentes se encarga del mantenimiento constante de la titularidad, así como de su seguimiento, rastreo y comunicación.

4.1. Detección y registro de incidentes

Un incidente puede ser detectado por un grupo de apoyo, las herramientas de control automatizado o el personal técnico que esté llevando a cabo labores de vigilancia rutinarias.

Una vez detectado, el incidente debe ser registrado, asignándosele un identificador único que permita un rastreo y seguimiento adecuados. El identificador único de un incidente es el identificador asignado en el sistema común de casos por el servicio de asistencia de la Parte (la UE o la CH) que haya comunicado el incidente, y debe utilizarse en todas las comunicaciones relacionadas con este.

Para todos los incidentes, el punto de contacto será el servicio de asistencia de la Parte que haya registrado el tique.

4.2. Clasificación y apoyo inicial

La clasificación de incidentes tiene por objeto comprender e identificar qué sistema o servicio se está viendo afectado por un incidente, y en qué medida. Para ser eficaz, la clasificación debe canalizar el incidente hacia el recurso correcto al primer intento, a fin de acelerar su resolución.

La fase de clasificación debe categorizar y priorizar el incidente en función de su impacto y su urgencia, para que pueda ser tratado en los términos establecidos para cada nivel de prioridad.

Si el incidente puede afectar a la confidencialidad o la integridad de los datos sensibles o tener un impacto en la disponibilidad del sistema, el incidente se declarará también como incidente de seguridad y, a continuación, se gestionará con arreglo al proceso definido en el capítulo relativo a la gestión de incidentes de seguridad del presente documento.

Si es posible, el servicio de asistencia que haya registrado el tique realizará un diagnóstico inicial. Para ello, comprobará si el incidente es un error conocido. En caso afirmativo, el método para resolver o sortear el problema ya es conocido y está documentado.

Si el servicio de asistencia logra resolver el incidente, lo cerrará efectivamente en este momento, ya que se ha cumplido la principal finalidad de la gestión de incidentes (a saber, la rápida restauración del servicio para el usuario final). En caso contrario, el servicio de asistencia deberá transferir el incidente al grupo de resolución apropiado para que este ponga en marcha el proceso de investigación y diagnóstico.

4.3. Investigación y diagnóstico

El proceso de investigación y diagnóstico de incidentes se pone en marcha cuando el servicio de asistencia no puede resolver un incidente en el marco del diagnóstico inicial, por lo que lo transfiere al nivel adecuado. La activación de los niveles sucesivos de intervención en caso de incidente forma parte integral del proceso de investigación y diagnóstico.

Una práctica común en la fase de investigación y diagnóstico es el intento de recrear el incidente en condiciones controladas. En el proceso de investigación y diagnóstico de incidentes, es importante comprender el orden de los hechos que dieron lugar al incidente.

La activación de los niveles sucesivos de intervención es el reconocimiento de que un incidente no puede resolverse en el nivel de apoyo actual y debe transferirse a un grupo de apoyo de nivel superior o a la otra Parte. La activación de los niveles sucesivos de intervención puede seguir dos vías: horizontal (funcional) o vertical (jerárquica).

El servicio de asistencia que ha registrado y activado el incidente es responsable de transferir el incidente al recurso adecuado y de hacer un rastreo de la situación general y de la asignación del incidente.

La Parte a la que se haya asignado el incidente es la encargada de garantizar que las acciones solicitadas se lleven a cabo a su debido tiempo y de informar al respecto al servicio de asistencia de su propia Parte.

4.4. Resolución y reanudación del servicio

Una vez que se ha entendido perfectamente el incidente, se procede a resolverlo y se reanuda el servicio. La resolución de un incidente implica que se ha encontrado una forma de subsanar el problema. La aplicación de la solución constituye la fase de reanudación del servicio.

Una vez que los recursos adecuados remedian el fallo del servicio, el incidente se devuelve al servicio de asistencia correspondiente, que es el que ha registrado el incidente, y ese servicio de asistencia confirma con quien ha señalado primero el incidente que el error se ha corregido y que puede cerrarse el incidente. Se registrarán para usos futuros los resultados del procesamiento del incidente.

La reanudación del servicio puede realizarse confiando la tarea a personal de apoyo informático o proporcionando al usuario final una serie de instrucciones.

4.5. Cierre de incidentes

El cierre es el último paso en el proceso de gestión de incidentes y se produce poco después de la resolución del incidente.

En la lista de control de las actividades que deben realizarse durante la fase de cierre, destacan las siguientes:

— la verificación de la categorización inicial que se asignó al incidente,

— la recopilación adecuada de toda la información relativa al incidente,

— la documentación adecuada del incidente y la actualización de la base de conocimientos,

— la comunicación adecuada a todos los interesados, directa o indirectamente afectados por el incidente.

Un incidente se cierra oficialmente una vez que el servicio de asistencia ha completado la fase de cierre del incidente y comunicado este extremo a la otra Parte.

Una vez cerrado un incidente, este no puede volver a abrirse. En el caso de que un mismo incidente vuelva a producirse a corto plazo, no se reabrirá el incidente original, sino que deberá registrarse un nuevo incidente.

Si el incidente es objeto de rastreo por los servicios de asistencia tanto de la UE como de la CH, el cierre definitivo corresponde al servicio de asistencia que haya registrado el tique.

5. GESTIÓN DE PROBLEMAS

Este procedimiento debe seguirse siempre que se detecte un problema y, por tanto, se active el proceso de gestión de problemas. La gestión de problemas tiene por objeto principal mejorar la calidad del proceso y reducir el volumen de incidentes planteados. Un problema puede ser la causa de uno o más incidentes. Cuando se notifica un incidente, el objetivo de la gestión de incidentes es restablecer lo antes posible el servicio, posiblemente a través de soluciones provisionales. Cuando se notifica un problema, el objetivo es investigar la causa profunda a fin de identificar un cambio que garantice que el problema y los incidentes conexos ya no volverán a producirse.

5.1. Identificación y registro del problema

Dependiendo de qué Parte haya creado el tique, el punto de contacto para los asuntos relacionados con el problema será el servicio de asistencia de la UE o el servicio de asistencia de la CH.

El identificador único de un problema es el identificador asignado por la Gestión de Servicios de TI (GSTI). Dicho identificador debe utilizarse en todas las comunicaciones relacionadas con el problema.

Un problema puede notificarse como consecuencia de un incidente o abrirse por iniciativa propia con vistas a resolver los fallos detectados en el sistema en cualquier momento.

5.2. Priorización de problemas

Al igual que los incidentes, los problemas pueden clasificarse según su gravedad y prioridad para facilitar su rastreo, teniendo en cuenta el impacto de los incidentes conexos y la frecuencia con la que se producen.

5.3. Investigación y diagnóstico de problemas

Cualquiera de las Partes puede comunicar un problema. El servicio de asistencia de la Parte que ha señalado primero el incidente será responsable de registrarlo, asignándolo al recurso adecuado y rastreando la situación general del problema.

El grupo de resolución al que se transfiera el problema es responsable de gestionarlo a su debido tiempo y en comunicación con el servicio de asistencia.

Previa solicitud, ambas Partes serán responsables de velar por que se lleven a cabo las acciones que se les hayan asignado y de proporcionar información al servicio de asistencia de su propia Parte.

5.4. Resolución

El grupo de resolución al que se asigna el problema es responsable de resolverlo y de proporcionar información pertinente al servicio de asistencia de su propia Parte.

Los resultados del tratamiento del problema se registrarán para su utilización futura.

5.5. Cierre del problema

Un problema se cierra oficialmente una vez que se resuelve mediante la aplicación del cambio previsto. La fase de cierre del problema correrá a cargo del servicio de asistencia que haya registrado el problema e informado al servicio de asistencia de la otra Parte.

6. EJECUCIÓN DE SOLICITUDES

El proceso de ejecución de solicitudes es la gestión integral de extremo a extremo de la solicitud de un servicio nuevo o existente desde el momento en que se registra y se aprueba hasta el momento del cierre. Las solicitudes de servicio son generalmente solicitudes pequeñas, predefinidas, repetibles, frecuentes, aprobadas previamente y de procedimiento.

A continuación, se recogen los principales pasos que deben seguirse:

6.1. Inicio de solicitudes

La información relacionada con una solicitud de servicio se transmite al servicio de asistencia de la UE o de la CH por correo electrónico o llamada telefónica, o a través de la herramienta de Gestión de Servicios de TI (GSTI) o cualquier otro canal de comunicación acordado.

6.2. Registro y análisis de solicitudes

Para todas las solicitudes de servicio, el punto de contacto debe ser el servicio de asistencia de la UE o de la CH, en función de cuál de las Partes haya solicitado el servicio. Este servicio será responsable de registrar y analizar la solicitud de servicio con la debida diligencia.

6.3. Aprobación de solicitudes

El agente del servicio de asistencia de la Parte que haya solicitado el servicio comprobará si se precisa alguna autorización de la otra Parte y, en su caso, procederá a recabarla. Si no se aprueba la solicitud de servicio, el servicio de asistencia actualiza y cierra el tique.

6.4. Ejecución de solicitudes

Este paso sirve para garantizar una gestión eficaz y eficiente de las solicitudes de servicio. Se debe hacer una distinción entre los siguientes casos:

— La ejecución de la solicitud de servicio solo afecta a una Parte. En este caso, esta Parte emite las órdenes de ejecución y coordina la ejecución.

— La ejecución de la solicitud de servicio afecta tanto a la UE como a la CH. En este caso, los servicios de asistencia emiten las órdenes de ejecución en su esfera de responsabilidad. Los dos servicios de asistencia coordinan la tramitación de la ejecución de solicitudes de servicio. La responsabilidad general recae en el servicio de asistencia que recibió e inició la solicitud de servicio.

Una vez satisfecha la solicitud de servicio, debe cambiarse su estado a «resuelta».

6.5. Transferencia de solicitudes

El servicio de asistencia puede transferir la solicitud de servicio pendiente al recurso adecuado (un tercero) en caso necesario.

Las solicitudes se transfieren a los terceros respectivos, lo que implica que el servicio de asistencia de la UE tendrá que pasar a través del servicio de asistencia de la CH para transferir la solicitud a un tercero de la CH, y viceversa.

El tercero al que se haya transferido la solicitud de servicio es el responsable de tramitar dicha solicitud a su debido tiempo y de comunicarse con el servicio de asistencia que la haya transferido.

El servicio de asistencia que registró la solicitud de servicio es responsable de hacer un rastreo de la situación general y de la asignación de una solicitud de servicio.

6.6. Revisión de la ejecución de solicitudes

El servicio de asistencia responsable debe someter el registro de solicitudes de servicio a un control de calidad final antes de su cierre. El objetivo es garantizar que la solicitud de servicio se tramita realmente y que se ofrece con suficiente detalle toda la información necesaria para describir el ciclo de vida de la solicitud. Además, los resultados de la tramitación de la solicitud deben registrarse para su uso futuro.

6.7. Cierre de solicitudes

Si las Partes asignadas coinciden en que la solicitud de servicio se ha cumplido y el solicitante considera resuelto el caso, deberá cambiarse su estado a «cerrada».

Una solicitud de servicio se cierra formalmente una vez que el servicio de asistencia que la registró haya ejecutado la fase de cierre de la solicitud e informado al servicio de asistencia de la otra Parte.

7. GESTIÓN DE CAMBIOS

El objetivo es garantizar que se utilizan métodos y procedimientos normalizados para el tratamiento eficaz y rápido de todos los cambios en la infraestructura de TI, con el fin de reducir al mínimo el número de incidentes relacionados y su incidencia en el servicio. Los cambios en la infraestructura de TI pueden producirse de forma reactiva, en respuesta a problemas o a requisitos impuestos externamente —por ejemplo, cambios legislativos—, o de manera proactiva, al tratar de conseguir una mayor eficiencia y eficacia o para permitir o reflejar iniciativas empresariales.

El proceso de gestión de cambios incluye diferentes medidas que registran todos los detalles sobre una solicitud de cambio para un futuro rastreo. Estos procesos garantizan que el cambio sea validado y comprobado antes de su despliegue. El proceso de gestión de versiones es responsable de la correcta aplicación del despliegue.

7.1. Solicitud de cambio

La solicitud de cambio (SDC) se presenta al equipo de gestión de cambios para su validación y aprobación. Para todas las solicitudes de cambio, el punto de contacto debe ser el servicio de asistencia de la UE o de la CH, en función de la Parte que haya solicitado el servicio. Este servicio de asistencia será responsable de registrar y analizar la solicitud con la debida diligencia.

Las solicitudes de cambio podrán responder a:

— un incidente que provoca un cambio,

— un problema existente que da lugar a un cambio,

— un usuario final que solicita un nuevo cambio,

— un cambio resultante de un mantenimiento en curso,

— cambios legislativos.

7.2. Evaluación y planificación de cambios

Esta fase consiste en la evaluación de los cambios y de las actividades de planificación. Incluye actividades de priorización y planificación para minimizar el riesgo y el impacto.

Si la aplicación de la solicitud de cambio afecta tanto a la UE como a la CH, la Parte que haya registrado dicha solicitud verifica la evaluación y planificación del cambio con la otra Parte.

7.3. Aprobación del cambio

Toda solicitud de cambio registrada debe ser aprobada por el nivel de intervención correspondiente.

7.4. Ejecución del cambio

La ejecución del cambio se gestiona en el marco del proceso de gestión de versiones. Los equipos de gestión de versiones de ambas Partes siguen sus propios procesos, que implican la planificación y la comprobación. El examen de los cambios se produce una vez que se ha completado la ejecución. Para garantizar que todo se ha hecho de acuerdo con el plan, el actual proceso de gestión de cambios se revisa constantemente y se actualiza cuando es necesario.

8. GESTIÓN DE VERSIONES

Una versión representa uno o varios cambios en un servicio de TI, recogidos en un plan de versiones, que deberán ser autorizados, elaborados, desarrollados, comprobados y desplegados de manera conjunta. Una versión puede corresponder a la corrección de un fallo, cambios en los equipos informáticos o en algún componente, la modificación de los programas informáticos, actualizaciones de las versiones de aplicación o cambios en la documentación o en los procesos. El contenido de cada versión se gestiona, se comprueba y se despliega como una entidad única.

La gestión de versiones tiene por objeto planificar, desarrollar, comprobar y validar una versión y ofrecer la capacidad necesaria para prestar los servicios designados, lo que permitirá satisfacer los requisitos de las partes interesadas y alcanzar los objetivos previstos. Los criterios de aceptación para todos los cambios del servicio se definirán y documentarán durante la coordinación del diseño y se proporcionarán a los equipos de gestión de versiones.

La versión consistirá normalmente en una serie de soluciones a problemas y mejoras en un servicio. Contendrá los programas informáticos nuevos o modificados y cualesquiera equipos informáticos nuevos o modificados necesarios para aplicar los cambios aprobados.

8.1. Planificación de la versión

El primer paso del proceso consiste en reagrupar los cambios autorizados en los paquetes de versiones y definir el alcance y el contenido de estas. Sobre la base de esta información, el subproceso de planificación de versiones establece un calendario para el desarrollo, la comprobación y el despliegue de la versión.

La planificación debe definir:

— el alcance y el contenido de la versión,

— la evaluación del riesgo y el perfil de riesgo de la versión,

— los clientes o usuarios afectados por la versión,

— el equipo responsable de la versión,

— la entrega y la estrategia de despliegue de la versión,

— los recursos necesarios para la versión y el despliegue.

Ambas Partes se informan mutuamente sobre sus períodos de planificación y mantenimiento de las versiones. Si una versión afecta tanto a la UE como a la CH, coordinan la planificación y definen un período común de mantenimiento.

8.2. Paquete de medidas de desarrollo y comprobación de la versión

La etapa de desarrollo y comprobación del proceso de gestión de versiones establece el enfoque aplicable a la hora de ejecutar la versión o el paquete de versiones y mantener los entornos controlados antes de cambiar la producción, así como de comprobar todos los cambios en todos los entornos de la versión.

Si una versión afecta tanto a la UE como a la CH, estas coordinan los planes de entrega y las comprobaciones. Esta coordinación abarca los siguientes aspectos:

— cómo y cuándo se entregarán las unidades de versión y los componentes de servicio,

— cuáles son los plazos de ejecución habituales y qué sucede en caso de retraso,

— cómo rastrear la evolución de la entrega y obtener confirmación,

— los indicadores para el seguimiento y la determinación del éxito del esfuerzo de despliegue de la versión,

— casos de prueba comunes para las funcionalidades y cambios pertinentes.

Una vez finalizado este subproceso, todos los componentes de la versión requeridos estarán listos para entrar en la fase de despliegue en directo.

8.3. Preparación del despliegue

El subproceso de preparación garantiza que los planes de comunicación se definan correctamente, que las notificaciones estén listas para ser enviadas a todas las partes interesadas y usuarios finales afectados, y que la versión se integre en el proceso de gestión de cambios para garantizar que todos los cambios se lleven a cabo de manera controlada y sean aprobados por los foros competentes.

Si una versión afecta tanto a la UE como a la CH, estas coordinarán las siguientes actividades:

— el registro de la solicitud de cambio para la programación y preparación del despliegue en el entorno de producción,

— la creación del plan de ejecución,

— el enfoque de reversión, de modo que, en caso de que falle el despliegue, pueda volverse al estado anterior,

— las notificaciones enviadas a todas las partes interesadas,

— la obtención de la aprobación del nivel de intervención correspondiente en cuanto a la aplicación de la versión.

8.4. Reversión de la versión

En caso de que se haya producido un fallo en el despliegue, o se haya detectado en la comprobación que el despliegue no ha tenido éxito o no ha cumplido los criterios de aceptación o calidad acordados, los equipos de gestión de versiones de ambas Partes tendrán que volver al estado anterior. Será necesario informar a todas las partes interesadas, incluidos los usuarios finales destinatarios o afectados. A la espera de esta aprobación, el proceso puede reanudarse en cualquiera de las fases anteriores.

8.5. Revisión y cierre de la versión

En la revisión del despliegue, deben incluirse las siguientes actividades:

— obtener información sobre la satisfacción de los clientes y los usuarios, y sobre la calidad del servicio a raíz del despliegue (recabar la información y tenerla en cuenta con vistas a una mejora continua del servicio),

— analizar todos los criterios de calidad que no se hayan cumplido,

— comprobar que se han ejecutado todas las acciones, las soluciones necesarias y los cambios,

— asegurarse de que no existen problemas de aptitudes, recursos, capacidad o rendimiento al final del despliegue,

— comprobar que el cliente, los usuarios finales, el apoyo operativo y otras partes afectadas han documentado y aceptado los eventuales problemas, errores conocidos y soluciones provisionales,

— vigilar los incidentes y problemas causados por el despliegue (proporcionar apoyo desde el primer momento a los equipos operativos en caso de que la versión haya provocado un aumento de los volúmenes de trabajo),

— actualizar la documentación de apoyo (es decir, los documentos de información técnica),

— transferir formalmente el despliegue de la versión a las operaciones de servicio,

— documentar las lecciones aprendidas,

— recabar el documento de síntesis de la versión de los equipos de aplicación,

— cerrar formalmente la versión tras haber comprobado el registro de la solicitud de cambio.

9. GESTIÓN DE INCIDENTES DE SEGURIDAD

La gestión de incidentes de seguridad es un proceso de tratamiento de incidentes de la seguridad a efectos de la comunicación de los incidentes a las partes interesadas potencialmente afectadas; la evaluación y priorización de los incidentes; y la respuesta a los incidentes para solucionar cualquier posible violación de la confidencialidad, la disponibilidad o la integridad de los recursos de información sensible.

9.1. Categorización de incidentes de seguridad de la información

Se analizarán todos los incidentes que afecten al enlace entre el Registro de la Unión y el Registro suizo para determinar la posible pérdida de confidencialidad, integridad o disponibilidad de cualquier información confidencial registrada en la Lista de Información Sensible (LIS).

En tal caso, el incidente se caracterizará como un incidente en la seguridad de la información, se registrará inmediatamente en la herramienta de Gestión de Servicios de TI (GSTI) y se gestionará como tal.

9.2. Tratamiento de incidentes de seguridad de la información

Los incidentes de seguridad son responsabilidad del tercer nivel de intervención y la resolución de los incidentes corre a cargo de un equipo encargado de la gestión de incidentes (IMT).

El IMT se encarga de:

— realizar un primer análisis, categorizar y clasificar la gravedad del incidente,

— coordinar las acciones entre todas las partes interesadas, incluida la documentación completa del análisis del incidente, las decisiones adoptadas para hacer frente al incidente y cualquier posible deficiencia detectada,

— transferir el incidente de seguridad, en función de su gravedad y de manera oportuna, al nivel adecuado para información o la toma de una decisión.

En el proceso de gestión de la seguridad de la información, toda la información relativa a los incidentes se clasifica en el nivel más alto de confidencialidad de la información, pero en ningún caso inferior a «SENSIBLE: *RCDE*».

Para una investigación en curso o una deficiencia que pueda ser aprovechada, y hasta su resolución, la información se clasifica como «TRATAMIENTO ESPECIAL: *RCDE Crítico*».

9.3. Identificación de incidentes de seguridad

Sobre la base del tipo de incidente de seguridad, el responsable de la seguridad de la información establece cuáles son las organizaciones apropiadas para participar y formar parte del IMT.

9.4. Análisis de incidentes de seguridad

El IMT mantiene contactos con todas las organizaciones implicadas y con los miembros pertinentes de sus equipos, según proceda, para revisar el incidente. Durante el análisis, se identificará el alcance de la pérdida de confidencialidad, integridad o disponibilidad de un recurso, y se evaluarán las consecuencias para todas las organizaciones afectadas. A continuación, se definen las medidas iniciales y de seguimiento para resolver el incidente y gestionar su impacto, incluida la incidencia de estas acciones en el uso de los recursos.

9.5. Evaluación de la gravedad de los incidentes de seguridad, activación de los niveles sucesivos de intervención y presentación de informes

El IMT evaluará la gravedad de cualquier nuevo incidente de seguridad después de su caracterización como incidente de seguridad y pondrá en marcha de forma inmediata las actuaciones necesarias en función de la gravedad.

9.6. Informes de respuesta en materia de seguridad

El IMT incluye los resultados de la contención del incidente y la reanudación del servicio en el informe de respuesta a un incidente en la seguridad de la información. El informe se presenta al tercer nivel de intervención utilizando el sistema de correo electrónico seguro u otros medios mutuamente aceptados para una comunicación segura.

La Parte responsable revisa los resultados de contención y reanudación del servicio, y:

— reconecta el registro en caso de desconexión previa,

— facilita las comunicaciones de incidentes a los equipos de registro,

— cierra el incidente.

El IMT debe incluir, de manera segura, los detalles pertinentes en el informe sobre los incidentes de seguridad de la información, con el fin de garantizar un registro y una comunicación coherentes y permitir una acción rápida y apropiada para contener el incidente. Tras su finalización, el IMT proporciona el informe final del incidente de seguridad de la información a su debido tiempo.

9.7. Seguimiento, desarrollo de las capacidades y mejora continua

El IMT proporcionará informes para todos los incidentes de seguridad al tercer nivel de intervención. Este nivel de intervención utilizará los informes para determinar:

— los puntos débiles en los controles de seguridad o en el funcionamiento que deben reforzarse,

— la posible necesidad de reforzar este procedimiento para mejorar la eficacia de la respuesta a los incidentes,

— la formación y las oportunidades de desarrollo de capacidades para reforzar en mayor medida la resiliencia de la seguridad de la información de los sistemas de registro, reducir el riesgo de futuros incidentes y minimizar su impacto.

10. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La gestión de la seguridad de la información tiene por objeto garantizar la confidencialidad, integridad y disponibilidad de la información clasificada, los datos y los servicios informáticos de una organización. Además de los componentes técnicos, incluidos su diseño y comprobación (véanse las NTE), se requieren los siguientes procedimientos operativos comunes para cumplir los requisitos de seguridad del enlace permanente entre los registros.

10.1. Identificación de la información sensible

La confidencialidad de un elemento de información se evalúa determinando el nivel de impacto que podría tener en la actividad (por ejemplo, pérdidas financieras, degradación de la imagen, infracción de la ley, etc.) una vulneración de la seguridad relacionado con esta información.

Los recursos de información sensible se identificarán sobre la base de su impacto en la vinculación.

El nivel de confidencialidad de esta información se evaluará con arreglo a la escala de confidencialidad aplicable a esta vinculación, que se detalla en la sección «Tratamiento de incidentes de seguridad de la información» del presente documento.

10.2. Niveles de confidencialidad de los recursos de información

Una vez determinado, el recurso de información se clasifica aplicando las normas siguientes:

— la identificación de al menos un grado único de confidencialidad, integridad o disponibilidad ALTO hará que el recurso se clasifique como «TRATAMIENTO ESPECIAL: *RCDE Crítico*»,

— la identificación de al menos un grado único de confidencialidad, integridad o disponibilidad MEDIO hará que el recurso se clasifique como «SENSIBLE: *RCDE*»,

— la identificación de grados de confidencialidad, integridad o disponibilidad únicamente BAJOS hará que el recurso se clasifique con la indicación de la UE «SENSIBLE: *Adquisición conjunta del RCDE*» o la indicación de la CH: «LIMITADO: *RCDE*».

10.3. Asignación del titular de los recursos de información

Todos los recursos de información deben tener un titular asignado. Los recursos de información del RCDE que formen parte del enlace entre el DTUE y el DTSS o que estén asociados a dicho enlace deben incluirse en un inventario común de recursos mantenido por ambas Partes. Los recursos de información del RCDE no asociados al enlace entre el DTUE y el DTSS deben incluirse en un inventario de recursos mantenido por la Parte respectiva.

La titularidad de cada recurso de información que forme parte del enlace entre el DTUE y el DTSS o que esté asociado a dicho enlace deberá ser acordada por las Partes. El titular de un recurso de información es el responsable de evaluar su confidencialidad.

El titular debe tener un nivel de responsabilidad adecuado con respecto al valor del recurso o recursos asignados. La responsabilidad del titular con respecto al recurso o recursos y su obligación de mantener el grado de confidencialidad, integridad y disponibilidad requerido deben acordarse y formalizarse.

10.4. Registro de información sensible

Toda la información sensible se registrará en la Lista de Información Sensible (LIS).

Cuando proceda, se tendrá en cuenta y se registrará en la LIS la agregación de información sensible que pueda tener un impacto mayor que el impacto de un único elemento de información (por ejemplo, un conjunto de datos almacenados en la base de datos del sistema).

La LIS no es estática. Las amenazas, las vulnerabilidades, la probabilidad o las consecuencias de los incidentes de seguridad relacionados con los activos pueden cambiar sin indicación alguna, por lo que podrían introducirse nuevos recursos en el funcionamiento de los sistemas de registro.

Por consiguiente, la LIS se revisará periódicamente y toda nueva información identificada como sensible se registrará inmediatamente en ella.

La LIS contendrá, como mínimo, la siguiente información sobre cada entrada:

— descripción de la información,

— titular de la información,

— nivel de confidencialidad,

— indicación de si la información incluye datos personales,

— información adicional, en su caso.

10.5. Tratamiento de la información sensible

Cuando se procese fuera del enlace entre el Registro de la Unión y el Registro suizo, la información sensible se tratará de conformidad con las instrucciones de tratamiento.

La información sensible procesada por el enlace entre el Registro de la Unión y el Registro suizo será tratada por las Partes de conformidad con los requisitos de seguridad.

10.6. Gestión del acceso

El objetivo de la gestión del acceso es conceder a los usuarios autorizados el derecho a utilizar un servicio, impidiendo al mismo tiempo el acceso a los usuarios no autorizados. En ocasiones, la gestión del acceso se denomina «gestión de derechos» o «gestión de identidades».

Para el enlace permanente entre los registros y su funcionamiento, ambas Partes deben tener acceso a los siguientes componentes:

— el wiki: un entorno colaborativo para el intercambio de información común, como la planificación de versiones,

— la herramienta de gestión de servicios de TI (GSTI) para la gestión de incidentes y problemas (véase el capítulo 3 «Enfoque y normas»),

— el sistema de intercambio de mensajes: cada Parte proporcionará un sistema seguro para la transferencia de los mensajes que contengan los datos relativos a las operaciones.

El administrador del Registro suizo y el administrador central de la Unión velarán por que los accesos estén actualizados y actúen como puntos de contacto de sus respectivas Partes para las actividades de gestión del acceso. Las solicitudes de acceso se tramitan de acuerdo con los procedimientos de ejecución de solicitudes.

10.7. Gestión de certificados o claves

Cada Parte es responsable de su propia gestión de certificados o claves (generación, registro, almacenamiento, instalación, uso, renovación, revocación, copia de seguridad y recuperación de certificados o claves). Tal como se indica en las Normas Técnicas de Enlace (NTE), solo se utilizarán los certificados digitales expedidos por una autoridad de certificación (AC) que cuenten con la confianza de ambas Partes. El tratamiento y almacenamiento de los certificados o claves deben seguir las disposiciones de las instrucciones de tratamiento.

Toda revocación o renovación de certificados y claves será coordinada por ambas Partes. Esto se lleva a cabo con arreglo a los procedimientos de ejecución de solicitudes.

El administrador del Registro suizo y el administrador central de la Unión intercambiarán los certificados o claves a través de medios de comunicación seguros con arreglo a lo dispuesto en las instrucciones de tratamiento.

Toda comprobación de los certificados o claves entre las Partes se realizará fuera de banda, independientemente del medio utilizado.

ANEXO III

NORMAS TÉCNICAS DE ENLACE (NTE) DE CONFORMIDAD CON EL 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 el enlace permanente entre los registros

Índice

1. GLOSARIO . . . 23
2. INTRODUCCIÓN . . . 25
2.1. Ámbito de aplicación . . . 25
2.2. Destinatarios . . . 25
3. DISPOSICIONES GENERALES . . . 25
3.1. Arquitectura del enlace de comunicación . . . 25
3.1.1. Intercambio de mensajes . . . 26
3.1.2. Mensaje XML – Nivel de descripción superior . . . 26
3.1.3. Períodos de ingesta . . . 26
3.1.4. Flujo de mensajes de transacción . . . 27
3.2. Seguridad de la transferencia de datos . . . 29
3.2.1. Cortafuegos e interconexión de redes . . . 29
3.2.2. Red privada virtual (VPN) . . . 29
3.2.3. Aplicación de IPsec . . . 29
3.2.4. Protocolo seguro de transferencia para el intercambio de mensajes . . . 30
3.2.5. Firma y cifrado XML . . . 30
3.2.6. Claves criptográficas . . . 30
3.3. Lista de funciones en el marco del enlace . . . 30
3.3.1. Transacciones de actividad . . . 30
3.3.2. Protocolo de conciliación . . . 31
3.3.3. Mensaje de prueba . . . 31
3.4. Requisitos relativos al registro de datos . . . 31
3.5. Requisitos operativos . . . 32
4. DISPOSICIONES SOBRE DISPONIBILIDAD . . . 32
4.1. Diseño que garantice la disponibilidad de las comunicaciones . . . 32
4.2. Inicialización, comunicación, reactivación y plan de pruebas . . . 33
4.2.1. Pruebas de la infraestructura interna de TIC . . . 33
4.2.2. Pruebas de comunicación . . . 33
4.2.3. Pruebas del sistema completo (de extremo a extremo) . . . 33
4.2.4. Pruebas de seguridad . . . 33
4.3. Entornos de prueba/validación . . . 34
5. DISPOSICIONES SOBRE CONFIDENCIALIDAD E INTEGRIDAD . . . 34
5.1. Infraestructura para las pruebas de seguridad . . . 34
5.2. Disposiciones relativas a la suspensión y la reactivación del enlace . . . 35

5.3. Disposiciones relativas a las vulneraciones de la seguridad 35
5.4. Directrices para las pruebas de seguridad 35
5.4.1. Programas informáticos 35
5.4.2. Infraestructuras 36
5.5. Disposiciones relativas a la evaluación del riesgo 36

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 de cualquiera de las entidades.
CH	Confederación Suiza.
CHU	Tipo de derecho fijo, también denominado CHU2 (referido al segundo período de compromiso del Protocolo de Kioto), expedido por la CH.
CHUA	Derecho de emisión de Suiza en el sector de la aviación.
POC	Procedimientos operativos comunes. Procedimientos elaborados conjuntamente para hacer operativo 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	Criptografía que utiliza claves públicas y privadas para cifrar y descifrar datos.
Autoridad de certificación (AC)	Entidad que emite certificados digitales.
Clave criptográfica	Información que determina el resultado funcional de un algoritmo criptográfico.
Descodificación	Proceso inverso al 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 lectura de un fichero.
Cortafuegos	Dispositivos o programas informáticos para garantizar la seguridad de la red, que supervisan y controlan el tráfico 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 y permite la sincronización con otras partes de un sistema de proceso de datos.
IPSec	IP SECurity. Serie de protocolos de red que autentican 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 vulnerabilidades 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 procedentes de diferentes aplicaciones y 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, «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, se establecerá, 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 fuera operativo, se aplicó una solución provisional en 2020. A partir de 2023, el enlace entre los registros de los dos sistemas de comercio de derechos de emisión se irá transformando gradualmente en un enlace permanente entre los registros, cuya aplicación está prevista a más tardar en 2024, para permitir el funcionamiento de los mercados vinculados con respecto a los beneficios de la liquidez del mercado y la ejecución de las transacciones entre los dos sistemas vinculados, de manera equivalente a un único mercado compuesto por dos sistemas y que permita a los participantes en el mercado actuar como si estuvieran en un único mercado, sujeto únicamente a las disposiciones reglamentarias individuales de las Partes (anexo II del Acuerdo).

De conformidad con el artículo 3, apartado 7, del Acuerdo, el administrador del Registro suizo y el administrador central de la Unión elaborarán normas técnicas de enlace (NTE), sobre la base de los principios dispuestos en el anexo II del Acuerdo, en las que se describirán 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.

Las NTE fueron adoptadas por el Comité Mixto mediante la Decisión n.º 2/2020. El Comité Mixto aprobará las NTE actualizadas, tal como figuran en el presente documento, mediante la Decisión n.º 1/2024. De conformidad con la presente Decisión y con las solicitudes del Comité Mixto, el administrador del Registro suizo y el administrador central del Registro de la Unión han elaborado, y actualizarán, directrices técnicas adicionales para hacer operativo el enlace y garantizar que estas se vayan adaptando constantemente al progreso técnico y a los nuevos requisitos relativos a la seguridad y la 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 hacer operativo el enlace.

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 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 al administrador central 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 los registros, se han adoptado todas las medidas necesarias para disponer de una arquitectura sólida. El enlace permanente entre los registros utiliza un mecanismo de intercambio de archivos securizado mediante un entorno *Air Gap*.

La solución técnica es la siguiente:

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

— mensajes XML,

— firma digital y cifrado XML,

— VPN.

3.1.1. Intercambio de mensajes

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

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

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

Los errores y contingencias se tratan 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 o 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

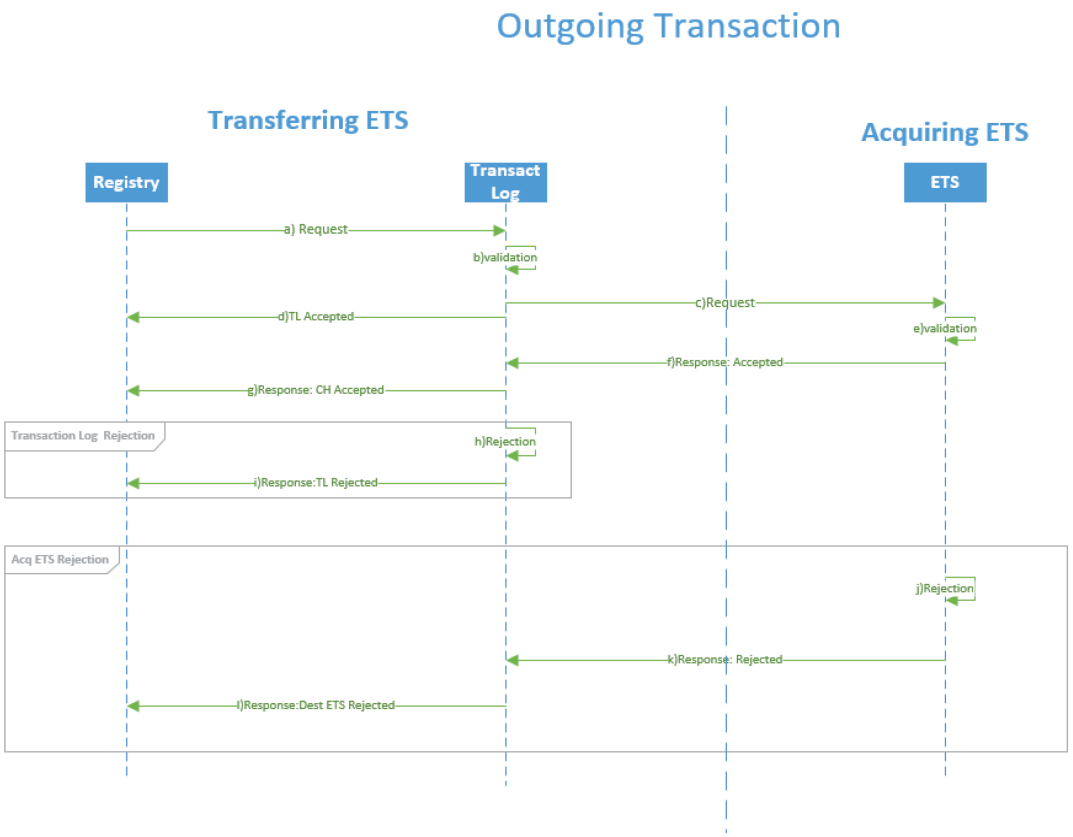
El enlace permanente entre los registros se basa en períodos de ingesta predefinidos, seguidos de un conjunto de eventos designados. Las solicitudes de transacción recibidas a través del enlace solo se ingerirán a intervalos predefinidos. Los períodos de ingesta incluyen una validación técnica para las 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 dichos eventos se tratarán siguiendo los procedimientos operativos establecidos en el proceso de ejecución de las solicitudes de los POC.

3.1.4. Flujo de mensajes de transacción

Transacciones salientes

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



El flujo principal muestra las etapas siguientes (como 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» [como se muestra en el diagrama anterior, a partir de la letra a) en el flujo principal]:

a) en el sistema 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 no valida la solicitud,

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

Flujo alternativo en el caso de «denegación del RCDE» [como se muestra en el diagrama anterior, a partir de la letra d) en el flujo principal]:

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,

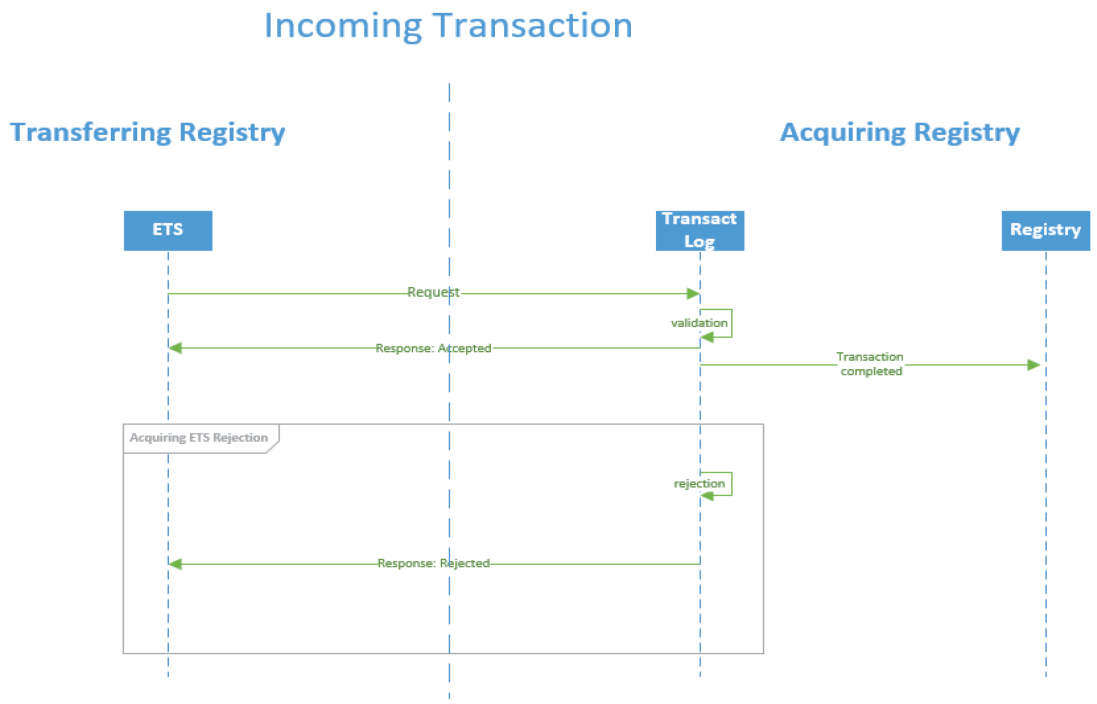
e) el diario de transacciones del RCDE que recibe los datos no valida la transacción,

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 respuesta de 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 cerrada» 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 los datos à RCDE que recibe los datos.

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

  — Aceptación: transacción completada.

  — Denegación: transacción cancelada.

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» (completada/cancelada) 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» (completada/cancelada) 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.

— Las transacciones del RCDE que recibe los datos adquirirán el estado «terminated» (cancelada) si cualquier transacción propuesta se mantiene 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»: VPN;

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 red privada virtual (VPN). Las tecnologías VPN permiten crear un «túnel» de un punto a otro a través de una red (como internet), protegiendo todas las comunicaciones. Antes de la creación del túnel VPN, se expide un certificado digital a un cliente potencial, lo que le permite probar su 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.

En general, la Unión Europea utiliza s-TESTA (Servicios transeuropeos seguros de telemática entre administraciones) como una red privada basada en IP. Por lo tanto, esta red también es adecuada para el enlace permanente entre los registros.

3.2.3. Aplicación de IPsec

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 un certificado digital facilitad 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

El enlace permanente entre los registros 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. A nivel de aplicación, los ficheros se transfieren utilizando un protocolo seguro de transferencia para el intercambio de mensajes a nivel de sesión.

3.2.5. Firma y cifrado XML

En los ficheros XML, la firma y el cifrado ocurren en 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 aceptación 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, se sigue el mismo proceso 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 del 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,

    — 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 deban anularse 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 deba anularse en su totalidad, y solo los derechos asignados en exceso deban 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 cualquier horario. Puede programarse diariamente una conciliación si así lo acuerdan ambas Partes. Como mínimo, una vez realizada cada ingesta, se efectuará al menos una conciliación programada.

En cualquier caso, cada una de las Partes podrá efectuar conciliaciones manuales en cualquier momento.

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 POC.

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. 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 dichos registros se conservarán al menos durante tres 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 meses de antigüedad podrán 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.

Diarios de transacciones

Los subsistemas DTUE y DTSS ejecutan los diarios de transacciones.

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 el enlace permanente entre los registros, los mensajes de conciliación forman parte integrante de los mensajes intercambiados y, por tanto, se almacenan como se describe en la sección «Archivo de mensajes».

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 (ficheros XML), enviados y recibidos, así como la indicación de si los mensajes o ficheros 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.

3.5. Requisitos operativos

El intercambio de datos entre los dos sistemas no es totalmente autónomo en el enlace permanente entre los registros, lo que significa que se requieren operadores y procedimientos para hacer operativo el enlace. A tal fin, en este proceso se detallan varias funciones y herramientas.

4. DISPOSICIONES SOBRE DISPONIBILIDAD

4.1. Diseño que garantice la disponibilidad de las comunicaciones

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

Resiliencia de la infraestructura de TIC

En el capítulo de disposiciones generales del presente documento se detallan los elementos básicos de la arquitectura del enlace. En lo que respecta a la infraestructura de TIC, el enlace permanente entre los registros establece una red VPN resiliente que crea túneles de comunicación seguros que permiten un intercambio seguro de mensajes. Los demás elementos de la infraestructura están configurados para garantizar un elevado nivel de 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, durante un determinado período de tiempo, restablecer la comunicación con el otro extremo si, por alguna razón, este no está disponible.

Resiliencia de los servicios

En el enlace permanente entre los registros, los intercambios de datos entre las Partes se producen a intervalos predefinidos. 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 definirán intervalos de tiempo importantes para cada etapa,

— los módulos de programas informáticos del enlace permanente entre los registros 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 la 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 del enlace permanente entre los registros 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. Tales pruebas operativas constituyen una condición previa imperativa siempre que el enlace permanente entre los registros deba pasar del estado «suspended» («suspendido») al estado «operational» («operativo») en la plataforma.

La activación del estado operativo del enlace exige pues la ejecución satisfactoria de un plan de prueba predefinido. Esto confirmará que cada registro ha realizado un conjunto de pruebas internas primero, seguidas de la validación de la conectividad de extremo a extremo, antes de comenzar el envío de transacciones reales 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 previstos (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

Estas pruebas están concebidas para su realización o verificación individual por parte de los administradores del registro 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 estas pruebas, debiendo 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 y que se dispone de conectividad IP entre emplazamientos. Deben 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 los administradores del registro 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 permanente entre los registros después de que las cuatro fases o bloques hayan dado lugar a resultados previsibles.

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 sus sistemas respectivos 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 o de los programas informáticos. 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 del enlace permanente entre los registros implementarán la supervisión de la comunicación del sistema a nivel de aplicación (manualmente o a intervalos regulares), lo que permitirá probar la disponibilidad de extremo a extremo de la vinculación simulando algunas de las transacciones previstas.

4.3. Entornos de prueba/validación

La arquitectura del Registro de la Unión y del Registro suizo consiste en 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, 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.

En cuanto a la configuración VPN, la comunicación entre los tres entornos debe ser totalmente independiente, lo que se garantiza mediante el uso de s-TESTA.

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 se aplicará siempre que se considere necesario. No obstante, puede no ser de aplicación a todas las acciones emprendidas por los administradores de los registros.

Los requisitos de seguridad se contemplan y abordan en el plan de gestión de la seguridad, que también incluye los procesos relacionados con el tratamiento de los incidentes de seguridad tras una posible vulneración de la 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 separarse de la infraestructura de producción, tanto a nivel de red como de infraestructura. Es en la infraestructura de pruebas en donde se realizan las pruebas de seguridad necesarias para verificar el cumplimiento de los requisitos de seguridad.

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

Si se sospecha que la seguridad del Registro de Suiza, del DTSS, del Registro de la Unión o del 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 POC.

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 a 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 el enlace entre los registros 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, «Inicialización, comunicación, reactivación y plan de pruebas».

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 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.

La información directamente relacionada con la vulneración de la seguridad se considerará sensible, llevará la indicación «TRATAMIENTO ESPECIAL: *RCDE Crítico*» y se tratará de conformidad con las instrucciones de tratamiento, salvo que se especifique lo contrario.

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 para 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 del sistema vigente en la que se tenga 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 las aplicaciones web respetarán las normas abiertas internacionales, como las establecidas por el Proyecto de seguridad de aplicaciones web abiertas (OWASP).

5.4.2. Infraestructuras

Las infraestructuras que respalden el sistema de producción deberán verificarse con regularidad para detectar vulnerabilidades (al menos una vez al mes), y las vulnerabilidades detectadas deberán solucionarse sobre la base del mismo principio definido en la sección anterior, utilizando una base de datos actualizada de vulnerabilidades.

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 las pruebas de seguridad, siempre que dicha empresa:

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

— no rinda cuentas directamente ante el desarrollador responsable o la parte contratante 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 de la forma correspondiente al nivel «TRATAMIENTO ESPECIAL: RCDE *Crítico*», de acuerdo con las instrucciones de tratamiento.