COMISIÓN
EUROPEA

Bruselas, 23.6.2020
COM(2020) 255 final

ANNEX

ANEXO

de la

Propuesta de Decisión del Consejo

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 adopción de procedimientos operativos comunes

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 …
sobre los procedimientos operativos comunes (POC)

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, el «Acuerdo»), y en particular su artículo 3,

Considerando lo siguiente:

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

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

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

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

(5) De conformidad con el artículo 13, apartado 1, del Acuerdo, el Comité Mixto podrá aprobar directrices técnicas para garantizar la correcta aplicación del Acuerdo, incluidas las cuestiones técnicas o de otra índole necesarias para el funcionamiento de la vinculación, teniendo en cuenta las prioridades de la legislación nacional. La elaboración de las directrices técnicas puede encomendarse a un grupo de trabajo constituido de conformidad con el artículo 12, apartado 5, del Acuerdo. El grupo de trabajo debe como mínimo incluir entre sus miembros al administrador del Registro suizo y al administrador central del Registro de la Unión, y debe además asistir al Comité Mixto en las funciones que le asigna el artículo 13 del Acuerdo.

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

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

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Se adoptan los procedimientos operativos comunes (POC) que figuran en el anexo de la presente Decisión.

Artículo 2

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

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

Artículo 3

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

Hecho en inglés en Bruselas, el XX de 2020.

Por el Comité Mixto

Secretario por la Unión Europea *El Presidente* *Secretario por Suiza*

APÉNDICE

ANEXO

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 la Solución Provisional -

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
Activo 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
SS	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, «el Acuerdo»), prevé el reconocimiento mutuo de los derechos de emisión que pueden utilizarse para el cumplimiento del régimen de comercio de derechos de emisión de la Unión Europea («RCDE UE») o del régimen de comercio de derechos de emisión de Suiza («RCDE de Suiza»). A fin de 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). A fin de hacer operativo el enlace entre el RCDE UE y el RCDE de Suiza, se aplicará una solución provisional en mayo de 2020 o lo antes posible a partir de esa fecha. Las Partes cooperarán con el objeto de sustituir el enlace provisional entre los registros por uno permanente lo antes posible (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 de la vinculación, 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.

El Comité Mixto aprobará los POC, tal como figuran en el presente documento, mediante la Decisión n.º 1/2020. De conformidad con la presente Decisión, el Comité Mixto solicitará al administrador del Registro suizo y al administrador central de la Unión que elaboren nuevas directrices técnicas para hacer operativo el enlace y garanticen que estas se irán 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. Alcance

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 poner en marcha el enlace.

Para el 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 el 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 la solución provisional acordada, 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

Con el despliegue del enlace permanente entre los registros en una fecha posterior, los POC deberán adaptarse y completarse cuando sea necesario.

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 3). Las prácticas extraídas de esta norma se reutilizan y adaptan a las exigencias específicas relacionadas con la solución provisional.
- 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 del Registro 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 sucesivos de intervención	**UE**	**CH**
1.er nivel	Servicio de asistencia de la UE	Servicio de asistencia de la CH
2.º nivel	Gestor de operaciones de la UE	Gestor de la aplicación de Registro de la CH
3.er nivel	Comité Mixto (que puede delegar esta responsabilidad con arreglo al artículo 12, apartado 5, del Acuerdo)	
4.º nivel	mité 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 de la gestión de incidentes es recuperar lo antes posible un nivel de servicio normal de los servicios informáticos 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 de tiques común 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, 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 confidenciales, 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 punto, 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. Encontrar una solución a un incidente implica que se ha identificado 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 quien confirma, de acuerdo con el servicio que 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 LOS 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 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, preferiblemente a través de soluciones provisionales. Cuando surge 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 activarse como consecuencia de un incidente o abrirse por iniciativa propia con vistas a resolver los fallos detectados en el sistema, en cualquiera de sus fases.

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

Cada Parte puede comunicar un problema y 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.

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, prehomologadas y de procedimiento.

Se recogen a continuación los principales pasos a seguir:

6.1. Introducción de la solicitud

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. Solicitud de registro y análisis

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. Solicitud de aprobación

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:

- El cumplimiento de la solicitud de servicio solo afecta a una Parte. En este caso, esta Parte emite las órdenes de ejecución y coordina la ejecución.
- El cumplimiento de la solicitud de servicio afecta tanto a la UE como a la CH. En este caso, los servicios de asistencia expiden las órdenes de ejecución en los ámbitos de su competencia. 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, su estatus debe ser «resuelta».

6.5. Solicitud de transferencia

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, es decir, 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. Solicitud de cierre

Si las Partes asignadas coinciden en que la solicitud de servicio se ha cumplido y el solicitante considera resuelto el caso, el siguiente estado que deberá asignarse será el de «Cerrado».

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 y el impacto de cualquier incidente relacionado 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, para conseguir una mayor eficiencia y eficacia, o para permitir o reflejar iniciativas del servicio.

El proceso de gestión de cambios incluye diferentes medidas que registran todos los detalles sobre una petición 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 que da lugar a un cambio;
- un usuario final que solicita un nuevo cambio;
- un cambio resultante de un mantenimiento en curso;
- novedades legislativas

7.2. Evaluación y planificación de cambios

Esta fase se ocupa de 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 de la 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 aplicación. 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 cada vez que 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 única puede representar 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 los interesados 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 arreglos de fallos y de mejoras de 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 las versiones. 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/usuarios afectados por la versión;
- el equipo responsable de la versión;
- la estrategia y el 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 para ejecutar la versión o el paquete de versiones y mantener los entornos controlados antes de cambiar la producción, así como 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; 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.

Al final de estos subprocesos, todos los componentes de versión requeridos están 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 y 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 aplicación;
- 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 versión inmediata

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);
- revisar 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 existan 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 consistente en: la gestión de dichos incidentes a fin de poder comunicarlos 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 confidenciales.

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 violación de la confidencialidad, la integridad o la

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. Gestión 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 las posibles deficiencias detectadas;
- en función de la gravedad del incidente, transferirlo a un nivel adecuado de información o 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 menor que el RCDE SENSIBLE espacio.

Para una investigación en curso o una deficiencia que pueda ser aprovechada y hasta su resolución, la información se clasifica como CRÍTICA RCDE.

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 en el uso de los recursos de estas acciones.

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 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 las informaciones y datos clasificados y de los servicios informáticos confidenciales 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 de la solución provisional.

10.1. Caracterización de la información confidencial

La confidencialidad de una información se evalúa determinando el nivel de impacto sobre la actividad (por ejemplo, pérdidas financieras, degradación de la imagen, infracción de la ley, etc.) de una violación de la seguridad relacionada con esta información.

Los recursos de información confidencial 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

Tras su identificación, 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 «CRÍTICO RCDE»;

- 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 como «LIMITADO RCDE».

10.3. Cesión de 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 el nivel de responsabilidad adecuado con respecto al valor del recurso o recursos asignados. La responsabilidad del titular con respecto al recurso o recursos y la obligación de mantener el grado de confidencialidad, integridad y disponibilidad requeridos deberían ser objeto de acuerdo y formalización.

10.4. Registro de información confidencial

Toda la información confidencial 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 confidencial que pueda tener un impacto mayor que el impacto de una información única (por ejemplo, información almacenada 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 y 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 confidencial se registrará inmediatamente en la LIS.

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

- Descripción de la información
- Titular de la información
- Grado de confidencialidad
- Indicación de si la información incluye datos personales
- Información adicional, en su caso

10.5. Tratamiento de la información confidencial

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

La información confidencial 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 la solución provisional y su funcionamiento, ambas Partes deben tener acceso a los siguientes componentes:

- el wiki: un entorno de colaboración para el intercambio de información común, como la planificación de la versión;
- la herramienta de gestión de servicios TI (GSTI) para la gestión de incidentes y problemas (véase el capítulo «Enfoque y normas»);
- el sistema de intercambio de mensajes: cada Parte proporcionará un sistema seguro de transferencia de mensajes para la transmisión 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. La manipulación 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.