COMISIA
EUROPEANĂ

Bruxelles, 23.6.2020
COM(2020) 255 final

ANNEX

ANEXĂ

la

Propunerea de Decizie a Consiliului

privind poziția care urmează să fie adoptată în numele Uniunii Europene în cadrul comitetului mixt instituit prin Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră, în ceea ce privește adoptarea unor procedee comune de funcționare

DECIZIA NR. 1/2020 A COMITETULUI MIXT INSTITUIT PRIN ACORDUL DINTRE UNIUNEA EUROPEANĂ ŞI CONFEDERAŢIA ELVEŢIANĂ PENTRU CREAREA UNEI LEGĂTURI ÎNTRE RESPECTIVELE LOR SCHEME DE COMERCIALIZARE A CERTIFICATELOR DE EMISII DE GAZE CU EFECT DE SERĂ

din …

în ceea ce privește adoptarea unor procedee comune de funcționare

COMITETUL MIXT

având în vedere Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră[1] (denumit în continuare „acordul”), în special articolul 3,

întrucât:

(1) Decizia nr. 2/2019 a comitetului mixt din 5 decembrie 2019 a modificat anexele I și II la acord, îndeplinind astfel condițiile prevăzute în acord pentru crearea legăturii.

(2) După adoptarea Deciziei nr. 2/2019 a comitetului mixt și în temeiul articolului 21 alineatul (3) din acord, părțile au făcut schimb de instrumente de ratificare sau aprobare, deoarece consideră că au fost îndeplinite toate condițiile pentru crearea legăturii, astfel cum sunt prevăzute în acord.

(3) În conformitate cu articolul 21 alineatul (4) din acord, acordul a intrat în vigoare la 1 ianuarie 2020.

(4) În temeiul articolului 3 alineatul (6) din acord, administratorul registrului elvețian și administratorul central al Uniunii ar trebui să stabilească procedeele comune de funcționare pentru aspectele tehnice sau alte aspecte care sunt necesare pentru funcționarea legăturii dintre Registrul de tranzacții al Uniunii Europene (EUTL) din cadrul registrului Uniunii și Registrul suplimentar de tranzacții al Elveției (SSTL) din cadrul registrului elvețian, ținând cont de prioritățile din legislația națională. Procedeele comune de funcționare ar trebui să producă efecte după ce vor fi adoptate prin decizia comitetului mixt.

(5) În conformitate cu articolul 13 alineatul (1) din acord, comitetul mixt ar trebui să convină asupra unor orientări tehnice pentru a asigura punerea în aplicare corespunzătoare a acordului, inclusiv asupra aspectelor tehnice sau a altor aspecte care sunt necesare pentru funcționarea legăturii, ținând cont de prioritățile din legislația națională. Orientările tehnice pot fi elaborate de un grup de lucru instituit în temeiul articolului 12 alineatul (5) din acord. Grupul de lucru ar trebui să-i aibă în componența sa cel puțin pe administratorul registrului elvețian și pe administratorul central al registrului Uniunii și ar trebui să sprijine comitetul mixt în exercitarea funcțiilor sale prevăzute la articolul 13 din acord.

(6) Având în vedere caracterul tehnic al orientărilor și necesitatea adaptării acestora la evoluțiile actuale, orientările tehnice elaborate de administratorul registrului elvețian și de administratorul central al Uniunii ar trebui să fie transmise comitetului mixt pentru informare sau, după caz, pentru aprobare,

[1] JO L 322, 7.12.2017, p. 3.

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Se adoptă procedeele comune de funcționare, astfel cum sunt anexate la prezenta decizie.

Articolul 2

Se instituie un grup de lucru în temeiul articolului 12 alineatul (5) din acord. Acesta sprijină comitetul mixt pentru asigurarea punerii în aplicare corespunzătoare a acordului, inclusiv la elaborarea orientărilor tehnice pentru punerea în aplicare a procedeelor comune de funcționare.

Grupul de lucru îi are în componența sa cel puțin pe administratorul registrului elvețian și pe administratorul central al registrului Uniunii.

Articolul 3

Prezenta decizie intră în vigoare la data adoptării sale.

Redactată în limba engleză la Bruxelles, la XX 2020.

Pentru comitetul mixt

Secretarul pentru Uniunea Europeană	*Președintele*	*Secretarul pentru Elveția*

APENDICE

ANEXĂ

PROCEDEELE COMUNE DE FUNCȚIONARE

în temeiul articolului 3 alineatul (6) din Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră

- Procedee pentru o soluție provizorie -

1. GLOSAR

Tabelul 1-1 Acronime și definiții

Acronim/termen	Definiție
Autoritate de certificare (CA)	Entitatea care emite certificate digitale
CH	Confederația Elvețiană
ETS	Sistemul de comercializare a certificatelor de emisii
UE	Uniunea Europeană
IMT	Echipa de gestionare a incidentelor
Activ informațional	O informație care prezintă valoare pentru o societate sau o organizație
IT	Tehnologia informației
ITIL	Bibliotecă pentru infrastructura tehnologiei informației
ITSM	Gestionarea serviciilor IT
LTS	Standarde tehnice de creare a legăturii
Registru	Un sistem de contabilizare a certificatelor emise în cadrul ETS, care ține evidența drepturilor de proprietate asupra certificatelor deținute în conturile electronice.
RFC	Cererea de modificare
SIL	Evidența informațiilor sensibile
SR	Cerere de servicii
Wiki	Site web care permite utilizatorilor să facă schimb de informații și de cunoștințe prin adăugarea sau adaptarea conținutului în mod direct prin intermediul unui browser web.

2. INTRODUCERE

Acordul dintre Uniunea Europeană și Confederația Elvețiană pentru crearea unei legături între respectivele lor scheme de comercializare a certificatelor de emisii de gaze cu efect de seră din 23 noiembrie 2017 (denumit în continuare „acordul”) prevede recunoașterea reciprocă a certificatelor de emisii care pot fi utilizate pentru asigurarea conformității în cadrul sistemului de comercializare a certificatelor de emisii (denumit în continuare „EU ETS”) sau în cadrul sistemului Elveției de comercializare a certificatelor de emisii (denumit în continuare „ETS-ul Elveției). În vederea activării legăturii dintre EU ETS și ETS-ul Elveției, se creează o legătură directă între Registrul de tranzacții al Uniunii Europene (EUTL) din cadrul registrului Uniunii și Registrul suplimentar de tranzacții al Elveției (SSTL) din cadrul registrului elvețian, ceea ce va permite transferul dintr-un registru în altul al certificatelor de emisii emise în cadrul oricăruia dintre ETS-uri [articolul 3 alineatul (2) din acord]. Pentru activarea legăturii dintre EU ETS și ETS-ul Elveției, este instituită o soluție provizorie până în mai 2020 sau cât mai curând posibil după această dată. Părțile cooperează pentru a înlocui în cel mai scurt timp posibil soluția provizorie cu o legătură permanentă între registre (anexa II la acord).

În temeiul articolului 3 alineatul (6) din acord, administratorul registrului elvețian și administratorul central al Uniunii stabilesc procedeele comune de funcționare pentru aspectele tehnice sau alte aspecte care sunt necesare pentru funcționarea legăturii, ținând cont de prioritățile din legislația națională. Procedeele comune de funcționare elaborate de administratori produc efecte după ce sunt adoptate prin decizia comitetului mixt.

Procedeele comune de funcționare, astfel cum sunt specificate în prezentul document, urmează să fie adoptate prin Decizia nr. 1/2020 a comitetului mixt. În conformitate cu prezenta decizie, comitetul mixt solicită administratorului registrului elvețian și administratorului central al Uniunii să elaboreze orientări tehnice suplimentare pentru activarea legăturii și să se asigure că acestea sunt adaptate permanent la progresul tehnic și la noile cerințe privind siguranța și securitatea legăturii și funcționarea efectivă și eficientă a acesteia.

2.1. Domeniul de aplicare

Prezentul document reprezintă înțelegerea comună între părțile la acord cu privire la stabilirea fundamentelor procedurale ale legăturii dintre registrele EU ETS și ETS-ul Elveției. Acesta prezintă cerințele procedurale generale în ceea ce privește operațiunile, însă vor fi necesare unele orientări tehnice suplimentare pentru activarea legăturii.

Pentru funcționarea corespunzătoare, legătura va necesita specificații tehnice pentru operaționalizarea în continuare a acesteia. În temeiul articolului 3 alineatul (7) din acord, aceste aspecte sunt prezentate în detaliu în documentul privind standardele tehnice de creare a legăturii (LTS), care urmează să fie adoptat separat prin decizia comitetului mixt.

Obiectivul procedeelor comune de funcționare este de a asigura prestarea efectivă și eficientă a serviciilor IT asociate cu funcționarea legăturii dintre registrele EU ETS și ETS al Elveției, în special în ceea ce privește soluționarea cererilor de servicii, rezolvarea cazurilor de prestare necorespunzătoare a serviciilor, remedierea problemelor, precum și îndeplinirea sarcinilor operaționale de rutină în conformitate cu standardele internaționale privind gestionarea serviciilor IT.

Pentru soluția provizorie convenită, vor fi necesare doar următoarele procedee comune de funcționare, incluse în prezentul document:

- Gestionarea incidentelor

- Gestionarea problemelor
- Soluționarea cererilor
- Gestionarea modificărilor
- Gestionarea versiunilor
- Gestionarea incidentelor de securitate
- Managementul securității informațiilor

După implementarea legăturii permanente între registre la o dată ulterioară, procedeele comune de funcționare trebuie adaptate și completate, dacă este necesar.

2.2. Destinatari

Beneficiarii vizați ai prezentelor procedee comune de funcționare sunt echipele de asistență ale registrelor din UE și Elveția.

3. ABORDARE ȘI STANDARDE

Următorul principiu se aplică tuturor procedeelor comune de funcționare:

- UE și CH convin asupra definirii procedeelor comune de funcționare pe baza ITIL (Biblioteca pentru infrastructura tehnologiei informației, versiunea 3). Practicile specificate în acest standard sunt reutilizate și adaptate necesităților specifice legate de soluția provizorie.
- Comunicarea și coordonarea necesare pentru prelucrarea procedeelor comune de funcționare dintre cele două părți se realizează prin intermediul serviciilor de asistență ale registrelor din CH și UE. Sarcinile sunt întotdeauna atribuite în cadrul uneia dintre părți.
- În cazul unui dezacord cu privire la gestionarea unui procedeu comun de funcționare, acesta va fi analizat și soluționat între cele două servicii de asistență. În cazul în care nu se poate ajunge la niciun acord, găsirea unei soluții comune este transmisă la nivelul următor.

Niveluri de transmitere	**UE**	**CH**
Nivelul 1	Serviciul de asistență EU	Serviciul de asistență CH
Nivelul 2	Managerul pentru operațiuni al UE	Managerul pentru aplicații din cadrul registrului CH
Nivelul 3	Comitetul mixt [care poate delega această responsabilitate în temeiul articolului 12 alineatul (5) din acord]	
Nivelul 4	Comitetul mixt, în cazul delegării responsabilității de la nivelul 3	

- Fiecare parte poate stabili procedeele de funcționare pentru propriul sistem de registre, ținând cont de cerințele și interfețele asociate cu prezentele procedee comune de funcționare.

- Se utilizează un instrument de gestionare a serviciilor IT (ITSM) în vederea furnizării de asistență în ceea ce privește procedeele comune de funcționare, în special gestionarea incidentelor, gestionarea problemelor și soluționarea cererilor, precum și comunicarea între cele două părți.
- În plus, este permis schimbul de informații prin e-mail.
- Ambele părți se asigură că sunt respectate cerințele privind securitatea informațiilor, în conformitate cu Instrucțiunile de gestionare.

4. GESTIONAREA INCIDENTELOR

Obiectivul procesului de gestionare a incidentelor este de a readuce serviciile IT la un nivel normal cât mai repede posibil și cu o perturbare minimă a activității.

În cadrul procesului de gestionare a incidentelor ar trebui, de asemenea, să se țină o evidență a incidentelor în scopul raportării, care să fie integrată în alte procese pentru favorizarea unei îmbunătățiri continue.

- În general, procesul de gestionare a incidentelor cuprinde următoarele activități:
- Identificarea și înregistrarea incidentelor
- Clasificare și asistență inițială
- Investigare și diagnosticare
- Rezolvare și restabilirea sistemului
- Închiderea incidentelor

Pe parcursul ciclului de viață al unui incident, procesul de gestionare a incidentelor este responsabil pentru gestionarea permanentă a drepturilor de proprietate, pentru monitorizare, urmărire și comunicare.

4.1. Identificarea și înregistrarea incidentelor

Un incident poate fi identificat de un grup de asistență, prin intermediul unor instrumente de monitorizare automatizate sau de către personalul tehnic care asigură supravegherea de rutină.

Odată identificat, un incident trebuie înregistrat, fiindu-i atribuit un identificator unic care permite urmărirea și monitorizarea corespunzătoare a acestuia. Identificatorul unic al unui incident este identificatorul atribuit în sistemul comun de tichete de către serviciul de asistență al părții (fie UE, fie CH) care a semnalat incidentul și trebuie utilizat în toate comunicările referitoare la respectivul incident.

Pentru toate incidentele, punctul de contact ar trebui să fie serviciul de asistență al părții care a introdus tichetul.

4.2. Clasificare și asistență inițială

Clasificarea incidentelor are ca scop înțelegerea și identificarea sistemului și/sau a serviciului afectat și a măsurii în care este afectat acesta. Pentru a fi eficientă, clasificarea ar trebui să direcționeze de prima dată soluționarea incidentului către resursa corectă, pentru a accelera rezolvarea acestuia.

Faza de clasificare ar trebui să includă clasificarea și ierarhizarea incidentului în funcție de impactul și de nivelul de urgență al acestuia, pentru a fi tratat în intervalul de timp stabilit în funcție de priorități.

Dacă incidentul are un potențial impact asupra confidențialității sau integrității datelor sensibile și/sau are un impact asupra disponibilității sistemului, este, de asemenea, declarat drept incident de securitate și, ulterior, va fi gestionat conform procesului definit în capitolul „Gestionarea incidentelor de securitate” din prezentul document.

Dacă este posibil, serviciul de asistență care a introdus tichetul efectuează o diagnosticare inițială. În acest scop, serviciul de asistență va analiza dacă incidentul reprezintă o eroare cunoscută. În caz afirmativ, calea de rezolvare sau soluția de evitare este deja cunoscută și documentată.

Dacă serviciul de asistență reușește să rezolve incidentul, atunci va închide efectiv incidentul în această fază, întrucât scopul principal al procesului de gestionare a incidentelor a fost atins (și anume restaurarea rapidă a serviciului pentru utilizatorul final). În caz contrar, serviciul de asistență va transmite incidentul grupului de rezolvare corespunzător pentru o investigare și o diagnosticare suplimentare.

4.3. Investigare și diagnosticare

Procesul de investigare și diagnosticare a incidentelor se aplică atunci când un incident nu poate fi rezolvat de către serviciul de asistență în cadrul diagnosticării inițiale și, prin urmare, este transmis în mod corespunzător. Transmiterea incidentelor constituie o parte integrantă din procesul de investigare și diagnosticare.

O practică comună în faza de investigare și diagnosticare este încercarea de a recrea incidentul în condiții controlate. Atunci când se efectuează investigarea și diagnosticarea incidentului, este important să se înțeleagă ordinea corectă a evenimentelor care au cauzat incidentul.

Transmiterea reprezintă recunoașterea faptului că un incident nu poate fi rezolvat la nivelul curent de asistență și trebuie transmis unui grup de asistență de nivel superior sau celeilalte părți. Transmiterea poate urma două căi: orizontală (funcțională) sau verticală (ierarhică).

Serviciul de asistență care a înregistrat și a declanșat incidentul este responsabil pentru transmiterea acestuia către resursa corespunzătoare și pentru urmărirea stadiului general și atribuirea incidentului.

Partea căreia i s-a atribuit incidentul este responsabilă pentru asigurarea efectuării în timp util a acțiunilor solicitate și pentru furnizarea de feedbackuri propriului serviciu de asistență.

4.4. Rezolvare și restabilirea sistemului

Rezolvarea incidentului și restabilirea sistemului se efectuează după înțelegerea în totalitate a acestuia. Găsirea unei soluții de rezolvare a unui incident înseamnă că a fost identificată o modalitate de a remedia problema. Aplicarea soluției de rezolvare reprezintă faza de restabilire a sistemului.

După remedierea erorii serviciului de către resursele corespunzătoare, incidentul este redirecționat către serviciul de asistență competent care a semnalat incidentul și care confirmă, împreună cu inițiatorul incidentului, că eroarea a fost remediată și că incidentul poate fi închis. Elementele identificate în timpul procesării incidentului trebuie înregistrate pentru a fi utilizate ulterior.

Restabilirea sistemului poate fi efectuată de către personalul de asistență IT sau prin punerea la dispoziția utilizatorului final a unui set de instrucțiuni care trebuie urmate.

4.5. Închiderea incidentelor

Închiderea este ultima etapă a procesului de gestionare a incidentelor și se efectuează la scurt timp după rezolvarea acestora.

Printre activitățile din lista de verificare care trebuie desfășurate în faza de închidere, se evidențiază următoarele:

- verificarea clasificării inițiale care a fost atribuită incidentului;
- colectarea corespunzătoare a tuturor informațiilor referitoare la incident;
- documentarea corespunzătoare a incidentului și actualizarea bazei de informații;
- informarea corespunzătoare a fiecărei părți interesate afectate în mod direct sau indirect de incident.

Un incident este închis în mod oficial după executarea fazei de închidere a incidentului de către serviciul de asistență și după informarea în acest sens a celeilalte părți.

Odată închis un incident, acesta nu mai este redeschis. Dacă un incident reapare într-un interval scurt de timp, incidentul inițial nu este redeschis, ci trebuie înregistrat un nou incident.

Dacă incidentul este urmărit atât de serviciul de asistență al UE, cât și de cel al CH, responsabilitatea închiderii finale a acestuia îi revine serviciului de asistență care a introdus tichetul.

5. GESTIONAREA PROBLEMELOR

Această procedură ar trebui respectată ori de câte ori este identificată o problemă și se declanșează procesul de gestionare a problemelor. Procesul de gestionare a problemelor se axează pe îmbunătățirea calității și pe reducerea volumului de incidente semnalate. O problemă poate fi cauza unuia sau a mai multor incidente. Atunci când este raportat un incident, obiectivul procesului de gestionare a incidentelor este de a restabili serviciul cât mai repede posibil, implicând, eventual, soluții de evitare. Atunci când se creează o problemă, obiectivul este de a investiga cauza principală a problemei pentru a identifica o modificare care să garanteze faptul că problema și incidentele conexe nu vor mai apărea.

5.1. Identificarea și înregistrarea problemelor

În funcție de partea care a introdus tichetul, fie serviciul de asistență al UE, fie cel al CH va fi punctul de contact pentru aspectele legate de probleme.

Identificatorul unic al unei probleme reprezintă identificatorul atribuit de echipa de gestionare a serviciilor IT (ITSM). Acesta trebuie utilizat în toate comunicările referitoare la respectiva problemă.

O problemă poate fi declanșată de un incident sau poate fi deschisă din proprie inițiativă pentru a remedia problemele descoperite în cadrul sistemului în orice fază.

5.2. Ierarhizarea problemelor

Problemele pot fi clasificate în funcție de gravitatea și prioritatea acestora, în același mod ca incidentele, pentru a facilita urmărirea acestora, luând în considerare impactul incidentelor asociate și frecvența de apariție a acestora.

5.3. Investigarea și diagnosticarea problemelor

Fiecare parte poate semnala o problemă, iar serviciul de asistență al părții inițiatoare va fi responsabil pentru înregistrarea problemei, pentru atribuirea soluționării acesteia resursei corespunzătoare și pentru monitorizarea stadiului general.

Grupul de rezolvare căruia i-a fost transmisă problema este responsabil pentru gestionarea în timp util a acesteia și pentru comunicarea cu serviciul de asistență.

La cerere, ambele părți sunt responsabile pentru asigurarea executării acțiunilor atribuite și pentru transmiterea de feedbackuri propriului serviciu de asistență.

5.4. Rezolvare

Grupul de rezolvare căruia i se atribuie problema este responsabil pentru soluționarea acesteia și pentru furnizarea de informații relevante propriului serviciu de asistență.

Elementele identificate în timpul procesării problemei trebuie înregistrate pentru a fi utilizate ulterior.

5.5. Închiderea problemei

O problemă este închisă oficial după soluționarea sa prin aplicarea modificării. Faza de închidere a problemei va fi executată de serviciul de asistență care a semnalat problema și a informat în acest sens serviciul de asistență al celeilalte părți.

6. SOLUȚIONAREA CERERILOR

Procesul de soluționare a cererilor reprezintă gestionarea integrală a unei cereri pentru un serviciu nou sau existent din momentul înregistrării și aprobării acesteia și până la închiderea sa. Cererile de servicii sunt de obicei solicitări minore, predefinite, repetabile, frecvente, aprobate în prealabil și procedurale.

Principalele etape care trebuie parcurse sunt menționate în continuare:

6.1. Inițierea cererii

Informațiile cu privire la o cerere de servicii sunt transmise către serviciul de asistență al UE sau al CH prin e-mail, telefon sau prin instrumentul de gestionare a serviciilor IT (ITSM) sau prin orice alt canal de comunicare convenit.

6.2. Înregistrarea și analiza cererilor

Pentru toate cererile de servicii, punctul de contact ar trebui să fie serviciul de asistență al UE sau al CH, în funcție de partea care a transmis cererea de servicii. Respectivul serviciu de asistență va fi responsabil pentru înregistrarea și analizarea cererii de servicii cu diligența corespunzătoare.

6.3. Aprobarea cererilor

Agentul din cadrul serviciului de asistență al părții care a transmis cererea de servicii verifică dacă sunt necesare aprobări din partea celeilalte părți și, dacă este cazul, face demersurile necesare pentru obținerea acestora. Dacă cererea de servicii nu este aprobată, serviciul de asistență actualizează și închide tichetul.

6.4. Soluționarea cererilor

Această etapă se referă la gestionarea efectivă și eficientă a cererilor de servicii. Trebuie să se facă distincția între următoarele cazuri:

- Soluționarea cererii de servicii afectează doar una dintre părți. În acest caz, respectiva parte emite ordinele de lucru și coordonează executarea acestora.
- Punerea în aplicare a cererii de servicii afectează atât UE, cât și CH. În acest caz, serviciile de asistență emit ordine de lucru în sfera lor de responsabilitate. Derularea procesului de soluționare cererii de servicii este coordonată de ambele servicii. Responsabilitatea generală îi revine serviciului de asistență care a primit și a inițiat cererea de servicii.

Dacă cererea de servicii a fost soluționată, stadiul acesteia trebuie modificat în „Rezolvată”.

6.5. Transmiterea cererilor

Serviciul de asistență poate transmite cererea de servicii nesoluționată către resursa corespunzătoare (o terță parte), dacă este necesar.

Transmiterile sunt efectuate către părțile terțe corespunzătoare, și anume serviciul de asistență al UE va trebui să apeleze la serviciul de asistență al CH pentru transmiterea către o terță parte a CH și viceversa.

Terța parte către care a fost transmisă cererea de servicii este responsabilă pentru gestionarea în timp util a cererii și pentru comunicarea cu serviciul de asistență care a transmis cererea de servicii.

Serviciul de asistență care a înregistrat cererea de servicii este responsabil pentru monitorizarea stadiului general și atribuirea unei cereri de servicii.

6.6. Verificarea procesului de soluționare a cererii

Serviciul de asistență responsabil supune evidențele privind cererea de servicii unui control al calității final înainte de închidea acesteia. Scopul este de a se asigura că cererea de servicii este efectiv procesată și că toate informațiile necesare pentru descrierea ciclului de viață al cererii sunt suficient de detaliate. În plus, elementele identificate în timpul procesării cererii trebuie înregistrate pentru a fi utilizate ulterior.

6.7. Închiderea cererii

Dacă părțile desemnate sunt de acord cu faptul că cererea de servicii a fost soluționată și solicitantul consideră cazul rezolvat, stadiul cererii devine „Închisă”.

O cerere de servicii este oficial închisă după ce serviciul de asistență care a înregistrat cererea de servicii a executat faza de închidere a acesteia și a informat în acest sens serviciul de asistență al celeilalte părți.

7. GESTIONAREA MODIFICĂRILOR

Obiectivul acestui proces de a asigura faptul că sunt utilizate metode și proceduri standardizate pentru o gestionare eficientă și promptă a tuturor modificărilor legate de controlul infrastructurii IT, în scopul reducerii la minimum a numărului și a impactului oricăror incidente conexe asupra serviciului. Modificări ale infrastructurii IT pot apărea reactiv ca răspuns la probleme sau cerințe impuse din exterior, de exemplu, modificări legislative, sau, proactiv, rezultate din încercarea de a îmbunătăți eficiența și eficacitatea sau pentru a permite sau a reflecta inițiative de afaceri.

Procesul de gestionare a modificărilor include diferite etape care surprind fiecare detaliu cu privire la o cerere de modificare în vederea monitorizării ulterioare. Aceste procese asigură faptul că modificarea este validată și testată înainte de a fi implementată. Procesul de gestionare a versiunilor este responsabil pentru implementarea cu succes a acestora.

7.1. Cererea de modificare

O cerere de modificare (RFC) este prezentată echipei de gestionare a modificărilor, pentru validare și aprobare. Pentru toate cererile de modificare, punctul de contact ar trebui să fie serviciul de asistență al UE sau al CH, în funcție de partea care a transmis cererea. Respectivul serviciu de asistență va fi responsabil pentru înregistrarea și analizarea cererii cu diligența corespunzătoare.

Cererile de modificare pot fi determinate de:

- un incident care a cauzat o modificare;
- o problemă existentă care are ca rezultat o modificare;
- un utilizator final care solicită o nouă modificare;
- o modificare ca urmare a operațiunii de întreținere continuă;
- o modificare legislativă.

7.2. Evaluarea și planificarea modificărilor

Această etapă implică activitățile de evaluare și de planificare a modificărilor. Aceasta include activități de ierarhizare și de planificare pentru a reduce la minimum riscul și impactul.

Dacă punerea în aplicare a cererii de modificare afectează atât UE, cât și CH, partea care a înregistrat cererea de modificare verifică împreună cu cealaltă parte procesul de evaluare și de planificare a modificărilor.

7.3. Aprobările modificărilor

Orice cerere de modificare înregistrată trebuie să fie aprobată de nivelul de transmitere competent.

7.4. Punerea în aplicare a modificărilor

Etapa de aplicare a modificărilor se realizează în cadrul procesului de gestionare a versiunilor. Echipele de gestionare a versiunilor ale ambelor părți urmează propriile procese care implică planificarea și testarea. Revizuirea modificărilor se efectuează după finalizarea etapei de punere în aplicare a modificării. Pentru a asigura aplicarea modificărilor conform planului, procesul de gestionare a modificărilor este revizuit și actualizat în mod constant, dacă este necesar.

8. GESTIONAREA VERSIUNILOR

O versiune reprezintă una sau mai multe modificări ale unui serviciu IT, incluse într-un plan privind versiunile, care va trebui autorizat, pregătit, conceput, testat și implementat în ansamblu. O singură versiune poate reprezenta remedierea unor erori, o modificare a hardware-ului sau a altor componente, modificări ale software-ului, actualizări ale versiunilor de aplicații, modificări ale documentației și/sau ale unor procese. Conținutul fiecărei versiuni este gestionat, testat și implementat ca un tot unitar.

Procesul de gestionare a versiunilor vizează planificarea, conceperea, testarea și validarea, precum și asigurarea capacității de furnizare a serviciilor concepute, care să răspundă cerințelor părților interesate și să îndeplinească obiectivele propuse. Criteriile de acceptare pentru toate modificările aduse serviciului vor fi definite și documentate pe parcursul etapei de coordonare a procesului de concepere și vor fi furnizate echipelor de gestionare a versiunilor.

Versiunea va consta, în mod obișnuit, dintr-o serie de soluționări de probleme și de îmbunătățiri aduse unui serviciu. Aceasta conține software-ul nou sau modificat necesar și orice hardware nou sau modificat necesar pentru a pune în aplicare modificările aprobate.

8.1. Planificarea versiunii

Prima etapă a procesului include alocarea modificărilor autorizate pachetelor de versiuni și definirea domeniului de aplicare și a conținutului versiunilor. Pe baza acestor informații, în cadrul subprocesului de planificare a versiunilor se elaborează un calendar pentru conceperea, testarea și implementarea versiunii.

În cadrul planificării ar trebui definite următoarele:

- domeniul de aplicare și conținutul versiunii;
- evaluarea riscurilor și profilul de risc al versiunii;
- clienții/utilizatorii afectați de versiune;
- echipa responsabilă pentru versiune;
- strategia de furnizare și de implementare;
- resursele alocate pentru versiune și pentru implementarea acesteia.

Ambele părți se informează reciproc cu privire la perioadele de planificare și de întreținere a versiunii. Dacă o versiune afectează atât UE, cât și CH, acestea coordonează etapa de planificare și definesc o perioadă comună pentru întreținere.

8.2. Conceperea și testarea pachetului de versiuni

Etapa de concepere și de testare a procesului de gestionare a versiunilor stabilește abordarea privind executarea versiunii sau a pachetului de versiuni și menținerea mediilor controlate înainte de modificarea producției, precum și testarea tuturor modificărilor din toate mediile lansate.

Dacă o versiune afectează atât UE, cât și CH, acestea coordonează planurile de livrare și testele. Acestea includ următoarele aspecte:

- cum și când vor fi livrate versiunile și componentele serviciilor;
- care sunt timpii de livrare obișnuiți; ce se întâmplă în cazul unei întârzieri;
- modul de monitorizare a progresului livrării și de obținere a confirmării;
- indicatori pentru monitorizarea și stabilirea gradului de reușită a efortului de implementare a versiunii;
- cazurile comune de testare a funcționalităților și a modificărilor relevante.

La finalul acestui subproces, toate componentele necesare ale versiunii sunt pregătite pentru faza de implementare concretă.

8.3. Pregătirea implementării

Subprocesul de pregătire asigură faptul că planurile de comunicare sunt corect definite, că notificările pot fi trimise tuturor părților interesate și utilizatorilor finali afectați și că versiunea este integrată în procesul de gestionare a modificărilor pentru a asigura faptul că toate modificările sunt efectuate într-un mod controlat și sunt aprobate de forurile competente.

Dacă o versiune afectează atât UE, cât și CH, acestea coordonează următoarele activități:

- modificarea înregistrării cererii pentru programarea și pregătirea aplicării în mediul de producție;
- crearea unui plan de punere în aplicare;
- abordarea revenirii la starea anterioară, astfel încât, în cazul unei probleme legate de implementare, să se poată reveni la starea anterioară;
- transmiterea de notificări tuturor părților relevante;
- solicitarea aprobării pentru punerea în aplicare a versiunii de la nivelul de transmitere relevant.

8.4. Readucerea versiunii la starea anterioară

În cazul unei implementări nereușite sau în cazul în care, pe parcursul testării, s-a constatat că implementarea a fost nereușită sau nu a îndeplinit criteriile de acceptare/calitate convenite, echipele de gestionare a versiunii ale ambelor părți vor trebui să readucă versiunea la starea anterioară. Toate părțile interesate relevante vor trebui informate, inclusiv utilizatorii finali afectați/vizați. În așteptarea aprobării, procesul poate reporni în oricare dintre etapele anterioare.

8.5. Evaluarea și finalizarea versiunii

În evaluarea implementării unei versiuni ar trebui incluse următoarele activități:

- înregistrarea feedbackurilor privind gradul de satisfacție a clienților, a utilizatorilor și legat de prestarea serviciilor în ceea ce privește implementarea versiunii (colectarea feedbackurilor și luarea în considerare a acestora pentru îmbunătățirea continuă a serviciului);
- analizarea tuturor criteriilor de calitate care nu au fost îndeplinite;
- verificarea finalizării tuturor acțiunilor, corecțiilor și modificărilor necesare;
- asigurarea faptului că, la finalul implementării, nu există eventuale probleme legate de capabilități, resurse, capacitate sau performanță;
- verificarea documentării și acceptării de către client, utilizatorii finali, echipa de asistență operațională și de către alte părți afectate a problemelor, erorilor și soluțiilor de evitare cunoscute;
- monitorizarea incidentelor și a problemelor cauzate de implementare (asigurarea din timp a asistenței necesare echipelor operaționale în cazul în care versiunea a generat o creștere a volumului de lucru);
- actualizarea documentației de asistență (și anume, documentele cu informații tehnice);
- încredințarea în mod oficial a implementării versiunii echipelor operaționale din cadrul serviciilor;
- documentarea lecțiilor învățate;
- preluarea documentului de sinteză privind versiunea de la echipele de punere în aplicare;
- finalizarea oficială a versiunii după verificarea evidenței cererilor de modificare.

9. GESTIONAREA INCIDENTELOR DE SECURITATE

Gestionarea incidentelor de securitate este un proces de gestionare a incidentelor de securitate pentru a permite comunicarea incidentelor părților interesate potențial afectate, evaluarea și ierarhizarea incidentelor și răspunsul la incidente în vederea soluționării oricărei încălcări reale, suspectate sau potențiale a confidențialității, a disponibilității sau a integrității activelor informaționale sensibile.

9.1. Clasificarea incidentelor de securitate a informațiilor

Toate incidentele care afectează legătura dintre registrul Uniunii și registrul elvețian sunt analizate pentru a stabili o posibilă încălcare a confidențialității, a integrității sau a disponibilității oricărei informații sensibile înregistrate în Evidența informațiilor sensibile (SIL).

În acest caz, incidentul este caracterizat ca incident de securitate a informațiilor, este înregistrat imediat în instrumentul de gestionare a serviciilor IT (ITSM) și gestionat ca atare.

9.2. Gestionarea incidentelor de securitate a informațiilor

Incidentele de securitate se află în responsabilitatea celui de-al treilea nivel de transmitere, iar de rezolvarea acestora se va ocupa o echipă dedicată de gestionare a incidentelor (IMT).

IMT este responsabilă cu:

- efectuarea unei analize inițiale, clasificarea și evaluarea gradului de gravitate a incidentului;
- coordonarea acțiunilor între toate părțile interesate, inclusiv documentarea completă a analizei incidentului, deciziile luate pentru a rezolva incidentul și eventualele puncte slabe identificate;
- în funcție de gravitatea incidentelor de securitate, transmiterea în timp util la nivelul corespunzător pentru informare și/sau luarea unor decizii.

În cadrul procesului de management al securității informațiilor, toate informațiile referitoare la incidente sunt clasificate la cel mai înalt nivel de sensibilitate a informațiilor, dar în orice caz nu la un nivel mai mic decât nivelul ETS SENSITIVE (informații ETS sensibile).

În cazul unei investigări în curs de desfășurare și/sau al unui punct slab care ar putea fi exploatat și până la remedierea acestuia, informațiile sunt clasificate drept ETS CRITICAL (informații ETS deosebit de sensibile).

9.3. Identificarea incidentelor de securitate

În funcție de tipul de eveniment de securitate, responsabilul cu securitatea informațiilor stabilește organizațiile competente care trebuie implicate și care vor face parte din echipa de gestionare a incidentelor.

9.4. Analiza incidentelor de securitate

IMT asigură legătura cu toate organizațiile implicate și, după caz, cu membrii relevanți ai echipelor acestora în vederea analizării incidentului. În cadrul analizei, se identifică amploarea pierderii confidențialității, integrității sau disponibilității unui activ și se evaluează consecințele pentru toate organizațiile afectate. În continuare, sunt definite măsurile inițiale și de monitorizare pentru rezolvarea incidentului și gestionarea impactului acestuia, inclusiv a impactului acestor măsuri asupra resurselor.

9.5. Evaluarea gravității incidentelor de securitate, transmiterea și raportarea acestora

IMT evaluează gravitatea fiecărui incident de securitate nou după caracterizarea acestuia și ia imediat măsurile necesare în funcție de gravitatea acestuia.

9.6. Raportarea răspunsurilor la incidentele de securitate

IMT include în raportul de răspuns la incidentele de securitate a informațiilor rezultatele privind sistarea incidentelor și restabilirea sistemului. Raportul este transmis până la nivelul al treilea de transmitere prin intermediul unui e-mail securizat sau prin intermediul altor mijloace de comunicare securizate, acceptate de ambele părți.

Partea responsabilă analizează rezultatele privind sistarea și restabilirea sistemului și:

- reconectează registrul în cazul deconectării prealabile;
- transmite echipelor din cadrul registrelor informări cu privire la incident;
- închide incidentul.

În raportul privind incidentele de securitate a informațiilor, IMT ar trebui să includă - într-o manieră securizată - detalii relevante pentru a asigura coerența înregistrării și a comunicării și pentru a permite o acțiune promptă și adecvată pentru stoparea incidentului. După finalizarea acestuia, IMT transmite în timp util raportul final privind incidentele de securitate a informațiilor.

9.7. Monitorizare, consolidarea capacităților și îmbunătățirea continuă

IMT va furniza rapoarte pentru toate incidentele de securitate până la nivelul al treilea de transmitere. Rapoartele vor fi utilizate la acest nivel de transmitere pentru a stabili următoarele:

- punctele slabe în ceea ce privește controalele de securitate și/sau operațiunile care trebuie consolidate;
- eventualele necesități de îmbunătățire a acestei proceduri în vederea îmbunătățirii eficacității răspunsului la incidente;

- oportunități de formare și de consolidare a capacităților pentru a îmbunătăți mai mult reziliența sistemelor registrelor în ceea ce privește securitatea informațiilor, pentru a reduce riscul unor incidente viitoare și pentru a reduce la minimum impactul acestora.

10. MANAGEMENTUL SECURITĂȚII INFORMAȚIILOR

Managementul securității informațiilor vizează asigurarea confidențialității, a integrității și a disponibilității informațiilor, datelor și serviciilor IT clasificate ale unei organizații. Pe lângă componentele tehnice, inclusiv conceperea și testarea acestora (a se vedea LTS), sunt necesare următoarele procedee comune de funcționare în vederea îndeplinirii cerințelor de securitate pentru soluția provizorie.

10.1. Identificarea informațiilor sensibile

Nivelul de sensibilitate al unei informații este evaluat prin stabilirea nivelului impactului asupra întreprinderii (de exemplu, pierderi financiare, afectarea imaginii, încălcări ale legii etc.) pe care l-ar putea avea o încălcare a securității respectivelor informații.

Activele informaționale sensibile sunt identificate pe baza impactului lor asupra legăturii.

Nivelul de sensibilitate al acestor informații este evaluat în funcție de scala de sensibilitate aplicabilă pentru această legătură și este prezentat în detaliu în secțiunea „Gestionarea incidentelor de securitate a informațiilor” din prezentul document.

10.2. Nivelurile de sensibilitate ale activelor informaționale

După identificarea sa, activul informațional este clasificat aplicând următoarele reguli:

- identificarea cel puțin a unui nivel RIDICAT de confidențialitate, integritate sau disponibilitate clasifică activul drept ETS CRITICAL (informații ETS deosebit de sensibile);
- identificarea cel puțin a unui nivel MEDIU de confidențialitate, integritate sau disponibilitate clasifică activul drept ETS SENSITIVE (informații ETS sensibile);
- identificarea cel puțin a unui nivel REDUS de confidențialitate, integritate sau disponibilitate clasifică activul drept ETS LIMITED (informații ETS cu circulație limitată).

10.3. Desemnarea proprietarului activelor informaționale

Toate activele informaționale ar trebui să aibă un proprietar desemnat. Activele informaționale ale ETS, care aparțin legăturii dintre EUTL și SSTL sau se referă la aceasta ar trebui incluse într-o listă comună de inventariere a activelor, menținută de ambele părți. Activele informaționale ale ETS din afara legăturii dintre EUTL și SSTL ar trebui incluse într-o listă de inventariere a activelor, menținută de partea corespunzătoare.

Dreptul de proprietate asupra fiecărui activ informațional care aparține legăturii dintre EUTL și SSTL sau se referă la aceasta va fi convenit de către părți. Proprietarul unui activ informațional este responsabil pentru evaluarea nivelului de sensibilitate al acestuia.

Proprietarul ar trebui să aibă o experiență corespunzătoare pentru evaluarea activului (activelor) atribuit(e). Responsabilitatea proprietarului în ceea ce privește activul (activele), precum și obligația acestuia de a menține confidențialitatea, integritatea și nivelul de disponibilitate necesare ar trebui să fie convenite și oficializate.

10.4. Înregistrarea informațiilor sensibile

Toate informațiile sensibile sunt înregistrate în Evidența informațiilor sensibile (SIL).

Dacă este cazul, agregarea unor informații sensibile care ar putea avea un impact mai mare decât impactul unei singure informații trebuie luată în considerare și înregistrată în SIL (de exemplu, un set de informații stocate în baza de date a sistemului).

SIL nu este statică. Amenințările, vulnerabilitățile, probabilitatea sau consecințele incidentelor de securitate legate de active se pot schimba fără nicio indicație și pot fi introduse active noi în operarea sistemele registrelor.

Prin urmare, SIL este revizuită periodic și toate informațiile noi considerate ca fiind sensibile vor fi înregistrate imediat în SIL.

SIL conține cel puțin următoarele informații pentru fiecare înregistrare:

- Descrierea informațiilor
- Proprietarul informațiilor
- Nivelul de sensibilitate

- O mențiune care să indice dacă informațiile includ date cu caracter personal
- Informații suplimentare, dacă este cazul

10.5. Gestionarea informațiilor sensibile

Atunci când sunt prelucrate în afara legăturii dintre registrul Uniunii și registrul elvețian, informațiile sensibile sunt gestionate în conformitate cu Instrucțiunile de gestionare.

Informațiile sensibile prelucrate prin intermediul legăturii dintre registrul Uniunii și registrul elvețian sunt gestionate de către părți în conformitate cu cerințele în materie de securitate.

10.6. Managementul accesului

Obiectivul procesului de management al accesului este de a acorda utilizatorilor autorizați dreptul de a utiliza un serviciu, împiedicând în același timp accesul utilizatorilor neautorizați. Managementul accesului este uneori denumit și „managementul drepturilor” sau „managementul identității”.

Pentru soluția provizorie și funcționarea acesteia, ambele părți au nevoie de acces la următoarele componente:

- Wiki: un mediu de colaborare pentru schimbul de informații comune, cum ar fi planificarea versiunilor;
- Instrumentul de gestionare a serviciilor IT (ITSM) pentru gestionarea incidentelor și a problemelor (a se vedea capitolul „Abordare și standarde”);
- Sistemul de schimb de mesaje: fiecare parte pune la dispoziție un sistem securizat de transfer de mesaje pentru transmiterea mesajelor care conțin date privind tranzacțiile.

Administratorul registrului elvețian și administratorul central al Uniunii se asigură că accesurile sunt actualizate și funcționează ca puncte de contact pentru părțile lor în cadrul activităților de management al accesului. Cererile de acces sunt gestionate conform procedurilor de soluționare a cererilor.

10.7. Gestionarea certificatelor/cheilor

Fiecare parte răspunde de gestionarea propriilor certificate/chei (generare, înregistrare, stocare, instalare, utilizare, reînnoire, revocare, realizarea de copii de rezervă și recuperarea certificatelor/cheilor). Conform standardelor tehnice de creare a legăturii (LTS), se utilizează numai certificate digitale emise de o autoritate de certificare (CA) acceptată de ambele părți. Gestionarea și stocarea certificatelor/cheilor trebuie să respecte dispozițiile din Instrucțiunile de gestionare.

Orice revocare și/sau reînnoire a certificatelor și a cheilor este coordonată de ambele părți. Aceasta se realizează conform procedurilor de soluționare a cererilor.

Administratorul registrului elvețian și administratorul central al Uniunii vor face schimb de certificate/chei prin mijloace de comunicare securizate în conformitate cu dispozițiile din Instrucțiunile de gestionare.

Orice verificare a certificatelor/cheilor prin orice mijloc între părți se va realiza în afara benzii.