2024/1873

5.7.2024

DECISIONE (UE) 2024/1873 DEL CONSIGLIO

del 24 giugno 2024

relativa alla posizione da adottare a nome dell'Unione europea in sede di comitato misto istituito dall'accordo tra l'Unione europea e la Confederazione svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra, riguardo alla modifica dall'allegato II e delle procedure operative comuni e delle norme tecniche di collegamento

(Testo rilevante ai fini del SEE)

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 192, paragrafo 1, in combinato disposto con l'articolo 218, paragrafo 9,

vista la proposta della Commissione europea,

considerando quanto segue:

(1) L'accordo tra l'Unione europea e la Confederazione svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione dei gas a effetto serra ([1]) («accordo») è stato firmato il 23 novembre 2017 conformemente alla decisione (UE) 2017/2240 del Consiglio ([2]).

(2) L'accordo è stato concluso con la decisione (UE) 2018/219 del Consiglio ([3]) ed è entrato in vigore il 1º gennaio 2020.

(3) A norma dell'articolo 12, paragrafo 3, dell'accordo, il comitato misto può adottare decisioni che, a decorrere dalla loro entrata in vigore, devono essere vincolanti per le parti.

(4) L'articolo 13, paragrafo 2, dell'accordo stabilisce che il comitato misto può modificare gli allegati dell'accordo.

(5) L'articolo 3, paragrafi 6 e 7, prevede che le procedure operative comuni e le norme tecniche di collegamento debbano entrare in vigore una volta adottate con decisione del comitato misto. Con le decisioni n. 1/2020 ([4]) e n. 2/2020 ([5]), il comitato congiunto ha adottato, rispettivamente, le procedure operative comuni e le norme tecniche di collegamento.

(6) È opportuno modificare l'allegato II dell'accordo per tenere conto dell'evoluzione del collegamento tra i registri del sistema di scambio di quote di emissione dell'UE e del sistema di scambio di quote di emissione della Svizzera e razionalizzare le disposizioni dell'allegato II alla luce degli sviluppi tecnologici. Per garantire la coerenza delle procedure operative comuni e delle norme tecniche di collegamento con l'allegato II, è opportuno modificare anche tali documenti.

([1]) GU L 322 del 7.12.2017, pag. 3.
([2]) Decisione (UE) 2017/2240 del Consiglio, del 10 novembre 2017, relativa alla firma, a nome dell'Unione, e all'applicazione provvisoria dell'accordo tra l'Unione europea e la Confederazione svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra (GU L 322 del 7.12.2017, pag. 1).
([3]) Decisione (UE) 2018/219 del Consiglio, del 23 gennaio 2018, relativa alla conclusione dell'accordo tra l'Unione europea e la Confederazione svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra (GU L 43 del 16.2.2018, pag. 1).
([4]) Decisione n. 1/2020 del comitato misto istituito dall'accordo tra l'Unione europea e la Confederazione Svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra del 5 novembre 2020 sull'adozione delle procedure operative comuni (POC) [2021/1033] (GU L 226 del 25.6.2021, pag. 2).
([5]) Decisione n. 2/2020 del comitato misto istituito dall'accordo tra l'Unione europea e la Confederazione Svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra del 5 novembre 2020 relativa alla modifica degli allegati I e II dell'accordo e all'adozione delle norme tecniche di collegamento (NTC) [2021/1034] (GU L 226 del 25.6.2021, pag. 16).

(7) Nella sua settima riunione, o precedentemente mediante procedura scritta a norma dell'articolo 8, paragrafo 4, del suo regolamento interno ([6]), il comitato misto sarà chiamato ad adottare una decisione relativa alla modifica dell'allegato II dell'accordo e alla modifica delle procedure operative comuni e delle norme tecniche di collegamento.

(8) È opportuno stabilire la posizione da adottare a nome dell'Unione in sede di comitato misto riguardo alla modifica dall'allegato II e alla modifica delle procedure operative comuni e delle norme tecniche di collegamento, poiché la decisione vincolerà l'Unione.

(9) La posizione dell'Unione in seno al Comitato misto dovrebbe basarsi sul progetto di decisione accluso,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

La posizione da adottare a nome dell'Unione nella settima riunione del comitato misto o precedentemente mediante procedura scritta a norma dell'articolo 8, paragrafo 4, del regolamento interno del comitato misto, si basa sul progetto di decisione del comitato misto accluso alla presente decisione.

Articolo 2

La presente decisione entra in vigore il giorno dell'adozione.

Fatto a Lussemburgo, il 24 giugno 2024

Per il Consiglio

Il presidente

D. CLARINVAL

([6]) Decisione n. 1/2019 del comitato misto istituito dall'accordo tra l'Unione europea e la Confederazione svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra, del 25 gennaio 2019, recante adozione del regolamento interno del comitato misto, e decisione (UE) 2018/1279 del Consiglio, del 18 settembre 2018, relativa alla posizione da adottare a nome dell'Unione europea in sede di comitato misto istituito dall'accordo tra l'Unione europea e la Confederazione svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra, in riferimento all'adozione del regolamento interno del comitato misto (GU L 239 del 24.9.2018, pag. 8).

DECISIONE N. 1/2024 DEL COMITATO MISTO ISTITUITO DALL'ACCORDO TRA L'UNIONE EUROPEA E LA CONFEDERAZIONE SVIZZERA CONCERNENTE IL COLLEGAMENTO DEI RISPETTIVI SISTEMI DI SCAMBIO DI QUOTE DI EMISSIONE DI GAS A EFFETTO SERRA

del …

concernente la modifica dell'allegato II dell'accordo e delle procedure operative comuni e delle norme tecniche di collegamento

IL COMITATO MISTO,

visto l'accordo tra l'Unione europea e la Confederazione svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione dei gas a effetto serra ([1]) («accordo»), in particolare l'articolo 9 e l'articolo 13, paragrafo 2,

considerando quanto segue:

(1) La decisione n. 2/2019 del comitato misto ([2]) ha previsto una soluzione provvisoria per rendere operativo il collegamento tra l'EU ETS e l'ETS della Svizzera.

(2) Nella sua terza riunione il comitato misto ha convenuto sulla necessità di analizzare l'efficacia in termini di costi di un collegamento permanente tra il registro dell'Unione e il registro svizzero.

(3) Nella sua quinta riunione il comitato misto ha approvato la relazione presentata dal gruppo di lavoro istituito dalle decisioni n. 1/2020 ([3]) e n. 2/2020 ([4]) del comitato misto e in cui il gruppo di lavoro ha analizzato e raccomandato un approccio per attuare il collegamento permanente tra il registro dell'Unione e il registro svizzero.

(4) Per rispecchiare le disposizioni tecniche per il collegamento permanente tra il registro dell'Unione e il registro svizzero e per razionalizzare le disposizioni dell'allegato II dell'accordo alla luce degli sviluppi tecnologici, è opportuno modificare l'allegato II dell'accordo.

(5) Per garantire la coerenza delle procedure operative comuni e delle norme tecniche di collegamento con l'allegato II dell'accordo, è opportuno modificare anche tali documenti,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

1. L'allegato II dell'accordo è sostituito dal testo che figura nell'allegato I della presente decisione.

2. Le procedure operative comuni di cui all'articolo 3, paragrafo 6, dell'accordo figurano nell'allegato II della presente decisione. Esse sostituiscono le procedure operative comuni che figurano nell'allegato della decisione n. 1/2020.

3. Le norme tecniche di collegamento di cui all'articolo 3, paragrafo 7, dell'accordo figurano nell'allegato III della presente decisione. Esse sostituiscono le norme tecniche di collegamento che figurano nell'allegato della decisione n. 2/2020.

([1]) GU L 322 del 7.12.2017, pag. 3.

([2]) Decisione n. 2/2020 del comitato misto istituito dall'accordo tra l'Unione europea e la Confederazione Svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra del 5 novembre 2020 relativa alla modifica degli allegati I e II dell'accordo e all'adozione delle norme tecniche di collegamento (NTC) [2021/1034] (GU L 314 del 29.9.2020, pag. 68).

([3]) Decisione n. 1/2020 del comitato misto istituito dall'accordo tra l'Unione europea e la Confederazione Svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra del 5 novembre 2020 sull'adozione delle procedure operative comuni (POC) [2021/1033] (GU L 226 del 25.6.2021, pag. 2).

([4]) Decisione n. 2/2020 del comitato misto istituito dall'accordo tra l'Unione europea e la Confederazione Svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra del 5 novembre 2020 relativa alla modifica degli allegati I e II dell'accordo e all'adozione delle norme tecniche di collegamento (NTC) [2021/1034] (GU L 226 del 25.6.2021, pag. 16).

Articolo 2

La presente decisione entra in vigore il giorno dell'adozione.

Fatto a …., il …

Per il Comitato misto

Il segretario per l'Unione europea	*Il presidente*	*Il segretario per la Svizzera*

ALLEGATO I

«ALLEGATO II

NORME TECNICHE DI COLLEGAMENTO

Nel 2020 è stata attuata una soluzione provvisoria per rendere operativo il collegamento tra l'EU ETS e l'ETS della Svizzera. A partire dal 2023, il collegamento tra i due sistemi di scambio di quote di emissione si trasformerà gradualmente in un collegamento permanente dei registri, la cui attuazione è prevista entro il 2024, che consentirà ai mercati collegati, in termini di vantaggi derivanti dalla liquidità del mercato e dall'esecuzione di operazioni tra i due sistemi collegati, di funzionare in modo equivalente a un mercato composto da due sistemi che si presenta ai partecipanti come un unico mercato, subordinatamente alle sole disposizioni regolamentari individuali delle parti.

Le norme tecniche di collegamento (NTC) precisano:

— l'architettura del collegamento di comunicazione;

— le comunicazioni tra l'SSTL e l'EUTL;

— la sicurezza del trasferimento dei dati;

— l'elenco delle funzioni (operazioni, spunta contabile ecc.);

— la definizione del livello di trasporto (*transport layer*);

— le disposizioni relative alla registrazione dei dati;

— le modalità operative (servizio di chiamata, assistenza);

— il piano di attivazione della comunicazione e la procedura di prova;

— la procedura di prova della sicurezza.

Le NTC specificano che gli amministratori devono adottare tutte le misure ragionevoli per assicurare che l'SSTL, l'EUTL e il collegamento siano operativi 24 ore al giorno e 7 giorni su 7 e che le interruzioni dell'attività dell'SSTL, dell'EUTL e del collegamento devono essere ridotte al minimo.

Le NTC stabiliscono per il registro della Svizzera, l'SSTL, il registro dell'Unione e l'EUTL prescrizioni supplementari di sicurezza che sono documentate in un "piano di gestione della sicurezza". In particolare, precisano che:

— se si sospetta che la sicurezza del registro svizzero, dell'SSTL, del registro dell'Unione o dell'EUTL sia stata compromessa, entrambe le parti si informano reciprocamente e immediatamente e sospendono il collegamento tra l'SSTL e l'EUTL;

— in caso di violazione della sicurezza, le parti si impegnano a condividere immediatamente tra loro le informazioni. Nella misura in cui sono disponibili dettagli tecnici, entro 24 ore dall'individuazione di un incidente identificato come violazione della sicurezza l'amministratore del registro della Svizzera e l'amministratore centrale dell'Unione si scambiano una relazione che illustra l'evento (data, causa, impatto, misure correttive).

La procedura di prova della sicurezza di cui alle NTC è completata prima dell'istituzione del collegamento di comunicazione tra l'SSTL e l'EUTL e ogniqualvolta si rende necessaria una nuova versione dell'SSTL o dell'EUTL.

Le NTC prevedono due ambienti di prova oltre all'ambiente di produzione: un ambiente di prova dello sviluppatore e un ambiente di collaudo.

Le parti dimostrano, tramite l'amministratore del registro della Svizzera e l'amministratore centrale dell'Unione, che è stata effettuata una valutazione indipendente della sicurezza dei loro sistemi nei 12 mesi precedenti, in conformità delle prescrizioni di sicurezza di cui alle NTC. Le prove di sicurezza, in particolare i test di penetrazione, sono effettuate su tutte le nuove versioni rilevanti del software in conformità delle prescrizioni di sicurezza di cui alle NTC. I test di penetrazione non sono eseguiti dallo sviluppatore del software né da un suo subappaltatore.».

ALLEGATO II

PROCEDURE OPERATIVE COMUNI (POC) A NORMA DELL'ARTICOLO 3, PARAGRAFO 6, DELL'ACCORDO TRA L'UNIONE EUROPEA E LA CONFEDERAZIONE SVIZZERA CONCERNENTE IL COLLEGAMENTO DEI RISPETTIVI SISTEMI DI SCAMBIO DI QUOTE DI EMISSIONE DI GAS A EFFETTO SERRA

Procedure per il collegamento permanente dei registri

Sommario

1. GLOSSARIO . . . 9
2. INTRODUZIONE . . . 9
2.1. Ambito di applicazione . . . 10
2.2. Destinatari . . . 10
3. APPROCCIO E NORME . . . 10
4. GESTIONE DEGLI INCIDENTI . . . 11
4.1. Individuazione e registrazione degli incidenti . . . 11
4.2. Classificazione e sostegno iniziale . . . 11
4.3. Indagini e diagnosi . . . 12
4.4. Risoluzione e ripristino del servizio . . . 12
4.5. Chiusura dell'incidente . . . 12
5. GESTIONE DEI PROBLEMI . . . 13
5.1. Individuazione e registrazione del problema . . . 13
5.2. Classificazione dei problemi in funzione della loro priorità . . . 13
5.3. Indagini e diagnosi . . . 13
5.4. Risoluzione . . . 13
5.5. Chiusura del problema . . . 13
6. SODDISFACIMENTO DELLE RICHIESTE . . . 13
6.1. Avvio della richiesta . . . 13
6.2. Registrazione e analisi della richiesta . . . 14
6.3. Approvazione della richiesta . . . 14
6.4. Soddisfacimento delle richieste . . . 14
6.5. Attivazione dei livelli successivi di intervento per le richieste . . . 14
6.6. Esame del soddisfacimento delle richieste . . . 14
6.7. Chiusura della richiesta . . . 14
7. GESTIONE DELLE MODIFICHE . . . 14
7.1. Richiesta di modifica . . . 15
7.2. Valutazione e pianificazione delle modifiche . . . 15
7.3. Approvazione delle modifiche . . . 15
7.4. Attuazione delle modifiche . . . 15
8. GESTIONE DEL RILASCIO DELLE NUOVE VERSIONI . . . 15
8.1. Programmazione dei rilasci . . . 15
8.2. Costruire e testare un pacchetto di rilasci . . . 16
8.3. Preparare l'implementazione . . . 16

8.4. Ripristino della situazione precedente . . . 16
8.5. Verifica e chiusura del rilascio . . . 16
9. GESTIONE DEGLI INCIDENTI DI SICUREZZA . . . 17
9.1. Classificazione degli incidenti relativi alla sicurezza delle informazioni . . . 17
9.2. Trattamento degli incidenti relativi alla sicurezza delle informazioni . . . 17
9.3. Individuazione degli incidenti di sicurezza . . . 17
9.4. Analisi degli incidenti di sicurezza . . . 17
9.5. Valutazione della gravità dell'incidente di sicurezza, trasferimento dell'incidente al livello adeguato e elaborazione delle relazioni . . . 17
9.6. Relazione in risposta ad un incidente . . . 18
9.7. Monitoraggio, rafforzamento delle capacità e miglioramento continuo . . . 18
10. GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI . . . 18
10.1. Individuazione delle informazioni riservate . . . 18
10.2. Livelli di riservatezza delle risorse di informazione . . . 18
10.3. Designazione del titolare della risorsa di informazione . . . 18
10.4. Registrazione delle informazioni riservate . . . 19
10.5. Trattamento delle informazioni sensibili . . . 19
10.6. Gestione dell'accesso . . . 19
10.7. Gestione di certificati/chiavi . . . 19

1. GLOSSARIO

Tabella 1-1 Acronimi e definizioni

Acronimo/Termine	Definizione
Autorità di certificazione (AC)	Organismo che rilascia certificati digitali
CH	Confederazione svizzera
EIR	Elenco delle informazioni riservate
ETS	Sistema di scambio di quote di emissione
IMT	Squadra di gestione degli incidenti (*Incident Management Team*)
IT	Tecnologie dell'informazione (*Information technology*)
ITIL	Biblioteca dell'infrastruttura delle tecnologie dell'informazione (*Information Technology Infrastructure Library*)
ITSM	Gestione dei servizi informatici (*IT Service Management*)
NTC	Norme tecniche di collegamento
RDM	Richiesta di modifica
Registro	Un sistema contabile per le quote rilasciate nell'ambito dell'ETS, che tiene traccia della titolarità delle quote detenute in conti elettronici.
Risorsa di informazione	Un'informazione utile per un'impresa o un'organizzazione
RS	Richiesta di servizio
UE	Unione europea
Wiki	Un sito web che consente agli utenti di scambiare informazioni e conoscenze aggiungendo o adattando i contenuti direttamente attraverso un browser.

2. INTRODUZIONE

L'accordo tra l'Unione europea e la Confederazione svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra, del 23 novembre 2017 («l'accordo»), prevede il riconoscimento reciproco delle quote di emissione che possono essere utilizzate per conformarsi al sistema di scambio di quote di emissione dell'Unione europea (EU ETS) o al sistema di scambio di quote di emissione della Svizzera (ETS della Svizzera). Per rendere operativo il collegamento tra l'EU ETS e l'ETS della Svizzera, sarà stabilito un collegamento diretto tra il catalogo delle operazioni dell'Unione europea (EUTL) del registro dell'Unione e il libro di bordo elettronico supplementare della Svizzera (SSTL) del registro svizzero tale da consentire il trasferimento da un registro all'altro delle quote di emissioni rilasciate nell'ambito dei due ETS (articolo 3, paragrafo 2, dell'accordo). Nel 2020 è stata attuata una soluzione provvisoria per rendere operativo il collegamento tra l'EU ETS e l'ETS della Svizzera. A partire dal 2023, il collegamento tra i due sistemi di scambio di quote di emissione si trasformerà gradualmente in un collegamento permanente dei registri, la cui attuazione è prevista entro il 2024, che consentirà ai mercati collegati, in termini di vantaggi derivanti dalla liquidità del mercato e dall'esecuzione di operazioni tra i due sistemi collegati, di funzionare in modo equivalente a un mercato composto da due sistemi che si presenta ai partecipanti come un unico mercato, subordinatamente alle sole disposizioni regolamentari individuali delle parti (allegato II dell'accordo).

A norma dell'articolo 3, paragrafo 6, dell'accordo, l'amministratore del registro della Svizzera e l'amministratore centrale dell'Unione stabiliscono procedure operative comuni (POC) relative a questioni tecniche o di altra natura necessarie al funzionamento del collegamento, tenuto conto delle priorità della normativa interna. Le POC elaborate dagli amministratori entrano in vigore una volta adottate con decisione del comitato misto.

Le POC sono state adottate dal comitato misto con decisione n. 1/2020. Le POC aggiornate descritte nel presente documento saranno adottate dal comitato misto conformemente alla decisione n. 1/2024. Conformemente alla presente decisione e a quanto chiesto dal comitato misto, l'amministratore del registro della Svizzera e l'amministratore centrale dell'Unione hanno elaborato e aggiorneranno ulteriori orientamenti tecnici per rendere operativo il collegamento e garantire che tali orientamenti siano costantemente adattati al progresso tecnico e alle nuove prescrizioni relative alla sicurezza interna ed esterna del collegamento e al suo funzionamento efficace ed efficiente.

2.1. Ambito di applicazione

Il presente documento rappresenta l'intesa comune tra le parti dell'accordo per quanto riguarda la definizione delle procedure di base del collegamento tra i registri dell'EU ETS e l'ETS della Svizzera. Illustra gli obblighi procedurali generali in termini di operazioni, ma saranno necessari ulteriori orientamenti tecnici per rendere operativo il collegamento.

Per il corretto funzionamento del collegamento, occorreranno specifiche tecniche che ne rafforzino l'operatività. A norma dell'articolo 3, paragrafo 7, dell'accordo, tali aspetti sono trattati dettagliatamente nel documento relativo alle norme tecniche di collegamento (NTC), che deve essere adottato separatamente mediante decisione del comitato misto.

L'obiettivo delle POC è garantire che i servizi informatici relativi al funzionamento del collegamento tra i registri del sistema EU ETS e del sistema ETS della Svizzera siano forniti in modo efficace ed efficiente, in particolare per soddisfare le richieste di servizio, rimediare ai disservizi, risolvere problemi e svolgere compiti operativi di routine conformemente alle norme internazionali per la gestione dei servizi informatici.

Per il collegamento permanente dei registri, saranno necessarie solo le POC seguenti, incluse nel presente documento:

— Gestione degli incidenti

— Gestione dei problemi

— Soddisfacimento delle richieste

— Gestione delle modifiche

— Gestione del rilascio delle versioni (*release management*)

— Gestione degli incidenti di sicurezza

— Gestione della sicurezza delle informazioni

2.2. Destinatari

I destinatari di queste POC sono le squadre di sostegno dei registri dell'UE e della Svizzera.

3. APPROCCIO E NORME

Il principio seguente si applica a tutte le POC:

— L'UE e la Svizzera convengono di definire le POC sulla base dell'ITIL (Biblioteca dell'infrastruttura delle tecnologie dell'informazione, versione 4). Le pratiche tratte da questa norma sono riutilizzate e adattate alle esigenze specifiche relazione al collegamento permanente dei registri.

— La comunicazione e il coordinamento necessari per il trattamento delle POC tra le due parti si svolgono attraverso gli sportelli di servizio dei registri della Svizzera e dell'UE. I compiti sono sempre assegnati in seno ad una parte.

— In caso di disaccordo sul trattamento di una POC, la questione sarà analizzata e risolta dai due sportelli di servizio. Se non è possibile raggiungere un accordo, la ricerca di una soluzione comune è trasferita al livello superiore.

Livelli successivi di interventi	UE	CH
1° livello	Sportello di servizio UE	Sportello di servizio CH
2° livello	Responsabile operativo dell'UE	Gestore delle applicazioni del registro CH
3° livello	Comitato misto (che può delegare tale responsabilità alla luce dell'articolo 12, paragrafo 5, dell'accordo)	
4° livello	Comitato misto, se al 3° livello si è ricorsi ad una delega	

— Ciascuna parte può stabilire le procedure per il funzionamento del proprio sistema di registro, tenendo conto delle prescrizioni e delle interfacce relative a queste POC.

— A sostegno delle POC, in particolare per la gestione degli incidenti, la gestione dei problemi e il soddisfacimento delle richieste, ma anche per la comunicazione tra le due parti viene utilizzato uno strumento di gestione dei servizi informatici (*IT Service management* - ITSM).

— È inoltre consentito lo scambio di informazioni via email.

— Entrambe le parti garantiscono il rispetto delle prescrizioni in materia di sicurezza delle informazioni conformemente alle istruzioni di trattamento.

4. GESTIONE DEGLI INCIDENTI

L'obiettivo del processo di gestione degli incidenti è riportare i servizi informatici a un normale livello di servizio il più rapidamente possibile dopo un incidente e con un'interruzione minima dell'attività.

La gestione degli incidenti dovrebbe inoltre tenere traccia degli incidenti avvenuti a fini di segnalazione e integrarsi con altri processi per favorire un miglioramento costante.

Da una prospettiva globale, la gestione degli incidenti comprende le seguenti attività:

— Individuazione e registrazione degli incidenti

— Classificazione e sostegno iniziale

— Indagini e diagnosi

— Risoluzione e ripristino del servizio

— Chiusura dell'incidente

Durante l'intero ciclo di vita di un incidente, il processo di gestione degli incidenti deve consentire il trattamento costante della titolarità, del monitoraggio, del tracciamento e della comunicazione.

4.1. Individuazione e registrazione degli incidenti

Un incidente può essere rilevato da una squadra di sostegno, da strumenti di monitoraggio automatico o da personale tecnico nel corso della sorveglianza di routine.

Una volta individuato, occorre registrare l'incidente e assegnargli un identificatore unico ai fini di un tracciamento e un monitoraggio adeguati. L'identificatore unico di un incidente è quello assegnato nel sistema di ticketing comune dallo sportello di servizio della parte (UE o CH) che ha segnalato l'incidente e deve essere utilizzato in ogni comunicazione relativa a questo incidente.

Per tutti gli incidenti il punto di contatto dovrebbe essere lo sportello di servizio della parte che ha registrato il ticket.

4.2. Classificazione e sostegno iniziale

La classificazione degli incidenti serve a capire e identificare il sistema e/o il servizio interessato dall'incidente e la gravità dell'evento. Per essere efficace, la classificazione dovrebbe permettere di far risalire l'incidente alla risorsa corretta al primo tentativo, al fine di accelerare la risoluzione degli incidenti.

Nella fase di classificazione si dovrebbe classificare l'incidente anche per ordine di priorità in funzione del suo impatto e della sua urgenza affinché possa essere trattato entro i tempi stabiliti per ogni livello di priorità.

Se ha un potenziale impatto sulla riservatezza o sull'integrità di dati riservati e/o sulla disponibilità del sistema, l'incidente è dichiarato anche come incidente di sicurezza e successivamente gestito secondo la procedura di cui al capitolo «Gestione degli incidenti di sicurezza» del presente documento.

Se possibile, lo sportello di servizio che ha effettuato la registrazione del ticket procede alla diagnosi iniziale. A tal fine, lo sportello di servizio verifica se l'incidente è legato ad un errore noto. In caso affermativo, il metodo per risolvere o aggirare il problema è già conosciuto e documentato.

Se riesce a risolvere l'incidente, lo sportello di servizio chiude l'incidente in questa fase, in quanto è stata conseguita la finalità principale della gestione degli incidenti (ossia il rapido ripristino del servizio per l'utente finale). In caso contrario, lo sportello di servizio trasmette l'incidente al gruppo risolutore competente per ulteriori indagini e diagnosi.

4.3. Indagini e diagnosi

L'indagine e la diagnosi si effettuano quando un incidente non può essere risolto dallo sportello di servizio nell'ambito della diagnosi iniziale ed è pertanto trasmesso al livello superiore adeguato. L'attivazione dei livelli successivi di intervento in caso di incidenti è parte integrante del processo investigativo e diagnostico.

Una pratica comune nella fase investigativa e di diagnosi è il tentativo di ricreare l'incidente in condizioni controllate. Nello svolgimento delle indagini e della diagnosi dell'incidente, è fondamentale comprendere l'effettivo ordine degli eventi che hanno portato all'incidente.

Questa procedura viene attivata quando si constata che l'incidente non può essere risolto al livello di supporto attuale e deve essere trasferito a un gruppo di supporto di livello superiore o all'altra parte. La procedura può seguire due percorsi: orizzontale (funzionale) o verticale (gerarchico).

Lo sportello di servizio che ha registrato e avviato la procedura di risoluzione è responsabile del trasferimento dell'incidente al livello di risorsa adeguato e del monitoraggio della situazione generale e dell'assegnazione dell'incidente.

La parte alla quale è stato assegnato l'incidente deve garantire che le azioni necessarie siano eseguite in modo tempestivo e deve fornire un riscontro al proprio sportello di servizio.

4.4. Risoluzione e ripristino del servizio

Una volta chiarita la dinamica dell'incidente si procede alla risoluzione dell'incidente e al ripristino del servizio. La risoluzione di un incidente significa che è stato individuato un modo per porre rimedio al problema. L'applicazione della soluzione costituisce la fase di ripristino.

Una volta risolta l'interruzione del servizio con le risorse adeguate, l'incidente è ritrasferito allo sportello di servizio competente che ha registrato l'incidente; quest'ultimo verifica con il servizio che per primo ha segnalato l'incidente che l'errore è stato corretto e che l'incidente può essere chiuso. Le informazioni emerse dal trattamento dell'incidente devono essere registrate per un uso futuro.

Il ripristino può essere eseguito dal personale di supporto informatico o fornendo all'utente finale una serie di istruzioni da seguire.

4.5. Chiusura dell'incidente

La chiusura è la tappa finale del processo di gestione degli incidenti e avviene poco dopo la risoluzione.

Nell'elenco delle operazioni da eseguire durante la fase di chiusura figurano in particolare:

— la verifica della classificazione iniziale attribuita all'incidente;

— la corretta acquisizione di tutte le informazioni relative all'incidente;

— l'adeguata documentazione dell'incidente e l'aggiornamento della base di conoscenze;

— la corretta comunicazione a tutti i portatori di interessi direttamente o indirettamente coinvolti.

Un incidente è ufficialmente chiuso non appena lo sportello di servizio effettua la fase di chiusura e lo comunica all'altra parte.

Una volta chiuso, l'incidente non viene riaperto. Se poco dopo si riverifica lo stesso incidente, l'incidente iniziale non è riaperto, ma viene registrato un nuovo incidente.

Se l'incidente è individuato da entrambi gli sportelli di servizio UE e CH, la chiusura finale spetta allo sportello di servizio che ha registrato il ticket.

5. GESTIONE DEI PROBLEMI

Questa procedura dovrebbe essere seguita ogni volta che viene individuato un problema, innescando quindi il processo di gestione dei problemi. La gestione dei problemi mira a migliorare la qualità e a ridurre il numero di incidenti segnalati. Un problema può determinare uno o più incidenti. Quando viene segnalato un incidente, l'obiettivo della gestione degli incidenti è ripristinare il servizio il più rapidamente possibile, eventualmente ricorrendo a espedienti tecnici. Quando viene registrato un problema, l'obiettivo è indagare sulle cause di fondo al fine di individuare una modifica che garantirà che il problema e gli incidenti che ne derivano non si verifichino più.

5.1. Individuazione e registrazione del problema

A seconda della parte che registra il ticket, lo sportello di servizio UE o CH diventeranno il punto di contatto per le questioni connesse al problema.

L'identificatore unico di un problema è l'identificatore assegnato dalla gestione dei servizi informatici (ITSM) che deve essere utilizzato in ogni comunicazione relativa a questo problema.

La procedura di gestione di un problema può essere avviata a seguito di un incidente o per iniziativa autonoma al fine di risolvere problemi individuati nel sistema in qualsiasi momento.

5.2. Classificazione dei problemi in funzione della loro priorità

Come gli incidenti, anche i problemi possono essere classificati in funzione della loro gravità e priorità al fine di facilitare il loro tracciamento, tenendo conto dell'impatto e della frequenza degli incidenti che ne derivano.

5.3. Indagini e diagnosi

Ciascuna parte può sollevare un problema e lo sportello di servizio della parte promotrice è responsabile della registrazione del problema, dell'assegnazione alla risorsa adeguata e del monitoraggio globale del problema.

Il gruppo risolutore a cui è stato trasferito il problema è responsabile del trattamento del problema in modo tempestivo e della comunicazione con lo sportello di servizio.

Su richiesta, entrambe le parti devono garantire l'attuazione delle azioni assegnate e la trasmissione di un feedback allo sportello di servizio della propria parte.

5.4. Risoluzione

Il gruppo risolutore a cui è assegnato il problema è responsabile della risoluzione del problema e della trasmissione delle informazioni pertinenti allo sportello di servizio della propria parte.

Le informazioni emerse dal trattamento del problema devono essere registrate per un uso futuro.

5.5. Chiusura del problema

Il problema è ufficialmente chiuso quando viene risolto apportando la modifica necessaria. La fase di chiusura del problema sarà effettuata dallo sportello di servizio che ha registrato il problema e informato lo sportello di servizio dell'altra parte.

6. SODDISFACIMENTO DELLE RICHIESTE

Il processo per il soddisfacimento delle richieste costituisce il trattamento da punto a punto di una richiesta di servizio nuovo o esistente dal momento in cui è registrata e approvata fino alla chiusura. Le richieste di servizio sono di solito di entità ridotta, predefinite, ripetibili, frequenti, preapprovate e si tratta perlopiù di richieste procedurali.

Le principali tappe da seguire sono illustrate di seguito.

6.1. Avvio della richiesta

Le informazioni relative ad una richiesta di servizio sono trasmesse allo sportello di servizio UE o CH per email, telefono o attraverso lo strumento di gestione dei servizi informatici (ITSM) o qualsiasi altro mezzo di comunicazione riconosciuto.

6.2. Registrazione e analisi della richiesta

Per tutte le richieste di servizio, il punto di contatto dovrebbe essere lo sportello di servizio UE o CH, in funzione della parte che ha presentato la richiesta. Allo sportello di servizio spetterà registrare e analizzare la richiesta di servizio con la dovuta diligenza.

6.3. Approvazione della richiesta

L'agente dello sportello di servizio della parte che ha avviato la richiesta di servizio verifica se siano necessarie approvazioni dell'altra parte e in caso affermativo si attiva per ottenerle. Se la richiesta di servizio non è approvata, lo sportello di servizio aggiorna e chiude il ticket.

6.4. Soddisfacimento delle richieste

Questa tappa serve a garantire il trattamento efficace e efficiente delle richieste di servizio. Occorre effettuare una distinzione tra i casi seguenti:

— il soddisfacimento della richiesta di servizio riguarda solo una parte – in questo caso, la parte in questione emette gli ordini di lavoro e coordina l'esecuzione;

— il soddisfacimento della richiesta di servizio riguarda sia l'UE che la Svizzera – in questo caso gli sportelli di servizio emettono gli ordini di lavoro nel loro ambito di competenza. L'elaborazione della richiesta di servizio è coordinata dagli sportelli di servizio di entrambe le parti. La responsabilità generale incombe allo sportello di servizio che ha ricevuto e avviato la richiesta di servizio.

Una volta che la richiesta di servizio è stata soddisfatta, il suo status deve essere modificato in «soddisfatto».

6.5. Attivazione dei livelli successivi di intervento per le richieste

Lo sportello di servizio può trasferire la richiesta di servizio in sospeso alla risorsa adeguata (terza parte) se necessario.

I trasferimenti ai livelli successivi di trattamento avvengono verso le terze parti rispettive: lo sportello di servizio dell'UE deve passare dallo sportello di servizio CH per l'attivazione di una terza parte svizzera, e viceversa.

La terza parte cui è stata trasferita la richiesta di servizio è responsabile del trattamento della richiesta in modo tempestivo e della comunicazione con lo sportello di servizio che ha effettuato il trasferimento.

Lo sportello di servizio che ha registrato la richiesta di servizio è responsabile del monitoraggio della situazione generale e dell'assegnazione di una richiesta di servizio.

6.6. Esame del soddisfacimento delle richieste

Lo sportello di servizio responsabile, prima di chiuderlo, sottopone il dossier della richiesta di servizio ad un controllo finale di qualità. L'obiettivo è garantire che la richiesta di servizio sia stata effettivamente trattata e che tutte le informazioni necessarie per descrivere l'iter della richiesta siano state fornite in modo sufficientemente dettagliato. Le informazioni emerse dal trattamento della richiesta devono inoltre essere registrate per un uso futuro.

6.7. Chiusura della richiesta

Se le parti cui la richiesta di servizio è stata assegnata convengono che la richiesta è stata soddisfatta e il richiedente ritiene che la questione sia stata risolta, lo status della richiesta passa a «chiusa».

Una richiesta di servizio è ufficialmente chiusa una volta che lo sportello di servizio che ha registrato la richiesta di servizio ha eseguito la fase di chiusura della richiesta e ha informato lo sportello di servizio dell'altra parte.

7. GESTIONE DELLE MODIFICHE

L'obiettivo è garantire che siano utilizzati metodi e procedure standardizzati per un trattamento efficace e tempestivo di tutte le modifiche che incidono sulle infrastrutture informatiche di controllo, al fine di ridurre al minimo il numero di incidenti e il loro impatto sul servizio. Le modifiche dell'infrastruttura informatica possono costituire una risposta a problemi o esigenze imposte dall'esterno, ad esempio modifiche legislative, o essere attuate in modo proattivo ai fini di una maggiore efficienza ed efficacia o per consentire o rispecchiare iniziative imprenditoriali.

La procedura di gestione delle modifiche prevede più fasi nel corso delle quali vengono registrate, in vista di un tracciamento successivo, tutte le informazioni relative ad una richiesta di modifica. Tali processi garantiscono che la modifica sia convalidata e testata prima di essere implementata. Il processo di gestione dei rilasci è alla base di una corretta implementazione.

7.1. Richiesta di modifica

Le richieste di modifica (RDM) sono trasmesse alla squadra di gestione delle modifiche ai fini della convalida e dell'approvazione. Per tutte le richieste di modifica, il punto di contatto dovrebbe essere lo sportello di servizio UE o CH, in funzione della parte che ha presentato la richiesta. Lo sportello di servizio in questione è responsabile di registrare e analizzare la richiesta con la dovuta diligenza.

Le richieste di modifica possono nascere da:

— un incidente che determina una modifica;

— un problema esistente che risulta in una modifica;

— un utente finale che richiede una nuova modifica;

— una modifica derivante da una manutenzione in corso;

— una modifica legislativa.

7.2. Valutazione e pianificazione delle modifiche

Nel corso di questa fase si svolgono le attività di valutazione delle modifiche e di pianificazione, che comprendono attività di definizione delle priorità e di pianificazione per ridurre al minimo i rischi e l'impatto.

Se l'attuazione della RDM interessa sia l'UE che la Svizzera, la parte che ha registrato l'RDM verifica la valutazione e la pianificazione della modifica con l'altra parte.

7.3. Approvazione delle modifiche

Qualsiasi richiesta di modifica registrata deve essere approvata dal livello di trattamento adeguato.

7.4. Attuazione delle modifiche

L'attuazione delle modifiche è gestita nell'ambito della gestione dei rilasci. Le squadre delle due parti responsabili della gestione dei rilasci seguono le proprie procedure che prevedono attività di pianificazione e di prova. L'esame delle modifiche avviene una volta completata l'attuazione. Al fine di garantire che tutto si sia svolto in modo corretto, il processo di gestione delle modifiche esistente è costantemente riesaminato e aggiornato ogniqualvolta necessario.

8. GESTIONE DEL RILASCIO DELLE NUOVE VERSIONI

Il rilascio di una nuova versione riguarda una o più modifiche di un servizio informatico, riunite in un piano di rilascio, che devono essere autorizzate, preparate, costruite, testate e attuate simultaneamente. Un rilascio può costituire la correzione di un errore in una procedura informatica, un cambiamento di hardware o di altri componenti, modifiche del software, aggiornamenti delle versioni delle applicazioni, modifiche della documentazione e/o dei processi. Il contenuto di ogni rilascio è gestito, testato e applicato come un'entità unica.

L'obiettivo della gestione dei rilasci è pianificare, costruire, testare e convalidare e garantire la capacità di fornire i servizi progettati, che consentiranno di soddisfare le esigenze dei portatori di interessi e di realizzare gli obiettivi previsti. I criteri di accettazione di tutte le modifiche apportate al servizio saranno definiti e documentati nel corso del coordinamento della progettazione e messi a disposizione delle squadre responsabili della gestione dei rilasci.

Il rilascio, di norma, consiste in una serie di soluzioni di problemi e di miglioramenti di un servizio. Contiene il software nuovo o modificato e qualsiasi hardware nuovo o modificato necessari per attuare le modifiche approvate.

8.1. Programmazione dei rilasci

La prima fase del processo assegna le modifiche autorizzate a pacchetti di rilasci e definisce la portata e il contenuto dei rilasci. Sulla base di queste informazioni, nell'ambito del sottoprocesso della pianificazione dei rilasci viene messo a punto un calendario per la costruzione, la prova e l'implementazione del rilascio.

La pianificazione dovrebbe stabilire:

— il campo di applicazione e il contenuto del rilascio;

— la valutazione del rischio e il profilo di rischio del rilascio;

— i clienti/utilizzatori interessati dal rilascio;

— la squadra responsabile del rilascio;

— la strategia di consegna e di implementazione;

— le risorse per il rilascio e l'implementazione.

Le due parti si informano reciprocamente in merito alla pianificazione dei rilasci e ai periodi di manutenzione. Se una versione interessa sia l'UE che la Svizzera, le due parti coordinano la pianificazione e definiscono un periodo di manutenzione comune.

8.2. Costruire e testare un pacchetto di rilasci

La fase di costruzione e di prova del processo di gestione del rilascio definisce le modalità di esecuzione del rilascio o del pacchetto di rilasci, avendo cura di mantenere gli ambienti controllati prima di modificare la produzione, e di testare tutte le modifiche in tutti gli ambienti di rilascio.

Se un rilascio interessa sia l'UE che la Svizzera, le due parti coordinano i piani di consegna e le prove. Questo coordinamento riguarda gli aspetti seguenti:

— come e quando le unità di rilascio e i componenti di servizio saranno consegnati;

— quali sono i tempi di realizzazione abituali; cosa succede in caso di ritardi;

— come seguire l'andamento delle consegne e ottenere una conferma;

— gli indicatori che consentono di monitorare e stabilire la riuscita dell'implementazione del rilascio;

— metodi di prova comuni per le funzionalità e le modifiche interessate.

Al termine di questo sottoprocesso, tutti i componenti necessari del rilascio sono pronti per entrare nella fase di implementazione vera e propria.

8.3. Preparare l'implementazione

Il sottoprocesso di preparazione assicura che i piani di comunicazione siano definiti correttamente, le notifiche siano pronte per essere inviate a tutti i portatori di interessi e agli utenti finali e il rilascio sia integrato nel processo di gestione delle modifiche per garantire che tutte le modifiche siano effettuate in modo controllato e approvate dai consessi competenti.

Qualora un rilascio riguardi sia l'UE che la Svizzera, le due parti coordinano le seguenti attività:

— registrazione della richiesta di modifica per programmare e preparare l'implementazione nell'ambiente di produzione;

— creazione del piano di attuazione;

— approccio del ritorno alla situazione precedente (*rollback*) in modo che, nel caso l'implementazione non vada a buon fine, si possa ripristinare lo stato precedente;

— invio di notifiche a tutte le parti interessate;

— richiesta di approvazione per l'esecuzione del rilascio dal livello di trattamento pertinente.

8.4. Ripristino della situazione precedente

Qualora l'implementazione non sia andata a buon fine o le prove abbiamo evidenziato che l'implementazione non è riuscita o non ha soddisfatto i criteri di accettazione/qualità concordati, le squadre di gestione dei rilasci di entrambe le parti dovranno ripristinare lo stato precedente. Tutti i portatori di interessi devono essere informati, compresi gli utilizzatori finali interessati/coinvolti. In attesa dell'approvazione, il processo può essere riavviato in una qualsiasi delle fasi precedenti.

8.5. Verifica e chiusura del rilascio

Al momento della verifica di un'implementazione, occorre:

— ottenere un feedback sulla soddisfazione dei clienti e degli utilizzatori e sulla qualità del servizio riguardo all'implementazione (raccogliere i feedback e valutare come migliorare costantemente il servizio);

— riesaminare i criteri di qualità che non sono stati rispettati;

— verificare che tutte le azioni, le correzioni e le modifiche necessarie siano state completate;

— garantire che al termine dell'implementazione non sussistano problemi legati alle funzionalità, alle risorse, alla capacità o alle prestazioni;

— verificare che eventuali problemi, errori noti e soluzioni di aggiramento siano documentati e accettati dal cliente, dagli utenti finali, dal sostegno operativo e dalle altre parti interessate;

— garantire il monitoraggio degli incidenti e dei problemi causati dall'implementazione (fornire un sostegno tempestivo alle squadre operative qualora il rilascio abbia comportato un aumento del carico del lavoro);

— aggiornare la documentazione di accompagnamento (ossia i documenti informativi tecnici);

— trasferire formalmente l'implementazione del rilascio alle operazioni di servizio;

— documentare gli insegnamenti tratti;

— recuperare il documento sintetico sul rilascio dalle squadre responsabili dell'implementazione;

— chiudere ufficialmente il rilascio dopo aver verificato la registrazione della richiesta di modifica.

9. GESTIONE DEGLI INCIDENTI DI SICUREZZA

La gestione degli incidenti di sicurezza è un processo per il trattamento di questo tipo di incidenti che consente di comunicare con i portatori di interessi potenzialmente coinvolti; di valutare e stabilire la priorità degli incidenti; di reagire per porre rimedio a qualsiasi violazione effettiva, sospettata o potenziale della riservatezza, della disponibilità o dell'integrità delle risorse di informazione riservate.

9.1. Classificazione degli incidenti relativi alla sicurezza delle informazioni

Tutti gli incidenti che hanno un impatto sul collegamento tra il registro dell'Unione e il registro svizzero sono analizzati per determinare un'eventuale violazione della riservatezza, dell'integrità o della disponibilità delle informazioni riservate registrate nell'elenco delle informazioni sensibili (EIR).

In tal caso, l'incidente è considerato un incidente relativo alla sicurezza delle informazioni, immediatamente registrato nello strumento informatico di gestione dei servizi informatici (ITSM) e gestito in quanto tale.

9.2. Trattamento degli incidenti relativi alla sicurezza delle informazioni

Gli incidenti di sicurezza sono posti sotto la responsabilità del 3º livello di trattamento e la risoluzione degli incidenti sarà trattata da una apposita squadra di gestione degli incidenti (*Incident management team* - IMT).

L'IMT è responsabile di:

— effettuare una prima analisi, classificare e valutare la gravità dell'incidente;

— coordinare le azioni di tutti i portatori di interessi, compresa la documentazione completa dell'analisi dell'incidente, le decisioni adottate per porre rimedio all'incidente e le eventuali carenze individuate;

— a seconda della gravità dell'incidente di sicurezza, trasferire tempestivamente le informazioni e/o le decisioni al livello più adeguato.

Nel processo di gestione della sicurezza delle informazioni, tutte le informazioni concernenti gli incidenti sono classificate al livello di riservatezza delle informazioni più elevato, e comunque non inferiore a «SENSITIVE: *ETS*».

Per un'indagine in corso e/o una carenza che potrebbe essere sfruttata e fino alla sua risoluzione, le informazioni sono classificate come «SPECIAL HANDLING: *ETS Critical*».

9.3. Individuazione degli incidenti di sicurezza

In base al tipo di evento di sicurezza, l'agente incaricato della sicurezza delle informazioni stabilisce quali siano le organizzazioni appropriate da coinvolgere e che faranno parte dell'IMT.

9.4. Analisi degli incidenti di sicurezza

L'IMT si mette in contatto con tutte le organizzazioni coinvolte e i membri competenti delle loro squadre, a seconda dei casi, per esaminare l'incidente. L'analisi consente di stabilire la portata della perdita di riservatezza, integrità o disponibilità di una risorsa di informazione e di valutare le conseguenze per tutte le organizzazioni interessate. Successivamente vengono definite le misure iniziali e di follow-up da adottare per risolvere l'incidente e gestirne l'impatto, nonché l'impatto di queste misure sulle risorse.

9.5. Valutazione della gravità dell'incidente di sicurezza, trasferimento dell'incidente al livello adeguato e elaborazione delle relazioni

L'IMT valuta la gravità di tutti i nuovi incidenti di sicurezza dopo la loro caratterizzazione come incidenti di sicurezza e avvia immediatamente le azioni necessarie in funzione della gravità dell'incidente.

9.6. Relazione in risposta ad un incidente

L'IMT include i risultati del contenimento degli incidenti e del ripristino del servizio nella relazione in risposta ad un incidente relativo alla sicurezza delle informazioni. La relazione è trasferita al 3º livello di trattamento utilizzando una email sicura o altri mezzi di comunicazione sicuri reciprocamente accettati.

La parte responsabile esamina i risultati del contenimento e del ripristino e:

— ricollega il registro in caso sia stato scollegato in precedenza;

— fornisce comunicazioni sull'incidente alle squadre del registro;

— chiude l'incidente.

Nella relazione sugli incidenti relativi alla sicurezza delle informazioni l'IMT dovrebbe riportare, in modo sicuro, i dettagli importanti al fine di garantire la coerenza della registrazione e della comunicazione e di consentire un intervento tempestivo e adeguato per contenere l'incidente. Dopo averla completata, l'IMT trasmette in tempo utile la relazione finale concernente l'incidente relativo alla sicurezza delle informazioni.

9.7. Monitoraggio, rafforzamento delle capacità e miglioramento continuo

L'IMT trasmette le relazioni relative a tutti gli incidenti di sicurezza al 3º livello di trattamento, che le utilizza al fine di determinare:

— i punti deboli nei controlli di sicurezza e/o nel funzionamento che devono essere rafforzati;

— l'eventuale necessità di rafforzare questa procedura per migliorare l'efficacia della risposta agli incidenti;

— le possibilità di formazione e di rafforzamento delle capacità per migliorare ulteriormente la resilienza dei sistemi di registri in presenza di incidenti relativi alla sicurezza delle informazioni, diminuire il rischio di incidenti futuri e ridurne al minimo l'impatto.

10. GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

La gestione della sicurezza delle informazioni mira a garantire la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati classificati e dei servizi informatici sensibili di un'organizzazione. Oltre alle componenti tecniche, compresa la loro progettazione e il loro collaudo (cfr. NTC), per soddisfare le prescrizioni in materia di sicurezza per il collegamento permanente dei registri sono necessarie le seguenti procedure operative comuni.

10.1. Individuazione delle informazioni riservate

La riservatezza di un'informazione viene valutata determinando il livello di impatto sull'attività (ad es. perdite finanziarie, degrado dell'immagine, violazione del diritto…) di una violazione della sicurezza relativa all'informazione in questione.

Le risorse di informazione riservate sono caratterizzate in funzione del loro impatto sul collegamento.

Il livello di sensibilità di queste informazioni è valutato in base alla scala di sensibilità applicabile a questo collegamento e illustrata nella sezione «Trattamento degli incidenti relativi alla sicurezza delle informazioni» del presente documento.

10.2. Livelli di riservatezza delle risorse di informazione

Al momento della sua caratterizzazione, la risorsa di informazione è classificata in base alle regole seguenti:

— l'individuazione di almeno un livello ELEVATO di riservatezza, integrità o disponibilità comporta la classificazione della risorsa come «SPECIAL HANDLING: *ETS Critical*»;

— l'individuazione di almeno un livello MEDIO di riservatezza, integrità o disponibilità comporta la classificazione della risorsa come «SENSITIVE: *ETS*»;

— l'individuazione di un livello BASSO di riservatezza, integrità o disponibilità comporta la classificazione della risorsa come Classificazione UE: SENSITIVE: *ETS Joint Procurement*. Classificazione CH: LIMITED: ETS.

10.3. Designazione del titolare della risorsa di informazione

Tutte le risorse di informazione dovrebbero avere un titolare designato. Le risorse di informazione dell'ETS che fanno parte o sono associate al collegamento tra l'EUTL e l'SSTL dovrebbero figurare in un elenco di inventario delle risorse comuni, gestito da entrambe le parti. Le risorse di informazione dell'ETS che non riguardano il collegamento tra l'EUTL e l'SSTL dovrebbero figurare in un elenco di inventario delle risorse, gestito dalla parte interessata.

La titolarità di ogni risorsa di informazione che fa parte o è associata al collegamento tra l'EUTL e l'SSTL deve essere concordata dalle parti. Il titolare di una risorsa di informazione è responsabile della valutazione della sensibilità di tale risorsa.

Il titolare dovrebbe avere un livello di responsabilità adeguato rispetto al valore della o delle risorse assegnate. La responsabilità del titolare in relazione alla o alle risorse e l'obbligo di garantire il livello richiesto di riservatezza, integrità e riservatezza dovrebbero essere concordati e formalizzati.

10.4. Registrazione delle informazioni riservate

Tutte le informazioni sensibili sono registrate nell'elenco delle informazioni riservate (EIR).

Se del caso, il raggruppamento di informazioni riservate che potrebbe comportare un impatto più elevato rispetto ad una singola informazione è preso in considerazione e registrato nell'EIR (ad esempio una serie di informazioni archiviate nella banca dati del sistema).

L'EIR non è statico. Le minacce, le vulnerabilità, la probabilità o le conseguenze degli incidenti di sicurezza legati alle risorse possono cambiare senza preavviso e possono essere introdotte nuove risorse nel funzionamento dei sistemi di registri.

L'EIR è pertanto riesaminato periodicamente e qualsiasi nuova informazione ritenuta sensibile deve essere immediatamente registrata nell'EIR.

Per ogni voce l'EIR contiene almeno le seguenti informazioni:

— la descrizione dell'informazione;

— il titolare dell'informazione;

— il livello di riservatezza;

— l'eventuale indicazione che l'informazione include dati personali;

— informazioni aggiuntive se necessarie.

10.5. Trattamento delle informazioni sensibili

Quando sono trattate al di fuori del collegamento tra il registro dell'Unione e il registro della Svizzera, le informazioni sensibili sono gestite conformemente alle istruzioni di trattamento.

Le informazioni riservate utilizzate dal collegamento tra il registro dell'Unione e il registro svizzero sono trattate dalle parti conformemente alle prescrizioni di sicurezza.

10.6. Gestione dell'accesso

L'obiettivo della gestione dell'accesso è di concedere agli utenti autorizzati il diritto di utilizzare un servizio, impedendo nel contempo l'accesso agli utenti non autorizzati. La gestione dell'accesso è talvolta indicata anche come «Gestione dei diritti» o «Gestione dell'identità».

Per il collegamento permanente dei registri e il suo funzionamento, entrambe le parti devono avere accesso ai seguenti elementi:

— Wiki ambiente di collaborazione per lo scambio di informazioni comuni, come la pianificazione dei rilasci;

— strumento di gestione dei servizi informatici (ITSM) per la gestione degli incidenti e dei problemi (cfr. capitolo 3, «Approccio e norme»).

— sistema di scambio di messaggi: ciascuna parte predispone un sistema sicuro di scambio di messaggi per la trasmissione dei messaggi contenenti i dati sulle operazioni.

L'amministratore del registro della Svizzera e l'amministratore centrale dell'Unione garantiscono che gli accessi siano aggiornati e fungono, per le rispettive parti, da punti di contatto per quanto riguarda le attività di gestione dell'accesso. Le richieste di accesso sono trattate conformemente alle procedure per il soddisfacimento delle richieste.

10.7. Gestione di certificati/chiavi

Ciascuna parte è responsabile della gestione dei propri certificati/chiavi (generazione, registrazione, stoccaggio, installazione, utilizzo, rinnovo, revoca, backup e recupero dei certificati/chiavi). Come indicato nelle norme tecniche di collegamento (NTC), sono utilizzati solo i certificati digitali rilasciati da un'autorità di certificazione (AC) ritenuta affidabile da entrambe le parti. Il trattamento e l'archiviazione di certificati/chiavi devono rispettare le disposizioni stabilite nelle istruzioni di trattamento.

La revoca e/o il rinnovo di certificati e chiavi sono coordinati da entrambe le parti. Ciò avviene secondo le procedure per il soddisfacimento delle richieste.

L'amministratore del registro della Svizzera e l'amministratore centrale dell'Unione procederanno a uno scambio di certificati/chiavi tramite mezzi di comunicazione sicuri conformemente alle disposizioni di cui alle istruzioni di trattamento.

Tutte le verifiche dei certificati/delle chiavi tra le parti avverranno fuori banda indipendentemente dal mezzo utilizzato.

ALLEGATO III

NORME TECNICHE DI COLLEGAMENTO (NTC) A NORMA DELL'ARTICOLO 3, PARAGRAFO 7, DELL'ACCORDO TRA L'UNIONE EUROPEA E LA CONFEDERAZIONE SVIZZERA CONCERNENTE IL COLLEGAMENTO DEI RISPETTIVI SISTEMI DI SCAMBIO DI QUOTE DI EMISSIONE DI GAS A EFFETTO SERRA

Norme per il collegamento permanente dei registri

Sommario

1.	GLOSSARIO	23
2.	INTRODUZIONE	25
2.1.	Ambito di applicazione	25
2.2.	Destinatari	25
3.	DISPOSIZIONI GENERALI	25
3.1.	Architettura del collegamento di comunicazione	25
3.1.1.	Scambio di messaggi	26
3.1.2.	Messaggio XML — Descrizione generale	26
3.1.3.	Finestre di immissione	26
3.1.4.	Flussi di messaggi delle operazioni	27
3.2.	Sicurezza del trasferimento dei dati	29
3.2.1.	Firewall e interconnessione della rete	29
3.2.2.	Rete privata virtuale (virtual private network - VPN)	29
3.2.3.	Attuazione dell'IPSec	29
3.2.4.	Protocollo di trasferimento sicuro per lo scambio di messaggi	30
3.2.5.	Firma e cifratura XLM	30
3.2.6.	Chiavi crittografiche	30
3.3.	Elenco delle funzioni nell'ambito del collegamento	30
3.3.1.	Operazioni «business»	30
3.3.2.	Protocollo di riconciliazione	31
3.3.3.	Messaggio di prova	31
3.4.	Requisiti relativi alla registrazione dei dati	31
3.5.	Requisiti operativi	32
4.	DISPOSIZIONI RELATIVE ALLA DISPONIBILITÀ	32
4.1.	Progettazione della disponibilità delle comunicazioni	32
4.2.	Piano di attivazione, comunicazione, riattivazione e prove	33
4.2.1.	Prove dell'infrastruttura TIC in interno	33
4.2.2.	Prove di comunicazione	33
4.2.3.	Prove sull'intero sistema (end-to-end)	33
4.2.4.	Prove di sicurezza	33
4.3.	Ambienti di accettazione/prova	34
5.	DISPOSIZIONI IN MATERIA DI RISERVATEZZA E INTEGRITÀ	34
5.1.	Infrastruttura per le prove di sicurezza	34
5.2.	Disposizioni relative alla sospensione e alla riattivazione del collegamento	35

5.3. Disposizioni in materia di violazioni della sicurezza 35
5.4. Linee guida in materia di prove di sicurezza 35
5.4.1. Software 35
5.4.2. Infrastruttura 36
5.5. Disposizioni in materia di valutazione dei rischi 36

1. GLOSSARIO

Tabella 1-1: Acronimi e definizioni del settore

Acronimo/termine	Definizione
CH	Confederazione svizzera
CHU	Tipo di diritto fisso, altrimenti detto CHU2 (con riferimento al secondo periodo di impegno del protocollo di Kyoto), rilasciato dalla Svizzera.
CHUA	Quota svizzera assegnata al trasporto aereo
ETR (*Emissions Trading registry*)	Registro dello scambio di quote di emissione
ETS (*Emission Trading system*)	Sistema di scambio di quote di emissione
EUA	Quota generale dell'UE
EUAA	Quota di emissione del trasporto aereo dell'UE
EUCR	Registro consolidato dell'Unione europea
EUTL	Catalogo delle operazioni dell'Unione europea
Operazione	Un processo in un registro che include il trasferimento di una quota da un conto a un altro conto
POC	Procedure operative comuni. Procedure elaborate congiuntamente per rendere operativo il collegamento tra l'EU ETS e l'ETS della Svizzera.
Quota di emissione	Il diritto di emettere una tonnellata di biossido di carbonio equivalente per un periodo determinato, valido unicamente per rispettare gli obblighi dell'ETS di ciascun soggetto.
Registro	Un sistema contabile per le quote rilasciate nell'ambito dell'ETS, che tiene traccia della titolarità delle quote detenute in conti elettronici.
Sistema di catalogo delle operazioni	Il catalogo delle operazioni contiene la registrazione di tutte le operazioni proposte inviate da un registro all'altro registro.
SSTL	Libro di bordo elettronico supplementare della Svizzera
UE	Unione europea

Tabella 1-2 Definizioni e acronimi tecnici

Acronimo	Definizione
Autorità di certificazione (AC)	Organismo che rilascia certificati digitali
Chiave crittografica	Un'informazione che determina il risultato funzionale di un algoritmo crittografico.
Cifratura	Il processo di conversione di informazioni o dati in un codice, in particolare per impedire l'accesso non autorizzato.
Crittografia asimmetrica	Utilizza chiavi pubbliche e private per cifrare e decifrare i dati.
Decifratura	Processo inverso della cifratura.
Firewall	Apparecchio o software per la sicurezza delle reti che monitora e controlla il traffico in entrata e in uscita in base a regole predeterminate.
Firma digitale	Tecnica matematica usata per convalidare l'autenticità e l'integrità di un messaggio, un software o un documento elettronico.
Immissione di file	Il processo di lettura di un file.
IPSec	Sicurezza IP. Suite di protocolli di reti che autentifica e cripta i pacchetti di dati per fornire una comunicazione cifrata sicura tra due computer su una rete IP.
Monitoraggio «Heartbeat» (strumento di diagnostica continua)	Segnale periodico generato e monitorato da hardware o software per indicare il funzionamento normale o per sincronizzare altre parti di un sistema informatico.
Processo di riconciliazione	Processo che mira a garantire la concordanza di due insiemi di registrazioni.
Test di penetrazione	Pratica che consiste nel testare un sistema informatico, una rete o un'applicazione web per individuare le vulnerabilità in materia di sicurezza che l'autore di un attacco potrebbe sfruttare.
VPN	Rete privata virtuale (*Virtual Private Network*).
XML	Linguaggio di marcatura estensibile (*Extensible Mark-up Language*). Questo linguaggio permette ai progettisti di creare tag personalizzati, che consentono la definizione, la trasmissione, la convalida e l'interpretazione di dati tra applicazioni e tra organizzazioni.

2. INTRODUZIONE

L'accordo tra l'Unione europea e la Confederazione svizzera concernente il collegamento dei rispettivi sistemi di scambio di quote di emissione di gas a effetto serra, del 23 novembre 2017 («l'accordo»), prevede il riconoscimento reciproco delle quote di emissione che possono essere utilizzate per conformarsi al sistema di scambio di quote di emissione dell'Unione europea (EU ETS) o al sistema di scambio di quote di emissione della Svizzera (ETS della Svizzera). Per rendere operativo il collegamento tra l'EU ETS e l'ETS della Svizzera, sarà stabilito un collegamento diretto tra il catalogo delle operazioni dell'Unione europea (EUTL) del registro dell'Unione e il libro di bordo elettronico supplementare della Svizzera (SSTL) del registro svizzero tale da consentire il trasferimento da un registro all'altro delle quote di emissioni rilasciate nell'ambito dei due ETS (articolo 3, paragrafo 2, dell'accordo). Nel 2020 è stata attuata una soluzione provvisoria per rendere operativo il collegamento tra l'EU ETS e l'ETS della Svizzera. A partire dal 2023, il collegamento tra i due sistemi di scambio di quote di emissione si trasformerà gradualmente in un collegamento permanente dei registri, la cui attuazione è prevista entro il 2024, che consentirà ai mercati collegati, in termini di vantaggi derivanti dalla liquidità del mercato e dall'esecuzione di operazioni tra i due sistemi collegati, di funzionare in modo equivalente a un mercato composto da due sistemi che si presenta ai partecipanti come un unico mercato, subordinatamente alle sole disposizioni regolamentari individuali delle parti (allegato II dell'accordo).

A norma dell'articolo 3, paragrafo 7, dell'accordo, l'amministratore del registro della Svizzera e l'amministratore centrale dell'Unione stabiliscono norme tecniche di collegamento (NTC) basate sui principi di cui all'allegato II dell'accordo, descrivendo in dettaglio le disposizioni per l'istituzione di una connessione solida e sicura tra l'SSTL e l'EUTL. Le NTC elaborate dagli amministratori entrano in vigore una volta adottate con decisione del comitato misto.

Le NTC sono state adottate dal comitato misto con decisione n. 2/2020. Le NTC aggiornate descritte nel presente documento saranno adottate dal comitato misto conformemente alla decisione n. 1/2024. Conformemente alla presente decisione e a quanto chiesto dal comitato misto, l'amministratore del registro della Svizzera e l'amministratore centrale dell'Unione hanno elaborato e aggiorneranno ulteriori orientamenti tecnici per rendere operativo il collegamento e di garantire che tali orientamenti siano costantemente adattati al progresso tecnico e/o alle nuove prescrizioni relative alla sicurezza interna ed esterna del collegamento e al suo funzionamento efficace ed efficiente.

2.1. Ambito di applicazione

Il presente documento rappresenta l'intesa comune tra le parti dell'accordo per quanto riguarda la definizione delle procedure di base del collegamento tra i registri dell'EU ETS e l'ETS della Svizzera. Descrive a grandi linee la base di riferimento per le specifiche tecniche in termini di requisiti di architettura, servizio e sicurezza, ma saranno necessari ulteriori orientamenti tecnici per rendere operativo il collegamento.

Per il corretto funzionamento del collegamento, occorreranno processi e procedure che ne rafforzino l'operatività. A norma dell'articolo 3, paragrafo 6, dell'accordo, tali aspetti sono trattati dettagliatamente in un documento separato relativo alle procedure operative comuni (POC), da adottare separatamente mediante decisione del comitato misto.

2.2. Destinatari

I destinatari del presente documento sono l'amministratore del registro svizzero e l'amministratore centrale dell'Unione.

3. DISPOSIZIONI GENERALI

3.1. Architettura del collegamento di comunicazione

Lo scopo della presente sezione è fornire una descrizione dell'architettura generale per la messa in opera del collegamento tra l'EU ETS e l'ETS della Svizzera e le diverse componenti coinvolte.

Poiché la sicurezza è un elemento fondamentale per la definizione dell'architettura del collegamento dei registri, sono state adottate tutte le misure per disporre di un'architettura solida. Il collegamento permanente dei registri utilizza un meccanismo di scambio di file, come attuazione di una connessione sicura *air gap*.

La soluzione tecnica utilizza:

— un protocollo di trasferimento sicuro per lo scambio di messaggi;

— messaggi XML;

— la firma digitale e la cifratura basate su XLM;

— VPN.

3.1.1. Scambio di messaggi

La comunicazione tra il registro dell'Unione e il registro svizzero si basa su un meccanismo di scambio di messaggi attraverso canali protetti. Ciascun ETS dispone del proprio archivio dei messaggi ricevuti.

Entrambe le parti conservano un registro dei messaggi ricevuti, unitamente ai dettagli relativi al trattamento.

Occorre segnalare gli errori o gli stati non previsti, come gli avvisi, e le squadre di sostegno dovrebbero interagire opportunamente fra loro.

Gli errori e gli eventi imprevisti sono trattati nel rispetto delle procedure operative stabilite nel processo di gestione degli incidenti delle POC.

3.1.2. Messaggio XML — Descrizione generale

Un messaggio XML contiene uno degli elementi seguenti:

— una o più richieste di operazioni e/o una o più risposte a operazioni;

— un'operazione/una risposta relativa alla procedura di conciliazione;

— un messaggio di prova.

Ciascun messaggio contiene un'intestazione che riporta:

— il sistema ETS da cui proviene (ETS di origine);

— il numero di sequenza.

3.1.3. Finestre di immissione

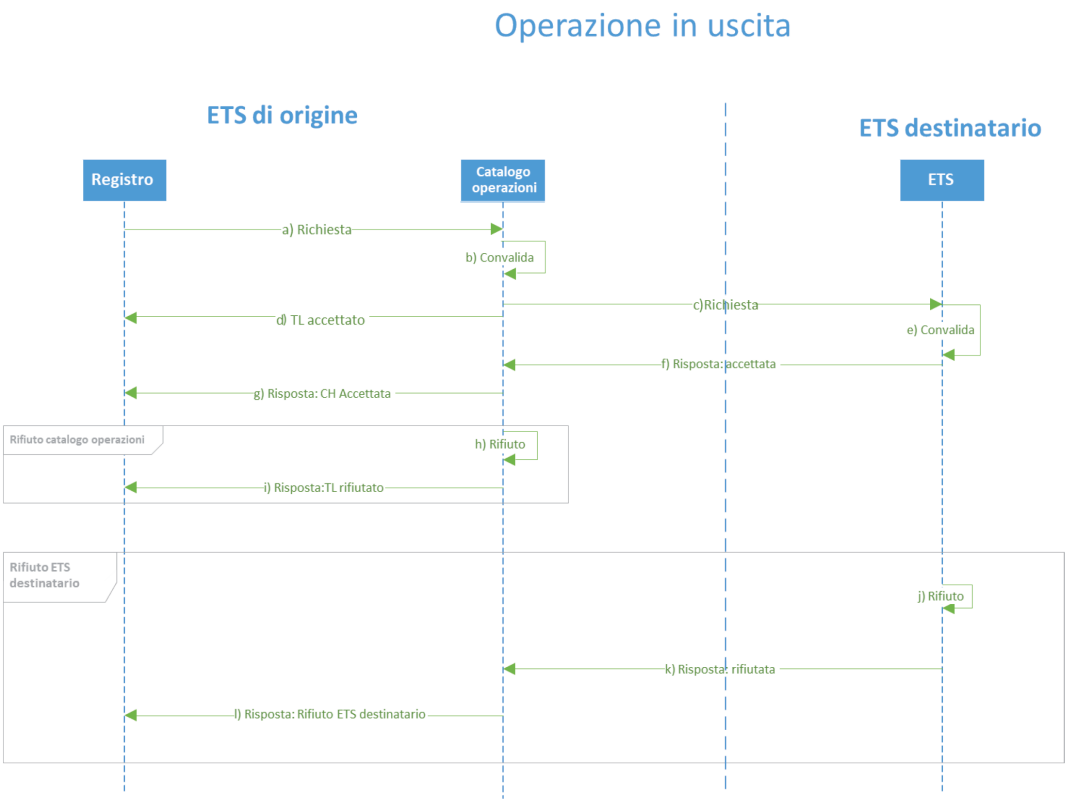
Il collegamento permanente dei registri si basa su finestre predefinite di immissione, seguite da una serie di eventi designati. Le richieste di operazioni ricevute attraverso il collegamento possono essere immesse solo a intervalli prestabiliti. Le finestre di immissione comprendono una convalida tecnica per le operazioni in entrata e in uscita. Inoltre, le riconciliazioni possono essere effettuate su base giornaliera e possono essere avviate manualmente.

Le modifiche nella frequenza/tempistica di tutti questi eventi saranno trattate nel rispetto delle procedure operative stabilite nel processo di gestione degli incidenti delle POC.

3.1.4. Flussi di messaggi delle operazioni

Operazioni in uscita

Queste operazioni riflettono il punto di vista dell'ETS di origine. Il flusso specifico è illustrato nel seguente grafico della sequenza:



Il flusso principale mostra le seguenti fasi (cfr. disegno sopra):

a) nell'ETS di origine la richiesta di operazione è inviata dal registro al catalogo delle operazioni, una volta terminati tutti i tempi di attesa di lavoro (24 ore, se del caso).

b) Il catalogo delle operazioni convalida la richiesta di operazione.

c) La richiesta di operazione è inviata all'ETS destinatario.

d) La risposta di accettazione è inviata al registro ETS di origine.

e) L'ETS destinatario convalida la richiesta di operazione.

f) L'ETS destinatario invia la risposta di accettazione al catalogo delle operazioni dell'ETS di origine.

g) Il catalogo delle operazioni invia la risposta di accettazione al registro.

Flusso alternativo «Rifiuto catalogo operazioni» (cfr. disegno di cui sopra, partendo dalla lettera a) del flusso principale):

a) Nel sistema di origine la richiesta di operazione è inviata dal registro al catalogo delle operazioni, una volta trascorsi tutti i tempi di attesa di lavoro (24 ore, se del caso).

b) Il catalogo delle operazioni non convalida la richiesta

c) Il messaggio di rifiuto è inviato al registro di origine.

Flusso alternativo «Rifiuto ETS» (cfr. disegno di cui sopra, partendo dalla lettera d) del flusso principale):

a) Nell'ETS di origine la richiesta di operazione è inviata dal registro al catalogo delle operazioni, una volta trascorsi tutti i tempi di attesa di lavoro (24 ore, se del caso).

b) Il catalogo delle operazioni convalida l'operazione.

c) La richiesta di operazione è inviata all'ETS destinatario.

d) Il messaggio di accettazione è inviato al registro dell'ETS di origine.

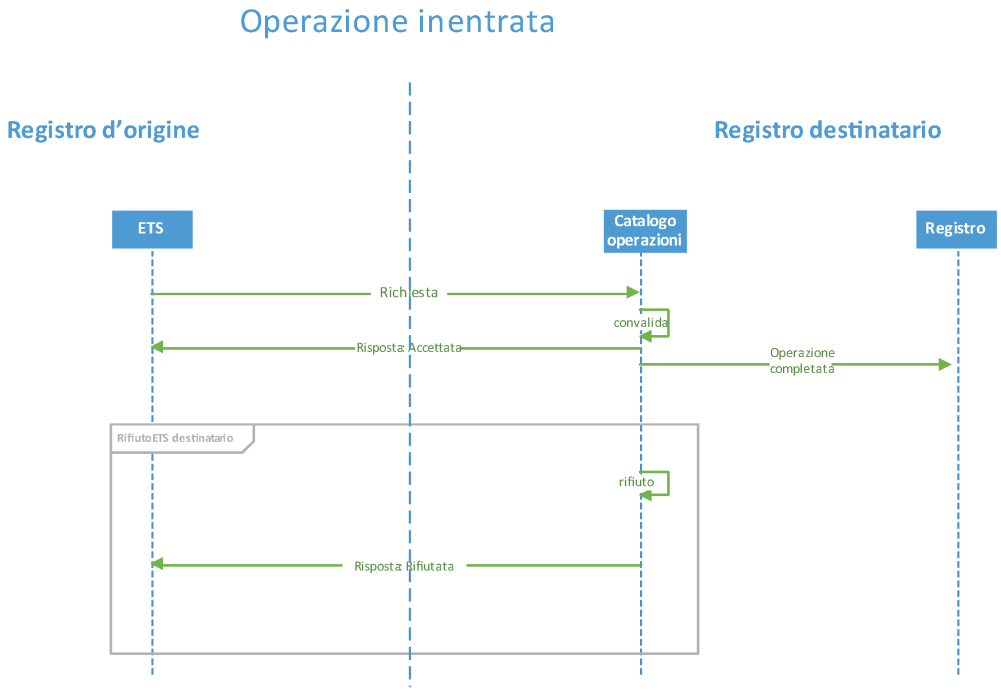
e) Il catalogo delle operazioni dell'ETS destinatario non convalida l'operazione.

f) L'ETS destinatario invia la risposta di rifiuto al catalogo delle operazioni dell'ETS di origine.

g) Il catalogo delle operazioni trasmette il rifiuto al registro.

Operazioni in entrata

Queste operazioni riflettono il punto di vista dell'ETS destinatario. Il flusso specifico è illustrato nel seguente grafico della sequenza:



Il grafico indica:

1) quando il catalogo delle operazioni dell'ETS destinatario convalida la richiesta, invia il messaggio di accettazione all'ETS di origine e un messaggio «operazione completata» al registro dell'ETS destinatario;

2) quando una richiesta in entrata viene rifiutata nel catalogo delle operazioni del destinatario, la richiesta di operazione non è inviata al registro dell'ETS destinatario.

Protocollo

Il ciclo dei messaggi delle operazioni comporta solo due messaggi:

— Proposta di operazione dall'ETS di origine à all'ETS destinatario.

— Risposta dall'ETS destinatario à all'ETS di origine circa l'operazione: accettata o rifiutata (includendo il motivo del rifiuto).

  — accettata: l'operazione è completata.

  — rifiutata: l'operazione è interrotta.

Status delle operazioni

— Lo status dell'operazione dell'ETS di origine sarà impostato su «proposta» («*proposed*») al momento dell'invio della richiesta.

— Lo status dell'operazione dell'ETS destinatario sarà impostato su «proposta» («*proposed*») al momento del ricevimento della richiesta e nel corso del suo trattamento.

— Lo status dell'operazione dell'ETS destinatario sarà impostato su «completata»/«interrotta» («*completed*»/«*terminated*») al termine del trattamento della proposta. L'ETS destinatario invierà quindi il messaggio di accettazione/rifiuto corrispondente.

— Lo status dell'operazione dell'ETS di origine sarà impostato su «completata»/«interrotta» («*completed*»/«*terminated*») quando il messaggio di accettazione/rifiuto viene ricevuto e nel corso del suo trattamento.

— Nell'ETS di origine lo status dell'operazione rimane «proposta» («*proposed*») fino a quando non arriva una risposta.

— Lo status dell'operazione dell'ETS destinatario imposterà su «interrotta» («*terminated*») se qualsiasi operazione proposta risulti come «proposta» («*proposed*») per oltre 30 minuti.

Gli incidenti relativi alle operazioni saranno trattati nel rispetto delle procedure operative stabilite nel processo di gestione degli incidenti delle POC.

3.2. Sicurezza del trasferimento dei dati

I dati in transito sono soggetti a quattro livelli di sicurezza:

1) controllo dell'accesso alla rete: firewall e strato dell'interconnessione di rete.

2) cifratura a livello di trasporto: VPN.

3) cifratura a livello di sessione: protocollo di trasferimento sicuro per lo scambio di messaggi.

4) cifratura a livello di applicazione: firma e cifratura XLM del contenuto.

3.2.1. Firewall e interconnessione della rete

Il collegamento è stabilito mediante una rete protetta da un firewall hardware. Il firewall è configurato secondo norme che permettono unicamente ai clienti «registrati» di effettuare collegamenti con il server VPN.

3.2.2. Rete privata virtuale (virtual private network – VPN)

Tutte le comunicazioni tra le parti sono protette mediante una tecnologia VPN. Le tecnologie VPN consentono di trasportare informazioni da un punto ad un altro attraverso un canale sicuro (tunnel) su una rete, come l'Internet, proteggendo l'insieme delle comunicazioni. Prima della creazione del tunnel VPN, un certificato digitale è rilasciato a un endpoint del potenziale cliente, consentendo a quest'ultimo di fornire la prova della sua identità durante la negoziazione della connessione. Ciascuna parte è responsabile dell'installazione del certificato nel proprio endpoint VPN. Utilizzando certificati digitali, ogni endpoint del server VPN avrà accesso ad un'autorità centrale per negoziare le credenziali di autenticazione. Durante il processo di creazione del tunnel, viene negoziata la cifratura, il che garantisce la protezione di tutte le comunicazioni che transitano nel tunnel.

Gli endpoint VPN del cliente sono configurati in modo che il tunnel resti sempre aperto al fine di consentire in qualsiasi momento una comunicazione affidabile, bidirezionale e in tempo reale tra le parti.

Solitamente l'Unione europea utilizza la rete di servizi transeuropei sicuri per la comunicazione telematica tra amministrazioni (sTESTA) come rete privata IP. Pertanto tale rete è adatta anche al collegamento permanente dei registri.

3.2.3. Attuazione dell'IPSec

L'utilizzo del protocollo IPSec per istituire l'infrastruttura VPN da sito a sito consentirà l'autenticazione, l'integrità dei dati e la cifratura dei dati da sito a sito. Le configurazioni VPN IPSec garantiscono un'adeguata autenticazione tra due endpoint in un collegamento VPN. Le parti individueranno e autenticheranno il cliente remoto tramite la connessione IPSec utilizzando i certificati digitali forniti da un'autorità di certificazione riconosciuta dall'altro ETS.

L'IPsec garantisce inoltre l'integrità dei dati di tutte le comunicazioni che transitano nel tunnel VPN. I pacchetti di dati sono sottoposti alla tecnica crittografica *hash* e firmati utilizzando le informazioni di autenticazione determinate dalla VPN. Anche la riservatezza dei dati è garantita mediante la cifratura IPSec.

3.2.4. Protocollo di trasferimento sicuro per lo scambio di messaggi

Il collegamento permanente dei registri ricorre ad una cifratura a più livelli che consente lo scambio sicuro di dati tra le parti. I due sistemi e i loro diversi ambienti sono interconnessi a livello di rete mediante tunnel VPN. A livello di applicazione i file sono trasferiti mediante un protocollo di trasferimento sicuro a livello di sessione.

3.2.5. Firma e cifratura XLM

Nei file XML, la firma e la cifratura sono effettuate su due livelli. Tutte le richieste di operazione, le risposte di operazione e i messaggi di riconciliazione sono firmati elettronicamente.

In una seconda fase, ogni sottoelemento dell'elemento «messaggio» è criptato separatamente.

Inoltre, nella terza fase, per garantire l'integrità e la non disconoscibilità dell'intero messaggio, l'elemento radice del messaggio è firmato elettronicamente. Ne consegue un elevato livello di protezione dei dati XML incorporati. L'esecuzione tecnica rispetta le norme del Consorzio mondiale del Web (W3C).

Per decifrare e verificare il messaggio, si segue lo stesso processo in ordine inverso.

3.2.6. Chiavi crittografiche

Per la cifratura e la firma si utilizzerà la crittografia a chiave pubblica.

Nel caso specifico dell'IPSec, viene utilizzato un certificato digitale rilasciato da un'autorità di certificazione ritenuta affidabile da entrambe le parti. L'AC in questione verifica l'identità del titolare del certificato e rilascia certificati che sono utilizzati per identificare formalmente un'organizzazione e istituire canali sicuri di comunicazione di dati tra le parti.

Le chiavi crittografiche sono usate per firmare e criptare canali di comunicazione e file di dati. Le parti si scambiano per via elettronica, attraverso canali protetti, i certificati pubblici che vengono verificati fuori banda. Questa procedura è parte integrante del processo di gestione della sicurezza delle informazioni delle POC.

3.3. Elenco delle funzioni nell'ambito del collegamento

Il collegamento comprende le specifiche del sistema di trasmissione per una serie di funzioni che attuano i processi «business» derivanti dall'accordo. Il collegamento include anche le specifiche per il processo di riconciliazione e i messaggi di prova che consentiranno l'attuazione di un sistema di monitoraggio *heartbeat*.

3.3.1. Operazioni «business»

Dal punto di vista «business», nell'ambito del collegamento sono previsti quattro (4) tipi di richieste di operazioni:

— Trasferimenti esterni

  — Dopo l'entrata in funzione del collegamento dei sistemi ETS, le quote dell'UE e le quote della Svizzera sono fungibili e dunque totalmente trasferibili tra le parti.

  — Un trasferimento effettuato tramite il collegamento presuppone un conto di origine su un ETS e un conto destinatario sull'altro ETS.

  — Il trasferimento può riguardare qualsiasi quantità dei quattro (4) tipi di quote:

    — Quote generiche della Svizzera (CHU)

    — Quote assegnate al trasporto aereo della Svizzera (CHUA)

    — Quote generiche dell'UE (EUA)

    — Quote assegnate al trasporto aereo UE (EUAA)

— Assegnazione internazionale:

  Gli operatori aerei amministrati da un ETS che hanno degli obblighi nei confronti dell'altro ETS e hanno il diritto di ricevere quote a titolo gratuito da questo secondo ETS, riceveranno gratuitamente quote di trasporto aereo da quest'ultimo, mediante un'operazione di assegnazione internazionale.

— Annullamento di un'assegnazione internazionale:

Questa operazione viene effettuata qualora occorra annullare l'insieme delle quote assegnate a titolo gratuito versate sul conto di deposito di un operatore aereo dall'altro ETS.

— Restituzione di quote in eccesso:

Procedura analoga a quella dell'annullamento, ma in cui non occorre annullare tutte le quote assegnate poiché devono essere restituite all'ETS che le ha assegnate solo le quote in eccesso.

3.3.2. Protocollo di riconciliazione

Le riconciliazioni avvengono unicamente dopo la chiusura delle finestre per l'immissione, la convalida e il trattamento dei messaggi.

Le riconciliazioni sono parte integrante delle misure di sicurezza e di coerenza del collegamento. Le parti concorderanno l'esatta tempistica delle riconciliazioni prima di stabilire un calendario. Con l'accordo di entrambe le parti si possono effettuare riconciliazioni giornaliere programmate. Dopo ciascuna immissione sarà effettuata almeno una riconciliazione programmata.

In ogni caso ciascuna parte può procedere in qualsiasi momento a riconciliazioni manuali.

Le modifiche della tempistica e della frequenza delle riconciliazioni programmate saranno trattate nel rispetto delle procedure operative stabilite nel processo di gestione degli incidenti delle POC.

3.3.3. Messaggio di prova

Per verificare la comunicazione end-to-end è previsto un messaggio di prova. Il messaggio conterrà dati che lo identificheranno come messaggio di prova e una volta pervenuto all'altro ETS questi invierà una risposta

3.4. Requisiti relativi alla registrazione dei dati

Per rispondere all'esigenza di entrambe le parti di garantire l'accuratezza e la coerenza delle informazioni e per fornire loro strumenti da utilizzare nel processo di riconciliazione per eliminare le incoerenze, entrambe le parti conservano quattro (4) tipi di registrazioni di dati:

— cataloghi delle operazioni;

— cataloghi delle riconciliazioni;

— archivio dei messaggi;

— cataloghi degli audit interni.

Tutti i dati di tali cataloghi dovranno essere conservati almeno per tre (3) mesi ai fini della risoluzione di problemi; la loro ulteriore conservazione ai fini di audit dipenderà invece dalla legge applicabile a ciascun ETS. I file dei cataloghi che risalgono a più di tre (3) mesi possono essere archiviati in un sistema informatico indipendente sicuro, a condizione che possano essere recuperati o vi si possa accedere entro un termine ragionevole.

Cataloghi delle operazioni

I cataloghi delle operazioni sono attuati nei sottosistemi EUTL e SSTL.

Più specificamente, i cataloghi delle operazioni registrano ogni operazione proposta inviata all'altro ETS. Ciascuna registrazione contiene tutti i campi relativi al contenuto dell'operazione e al suo risultato (la risposta dell'ETS destinatario). I cataloghi delle operazioni registrano le operazioni in entrata e le risposte inviate all'ETS di origine.

Cataloghi delle riconciliazioni

Il catalogo delle riconciliazioni contiene la registrazione di tutti i messaggi di riconciliazione scambiati tra le due parti, ivi compresi l'identificatore, la marcatura temporale e il risultato della riconciliazione: Status della riconciliazione «Superata» («*Pass*») o «Discrepanze» («*Discrepancies*»). Nel collegamento permanente dei registri i messaggi di riconciliazione sono parte integrante dei messaggi scambiati e sono pertanto conservati come descritto nella sezione «Archivio dei messaggi».

Entrambe le parti registrano le singole richieste e le relative risposte nel catalogo delle riconciliazioni. Anche se le informazioni contenute in questo catalogo non sono condivise direttamente nell'ambito della procedura di conciliazione vera e propria, l'accesso a tali informazioni potrebbe essere necessario per eliminare le incoerenze.

Archivio dei messaggi

Entrambe le parti sono tenute ad archiviare una copia dei dati scambiati (file XLM), inviati e ricevuti, indicando se il formato di questi messaggi XLM è corretto.

Questo archivio è utilizzato principalmente a fini di audit, per disporre di una prova di quello che è stato inviato e ricevuto da entrambe le parti. In quest'ottica, insieme ai file, occorre archiviare anche i relativi certificati.

Questi file forniscono inoltre informazioni aggiuntive ai fini della soluzione di eventuali problemi.

Cataloghi degli audit interni

Questi cataloghi sono predisposti e utilizzati da ciascuna parte separatamente.

3.5. Requisiti operativi

Nel collegamento permanente dei registri lo scambio di dati tra i due sistemi non è totalmente autonomo: sono infatti necessari operatori e procedure per rendere operativo il collegamento. A tal fine in questo processo sono descritti in dettaglio diversi ruoli e strumenti.

4. DISPOSIZIONI RELATIVE ALLA DISPONIBILITÀ

4.1. Progettazione della disponibilità delle comunicazioni

Fondamentalmente l'architettura del collegamento permanente dei registri consiste in un'infrastruttura TIC e un software che consentono la comunicazione tra l'ETS della Svizzera e l'EU ETS. Garantire livelli elevati di disponibilità, integrità e riservatezza per questo flusso di dati diventa pertanto un aspetto essenziale di cui tenere conto nella progettazione del collegamento permanente dei registri. Trattandosi di un progetto nel quale l'infrastruttura TIC, il software personalizzato e i processi svolgono un ruolo fondamentale, per progettare un sistema resiliente occorre tenere conto di questi tre elementi.

Resilienza dell'infrastruttura TIC

Il capitolo sulle disposizioni generali del presente documento descrive in dettaglio gli elementi costitutivi dell'architettura. Per quanto riguarda l'infrastruttura TIC, nell'ambito del collegamento permanente dei registri, è stata istituita una rete VPN resiliente che crea dei tunnel di comunicazione sicuri mediante i quali i messaggi possono essere scambiati in modo sicuro. Altri elementi dell'infrastruttura sono configurati in alta disponibilità e/o sono dotati di meccanismi di riserva.

Resilienza dei software personalizzati

I moduli software personalizzati consentono di potenziare la resilienza in quanto, per un determinato periodo di tempo, tentano di ristabilire la comunicazione con l'altro ETS quando, per un motivo qualsiasi, questo servizio non è disponibile.

Resilienza dei servizi

Nel collegamento permanente dei registri, gli scambi di dati tra le parti avvengono a intervalli predefiniti. Alcune delle fasi necessarie per gli scambi di dati preprogrammati richiedono l'intervento manuale dei gestori dei sistemi e/o degli amministratori dei registri. Tenendo conto di questo aspetto e per aumentare la disponibilità e l'adeguato svolgimento degli scambi:

— le procedure operative prevedono finestre temporali per l'esecuzione di ogni tappa;

— i moduli software per il collegamento permanente dei registri attuano una comunicazione asincrona;

— il processo automatico di riconciliazione individuerà eventuali problemi nell'immissione dei file di dati nei due ETS;

— i processi di monitoraggio (infrastruttura TIC e moduli software personalizzati) sono considerati nelle procedure di gestione degli incidenti e attivano queste procedure (definite nel documento relativo alle procedure operative comuni). Le procedure volte a ridurre il tempo necessario per ripristinare il normale funzionamento a seguito di incidenti sono fondamentali per garantire tassi di disponibilità elevati.

4.2. Piano di attivazione, comunicazione, riattivazione e prove

Tutti i diversi elementi dell'architettura del collegamento permanente dei registri devono superare una serie di prove individuali e collettive destinate a verificare che la piattaforma è pronta a livello dell'infrastruttura TIC e del sistema di informazione. Questi test operativi costituiscono una condizione preliminare obbligatoria ogni volta che il collegamento permanente dei registri passa dallo status «sospeso» («*suspended*») allo status «operativo» («*operational*»).

L'attivazione dello status operativo del collegamento presuppone l'adeguata esecuzione di un piano di prove predefinito. Ciò consente di verificare che per ciascun registro è stata effettuata dapprima una serie di prove interne, seguita dalla convalida della connettività end-to-end, prima di iniziare a trasmettere operazioni vere e proprie tra le due parti.

Il piano delle prove dovrebbe menzionare la strategia di prove generale e informazioni dettagliate sull'infrastruttura per le prove. In particolare, per ciascun elemento di ogni blocco di prova occorre disporre degli elementi seguenti:

— i criteri e gli strumenti di prova;

— i ruoli assegnati in vista dell'esecuzione delle prove;

— i risultati attesi (positivi e negativi);

— il calendario delle prove;

— la registrazione dei requisiti relativi ai risultati delle prove;

— la documentazione relativa alla risoluzione dei problemi;

— le disposizioni relative ai livelli successivi di intervento.

Il processo delle prove di attivazione dello status operativo potrebbe essere suddiviso in quattro (4) blocchi o fasi concettuali:

4.2.1. Prove dell'infrastruttura TIC in interno

Queste prove devono essere eseguite e/o verificate individualmente da entrambi gli amministratori dei registri nel proprio ETS.

Ogni elemento delle infrastrutture TIC degli ETS deve essere testato individualmente. Ciò vale anche per ogni singola componente dell'infrastruttura. Queste prove possono essere eseguite automaticamente o manualmente ma devono consentire di verificare che ogni elemento dell'infrastruttura è operativo.

4.2.2. Prove di comunicazione

Tali prove sono avviate da ciascuna parte individualmente e la conclusione delle prove richiede la cooperazione dell'altra parte.

Una volta resi operativi i singoli elementi, i canali di comunicazione tra i due registri devono essere testati. A tal fine, ciascuna parte verifica che l'accesso a Internet funzioni, che siano predisposti i tunnel VPN e che sia stabilita la connettività IP da sito a sito. L'accessibilità degli elementi di infrastruttura locali e remoti e la connettività IP dovrebbero quindi essere confermati all'altro ETS.

4.2.3. Prove sull'intero sistema (end-to-end)

Tali prove devono essere effettuate da ogni ETS e i risultati devono essere comunicati all'altra parte.

Una volta testati i canali di comunicazione e ciascuna singola componente di entrambi i registri, ciascun ETS deve predisporre una serie di operazioni simulate e di riconciliazioni che siano rappresentative di tutte le funzioni da attuare nell'ambito del collegamento.

4.2.4. Prove di sicurezza

Queste prove devono essere effettuate e/o attivate da entrambi gli amministratori dei registri nel proprio ETS seguendo le indicazioni di cui alle sezioni 5.4. «Linee guida in materia di prove di sicurezza» e 5.5. «Disposizioni in materia di valutazione dei rischi».

Solo dopo la fine delle quattro fasi/blocchi con esiti prevedibili, si può ritenere che il collegamento permanente dei registri è operativo.

Risorse destinate alle prove

Ciascuna parte si avvale di risorse specifiche destinate alle prove (software e hardware specifici delle infrastrutture TIC) e mette a punto funzioni di prova nel proprio sistema al fine di agevolare la convalida manuale e continua della piattaforma. Le procedure di prova manuali, effettuate separatamente o in cooperazione, possono essere eseguite in qualsiasi momento dagli amministratori dei registri. L'attivazione dello status operativo è un processo manuale in sé.

È previsto inoltre che la piattaforma effettui controlli automatici a intervalli regolari che mirano ad incrementare la disponibilità della piattaforma individuando rapidamente eventuali problemi a livello di infrastruttura o di software. Il piano di monitoraggio della piattaforma è costituito da due elementi:

— monitoraggio delle infrastrutture TIC: in entrambi gli ETS l'infrastruttura sarà monitorata dai fornitori di servizi di infrastruttura TIC. Le prove automatiche riguarderanno i diversi elementi dell'infrastruttura e la disponibilità dei canali di comunicazione.

— Monitoraggio delle applicazioni: i moduli software del collegamento permanente dei registri effettueranno il monitoraggio del sistema di comunicazione a livello di applicazione (manualmente e/o a intervalli regolari) che consentirà di verificare la disponibilità end-to-end del collegamento simulando alcune operazioni.

4.3. Ambienti di accettazione/prova

L'architettura del registro dell'Unione e del registro della Svizzera prevede i tre ambienti seguenti:

— Produzione (PROD): questo ambiente contiene dati reali e tratta operazioni effettive.

— Accettazione (ACC): questo ambiente contiene dati rappresentativi, fittizi o anonimizzati. Si tratta dell'ambiente in cui i gestori dei sistemi di entrambe le parti convalidano i nuovi rilasci di versioni.

— Prova (TEST): questo ambiente contiene dati rappresentativi, fittizi o anonimizzati. L'accesso è limitato agli amministratori dei registri e l'ambiente è destinato ad essere utilizzato da entrambe le parti per effettuare prove di integrazione.

Ad eccezione della VPN, i tre ambienti sono totalmente indipendenti l'uno dall'altro: l'hardware, il software, le basi di dati, gli ambienti virtuali, gli indirizzi IP e le porte sono configurati e funzionano in modo indipendente gli uni dagli altri.

Per quanto riguarda la configurazione della VPN, la comunicazione tra i tre ambienti deve essere pienamente indipendente, il che è garantito dall'utilizzo della rete sTESTA.

5. DISPOSIZIONI IN MATERIA DI RISERVATEZZA E INTEGRITÀ

I meccanismi e le procedure di sicurezza si basano sul «principio dei quattro occhi» per le operazioni effettuate nell'ambito del collegamento tra il registro dell'Unione e il registro svizzero. Questo principio si applica ogniqualvolta necessario. Tuttavia, potrebbe non applicarsi a tutte le azioni intraprese dagli amministratori dei registri.

I requisiti di sicurezza sono esaminati e trattati nel piano di gestione della sicurezza, che comprende anche i processi relativi alla gestione degli incidenti di sicurezza a seguito di un'eventuale violazione della sicurezza. La parte operativa di tali processi è descritta nelle POC.

5.1. Infrastruttura per le prove di sicurezza

Ciascuna parte si impegna a predisporre un'infrastruttura destinata alle prove di sicurezza (avvalendosi dell'insieme comune di software e hardware utilizzati per individuare le vulnerabilità nella fase di sviluppo e funzionamento):

— separata dall'ambiente di produzione;

— in cui la sicurezza è analizzata da un'équipe indipendente dallo sviluppo e dal funzionamento del sistema.

Le parti si impegnano ad effettuare analisi sia statiche che dinamiche.

Nel caso di analisi dinamiche (come i test di penetrazione), entrambe le parti si impegnano di norma a limitare le valutazioni agli ambienti di prova e di accettazione (definiti nella sezione 4.3. «Ambienti di accettazione/prova»). Le eventuali deroghe sono soggette all'approvazione di entrambe le parti.

Prima di essere utilizzato nell'ambiente di produzione, ogni modulo di software del collegamento (definito nella sezione 3.1. «Architettura del collegamento di comunicazione») è sottoposto a prove di sicurezza.

L'infrastruttura per le prove deve essere separata sia a livello di rete che di infrastruttura dall'infrastruttura di produzione. È nell'infrastruttura per le prove che vengono effettuate le prove di sicurezza necessarie per verificare la conformità ai requisiti di sicurezza.

5.2. Disposizioni relative alla sospensione e alla riattivazione del collegamento

Se si sospetta che la sicurezza del registro svizzero, dell'SSTL, del registro dell'Unione o dell'EUTL sia stata compromessa, qualsiasi parte informa immediatamente l'altra parte e sospende il collegamento tra l'SSTL e l'EUTL.

Le procedure per la condivisione delle informazioni, una decisione di sospendere e una decisione di riattivare fanno parte del processo per il soddisfacimento delle richieste delle POC.

Sospensioni

La sospensione del collegamento dei registri conformemente all'allegato II dell'accordo può avvenire per:

— ragioni amministrative (per esempio, manutenzione) che sono programmate;

— ragioni di sicurezza (o guasti dell'infrastruttura IT) che non sono previste.

In caso di emergenza, ciascuna parte informa l'altra parte e sospende unilateralmente il collegamento dei registri.

Se si decide di sospendere il collegamento dei registri, ciascuna parte provvederà a interrompere il collegamento a livello di rete (bloccando in parte o in toto le connessioni in entrata e in uscita).

La decisione di sospendere il collegamento dei registri, sia essa programmata o no, sarà adottata conformemente alla procedura per la gestione delle modifiche o alla procedura per la gestione degli incidenti di sicurezza delle POC.

Riattivazione della comunicazione

La decisione di riattivazione del collegamento dei registri sarà presa nella modalità specificata nelle POC e, in ogni caso, non prima di aver portato a termine con successo le procedure riguardanti prove di sicurezza, come specificato nelle sezioni 5.4. «Linee guida in materia di prove di sicurezza» e 4.2 «Piano di attivazione, comunicazione, riattivazione e prove».

5.3. Disposizioni in materia di violazioni della sicurezza

Una violazione della sicurezza è considerata un incidente di sicurezza che incide sulla riservatezza e l'integrità delle informazioni riservate e/o sulla disponibilità del sistema di trattamento di tali informazioni.

Le informazioni riservate sono identificate nell'elenco delle informazioni riservate e possono essere trattate nel sistema o in qualsiasi parte del sistema ad esso correlata.

Le informazioni direttamente connesse alla violazione della sicurezza saranno considerate riservate, contrassegnate come «SPECIAL HANDLING: *ETS Critical*» e trattate secondo le istruzioni di trattamento, salvo se diversamente specificato.

Tutte le violazioni della sicurezza saranno gestite nel rispetto delle procedure di cui al capitolo «Gestione degli incidenti di sicurezza» delle POC.

5.4. Linee guida in materia di prove di sicurezza

5.4.1. Software

Le prove di sicurezza, compresi gli eventuali test di penetrazione, devono essere eseguite quanto meno per tutti i nuovi principali rilasci di versioni del software, conformemente alle disposizioni in materia di sicurezza definiti nelle NTC, al fine di valutare la sicurezza del collegamento e i relativi rischi.

Se negli ultimi 12 mesi non è stato effettuato nessun rilascio importante di nuove versioni, è necessario effettuare prove di sicurezza sul sistema attuale, tenuto conto dell'evoluzione delle minacce informatiche verificatesi negli ultimi 12 mesi.

Le prove di sicurezza del collegamento del registro saranno effettuate nell'ambiente di accettazione e, se necessario, nell'ambiente di produzione, in coordinamento e con l'accordo di entrambe le parti.

Le prove sulle applicazioni web saranno eseguite conformemente agli standard aperti internazionali come quelli messi a punto dall'OWASP (*Open Web Application Security Project*).

5.4.2. Infrastruttura

Le infrastrutture alla base del sistema di produzione devono essere controllate periodicamente (almeno una volta al mese) al fine di individuare eventuali vulnerabilità cui occorrerà porre rimedio secondo il principio definito nella sezione precedente, utilizzando una base di dati aggiornata relativa alle vulnerabilità.

5.5. Disposizioni in materia di valutazione dei rischi

Se occorre effettuare test di penetrazione, questi devono essere inclusi nelle prove di sicurezza.

Ogni parte può affidare a una società specializzata l'esecuzione di prove di sicurezza, a condizione che questa:

— vanti competenze e esperienza nel settore;

— non faccia riferimento direttamente allo sviluppatore e/o al suo contraente, e non sia coinvolta nello sviluppo del software del collegamento né sia una subappaltatrice dello sviluppatore;

— abbia firmato un accordo di non divulgazione con cui si impegna a garantire la riservatezza dei risultati e a trattarli al livello di «SPECIAL HANDLING: ETS Critical» conformemente alle istruzioni di trattamento.