Conselho da
União Europeia

Bruxelas, 22 de março de 2024
(OR. en)

8159/24
ADD 1

Dossiê interinstitucional:
2024/0067 (NLE)

ENV 363
CLIMA 139
ENER 155
IND 187
COMPET 368
MI 359
ECOFIN 359
TRANS 176
AELE 24
CH 7

PROPOSTA

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	20 de março de 2024
para:	Thérèse BLANCHET, secretária-geral do Conselho da União Europeia
n.° doc. Com.:	COM(2024) 125 final – ANEXO
Assunto:	ANEXO da Proposta de Decisão do Conselho relativa à posição a tomar, em nome da União Europeia, no âmbito do Comité Misto criado pelo Acordo entre a União Europeia e a Confederação Suíça sobre a ligação dos respetivos regimes de comércio de licenças de emissão de gases com efeito de estufa, no que se refere à alteração do anexo II do Acordo, dos procedimentos operacionais comuns e das normas técnicas de ligação

Envia-se em anexo, à atenção das delegações, o documento COM(2024) 125 final – ANEXO.

Anexo: COM(2024) 125 final – ANEXO

COMISSÃO
EUROPEIA

Bruxelas, 20.3.2024
COM(2024) 125 final

ANNEX

ANEXO

da

Proposta de Decisão do Conselho

relativa à posição a tomar, em nome da União Europeia, no âmbito do Comité Misto criado pelo Acordo entre a União Europeia e a Confederação Suíça sobre a ligação dos respetivos regimes de comércio de licenças de emissão de gases com efeito de estufa, no que se refere à alteração do anexo II do Acordo, dos procedimentos operacionais comuns e das normas técnicas de ligação

DECISÃO N.º 1/2024 DO COMITÉ MISTO INSTITUÍDO PELO ACORDO ENTRE A UNIÃO EUROPEIA E A CONFEDERAÇÃO SUÍÇA SOBRE A LIGAÇÃO DOS RESPETIVOS REGIMES DE COMÉRCIO DE LICENÇAS DE EMISSÃO DE GASES COM EFEITO DE ESTUFA

de …

relativa à alteração do anexo II e do Acordo, dos procedimentos operacionais comuns e das normas técnicas de ligação

O COMITÉ MISTO,

Tendo em conta o Acordo entre a União Europeia e a Confederação Suíça sobre a ligação dos respetivos regimes de comércio de licenças de emissão de gases com efeito de estufa[1] (a seguir designado por «Acordo»), nomeadamente o artigo 9.º, e o artigo 13.º, n.º 2,

Considerando o seguinte:

(1) A Decisão n.º 2/2019[2] do Comité Misto previa uma solução provisória para operacionalizar a ligação entre o CELE da UE e o RCLE da Suíça.

(2) Na sua terceira reunião, o Comité Misto chegou a acordo sobre a necessidade de analisar a relação custo-eficácia de uma ligação permanente entre o Registo da União e o Registo Suíço.

(3) Na sua quinta reunião, o Comité Misto chegou a acordo sobre o relatório apresentado pelo grupo de trabalho criado pelas Decisões n.os 1/2020[3] e 2/2020[4] do Comité Misto e no qual este grupo de trabalho analisou e recomendou uma abordagem para implementar a ligação permanente entre o Registo da União e o Registo Suíço.

(4) Para refletir os requisitos técnicos da ligação permanente entre o Registo da União e o Registo Suíço, bem como para simplificar as disposições do anexo II do Acordo à luz da evolução tecnológica, o anexo II do Acordo deve ser alterado.

(5) A fim de assegurar a coerência e a compatibilidade dos procedimentos operacionais comuns e das normas técnicas de ligação com o anexo II do Acordo, estes documentos devem igualmente ser alterados.

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

1. O anexo II do Acordo é substituído pelo anexo I da presente decisão.

2. Os procedimentos operacionais comuns a que se refere o artigo 3.º, n.º 6, do Acordo constam do anexo II da presente decisão.

3. As normas técnicas de ligação referidas no artigo 3.º, n.º 7, do Acordo constam do anexo III da presente decisão.

Artigo 2.º

A presente decisão entra em vigor no dia da sua adoção.

---

1 JO L 322 de 7.12.2017, p. 3.
2 JO L 314 de 29.9.2020, p. 68.
3 JO L 226 de 25.6.2021, p. 2.
4 JO L 226 de 25.6.2021, p. 16.

Feito em língua inglesa, em [Bruxelas][Berna], em [XX de XX de 2024].

Pelo Comité Misto

Secretário/a da União Europeia	*O/A Presidente*	*Secretário/a da Suíça*

ANEXO I

«ANEXO II

NORMAS TÉCNICAS DE LIGAÇÃO

Para operacionalizar a ligação entre o CELE da UE e o RCLE da Suíça, em 2020 foi adotada uma solução provisória. A partir de 2023, a ligação dos registos dos dois regimes de comércio de licenças de emissão evoluirá gradualmente para uma ligação permanente entre registos, que deverá ser adotada o mais tardar em 2024, que permita o funcionamento dos mercados ligados no que diz respeito aos benefícios da liquidez do mercado e da execução de transações entre os dois sistemas interligados de forma equivalente a um mercado constituído por dois sistemas, e que permita aos participantes no mercado atuarem como se estivessem num único mercado, sujeito apenas a disposições regulamentares individuais das Partes. As normas técnicas de ligação (NTL) especificam:

– a arquitetura da ligação de comunicação,

– as comunicações entre o DOCS e o DOUE

– a segurança da transferência de dados,

– a lista de funções (operações, conciliação, etc.),

– as definições da camada de transporte

– os requisitos de entrada de dados

– os dispositivos operacionais (assistência telefónica, apoio),

– o plano de ativação das comunicações e o procedimento de ensaio,

– o procedimento de teste da segurança.

As normas técnicas de ligação especificam que os administradores devem tomar todas as medidas razoáveis para assegurar que o DOCS, o DOUE e a ligação de comunicação estão operacionais 24 horas por dia e 7 dias por semana, bem como para reduzir ao mínimo possível qualquer interrupção nas operações do DOCS, do DOUE e da ligação de comunicação.

As normas técnicas de ligação estabelecem requisitos de segurança adicionais para o Registo Suíço, o DOCS, o Registo da União e o DOUE e são documentadas num «plano de gestão da segurança». Em especial, as normas técnicas de ligação determinam o seguinte:

– caso exista uma suspeita de que a segurança do Registo Suíço, do DOCS, do Registo da União ou do DOUE esteja comprometida, cada Parte deve informar imediatamente a outra Parte e suspender a ligação entre o DOCS e o DOUE,

– em caso de violação da segurança, as Partes comprometem-se a partilhar imediatamente as informações entre si. Consoante a disponibilidade de informações técnicas pormenorizadas, será partilhado um relatório descritivo do incidente (data, causa, impacto, soluções) com o administrador do Registo Suíço e o administrador central do Registo da União no prazo de 24 horas após um incidente de segurança ser identificado como uma violação da segurança.

O procedimento de teste da segurança definido nas normas técnicas de ligação é executado na íntegra antes de ser estabelecida a ligação de comunicação entre o DOCS e o DOUE, e quando for necessária uma nova versão ou edição do DOCS ou do DOUE.

As normas técnicas de ligação preveem dois ambientes de testes, além do ambiente de produção: um ambiente de testes de programação e um ambiente de aceitação.

As Partes devem demonstrar, por intermédio do administrador do Registo Suíço e do administrador central do Registo da União, que a segurança dos seus sistemas foi objeto de uma avaliação independente, realizada nos doze meses precedentes, em conformidade com os requisitos de segurança estabelecidos nas normas técnicas de ligação. Todas as novas versões importantes do software devem ser sujeitas a testes de segurança, em particular testes de penetração de sistemas, em conformidade com os requisitos de segurança estabelecidos nas normas técnicas de ligação. Os testes de penetração de sistemas não podem ser efetuados pelo criador do software nem por um seu subcontratante.

ANEXO II

PROCEDIMENTOS OPERACIONAIS COMUNS

nos termos do artigo 3.º, n.º 6, do Acordo entre a União Europeia e a Confederação Suíça sobre a ligação dos respetivos regimes de comércio de licenças de emissão de gases com efeito de estufa

Procedimentos para a ligação permanente entre registos

Índice

1. Glossário 10
2. Introdução 11
2.1. Âmbito de aplicação 11
2.2. Destinatários 12
3. Abordagem e normas 12
4. Gestão de incidentes 13
4.1. Deteção e registo de incidentes 13
4.2. Classificação e apoio inicial 14
4.3. Investigação e diagnóstico 14
4.4. Resolução e recuperação 14
4.5. Encerramento de incidentes 15
5. Gestão de problemas 16
5.1. Identificação e registo de problemas 16
5.2. Priorização de problemas 16
5.3. Investigação e diagnóstico de problemas 16
5.4. Resolução 16
5.5. Encerramento de problemas 16
6. Cumprimento de pedidos 17
6.1. Apresentação de pedidos 17
6.2. Registo e análise de pedidos 17
6.3. Aprovação de pedidos 17
6.4. Cumprimento de pedidos 17
6.5. Aplicação do procedimento por etapas aos pedidos 17
6.6. Revisão do cumprimento de pedidos 18
6.7. Encerramento dos pedidos 18
7. Gestão das modificações 19

7.1. Pedido de alteração 19
7.2. Avaliação e planeamento de alterações 19
7.3. Aprovações de alterações 19
7.4. Execução de alterações 19
8. Gestão de versões 20
8.1. Planeamento de versões 20
8.2. Pacote de criação e teste de versões 20
8.3. Preparação da implantação 21
8.4. Restauração de versões 21
8.5. Revisão e encerramento de versões 21
9. Gestão de incidentes de segurança 22
9.1. Categorização de incidentes de segurança da informação 22
9.2. Tratamento de incidentes de segurança da informação 22
9.3. Identificação de incidentes de segurança 22
9.4. Análise de incidentes de segurança 22
9.5. Avaliação da gravidade dos incidentes de segurança, procedimento por etapas e comunicação 23
9.6. Comunicação da resposta de segurança 23
9.7. Monitorização, reforço da capacidade e melhoria contínua 23
10. Gestão da segurança da informação 23
10.1. Identificação de informações sensíveis 24
10.2. Níveis de sensibilidade dos ativos de informação 24
10.3. Atribuição de proprietários aos ativos de informação 24
10.4. Registo de informações sensíveis 24
10.5. Tratamento de informações sensíveis 25
10.6. Gestão de acessos 25
10.7. Gestão de chaves/certificados 25
1. Glossário 31
2. Introdução 34
2.1. Âmbito de aplicação 34
2.2. Destinatários 35
3. Disposições gerais 35
3.1. Arquitetura da ligação de comunicação 35

3.1.1. Intercâmbio de mensagens 35
3.1.2. Mensagem XML — Descrição de alto nível 35
3.1.3. Períodos de ingestão 36
3.1.4. Fluxos de mensagens de operações 36
3.2. Segurança da transferência de dados 39
3.2.1. Barreira de segurança e interconexão de redes 39
3.2.2. Rede privada virtual (RPV) 39
3.2.3. Execução de IPSec 40
3.2.4. Protocolo seguro de transferência de mensagens 40
3.2.5. Cifragem e assinatura XML 40
3.2.6. Chaves criptográficas 40
3.3. Lista de funções ao abrigo da ligação 40
3.3.1. Operações comerciais 41
3.3.2. Protocolo de conciliação 41
3.3.3. Mensagem de teste 41
3.4. Requisitos de registo de dados 42
3.5. Requisitos operacionais 43
4. Disposições em matéria de disponibilidade 44
4.1. Conceção que garante a disponibilidade das comunicações 44
4.2. Inicialização, comunicação, reativação e plano de teste 44
4.2.1. Testes da infraestrutura de TIC interna 45
4.2.2. Testes das comunicações 45
4.2.3. Testes do sistema completo (de extremo a extremo) 45
4.2.4. Testes da segurança 45
4.3. Ambientes de aceitação/teste 46
5. Disposições em matéria de confidencialidade e integridade 46
5.1. Infraestrutura de teste da segurança 47
5.2. Disposições em matéria de suspensão e reativação da ligação 47
5.3. Disposições em matéria de violação da segurança 48
5.4. Orientações relativas aos testes da segurança 48
5.4.1. Programas informáticos (software) 48
5.4.2. Infraestruturas 48
5.5. Disposições em matéria de avaliação de riscos 48

1. GLOSSÁRIO

Quadro 1-1 Acrónimos e definições

Acrónimo/Termo	Definição
Autoridade de Certificação (AC)	Entidade que emite certificados digitais
CH	Confederação Suíça
CELE	Sistema de comércio de licenças de emissão
UE	União Europeia
EGI	Equipa de Gestão de Incidentes
Ativo de informação	Uma informação valiosa para uma empresa ou organização
TI	Tecnologias da informação
ITIL	Biblioteca de Infraestruturas de Tecnologias da Informação
GSTI	Gestão de Serviços de Tecnologias da Informação
NTL	Normas técnicas de ligação
Registo	Um sistema contabilístico para as licenças emitidas ao abrigo do RCLE, que mantém um registo da propriedade das licenças depositadas em contas eletrónicas.
PA	Pedido de Alteração
LIS	Lista de Informações Sensíveis
PS	Pedido de Serviço
Wiki	Sítio Web que permite aos utilizadores trocar informações e conhecimentos, adicionando ou adaptando conteúdos diretamente através de um navegador Web.

2. INTRODUÇÃO

O Acordo entre a União Europeia e a Confederação Suíça sobre a ligação dos respetivos regimes de comércio de licenças de emissão de gases com efeito de estufa, de 23 de novembro de 2017 («Acordo»), prevê o reconhecimento mútuo das licenças de emissão que possam ser utilizadas para efeitos de conformidade ao abrigo do regime de comércio de licenças de emissão da União Europeia («RCLE-UE») [cuja designação foi entretanto alterada para «sistema de comércio de licenças de emissão da União», com o acrónimo «CELE»] ou do sistema de comércio de licenças de emissão da Suíça («RCLE da Suíça»). Com vista a operacionalizar a ligação entre o CELE da UE e o RCLE da Suíça, é estabelecida uma ligação direta entre o Diário de Operações da União Europeia (DOUE) do Registo da União e o Diário de Operações Complementares da Suíça (DOCS) do Registo Suíço, que permitirá a transferência entre registos das licenças de emissão atribuídas ao abrigo de cada um dos sistemas (artigo 3.º, n.º 2, do Acordo). Para operacionalizar a ligação entre o CELE da UE e o RCLE da Suíça, em 2020 foi adotada uma solução provisória. A partir de 2023, a ligação dos registos dos dois regimes de comércio de licenças de emissão evoluirá gradualmente para uma ligação permanente entre registos, que deverá ser adotada o mais tardar em 2024, que permita o funcionamento dos mercados ligados no que diz respeito aos benefícios da liquidez do mercado e da execução de transações entre os dois sistemas interligados de forma equivalente a um mercado constituído por dois sistemas, e que permita aos participantes no mercado atuarem como se estivessem num único mercado, sujeito apenas a disposições regulamentares individuais das Partes. (Anexo II do acordo).

Nos termos do artigo 3.º, n.º 6, do Acordo, o administrador do Registo Suíço e o administrador central do Registo da União determinam os procedimentos operacionais comuns (POC) relativos a questões técnicas ou de outra natureza que se afigurem necessárias para o funcionamento da ligação, tendo em conta as prioridades definidas na legislação interna. Os procedimentos operacionais comuns desenvolvidos pelos administradores produzem efeitos logo que a decisão do Comité Misto seja adotada.

Os procedimentos operacionais comuns foram adotados pelo Comité Misto através da sua Decisão n.º 1/2020. Os procedimentos operacionais comuns revistos, tal como constam do presente documento, serão adotados pelo Comité Misto através da sua Decisão n.º 1/2024. Em conformidade com a presente decisão e as solicitações do Comité Misto, o administrador do Registo Suíço e o administrador central do Registo da União elaboraram, e continuarão a atualizar, novas orientações técnicas para operacionalizar a ligação que assegurem que estas sejam continuamente adaptadas aos progressos técnicos e aos novos requisitos relativos à segurança da ligação e ao seu funcionamento eficaz e eficiente.

2.1. Âmbito de aplicação

O presente documento representa o entendimento comum entre as Partes do Acordo sobre o estabelecimento das bases processuais da ligação entre os registos do CELE da UE e do RCLE da Suíça. Embora descreva os requisitos processuais gerais em termos de operações, serão necessárias algumas orientações técnicas adicionais para operacionalizar a ligação.

Para assegurar o bom funcionamento da ligação, importa definir especificações técnicas que a tornem ainda mais operacional. Nos termos do artigo 3.º, n.º 7, do Acordo, essas questões são especificadas no documento que define as normas técnicas de ligação, a adotar separadamente por decisão do Comité Misto.

O objetivo dos procedimentos operacionais comuns consiste em garantir que os serviços de TI relacionados com o funcionamento da ligação entre os registos do CELE da UE e do RCLE da Suíça sejam prestados de forma eficaz e eficiente, especialmente no que se refere à satisfação de pedidos de serviço, à resolução de falhas do serviço, à resolução de problemas, bem como à execução de tarefas operacionais de rotina de acordo com as normas internacionais em matéria de gestão de serviços de tecnologias da informação.

Para a ligação permanente entre registos, apenas serão necessários os seguintes procedimentos operacionais comuns, que fazem parte do presente documento:

- Gestão de incidentes;
- Gestão de problemas;
- Cumprimento de pedidos;
- Gestão de alterações;
- Gestão de versões;
- Gestão de incidentes de segurança;
- Gestão da segurança da informação.

2.2. Destinatários

O público-alvo destes procedimentos operacionais comuns são as equipas de apoio do Registo da União e do Registo suíço.

3. ABORDAGEM E NORMAS

O princípio a seguir indicado aplica-se a todos os procedimentos operacionais comuns:

- A UE e a Confederação Suíça acordam em definir os procedimentos operacionais comuns com base na ITIL (Biblioteca de Infraestruturas de Tecnologias da Informação, versão 4). As práticas desta norma são reutilizadas e adaptadas às necessidades específicas relacionadas com a ligação permanente entre registos;
- A comunicação e a coordenação necessárias para o processamento dos procedimentos operacionais comuns entre as duas Partes realizam-se através dos serviços de assistência dos registos da Confederação Suíça e da UE. As tarefas são sempre atribuídas no seio de uma Parte;
- Em caso de desacordo sobre o tratamento de um procedimento operacional comum, este será analisado e resolvido por ambos os serviços de assistência. Se não for possível chegar a acordo, a procura de uma solução conjunta é remetida para o nível seguinte.

Níveis de intervenção	UE	CH
1.º nível	Serviço de assistência da UE	Serviço de assistência da Confederação Suíça
2.º nível	Gestor de operações da UE	Gestor de aplicações do Registo Suíço
3.º nível	Comité Misto (que pode delegar esta responsabilidade tendo em	

	consideração o disposto no artigo 12.º, n.º 5, do Acordo)
4.º nível	Comité Misto, se o 3.º nível for delegado

- Cada Parte pode determinar os procedimentos para o funcionamento do seu próprio sistema de registo, tendo em conta os requisitos e as interfaces relacionados com estes procedimentos operacionais comuns;
- É utilizada uma ferramenta de gestão de serviços de tecnologias da informação (GSTI) para apoiar os procedimentos operacionais comuns, em particular a gestão de incidentes, a gestão de problemas e o cumprimento de pedidos, bem como a comunicação entre ambas as Partes;
- Além disso, é permitido o intercâmbio de informações por correio;
- Ambas as Partes asseguram que os requisitos de segurança da informação sejam cumpridos em conformidade com as instruções de tratamento.

4. GESTÃO DE INCIDENTES

O objetivo do processo de gestão de incidentes consiste na reposição do nível normal dos serviços de TI o mais rapidamente possível após um incidente e com um mínimo de perturbações para a atividade.

O processo de gestão de incidentes deve igualmente manter um registo de incidentes para efeitos de comunicação de informações e articular-se com outros processos para promover a melhoria contínua.

Numa perspetiva global, o processo de gestão de incidentes abrange as seguintes atividades:

- Deteção e registo de incidentes;
- Classificação e apoio inicial;
- Investigação e diagnóstico;
- Resolução e recuperação;
- Encerramento de incidentes.

Ao longo do ciclo de vida de um incidente, o processo de gestão de incidentes é responsável pelo tratamento constante da propriedade, da monitorização, do acompanhamento e da comunicação.

4.1. Deteção e registo de incidentes

Um incidente pode ser detetado por um grupo de apoio, por ferramentas de monitorização automatizada ou pelo pessoal técnico durante operações de vigilância de rotina.

Uma vez detetado, um incidente deve ser registado, devendo ser-lhe atribuído um identificador único que permita o seu acompanhamento e monitorização adequados. O identificador único de um incidente é o identificador atribuído no sistema comum de apresentação de pedidos de apoio pelo serviço de assistência da Parte (UE ou Confederação Suíça) que comunicou o incidente, e tem de ser utilizado em todas as comunicações relacionadas com este incidente.

Para todos os incidentes, o ponto de contacto deve ser o serviço de assistência da Parte que registou o pedido de apoio.

4.2. Classificação e apoio inicial

A classificação de incidentes visa compreender e identificar que sistema e/ou serviço são afetados por um incidente e em que medida. Para ser eficaz, a classificação deve encaminhar o incidente para o recurso correto na primeira tentativa, a fim de acelerar a resolução do incidente.

A fase de classificação deve categorizar e priorizar o incidente em função do seu impacto e urgência, para que seja tratado de acordo com o prazo de prioridade pertinente.

Se o incidente tiver potencial impacto na confidencialidade ou na integridade de dados sensíveis, e/ou impacto na disponibilidade do sistema, deve igualmente ser declarado como incidente de segurança e, subsequentemente, gerido de acordo com o processo definido no capítulo intitulado «Gestão de incidentes de segurança» do presente documento.

Se possível, o serviço de assistência que registou o pedido de apoio realiza um diagnóstico inicial. Para tal, o serviço de assistência verificará se o incidente é um erro conhecido. Se assim for, o caminho para a sua resolução ou a solução alternativa já é conhecido e está documentado.

Se o serviço de assistência for bem sucedido na resolução do incidente, irá efetivamente encerrar o incidente nesse momento, uma vez que o objetivo principal do processo de gestão de incidentes terá sido cumprido (nomeadamente o rápido restabelecimento do serviço para o utilizador final). Caso contrário, o serviço de assistência irá remeter o incidente ao grupo de resolução adequado para uma investigação aprofundada e diagnóstico.

4.3. Investigação e diagnóstico

O processo de investigação e diagnóstico de incidentes é aplicado quando um incidente não pode ser resolvido pelo serviço de assistência no quadro do diagnóstico inicial, sendo-lhe, por conseguinte, aplicado um procedimento por etapas de forma adequada. O procedimento por etapas em caso de incidente é parte integrante do processo de investigação e diagnóstico.

Uma prática comum na fase de investigação e diagnóstico é a tentativa de recriar o incidente em condições controladas. Aquando da realização da investigação e do diagnóstico do incidente, é importante compreender a ordem correta dos acontecimentos que conduziram ao incidente.

O procedimento por etapas resulta do reconhecimento de que um incidente não pode ser resolvido no nível de apoio atual, pelo que deve ser remetido a um grupo de apoio de nível superior ou à outra Parte. O procedimento por etapas pode seguir dois caminhos: horizontal (funcional) ou vertical (hierárquico).

O serviço de assistência que registou e acionou o incidente é responsável pela aplicação do procedimento por etapas ao incidente, remetendo-o ao recurso adequado, bem como pelo acompanhamento do estado geral e pela atribuição do incidente.

A Parte à qual o incidente foi atribuído é responsável por assegurar que as ações solicitadas sejam executadas em tempo útil e pelo retorno de informação ao serviço de assistência da sua própria Parte.

4.4. Resolução e recuperação

A resolução do incidente e posterior recuperação são realizadas quando o incidente é totalmente compreendido. Encontrar uma resolução para um incidente significa que foi identificada uma forma de retificar o problema. O ato de aplicar a resolução corresponde à fase de recuperação.

Assim que os recursos adequados resolvam a falha do serviço, o incidente é encaminhado de volta ao serviço de assistência competente que registou o incidente, o qual confirma junto da pessoa que comunicou o incidente que o erro foi retificado e que o incidente pode ser encerrado. Os resultados do processamento do incidente devem ser registados para utilização futura.

A recuperação pode ser realizada pelo pessoal de apoio informático ou fornecendo ao utilizador final um conjunto de instruções que este deve seguir.

4.5. Encerramento de incidentes

O encerramento é a etapa final do processo de gestão de incidentes e ocorre logo após a resolução do incidente.

Entre a lista de verificação das atividades que é necessário realizar durante a fase de encerramento, destacam-se as seguintes:

- A verificação da categorização inicial que foi atribuída ao incidente;
- A recolha adequada de todas as informações associadas ao incidente;
- A documentação adequada do incidente e a atualização da base de conhecimentos;
- A comunicação adequada a todas as partes interessadas direta ou indiretamente afetadas pelo incidente.

Um incidente é formalmente encerrado assim que a fase de encerramento do incidente tenha sido executada pelo serviço de assistência e comunicada à outra Parte.

Uma vez encerrado, um incidente não é reaberto. Se um incidente voltar a ocorrer num curto período de tempo, o incidente original não é reaberto, devendo antes ser registado um novo incidente.

Se o incidente for acompanhado tanto pelos serviços de assistência da UE como pelos da Confederação Suíça, o encerramento final é da responsabilidade do serviço de assistência que tiver registado o pedido de apoio.

5. GESTÃO DE PROBLEMAS

Este procedimento deve ser seguido sempre que seja identificado um problema que desencadeie o processo de gestão de problemas. O processo de gestão de problemas concentra-se na melhoria da qualidade e na redução do volume de incidentes comunicados. Um problema pode ser a causa de um ou mais incidentes. Quando um incidente é comunicado, o objetivo do processo de gestão de incidentes consiste em restabelecer o serviço o mais rapidamente possível, recorrendo eventualmente a soluções alternativas. Quando é registado um problema, o objetivo consiste em investigar a sua causa profunda, a fim de identificar uma alteração que garanta que o problema e os incidentes conexos não ocorram novamente.

5.1. Identificação e registo de problemas

Dependendo da Parte que apresentou o pedido de apoio, o serviço de assistência da UE ou da Confederação Suíça será o ponto de contacto para assuntos relacionados com o problema em causa.

O identificador único de um problema é o identificador atribuído pela gestão de serviços de tecnologias da informação (GSTI). Tem de ser utilizado em todas as comunicações relacionadas com o problema em questão.

Um problema pode ser desencadeado por um incidente ou apresentado deliberadamente para corrigir problemas descobertos no sistema em qualquer momento.

5.2. Priorização de problemas

Os problemas podem ser categorizados em função da sua gravidade e prioridade, da mesma forma que os incidentes, a fim de facilitar o seu acompanhamento, tendo em conta o impacto dos incidentes conexos e a sua frequência de ocorrência.

5.3. Investigação e diagnóstico de problemas

Cada Parte pode chamar a atenção para um problema, sendo o serviço de assistência da Parte que o fez responsável pelo registo do problema, pela sua atribuição ao recurso adequado e pelo acompanhamento do estado geral do problema.

O grupo de resolução ao qual o problema foi remetido é responsável pelo tratamento atempado do problema e pela comunicação com o serviço de assistência.

Mediante solicitação, ambas as Partes são responsáveis por assegurar que as ações atribuídas sejam executadas e pelo retorno de informação ao serviço de assistência da sua própria Parte.

5.4. Resolução

O grupo de resolução ao qual o problema é atribuído é responsável pela resolução do problema e pelo fornecimento de informações pertinentes ao serviço de assistência da sua própria Parte.

Os resultados do processamento do problema devem ser registados para utilização futura.

5.5. Encerramento de problemas

Um problema é formalmente encerrado assim que é resolvido através da aplicação da alteração. A fase de encerramento do problema será levada a cabo pelo serviço de assistência que registou o problema e informou o serviço de assistência da outra Parte.

6. CUMPRIMENTO DE PEDIDOS

O processo de cumprimento de um pedido corresponde à gestão de extremo a extremo do pedido de um serviço novo ou existente, desde o momento em que este é registado e aprovado até ao seu encerramento. Geralmente, os pedidos de serviço são simples, predefinidos, repetíveis, frequentes, pré-aprovados e processuais.

As principais etapas que devem ser seguidas são descritas abaixo:

6.1. Apresentação de pedidos

As informações relacionadas com um pedido de serviço são apresentadas ao serviço de assistência da UE ou da Confederação Suíça por correio eletrónico, por telefone ou através da ferramenta de gestão de serviços de tecnologias da informação (GSTI) ou de qualquer outro canal de comunicação acordado.

6.2. Registo e análise de pedidos

Para todos os pedidos de serviço, o ponto de contacto deve ser o serviço de assistência da UE ou da Confederação Suíça, dependendo da Parte que apresentou o pedido. Este serviço de assistência será responsável pelo registo e pela análise do pedido de serviço com a devida diligência.

6.3. Aprovação de pedidos

O funcionário do serviço de assistência da Parte que apresentou o pedido de serviço verifica se são necessárias quaisquer aprovações da outra Parte e, em caso afirmativo, inicia o processo de obtenção das mesmas. Se o pedido de serviço não for aprovado, o serviço de assistência atualiza e encerra o pedido.

6.4. Cumprimento de pedidos

Esta etapa visa o tratamento eficaz e eficiente dos pedidos de serviço. Deve ser feita uma distinção entre os seguintes casos:

- O cumprimento do pedido de serviço só afeta uma Parte. Neste caso, esta Parte emite as ordens de trabalho e coordena a execução.
- A execução do pedido de serviço afeta tanto a UE como a Confederação Suíça. Neste caso, os serviços de assistência emitem as ordens de trabalho no respetivo domínio de competência. O processamento do cumprimento do pedido de serviço é coordenado entre ambos os serviços de assistência. A responsabilidade global cabe ao serviço de assistência que recebeu e deu início ao pedido de serviço.

Quando o pedido de serviço for executado, o seu estado deve ser assinalado como resolvido.

6.5. Aplicação do procedimento por etapas aos pedidos

O serviço de assistência pode remeter o pedido de serviço pendente ao recurso adequado (parte terceira), se necessário.

Estes pedidos são remetidos às respetivas partes terceiras, isto é, o serviço de assistência da UE terá de passar pelo serviço de assistência da Confederação Suíça para remeter um pedido a uma parte terceira da Confederação Suíça, e vice-versa.

A parte terceira à qual o pedido de serviço foi remetido é responsável pelo tratamento do pedido de serviço em tempo útil e pela comunicação com o serviço de assistência que remeteu o pedido de serviço.

O serviço de assistência que registou o pedido de serviço é responsável pelo acompanhamento do estado geral e pela atribuição de um pedido de serviço.

6.6. Revisão do cumprimento de pedidos

O serviço de assistência responsável submete o registo do pedido de serviço a um controlo de qualidade final antes de o mesmo ser encerrado. O objetivo consiste em assegurar que o pedido de serviço seja efetivamente processado e que todas as informações necessárias para descrever o ciclo de vida do pedido sejam fornecidas com um grau suficiente de pormenorização. Além disso, os resultados do processamento do pedido devem ser registados para utilização futura.

6.7. Encerramento dos pedidos

Se as Partes designadas concordarem em que o pedido de serviço foi cumprido e o requerente considerar o caso resolvido, o próximo estado a ser definido é o de «Encerrado».

Um pedido de serviço é formalmente encerrado assim que o serviço de assistência que registou o pedido de serviço tenha executado a fase de encerramento do pedido e informado o serviço de assistência da outra Parte.

7. GESTÃO DAS MODIFICAÇÕES

O objetivo consiste em assegurar a utilização de métodos e procedimentos normalizados para o tratamento eficiente e imediato de todas as alterações para controlar a infraestrutura de TI, a fim de minimizar o número e o impacto de quaisquer incidentes conexos no serviço. Podem surgir alterações na infraestrutura de TI de forma reativa, em resposta a problemas ou requisitos impostos externamente como, por exemplo, alterações legislativas, ou de forma proativa, decorrentes da procura de uma maior eficiência e eficácia ou para permitir ou refletir iniciativas empresariais.

O processo de gestão de alterações inclui diferentes etapas que recolhem todos os pormenores sobre um pedido de alteração para acompanhamento futuro. Estes processos garantem que a alteração seja validada e testada antes de passar para a fase de implantação. O processo de gestão de versões é responsável pelo sucesso da implantação.

7.1. Pedido de alteração

Um pedido de alteração (PA) é apresentado à equipa de gestão de alterações para validação e aprovação. Para todos os pedidos de alteração, o ponto de contacto deve ser o serviço de assistência da UE ou da Confederação Suíça, dependendo da Parte que apresentou o pedido. Este serviço de assistência será responsável pelo registo e pela análise do pedido com a devida diligência.

Os pedidos de alteração podem provir de:

- Incidentes que provoquem alterações;
- Problemas existentes que resultem em alterações;
- Pedidos de novas alterações apresentados pelos utilizadores finais;
- Alterações decorrentes de manutenções em curso;
- Alterações de caráter legislativo.

7.2. Avaliação e planeamento de alterações

Nesta etapa procede-se à avaliação de alterações e são abordadas as atividades de planeamento. Inclui atividades de planeamento e priorização para minimizar riscos e impactos.

Se a execução do PA afetar tanto a UE como a Confederação Suíça, a Parte que registou o PA verifica o planeamento e a avaliação da alteração junto da outra Parte.

7.3. Aprovações de alterações

Qualquer pedido de alteração registado necessita de ser aprovado pelo nível de intervenção pertinente.

7.4. Execução de alterações

A execução de alterações é tratada no âmbito do processo de gestão de versões. As equipas de gestão de versões de ambas as Partes seguem os seus próprios processos, que envolvem o planeamento e a realização de testes. A revisão das alterações é realizada após a conclusão da execução. Para garantir que tudo correu conforme planeado, o processo de gestão de alterações existente é constantemente revisto e atualizado sempre que necessário.

8. GESTÃO DE VERSÕES

Uma versão representa uma ou mais alterações a um serviço de TI, reunidas num plano de lançamento que terá de ser autorizado, elaborado, criado, testado e implantado em conjunto. Uma versão pode representar uma correção de um erro, uma alteração do equipamento informático ou de outros componentes, alterações dos programas informáticos, atualizações de versões de aplicações, alterações da documentação e/ou dos processos. O conteúdo de cada versão é gerido, testado e implantado como uma entidade única.

A gestão de versões visa planear, criar, testar e validar, bem como proporcionar capacidade para prestar os serviços concebidos, o que permitirá cumprir os requisitos das partes interessadas e alcançar os objetivos pretendidos. Os critérios de aceitação de todas as alterações do serviço serão definidos e documentados durante a coordenação da conceção e fornecidos às equipas da gestão de versões.

A versão consistirá tipicamente numa série de correções de problemas e de melhorias de um serviço. Contém os programas informáticos novos ou alterados necessários e quaisquer equipamentos informáticos novos ou alterados necessários para aplicar as alterações aprovadas.

8.1. Planeamento de versões

A primeira etapa do processo atribui alterações autorizadas aos pacotes das versões e define o âmbito e o conteúdo das versões. Com base nestas informações, o subprocesso do planeamento de versões desenvolve um calendário para criar, testar e implantar a versão.

O planeamento deve definir:

- O âmbito e o conteúdo da versão;
- A avaliação dos riscos e o perfil de risco da versão;
- Os clientes/utilizadores afetados pela versão;
- A equipa responsável pela versão;
- A estratégia de execução e de implantação;
- Os recursos para o lançamento e a implantação.

Ambas as Partes devem informar-se mutuamente sobre os respetivos períodos de planeamento e manutenção da versão. Se uma versão afetar tanto a UE como a Confederação Suíça, ambas as Partes coordenam o planeamento e definem um período de manutenção comum.

8.2. Pacote de criação e teste de versões

A etapa de criação e teste do processo de gestão de versões estabelece as modalidades de execução da versão ou do pacote da versão, de manutenção de ambientes controlados antes da alteração da produção e de teste de todas as alterações em todos os ambientes da versão.

Se uma versão afetar tanto a UE como a Confederação Suíça, ambas as Partes coordenam os testes e planos de execução. Tal inclui os seguintes aspetos:

- De que forma e quando serão lançadas as unidades da versão e os componentes de serviço;
- Quais os prazos de entrega habituais; o que acontece se houver um atraso;
- Como acompanhar o progresso da execução e obter confirmação;
- Métricas para monitorizar e determinar o êxito do esforço de implantação da versão;
- Situações de teste comuns para alterações e funcionalidades pertinentes.

No final deste subprocesso, todos os componentes da versão necessários estão prontos para entrar na fase de implantação em ambiente real.

8.3. Preparação da implantação

O subprocesso de preparação assegura que os planos de comunicação sejam definidos corretamente e as notificações estejam prontas para serem enviadas a todas as partes interessadas e utilizadores finais afetados, e que a versão seja integrada no processo de gestão de alterações para assegurar que todas as alterações sejam realizadas de forma controlada e aprovadas pelas instâncias necessárias.

Se uma versão afetar tanto a UE como a Confederação Suíça, ambas as Partes devem coordenar as seguintes atividades:

- O registo do pedido de alteração para efeitos de programação e preparação da implantação do ambiente de produção;
- A criação do plano de execução;
- A abordagem de retrocesso, para que, caso haja uma falha na implantação, se possa regressar ao estado anterior;
- O envio de notificações a todas as partes necessárias;
- A exigência de aprovação, por parte do nível de intervenção pertinente, da execução da versão.

8.4. Restauração de versões

Caso a implantação tenha falhado ou os testes tenham identificado que a implantação não foi bem sucedida ou não cumpriu os critérios de aceitação/qualidade acordados, as equipas de gestão de versões de ambas as Partes terão de regressar ao estado anterior. Todas as partes interessadas pertinentes terão de ser informadas, incluindo os utilizadores finais afetados/visados. Enquanto se aguarda a aprovação, o processo pode ser reiniciado em qualquer uma das etapas anteriores.

8.5. Revisão e encerramento de versões

Ao rever uma implantação, devem ser incluídas as seguintes atividades:

- Recolher observações sobre a satisfação do cliente, do utilizador e a qualidade do serviço na sequência da implantação (recolher observações e tê-las em consideração para melhorar continuamente o serviço);
- Rever quaisquer critérios de qualidade que não tenham sido cumpridos;
- Verificar se as ações, correções necessárias e alterações estão concluídas;
- Assegurar que não há problemas em termos de capacidade, recursos ou desempenho no final da implantação;
- Verificar se os eventuais problemas, erros conhecidos e soluções alternativas são documentados e aceites pelo cliente, pelos utilizadores finais, pelo apoio operacional e por outras partes afetadas;
- Monitorizar incidentes e problemas causados pela implantação (prestar apoio precoce às equipas operacionais caso a versão tenha provocado um aumento do volume de trabalho);
- Atualizar a documentação de apoio (isto é, os documentos de informação técnica);
- Entregar formalmente a implantação da versão às operações de serviço;
- Documentar os ensinamentos extraídos;
- Recolher o documento de síntese da versão junto das equipas de implantação;
- Encerrar formalmente a versão após verificação do registo do pedido de alteração.

9. GESTÃO DE INCIDENTES DE SEGURANÇA

A gestão de incidentes de segurança é um processo de tratamento de incidentes de segurança que visa permitir a comunicação de incidentes às partes interessadas potencialmente afetadas, a avaliação e priorização de incidentes, e a resposta a incidentes para resolver qualquer violação efetiva, suspeita ou potencial de confidencialidade, disponibilidade ou integridade de ativos de informação sensível.

9.1. Categorização de incidentes de segurança da informação

Todos os incidentes que afetem a ligação entre o registo da União e o registo suíço devem ser analisados para determinar uma possível violação da confidencialidade, da integridade ou da disponibilidade de quaisquer informações sensíveis registadas na lista de informações sensíveis (LIS).

Nesse caso, o incidente deve ser caracterizado como um incidente de segurança da informação, imediatamente registado na ferramenta de gestão de serviços de tecnologias da informação (GSTI) e gerido como tal.

9.2. Tratamento de incidentes de segurança da informação

Os incidentes de segurança são colocados sob a responsabilidade do 3.º nível de intervenção, ficando a resolução dos mesmos a cargo de uma equipa de gestão de incidentes (EGI) específica.

A equipa de gestão de incidentes é responsável por:

- Realizar uma primeira análise, categorizar e avaliar a gravidade do incidente;
- Coordenar ações entre todas as partes interessadas, incluindo a documentação completa da análise do incidente, as decisões tomadas para resolver o incidente e quaisquer possíveis pontos fracos identificados;
- Em função da gravidade do incidente de segurança, escalar o incidente em tempo útil para o nível adequado de informação e/ou decisão.

No processo de gestão da segurança da informação, todas as informações relativas a incidentes são classificadas ao mais alto nível de sensibilidade da informação, nível esse que, em todo o caso, nunca deve ser inferior a «SENSITIVE: *ETS*».

No que se refere a uma investigação em curso e/ou um ponto fraco que possa ser explorado, e até à sua resolução, a informação é classificada como «SPECIAL HANDLING: *ETS Critical*».

9.3. Identificação de incidentes de segurança

Com base no tipo de incidente de segurança, o responsável pela segurança da informação determina as organizações adequadas que devem ser envolvidas e fazer parte da equipa de gestão de incidentes.

9.4. Análise de incidentes de segurança

A equipa de gestão de incidentes assegura a ligação com todas as organizações envolvidas e os membros pertinentes das suas equipas, conforme adequado, para rever o incidente. Durante a análise, é identificada a extensão da perda de confidencialidade, integridade ou disponibilidade de um ativo e são avaliadas as consequências para todas as organizações afetadas. Em seguida, são definidas ações iniciais e de acompanhamento para resolver o incidente e gerir o seu impacto, incluindo o impacto destas ações nos recursos.

9.5. Avaliação da gravidade dos incidentes de segurança, procedimento por etapas e comunicação

A equipa de gestão de incidentes deve avaliar a gravidade de qualquer novo incidente de segurança após a sua caracterização como incidente de segurança e tomar imediatamente as medidas necessárias de acordo com o nível de gravidade.

9.6. Comunicação da resposta de segurança

A equipa de gestão de incidentes inclui os resultados da contenção de incidentes e posterior recuperação no relatório de resposta a incidentes de segurança da informação. O relatório é enviado ao 3.º nível de intervenção por correio eletrónico seguro ou por outros meios de comunicação seguros mutuamente aceites.

A Parte responsável analisa os resultados da contenção e da recuperação e:

- Volta a ligar o registo em caso de desconexão prévia;
- Envia as comunicações de incidentes às equipas dos registos;
- Encerra o incidente.

A equipa de gestão de incidentes deve incluir – de forma segura – pormenores pertinentes no relatório do incidente de segurança da informação, a fim de assegurar um registo e uma comunicação coerentes e de permitir uma ação rápida e adequada para conter o incidente. Após a sua conclusão, a equipa de gestão de incidentes envia, em tempo útil, o relatório final do incidente de segurança da informação.

9.7. Monitorização, reforço da capacidade e melhoria contínua

A equipa de gestão de incidentes apresentará relatórios relativamente a todos os incidentes de segurança até ao 3.º nível de intervenção. Os relatórios serão utilizados por este nível de intervenção para determinar o seguinte:

- Os pontos fracos nos controlos de segurança e/ou no funcionamento que necessitem de ser reforçados;
- A eventual necessidade de melhorar este procedimento para aumentar a sua eficácia na resposta a incidentes;
- Oportunidades de formação e de reforço da capacidade para reforçar ainda a resiliência da segurança da informação dos sistemas de registo, reduzir o risco de futuros incidentes e minimizar o seu impacto.

10. GESTÃO DA SEGURANÇA DA INFORMAÇÃO

A gestão da segurança da informação visa garantir a confidencialidade, a integridade e a disponibilidade das informações classificadas, dos dados e dos serviços de TI de uma organização. Além dos componentes técnicos, incluindo a sua conceção e a realização de testes (ver normas técnicas de ligação), são necessários os procedimentos operacionais comuns a seguir apresentados para cumprir os requisitos de segurança estabelecidos para a ligação permanente entre registos.

10.1. Identificação de informações sensíveis

A sensibilidade de um elemento de informação é avaliada por meio da determinação do nível de impacto a nível empresarial (por exemplo, perdas financeiras, degradação da imagem, violação da lei, etc.) de uma violação de segurança relacionada com a informação em causa.

Os ativos de informação sensível devem ser identificados com base no seu impacto na ligação.

O nível de sensibilidade destas informações deve ser avaliado de acordo com a escala de sensibilidade aplicável a esta ligação e apresentada em pormenor na secção intitulada «Tratamento de incidentes de segurança da informação» do presente documento.

10.2. Níveis de sensibilidade dos ativos de informação

Após a sua identificação, o ativo de informação é classificado aplicando as seguintes regras:

- A identificação de, pelo menos, um nível de confidencialidade, integridade ou disponibilidade ELEVADO classifica o ativo como «SPECIAL HANDLING: *ETS Critical*»;
- A identificação de, pelo menos, um nível de confidencialidade, integridade ou disponibilidade MÉDIO classifica o ativo como «SENSITIVE: *ETS*»;
- A identificação apenas de níveis de confidencialidade, integridade ou disponibilidade BAIXOS classifica o ativo como «EU**:** SENSITIVE: *ETS Joint Procurement».* Marcação na Suíça: «LIMITED: ETS».

10.3. Atribuição de proprietários aos ativos de informação

Todos os ativos de informação devem ter um proprietário atribuído. Os ativos de informação do CELE, pertencentes à ligação entre o DOUE e o DOCS ou associados à mesma, devem ser incluídos numa lista de inventário de ativos comuns, mantida por ambas as Partes. Os ativos de informação do CELE não pertencentes à ligação entre o DOUE e o DOCS devem ser incluídos numa lista de inventário de ativos, mantida pela respetiva Parte.

A propriedade de cada ativo de informação pertencente à ligação entre o DOUE e o DOCS ou associado à mesma deve ser acordada pelas Partes. O proprietário de um ativo de informação é responsável pela avaliação da sua sensibilidade.

O nível de antiguidade do proprietário deve ser adequado ao valor do(s) ativo(s) atribuído(s). A responsabilidade do proprietário pelo(s) ativo(s) e a sua obrigação de manter o nível de confidencialidade, integridade e disponibilidade exigido devem ser acordadas e formalizadas.

10.4. Registo de informações sensíveis

Todas as informações sensíveis devem ser registadas na lista de informações sensíveis (LIS).

Quando pertinente, a agregação de informações sensíveis que possam ter um impacto maior do que o impacto de um único elemento de informação deve ser tida em conta e registada na lista de informações sensíveis (por exemplo, um conjunto de informações armazenadas na base de dados do sistema).

A lista de informações sensíveis não é estática. Ameaças, vulnerabilidades, probabilidades ou consequências de incidentes de segurança relacionados com os ativos podem sofrer alterações sem qualquer indicação, podendo ser introduzidos novos ativos no funcionamento dos sistemas de registo.

Por conseguinte, a lista de informações sensíveis deve ser revista regularmente, devendo qualquer nova informação identificada como sensível ser imediatamente aí registada.

A lista de informações sensíveis deve conter, pelo menos, as seguintes informações para cada entrada:

- Descrição da informação;
- Proprietário da informação;
- Nível de sensibilidade;
- Indicação sobre se a informação inclui dados pessoais;
- Informações adicionais, se necessário.

10.5. Tratamento de informações sensíveis

Quando processadas fora da ligação entre o Registo da União e o Registo Suíço, as informações sensíveis devem ser tratadas em conformidade com as instruções de tratamento.

As informações sensíveis processadas pela ligação entre o Registo da União e o Registo Suíço devem ser tratadas pelas Partes em conformidade com os requisitos de segurança.

10.6. Gestão de acessos

O objetivo da gestão de acessos consiste em conceder a utilizadores autorizados o direito de utilizar um serviço, impedindo simultaneamente o acesso de utilizadores não autorizados. Por vezes, a gestão de acessos é igualmente designada por «gestão de direitos» ou «gestão da identidade».

Para a ligação permanente entre registos e o seu funcionamento, ambas as Partes necessitam de acesso aos seguintes componentes:

- Wiki: um ambiente de colaboração para o intercâmbio de informações comuns, como o planeamento de versões;
- Ferramenta de gestão de serviços de tecnologias da informação (GSTI) para a gestão de incidentes e de problemas (ver capítulo 3 «Abordagem e normas»);
- Sistema de intercâmbio de mensagens: cada Parte deve fornecer um sistema seguro de transferência de mensagens para a transmissão de mensagens que contenham os dados de operações.

O administrador do Registo Suíço e o administrador central do Registo da União garantem que os acessos estejam atualizados e atuam como pontos de contacto das respetivas Partes no que se refere a atividades de gestão de acessos. Os pedidos de acesso são tratados de acordo com os procedimentos de cumprimento de pedidos.

10.7. Gestão de chaves/certificados

Cada Parte é responsável pela sua própria gestão de chaves/certificados (criação, registo, armazenamento, instalação, utilização, renovação, revogação, cópia de segurança e recuperação de certificados/chaves). Conforme descrito nas normas técnicas de ligação, apenas devem ser utilizados certificados digitais emitidos por uma autoridade de certificação (AC) em que ambas as Partes confiem. O tratamento e armazenamento de certificados/chaves deve seguir as disposições estabelecidas nas instruções de tratamento.

Qualquer revogação e/ou renovação de certificados e chaves deve ser coordenada por ambas as Partes. Esta ação é realizada de acordo com os procedimentos de cumprimento de pedidos.

O administrador do Registo Suíço e o administrador central do Registo da União procederão ao intercâmbio de certificados/chaves através de meios de comunicação seguros, de acordo com as disposições estabelecidas nas instruções de tratamento.

Qualquer verificação de certificados/chaves através de quaisquer meios entre as Partes terá lugar fora de banda.

ANEXO III

NORMAS TÉCNICAS DE LIGAÇÃO (NTL)

nos termos do artigo 3.º, n.º 7, do Acordo entre a União Europeia e a Confederação Suíça sobre a ligação dos respetivos regimes de comércio de licenças de emissão de gases com efeito de estufa

Normas para a ligação permanente entre registos

Índice

1. Glossário 10
2. Introdução 11
2.1. Âmbito de aplicação 11
2.2. Destinatários 12
3. Abordagem e normas 12
4. Gestão de incidentes 13
4.1. Deteção e registo de incidentes 13
4.2. Classificação e apoio inicial 14
4.3. Investigação e diagnóstico 14
4.4. Resolução e recuperação 14
4.5. Encerramento de incidentes 15
5. Gestão de problemas 16
5.1. Identificação e registo de problemas 16
5.2. Priorização de problemas 16
5.3. Investigação e diagnóstico de problemas 16
5.4. Resolução 16
5.5. Encerramento de problemas 16
6. Cumprimento de pedidos 17
6.1. Apresentação de pedidos 17
6.2. Registo e análise de pedidos 17
6.3. Aprovação de pedidos 17
6.4. Cumprimento de pedidos 17
6.5. Aplicação do procedimento por etapas aos pedidos 17
6.6. Revisão do cumprimento de pedidos 18
6.7. Encerramento dos pedidos 18
7. Gestão das modificações 19

7.1. Pedido de alteração 19
7.2. Avaliação e planeamento de alterações 19
7.3. Aprovações de alterações 19
7.4. Execução de alterações 19
8. Gestão de versões 20
8.1. Planeamento de versões 20
8.2. Pacote de criação e teste de versões 20
8.3. Preparação da implantação 21
8.4. Restauração de versões 21
8.5. Revisão e encerramento de versões 21
9. Gestão de incidentes de segurança 22
9.1. Categorização de incidentes de segurança da informação 22
9.2. Tratamento de incidentes de segurança da informação 22
9.3. Identificação de incidentes de segurança 22
9.4. Análise de incidentes de segurança 22
9.5. Avaliação da gravidade dos incidentes de segurança, procedimento por etapas e comunicação 23
9.6. Comunicação da resposta de segurança 23
9.7. Monitorização, reforço da capacidade e melhoria contínua 23
10. Gestão da segurança da informação 23
10.1. Identificação de informações sensíveis 24
10.2. Níveis de sensibilidade dos ativos de informação 24
10.3. Atribuição de proprietários aos ativos de informação 24
10.4. Registo de informações sensíveis 24
10.5. Tratamento de informações sensíveis 25
10.6. Gestão de acessos 25
10.7. Gestão de chaves/certificados 25
1. Glossário 31
2. Introdução 34
2.1. Âmbito de aplicação 34
2.2. Destinatários 35
3. Disposições gerais 35
3.1. Arquitetura da ligação de comunicação 35

3.1.1. Intercâmbio de mensagens 35
3.1.2. Mensagem XML — Descrição de alto nível 35
3.1.3. Períodos de ingestão 36
3.1.4. Fluxos de mensagens de operações 36
3.2. Segurança da transferência de dados 39
3.2.1. Barreira de segurança e interconexão de redes 39
3.2.2. Rede privada virtual (RPV) 39
3.2.3. Execução de IPSec 40
3.2.4. Protocolo seguro de transferência de mensagens 40
3.2.5. Cifragem e assinatura XML 40
3.2.6. Chaves criptográficas 40
3.3. Lista de funções ao abrigo da ligação 40
3.3.1. Operações comerciais 41
3.3.2. Protocolo de conciliação 41
3.3.3. Mensagem de teste 41
3.4. Requisitos de registo de dados 42
3.5. Requisitos operacionais 43
4. Disposições em matéria de disponibilidade 44
4.1. Conceção que garante a disponibilidade das comunicações 44
4.2. Inicialização, comunicação, reativação e plano de teste 44
4.2.1. Testes da infraestrutura de TIC interna 45
4.2.2. Testes das comunicações 45
4.2.3. Testes do sistema completo (de extremo a extremo) 45
4.2.4. Testes da segurança 45
4.3. Ambientes de aceitação/teste 46
5. Disposições em matéria de confidencialidade e integridade 46
5.1. Infraestrutura de teste da segurança 47
5.2. Disposições em matéria de suspensão e reativação da ligação 47
5.3. Disposições em matéria de violação da segurança 48
5.4. Orientações relativas aos testes da segurança 48
5.4.1. Programas informáticos (software) 48
5.4.2. Infraestruturas 48
5.5. Disposições em matéria de avaliação de riscos 48

1. GLOSSÁRIO

Quadro 1-1 Acrónimos relativos à atividade comercial e definições

Acrónimo/Termo	Definição
Licença	Uma licença para emitir uma tonelada de equivalente de dióxido de carbono durante um determinado período, válida apenas para efeitos de cumprimento dos requisitos do CELE da UE ou do RCLE da Suíça.
CH	Confederação Suíça
CHU	Tipo de licenças fixas, também denominado CHU2 (referente ao período de compromisso 2 do Protocolo de Quioto), emitido pela Confederação Suíça
CHUA	Licença de emissão da aviação da Suíça.
POC	Procedimentos operacionais comuns Procedimentos desenvolvidos conjuntamente pelas Partes no Acordo com vista a operacionalizar a ligação entre o CELE da UE e o RCLE da Suíça.
Registo CELE	Registo de comércio de licenças de emissão.
CELE	Sistema de comércio de licenças de emissão
UE	União Europeia
LUE	Licenças de emissão gerais da UE
LUEa	Licença de emissão da aviação da UE.
RCUE	Registo Consolidado da União Europeia.
DOUE	Diário de Operações da União Europeia
Registo	Um sistema contabilístico para as licenças emitidas ao abrigo do RCLE, que mantém um registo da propriedade das licenças depositadas em contas eletrónicas.
DOCS	Diário de Operações Complementares da Suíça.
Operação	Um processo inscrito num registo, que inclui a transferência de uma licença de uma conta para outra.

Acrónimo/Termo	Definição
Sistema de diário de operações	O diário de operações contém um registo de cada operação proposta enviada de um registo para o outro.

Quadro 1-2 Acrónimos técnicos e definições

Acrónimo	Definição
Criptografia assimétrica	Utiliza chaves públicas e privadas para cifrar e decifrar dados.
Autoridade de Certificação (AC)	Entidade que emite certificados digitais.
Chave criptográfica	Um elemento de informação que determina o resultado funcional de um algoritmo criptográfico.
Decifragem	Processo inverso à cifragem.
Assinatura digital	Uma técnica matemática utilizada para validar a autenticidade e integridade de uma mensagem, software ou documento digital.
Cifragem	O processo de conversão de informações ou dados num código, especialmente para impedir o acesso não autorizado.
Ingestão de ficheiro	O processo de leitura de um ficheiro.
Barreira de segurança (firewall)	Dispositivo ou software de segurança de rede que monitoriza e controla o tráfego de entrada e saída da rede, com base em regras predefinidas.
Teste de SQE habilitado (heartbeat)	Sinal periódico gerado e monitorizado por equipamento informático ou software para indicar o funcionamento normal ou para sincronizar outras partes de um sistema informático.
IPSEC	Segurança IP. Conjunto de protocolos de rede que autentica e cifra os pacotes de dados para fornecer comunicações cifradas seguras entre dois computadores numa rede IP (Protocolo de Internet).
Testes de penetração	Prática de testar um sistema informático, rede ou aplicação Web para detetar vulnerabilidades de segurança que um atacante poderia explorar.
Processo de conciliação	Processo que visa garantir que dois conjuntos de registos estão de acordo.
RPV (VPN)	Rede privada virtual.

Acrónimo	Definição
XML	Linguagem de Marcação Extensível. Permite aos programadores criar as suas próprias etiquetas (tags) personalizadas, possibilitando a definição, transmissão, validação e interpretação de dados entre aplicações e organizações.

2. INTRODUÇÃO

O Acordo entre a União Europeia e a Confederação Suíça sobre a ligação dos respetivos regimes de comércio de licenças de emissão de gases com efeito de estufa, de 23 de novembro de 2017 («Acordo»), prevê o reconhecimento mútuo das licenças de emissão que possam ser utilizadas para efeitos de conformidade ao abrigo do regime de comércio de licenças de emissão da União Europeia («RCLE-UE») [cuja designação foi entretanto alterada para «sistema de comércio de licenças de emissão da União», com o acrónimo «CELE»] ou do sistema de comércio de licenças de emissão da Suíça («RCLE da Suíça»). Com vista a operacionalizar a ligação entre o CELE da UE e o RCLE da Suíça, é estabelecida uma ligação direta entre o Diário de Operações da União Europeia (DOUE) do Registo da União e o Diário de Operações Complementares da Suíça (DOCS) do Registo Suíço, que permita a transferência entre registos das licenças de emissão atribuídas ao abrigo de cada um dos sistemas (artigo 3.º, n.º 2, do Acordo). Para operacionalizar a ligação entre o CELE da UE e o RCLE da Suíça, em 2020 foi adotada uma solução provisória. A partir de 2023, a ligação dos registos dos dois regimes de comércio de licenças de emissão evoluirá gradualmente para uma ligação permanente entre registos, que deverá ser adotada o mais tardar em 2024, que permita o funcionamento dos mercados ligados no que diz respeito aos benefícios da liquidez do mercado e da execução de transações entre os dois sistemas interligados de forma equivalente a um mercado constituído por dois sistemas, e que permita aos participantes no mercado atuarem como se estivessem num único mercado, sujeito apenas a disposições regulamentares individuais das Partes (anexo II do Acordo).

Nos termos do artigo 3.º, n.º 7, do Acordo, o administrador do Registo Suíço e o administrador central do Registo da União elaboram normas técnicas de ligação com base nos princípios enunciados no anexo II do Acordo, descrevendo pormenorizadamente os requisitos relativos ao estabelecimento de uma conexão sólida e segura entre o DOCS e o DOUE. As normas técnicas de ligação elaboradas pelos administradores produzem efeitos logo que a decisão do Comité Misto seja adotada.

As normas técnicas de ligação foram adotadas pelo Comité Misto através da sua Decisão n.º 2/2020. As normas técnicas de ligação revistas, tal como constam do presente documento, serão adotadas pelo Comité Misto através da sua Decisão n.º 1/2024. Em conformidade com a presente decisão e as solicitações do Comité Misto, o administrador do Registo Suíço e o administrador central do Registo da União elaboraram, e continuarão a atualizar, novas orientações técnicas para operacionalizar a ligação que assegurem que estas sejam continuamente adaptadas aos progressos técnicos e/ou aos novos requisitos relativos à segurança da ligação e ao seu funcionamento eficaz e eficiente.

2.1. Âmbito de aplicação

O presente documento representa o entendimento comum entre as Partes no Acordo sobre o estabelecimento das bases técnicas da ligação entre os registos do CELE da UE e do RCLE da Suíça.

Embora defina a linha de base das especificações técnicas em termos de requisitos de arquitetura, serviço e segurança, serão necessárias orientações mais pormenorizadas para tornar a ligação operacional.

Para assegurar o bom funcionamento da ligação, importa definir processos e procedimentos que a tornem ainda mais operacional. Nos termos do artigo 3.º, n.º 6, do Acordo, essas questões são especificadas num documento que define os procedimentos operacionais comuns, adotado por decisão do Comité Misto.

2.2. Destinatários

Os destinatários do presente documento são o administrador do Registo Suíço e o administrador central do Registo da União.

3. DISPOSIÇÕES GERAIS

3.1. Arquitetura da ligação de comunicação

O objetivo da presente secção é fornecer uma descrição da arquitetura geral da operacionalização da ligação entre o CELE da UE e o RCLE da Suíça, bem como das diferentes componentes envolvidas na mesma.

Uma vez que a segurança é parte essencial da definição da arquitetura, foram adotadas todas as medidas para dispor de uma arquitetura sólida. A ligação permanente do registo utiliza um mecanismo de intercâmbio de ficheiros, que implementa uma ligação segura Air Gap.

A solução técnica utiliza:

- Um protocolo seguro de transferência de mensagens;
- Mensagens XML;
- Assinatura digital e cifragem baseadas em XML;
- RPV (VPN).

A figura seguinte apresenta uma visão global da arquitetura da ligação permanente do registo:

3.1.1. Intercâmbio de mensagens

A comunicação entre o Registo da União e o Registo Suíço baseia-se num mecanismo de troca de mensagens através de canais protegidos. Cada extremidade conta com o seu próprio repositório de mensagens recebidas.

Ambas as Partes mantêm um diário das mensagens recebidas, juntamente com os dados de tratamento.

Os erros ou estados inesperados devem ser comunicados, sob a forma de alertas, e as equipas de apoio devem estar em contacto.

Os erros e eventos inesperados são tratados de acordo com os procedimentos operacionais estabelecidos no processo de gestão de incidentes dos procedimentos operacionais comuns.

3.1.2. Mensagem XML — Descrição de alto nível

Uma Mensagem XML contém um dos seguintes elementos:

- Um ou vários pedidos de operações e/ou uma ou várias respostas a operações;
- Uma operação/resposta relacionada com a conciliação;
- Uma mensagem de teste.

Todas as mensagens contêm um cabeçalho com os seguintes elementos:

- Sistema RCLE de origem;
- Número sequencial.

3.1.3. Períodos de ingestão

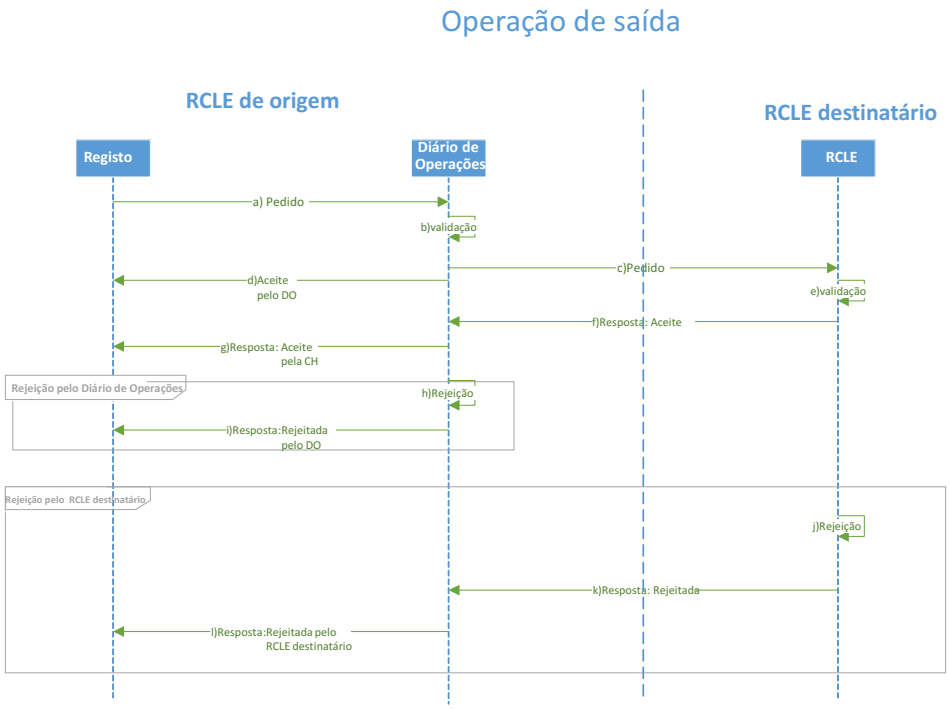
A ligação permanente entre registos baseia-se em períodos de ingestão predefinidos, seguidos de um conjunto de eventos designados. Os pedidos de operações recebidos através da ligação apenas serão ingeridos em intervalos predefinidos e serão alvo de validação técnica à saída e à entrada. Além disso, as conciliações podem ser executadas diariamente e acionadas manualmente.

As alterações da frequência e/ou do momento de realização de quaisquer destes eventos serão tratadas de acordo com os procedimentos operacionais estabelecidos no processo de cumprimento de pedidos dos procedimentos operacionais comuns.

3.1.4. Fluxos de mensagens de operações

Operações de saída

Esta secção reflete o ponto de vista do RCLE de origem da transferência. O fluxo específico é ilustrado no seguinte diagrama sequencial:



O fluxo principal mostra as seguintes etapas (como no desenho acima):

(a) No RCLE de origem da transferência, o pedido de operação é enviado do registo para o diário de operações, após o término de todos os prazos previstos para a atividade comercial (período de 24 horas, quando aplicável);
(b) O diário de operações valida o pedido de operação;
(c) O pedido de operação é enviado para o RCLE destinatário;
(d) A resposta de aceitação é enviada ao registo do RCLE de origem;
(e) O RCLE destinatário valida o pedido de operação;
(f) O RCLE destinatário envia a resposta de aceitação ao diário de operações do RCLE de origem;
(g) O diário de operações envia a resposta de aceitação ao registo.

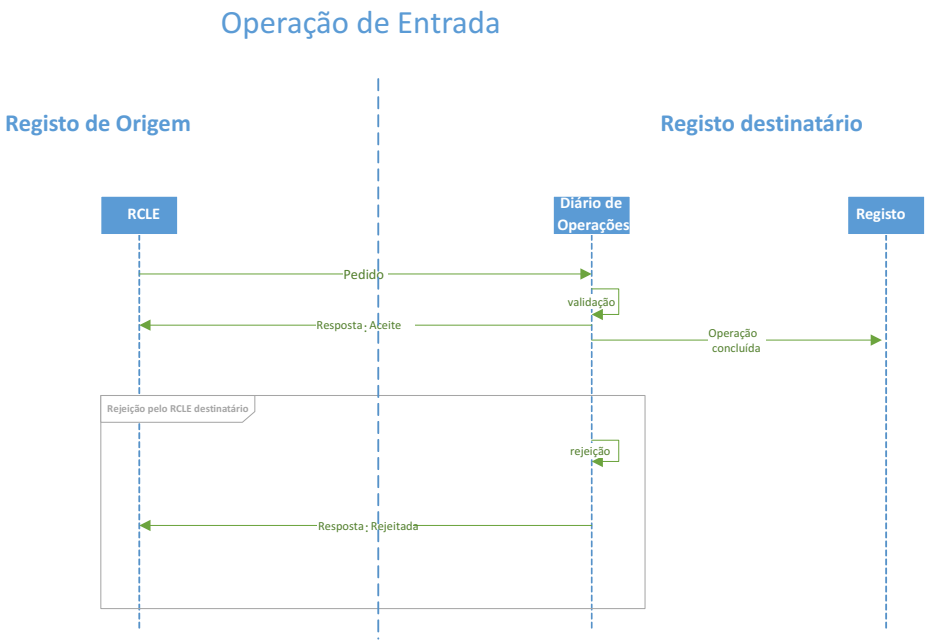
Fluxo alternativo «Rejeição do Diário de Operações» (como no desenho acima, começando por (a) no fluxo principal):

(a) No sistema de origem, o pedido de operação é enviado do registo para o diário de operações, após o término de todos os prazos previstos para a atividade comercial (período de 24 horas, quando aplicável);
(b) O diário de operações não valida o pedido;
(c) A mensagem de rejeição é enviada ao registo de origem.

Fluxo alternativo «Rejeição do RCLE» (como no desenho acima, começando por (d) no fluxo principal):

(a) No RCLE de origem, o pedido de operação é enviado do registo para o diário de operações, após o término de todos os prazos previstos para a atividade comercial (período de 24 horas, quando aplicável);
(b) O diário de operações valida a operação;
(c) O pedido de operação é enviado para o RCLE destinatário;
(d) A mensagem de aceitação é enviada ao registo do RCLE de origem.
(e) O diário de operações do RCLE destinatário da transferência não valida a operação;
(f) O RCLE destinatário da transferência envia a resposta de recusa ao diário de operações do RCLE de origem da transferência;
(g) O diário de operações envia a recusa ao registo.

Operações de entrada



Esta secção reflete o ponto de vista do RCLE destinatário da transferência. O fluxo específico é ilustrado no seguinte diagrama sequencial:

O diagrama mostra:

(1) Quando o diário de operações do RCLE destinatário da transferência valida o pedido, envia a mensagem de aceitação ao RCLE de origem da transferência e uma mensagem de «operação concluída» ao registo do RCLE destinatário.

(2) Quando um pedido recebido é recusado no diário de operações do RCLE destinatário da transferência, o pedido de operação não é enviado para o registo correspondente.

Protocolo

O ciclo de mensagens da operação engloba apenas duas mensagens:

- RCLE de origem da transferência→ Proposta de operação ao RCLE destinatário da transferência.
- RCLE destinatário da transferência→ Resposta à operação do RCLE de origem da transferência: aceite ou rejeitada (incluindo o motivo da rejeição).
  - Aceite: a operação é concluída.
  - Rejeitada: a operação é cessada.

Estado da operação

- O estado da operação do RCLE de origem da transferência será definido como «proposta» quando o pedido é enviado.
- O estado da operação do RCLE destinatário da transferência será definido como «proposta» quando o pedido é recebido e durante o seu tratamento.

- O estado da operação do RCLE destinatário da transferência será definido como «concluída»/«cessada» quando a proposta tiver sido tratada. O RCLE destinatário da transferência enviará então a mensagem de aceitação/rejeição correspondente.
- O estado da operação do RCLE origem da transferência será definido como «concluída»/«cessada» quando a aceitação/rejeição tiver sido recebida e tratada.
- No RCLE de origem da transferência, o estado da operação permanecerá como «proposta» se não for recebida uma resposta.
- O RCLE destinatário da transferência definirá como «cessada» qualquer operação que esteja no estado «proposta» durante mais de 30 minutos.

Os incidentes relacionados com operações serão tratados de acordo com os procedimentos operacionais estabelecidos no processo de gestão de incidentes dos procedimentos operacionais comuns.

3.2. Segurança da transferência de dados

Os dados em trânsito serão objeto de quatro níveis de segurança:

(1) Controlo do acesso à rede: barreira de segurança e camada de interconexão de redes;

(2) Cifragem ao nível do transporte: RPV (VPN).

(3) Cifragem ao nível da sessão: protocolo seguro de transferência de mensagens;

(4) Cifragem ao nível da aplicação: cifragem e assinatura de conteúdos XML.

3.2.1. Barreira de segurança e interconexão de redes

A ligação é estabelecida numa rede protegida por uma barreira de segurança (firewall) baseada em equipamento informático. A barreira de segurança é configurada com regras, de molde a permitir que apenas os clientes «registados» consigam estabelecer ligações ao servidor da RPV.

3.2.2. Rede privada virtual (RPV)

Todas as comunicações entre as Partes são protegidas com recurso a tecnologia de rede privada virtual (RPV). As tecnologias de RPV permitem criar um «túnel» entre dois pontos, através de uma rede como a Internet, protegendo todas as comunicações. Antes da criação do túnel da RPV, é emitido um certificado digital à extremidade de um potencial cliente, para que forneça uma prova de identidade durante a negociação da ligação. Cada Parte é responsável por instalar o certificado na respetiva extremidade da RPV. Utilizando certificados digitais, cada servidor da RPV de destino irá aceder a uma autoridade central para negociar as credenciais de autenticação. Durante o processo de criação do túnel, a cifragem é negociada, garantindo que todas as comunicações efetuadas através do mesmo são protegidas.

As extremidades da RPV do cliente serão configuradas para manter permanentemente o túnel da RPV, com vista a permitir uma comunicação fiável, bidirecional e em tempo real entre as Partes, em todos os momentos.

De um modo geral, a União Europeia utiliza os Serviços Telemáticos Transeuropeus Seguros entre Administrações (STESTA) como rede privada baseada no IP. Por conseguinte, esta rede é também adequada para a ligação permanente entre registos.

3.2.3. Execução de IPSec

A utilização do protocolo IPSec para formar a infraestrutura de RPV «site a site» (site-to-site) garantirá a autenticação «site a site», a integridade e a cifragem dos dados. As configurações de IPSec da RPV garantem a devida autenticação entre duas extremidades numa ligação RPV. As Partes irão identificar e autenticar o cliente remoto através da ligação IPSec, utilizando certificados digitais fornecidos por uma autoridade de certificação reconhecida mutuamente.

A IPSec também garante a integridade dos dados de todas as comunicações transmitidas pelo túnel da RPV. Os pacotes de dados são sujeitos a dispersão (hashed) e assinados com recurso às informações de autenticação estabelecidas pela RPV. A confidencialidade dos dados é também assegurada através da cifragem IPSec.

3.2.4. Protocolo seguro de transferência de mensagens

A ligação permanente entre registos recorre a várias camadas de cifragem para permitir a troca segura de dados entre as Partes. Ambos os sistemas e os seus diferentes ambientes são interligados ao nível da rede através de túneis da RPV. A nível da aplicação, os ficheiros são transferidos utilizando um protocolo seguro de transferência de mensagens a nível da sessão.

3.2.5. Cifragem e assinatura XML

Nos ficheiros XML, a assinatura e a cifragem ocorrem em dois níveis. Todos os pedidos de operações, respostas a operações e mensagens de conciliação são assinados digitalmente, de forma individual.

Numa segunda etapa, cada subelemento do elemento «mensagem» é cifrado individualmente.

Além disso, numa terceira etapa e para assegurar a integridade e a não rejeição de toda a mensagem, a mensagem do elemento raiz é assinada digitalmente, o que resulta num elevado nível de proteção dos dados incorporados no ficheiro XML. A execução técnica obedece às normas do Consórcio World Wide Web.

Para decifrar e verificar a mensagem, o processo segue a ordem inversa.

3.2.6. Chaves criptográficas

Será utilizada criptografia de chave pública para efeitos de cifragem e assinatura.

No caso específico da IPSec, é utilizado um certificado digital emitido por uma autoridade de certificação (AC) na qual ambas as Partes depositam confiança. Esta AC verifica a identidade e emite certificados que são utilizados para identificar uma organização com precisão e configurar canais de comunicação de dados seguros entre as Partes.

As chaves criptográficas são utilizadas para assinar e cifrar canais de comunicação e ficheiros de dados. As Partes trocam digitalmente certificados públicos, utilizando canais seguros, que são verificados fora de banda. Este procedimento é parte integrante do processo de gestão da segurança da informação dos procedimentos operacionais comuns.

3.3. Lista de funções ao abrigo da ligação

A ligação especifica o sistema de transmissão de várias funções que executam os processos comerciais decorrentes do Acordo. Do mesmo modo, inclui especificações relativas ao processo de conciliação e às mensagens de teste que permitirão a execução de um teste de SQE habilitado.

3.3.1. Operações comerciais

Em termos comerciais, a ligação contempla quatro (4) tipos de pedidos de operações:

- Transferência externa:
  - Após a entrada em vigor da ligação entre os RCLE, as licenças da UE e da Suíça são fungíveis e, por conseguinte, totalmente transferíveis entre as Partes;
  - Uma transferência enviada através da ligação irá envolver uma conta de origem num RCLE e uma conta destinatária da transferência no outro RCLE;
  - A transferência pode incluir qualquer quantidade dos quatro (4) tipos de licenças:
    - Licenças de emissão gerais da Suíça (CHU);
    - Licenças de emissão da aviação da Suíça (CHUA);
    - Licenças de emissão gerais da UE (LUE);
    - Licenças emissão da aviação da UE (LUEa).
- Atribuição internacional:

Os operadores de aeronaves geridos por um RCLE com obrigações no outro RCLE e que tenham direito a receber, do segundo, licenças de emissão a título gratuito irão receber licenças de emissão da aviação gratuitas do segundo RCLE através da operação de atribuição internacional.

- Estorno da atribuição internacional:

Esta operação ocorrerá apenas se for necessário estornar na totalidade as licenças de emissão atribuídas a título gratuito à conta de depósito de um operador de aeronaves pelo outro RCLE.

- Restituição dos excedentes atribuídos:

Semelhante ao estorno, mas neste caso não é necessário estornar na íntegra a atribuição, sendo apenas obrigatório restituir as licenças de emissão atribuídas em excesso ao RCLE de origem.

3.3.2. Protocolo de conciliação

As conciliações apenas irão ocorrer após o encerramento dos períodos de ingestão, validação e tratamento de mensagens.

As conciliações são parte integrante das medidas necessárias para assegurar a segurança e a coerência da ligação. As duas Partes acordarão o momento exato da conciliação antes de definir qualquer programação. Se ambas as Partes manifestarem o seu acordo, pode ser programada uma conciliação diária. Será, no entanto, executada, no mínimo, uma conciliação programada após a ingestão.

Não obstante, cada Parte pode iniciar conciliações manuais a qualquer momento.

As alterações do momento e da frequência da conciliação programada serão tratadas de acordo com os procedimentos operacionais estabelecidos no processo de cumprimento de pedidos dos procedimentos operacionais comuns.

3.3.3. Mensagem de teste

Está previsto o envio de uma mensagem para testar a comunicação de extremo a extremo. A mensagem irá conter dados que a identificarão como um teste e, uma vez recebida na outra extremidade, receberá uma resposta.

3.4. Requisitos de registo de dados

A fim de responder à necessidade, de ambas as Partes, de manter informações exatas e coerentes, bem como de disponibilizar ferramentas para resolver incoerências no âmbito do processo de conciliação, as Partes mantêm quatro (4) tipos de registos de dados:

- Diários de operações;
- Registos de conciliação;
- Arquivo de mensagens;
- Registos de auditorias internas.

Todos os dados constantes destes registos são mantidos, no mínimo, durante três (3) meses para fins de resolução de problemas, sendo que a sua conservação posterior irá depender da legislação aplicável em cada extremidade para efeitos de auditoria. Os ficheiros de registo com mais de três (3) meses podem ser arquivados num local seguro, num sistema de TI independente, desde que seja possível recuperá-los ou aceder aos mesmos num prazo razoável.

Diários de operações

Os subsistemas DOUE e DOCS são execuções do diário de operações. Dissociada entre ambos os sistemas CELE.

Mais especificamente, os diários de operações irão manter um registo de cada operação proposta enviada ao outro RCLE. Cada registo contém todos os campos do conteúdo da operação e o resultado posterior da mesma (a resposta do RCLE que recebe o pedido). Os diários de operações manterão também um registo das entradas de operações, bem como da resposta enviada ao RCLE de origem.

Registos de conciliação

O registo de conciliação contém um registo de cada mensagem de conciliação trocada entre as duas Partes, incluindo a identificação da conciliação, o carimbo temporal e o resultado da conciliação: estado de conciliação «aprovada» ou «discrepâncias». Na ligação permanente entre registos, as mensagens de reconciliação de ligações são parte integrante das mensagens trocadas e, por conseguinte, são armazenadas conforme descrito na secção «Arquivo de mensagens».

As duas Partes devem registar cada pedido e a respetiva resposta no registo de conciliação. Embora as informações deste registo não sejam partilhadas diretamente no âmbito do processo de conciliação propriamente dito, pode ser necessário aceder-lhes para resolver incoerências.

Arquivo de mensagens

Ambas as Partes têm de arquivar uma cópia dos dados trocados (os ficheiros XML), enviados e recebidos, indicando se essas mensagens XML estavam ou não no formato correto.

O arquivo destina-se sobretudo a fins de auditoria, permitindo dispor de um comprovativo do que foi enviado e recebido à/da outra Parte. Nesse sentido, juntamente com os ficheiros, também é necessário arquivar os certificados conexos.

Estes ficheiros fornecerão igualmente informações adicionais para efeitos de resolução de problemas.

Registo de auditoria interna

Estes registos são definidos e utilizados por cada Parte isoladamente.

3.5. Requisitos operacionais

Na ligação permanente entre registos, a troca de dados entre os dois sistemas não é totalmente autónoma, ou seja, são necessários operadores e procedimentos para operacionalizar a ligação. Para o efeito, são especificados vários papéis e instrumentos neste processo.

4. DISPOSIÇÕES EM MATÉRIA DE DISPONIBILIDADE

4.1. Conceção que garante a disponibilidade das comunicações

A arquitetura da ligação permanente entre registos consiste, fundamentalmente, numa infraestrutura de TIC e software que permitem a comunicação entre o RCLE da Suíça e o CELE da UE. Garantir elevados níveis de disponibilidade, integridade e confidencialidade deste fluxo de dados torna-se, então, um aspeto essencial a considerar na conceção da ligação permanente entre registos. Uma vez que se trata de um projeto em que a infraestrutura de TIC, o software personalizado e os processos desempenham um papel fundamental, é necessário ter em conta os três elementos para criar um sistema resiliente.

Resiliência da infraestrutura de TIC

O capítulo do presente documento intitulado «Disposições gerais» descreve em pormenor os elementos de base da arquitetura. Ao nível da infraestrutura de TIC, a ligação permanente entre registos cria uma rede RPV resiliente que cria túneis de comunicação seguros, nos quais a transferência de mensagens se processa em segurança. Outros elementos da infraestrutura são configurados em alta disponibilidade e/ou contam com mecanismos de reparação de falhas.

Resiliência do software personalizado

Os módulos de software personalizados reforçam a resiliência, uma vez que tentam restabelecer a comunicação com a outra extremidade durante um determinado período, se por qualquer motivo não estiver disponível.

Resiliência do serviço

Na ligação permanente entre registos, os intercâmbios de dados entre as Partes ocorrem em intervalos predefinidos. Algumas das etapas necessárias nas trocas de dados programadas exigem a intervenção manual dos operadores do sistema e/ou dos administradores dos registos. Tendo em conta este aspeto e para aumentar e disponibilidade e o êxito das trocas:

- Os procedimentos operacionais preveem períodos de tempo para realizar cada etapa;
- Os módulos de software da ligação permanente entre registos executam uma comunicação assíncrona;
- O processo de conciliação automático irá detetar se ocorreram problemas na ingestão dos ficheiros de dados em ambas as extremidades.
- Os processos de monitorização (infraestrutura de TIC e módulos de software personalizados) são considerados e ativam os procedimentos de gestão de incidentes (conforme definidos no documento relativo aos procedimentos operacionais comuns). Esses procedimentos, que visam reduzir o tempo necessário para restabelecer o funcionamento normal após a ocorrência de incidentes, são essenciais para assegurar índices de disponibilidade elevados.

4.2. Inicialização, comunicação, reativação e plano de teste

Os diferentes elementos envolvidos na arquitetura da ligação permanente entre registos são, todos eles, submetidos a vários testes individuais e coletivos, para confirmar que a plataforma está pronta ao nível da infraestrutura de TIC e do sistema de informação. Estes testes de operacionalidade são um pré-requisito obrigatório sempre que a plataforma altera o estado da ligação permanente entre registos de suspenso para operacional.

A ativação do estado operacional da ligação exige então uma execução bem-sucedida de um plano de teste predefinido, que confirmará que cada registo realizou primeiramente um conjunto de testes internos, seguido de uma validação da conectividade de extremo a extremo, antes de iniciar a apresentação de operações reais entre ambas as Partes.

O plano de teste deve mencionar a estratégia geral de teste e informações pormenorizadas sobre a infraestrutura de teste, nomeadamente, deve incluir, para cada elemento em todos os blocos de teste:

- Os critérios de teste e as respetivas ferramentas;
- As funções atribuídas para a realização do teste;
- Os resultados previstos (positivos e negativos);
- A programação do teste;
- Os requisitos de registo dos resultados do teste;
- Documentação de resolução de problemas;
- Disposições em matéria de escalonamento.

Enquanto processo, os testes de ativação do estado operacional podem ser divididos em quatro (4) blocos conceptuais ou fases:

4.2.1. Testes da infraestrutura de TIC interna

Estes testes destinam-se a ser realizados e/ou verificados individualmente pelos administradores de cada registo, em cada extremidade.

Todos os elementos da infraestrutura de TIC, em cada extremidade, são testados individualmente, incluindo cada componente da infraestrutura. Estes testes podem ser executados de forma automática ou manual, devendo verificar que todos os elementos da infraestrutura estão operacionais.

4.2.2. Testes das comunicações

Estes testes serão iniciados individualmente, por cada Parte, e concluídos em cooperação com a outra extremidade.

Quando os elementos individuais estiverem operacionais, será necessário testar os canais de comunicação entre os dois registos. Para este fim, cada Parte deverá verificar que o acesso à Internet funciona, que os túneis da RPV estão estabelecidos e que há conectividade IP «site a site». A acessibilidade dos elementos da infraestrutura locais e remotos e a conectividade IP devem então ser confirmadas à outra extremidade.

4.2.3. Testes do sistema completo (de extremo a extremo)

Estes testes destinam-se a ser executados em cada extremidade e os resultados são partilhados com a contraparte.

Quando os canais de comunicação e todos os componentes individuais de ambos os registos tiverem sido testados, cada extremidade irá preparar uma série de operações e conciliações simuladas, representativas de todas as funções a executar no âmbito da ligação.

4.2.4. Testes da segurança

Estes testes destinam-se a ser realizados ou acionados pelos administradores dos registos em cada extremidade, conforme indicado em pormenor nas secções «Orientações relativas a testes da segurança» e «Disposições de avaliação de riscos».

Só se poderá considerar que a ligação permanente entre registos está operacional quando as quatro fases/blocos terminarem com resultados previsíveis.

Recursos de teste

Cada Parte deve contar com recursos de teste específicos (software e equipamento informático específicos da infraestrutura de TIC) e desenvolver funções de teste no respetivo sistema, para apoiar a validação manual e contínua da plataforma. Os procedimentos de teste manuais, realizados individualmente ou em cooperação, podem ser executados em qualquer altura pelos administradores dos registos. A ativação do estado operacional é, em si, um processo manual.

Também está previsto que a plataforma realize verificações automáticas regularmente. Essas verificações destinam-se a aumentar a disponibilidade da plataforma, ao detetar precocemente potenciais problemas ao nível da infraestrutura ou do software. Este plano de monitorização da plataforma é composto por dois elementos:

- Monitorização das infraestruturas de TIC: em ambas as extremidades, os prestadores de serviços da infraestrutura de TIC procederão à sua monitorização. Os testes automáticos irão abranger os diferentes elementos da infraestrutura e a disponibilidade dos canais de comunicação.
- Monitorização da aplicação: os módulos do software da ligação permanente entre registos realizam uma monitorização das comunicações do sistema ao nível da aplicação (manualmente e/ou em intervalos regulares), que permitirá testar a disponibilidade da ligação de extremo a extremo simulando algumas das operações.

4.3. Ambientes de aceitação/teste

A arquitetura do Registo da União e do Registo Suíço é constituída pelos seguintes três ambientes:

- Produção (PROD): este ambiente contém os dados reais e processa operações reais.
- Aceitação (ACEIT): este ambiente contém dados representativos não reais ou anonimizados. É o ambiente onde os operadores do sistema de ambas as Partes validam as novas versões.
- Teste (TEST): este ambiente contém dados representativos não reais ou anonimizados. O seu acesso está limitado aos administradores dos registos e destina-se à realização de testes de integração por ambas as Partes.

Exceto no que respeita à RPV, os três ambientes são totalmente independentes uns dos outros, o que significa que o equipamento informático, o software, as bases de dados, os ambientes virtuais, os endereços IP e as portas são configurados e funcionam independentemente.

Quanto à configuração da RPV, a comunicação entre os três ambientes tem de ser totalmente independente, o que é assegurado pela utilização do STESTA.

5. DISPOSIÇÕES EM MATÉRIA DE CONFIDENCIALIDADE E INTEGRIDADE

Os mecanismos e procedimentos de segurança preveem uma função a cargo de duas pessoas (princípio dos «quatro olhos») para operações que ocorram na ligação entre o Registo da União e o Registo Suíço. A função a cargo de duas pessoas aplica-se sempre que necessário, mas pode não aplicar-se a todas as etapas realizadas pelos administradores dos registos.

Os requisitos de segurança são considerados e tratados no plano de gestão da segurança, que inclui igualmente processos relacionados com o tratamento dos incidentes de segurança na sequência de

uma eventual violação da segurança. A parte operacional destes processos é descrita nos procedimentos operacionais comuns.

5.1. Infraestrutura de teste da segurança

Cada Parte compromete-se a estabelecer uma infraestrutura de teste da segurança (recorrendo ao software e ao equipamento informático comuns utilizados na deteção de vulnerabilidades nas etapas de desenvolvimento e funcionamento):

- Separada do ambiente de produção;
- Em que a segurança é analisada por uma equipa independente do desenvolvimento e funcionamento do sistema.

Cada Parte compromete-se a realizar análises estáticas e dinâmicas.

No caso das análises dinâmicas (como os testes de penetração), as duas Partes comprometem-se a limitar as avaliações normalmente realizadas aos ambientes de teste e de aceitação (conforme definidos na secção «Ambientes de aceitação/teste»). As exceções à presente política estão sujeitas à aprovação das duas Partes.

Antes de serem implantados no ambiente de produção, todos os módulos de software da ligação (conforme definidos na secção «Arquitetura da ligação de comunicação») são submetidos a testes de segurança.

A infraestrutura de teste tem de ser separada, a nível da rede e da infraestrutura, da infraestrutura de produção e permitir a realização dos testes de segurança necessários para verificar o cumprimento dos requisitos de segurança.

5.2. Disposições em matéria de suspensão e reativação da ligação

Caso exista uma suspeita de que a segurança do Registo Suíço, do DOCS, do Registo da União ou do DOUE esteja comprometida, cada Parte deve informar imediatamente a outra Parte e suspender a ligação entre o DOCS e o DOUE,

Os procedimentos para a partilha de informações, a decisão de suspender e a decisão de reativar fazem parte do processo de cumprimento de pedidos dos procedimentos operacionais comuns.

Suspensões

A suspensão da ligação entre registos, em conformidade com o anexo II do Acordo, pode ocorrer devido a:

- Motivos administrativos (manutenção, etc.), sendo assim planeada;
- Motivos de segurança (ou falhas na infraestrutura de TI), sendo assim não planeada.

Em caso de emergência, cada Parte informará a outra e suspenderá unilateralmente a ligação entre registos.

Se for tomada a decisão de suspender a ligação entre registos, cada Parte irá assegurar que a ligação é interrompida a nível da rede (bloqueando parcialmente ou na totalidade as ligações de entrada e de saída).

A decisão de suspender a ligação entre registos, independentemente de ser ou não planeada, será tomada de acordo com os procedimentos de gestão de alterações ou de gestão de incidentes de segurança dos procedimentos operacionais comuns.

Reativação da comunicação

A decisão de reativação será tomada conforme descrito em pormenor nos procedimentos operacionais comuns e nunca antes de os procedimentos de teste da segurança (conforme indicados nas secções «Orientações relativas aos testes da segurança» e «Inicialização, comunicação, reativação e plano de teste») terem sido concluídos com êxito.

5.3. Disposições em matéria de violação da segurança

Uma violação da segurança é um incidente de segurança que afeta a confidencialidade e a integridade de informações sensíveis e/ou a disponibilidade do sistema que as trata.

As informações sensíveis são identificadas na lista de informações sensíveis e podem ser tratadas no sistema ou em qualquer parte conexa.

As informações diretamente relacionadas com a violação da segurança serão consideradas sensíveis, com a menção «SPECIAL HANDLING: *ETS Critical*» e tratadas de acordo com as instruções de tratamento, salvo especificação em contrário.

Todas as violações da segurança serão tratadas de acordo com o capítulo dos procedimentos operacionais comuns dedicado à gestão de incidentes de segurança.

5.4. Orientações relativas aos testes da segurança

5.4.1. Programas informáticos (software)

Todas as novas versões importantes do software são sujeitas a testes de segurança, incluindo testes de penetração, se aplicáveis, em conformidade com os requisitos de segurança estabelecidos nas normas técnicas de ligação, a fim de avaliar a segurança da ligação e os riscos associados.

Se não tiver sido produzida nenhuma versão importante nos últimos 12 meses, é realizado um teste da segurança do sistema atual que tenha em conta a evolução das ciberameaças ao longo desse período.

Os testes da segurança da ligação entre registos são realizados no ambiente de aceitação e, se necessário, no ambiente de produção, com a coordenação e o acordo mútuo de ambas as Partes.

Os testes da aplicação Web respeitarão as normas abertas internacionais, tais como as desenvolvidas pelo Projeto de Segurança de Aplicações Web Abertas (Open Web Application Security Project, OWASP).

5.4.2. Infraestruturas

A infraestrutura de apoio ao sistema de produção será analisada regularmente para identificar vulnerabilidades (no mínimo, uma vez por mês) e detetar vulnerabilidades corrigidas, de acordo com o princípio definido na secção anterior, utilizando uma base de dados de vulnerabilidades atualizada.

5.5. Disposições em matéria de avaliação de riscos

Se estiverem disponíveis testes de penetração, estes devem ser incluídos nos testes da segurança.

Cada Parte pode contratar uma empresa especializada com vista à realização dos testes da segurança, desde que a mesma:

- Disponha das competências e da experiência necessárias para a realização desses testes da segurança;
- Não esteja subordinada diretamente ao programador e/ou ao seu contratante, não esteja envolvida no desenvolvimento do software da ligação, nem seja uma subcontratante do programador;
- Tenha assinado um acordo de confidencialidade para manter os resultados confidenciais e os tratar de acordo com o nível «SPECIAL HANDLING: ETS Critical» e as instruções de tratamento.