Conselho da
União Europeia

Bruxelas, 24 de junho de 2020
(OR. en)

9068/20
ADD 1

Dossiê interinstitucional:
2020/0123(NLE)

ENV 373
CLIMA 123
ENER 213
IND 83
COMPET 289
MI 196
ECOFIN 532
TRANS 276
AELE 5
CH 11

PROPOSTA

de:	Secretária-geral da Comissão Europeia, com a assinatura de Jordi AYET PUIGARNAU, diretor
data de receção:	23 de junho de 2020
para:	Jeppe TRANHOLM-MIKKELSEN, Secretário-Geral do Conselho da União Europeia
n.° doc. Com.:	COM(2020) 255 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 adoção de procedimentos operacionais comuns

Envia-se em anexo, à atenção das delegações, o documento COM(2020) 255 final - ANEXO.

Anexo: COM(2020) 255 final - ANEXO

COMISSÃO
EUROPEIA

Bruxelas, 23.6.2020
COM(2020) 255 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 adoção de procedimentos operacionais comuns

DECISÃO N.º 1/2020 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

de ...

relativa a procedimentos operacionais comuns

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] (adiante designado por «Acordo»), nomeadamente o artigo 3.º,

Considerando o seguinte:

(1) A Decisão n.º 2/2019 do Comité Misto, de 5 de dezembro de 2019, alterou os anexos I e II do Acordo, satisfazendo assim as condições para o estabelecimento da ligação previstas no Acordo.

(2) Na sequência da adoção da Decisão n.º 2/2019 do Comité Misto e nos termos do artigo 21.º, n.º 3, do Acordo, as Partes trocaram os seus instrumentos de ratificação ou aprovação, pois entendem estar satisfeitas todas as condições para o estabelecimento da ligação previstas no Acordo.

(3) Nos termos do artigo 21.º, n.º 4, do Acordo, este entrou em vigor em 1 de janeiro de 2020.

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

(5) Em conformidade com o artigo 13.º, n.º 1, do Acordo, o Comité Misto deve acordar orientações técnicas para assegurar a correta aplicação do Acordo, designadamente no que respeita 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. As orientações técnicas podem ser elaboradas por um grupo de trabalho criado nos termos do artigo 12.º, n.º 5, do Acordo. O grupo de trabalho deve incluir, pelo menos, o administrador do Registo Suíço e o administrador central do Registo da União, devendo prestar assistência ao Comité Misto no exercício das suas funções nos termos do disposto no artigo 13.º do Acordo.

(6) Dada a natureza técnica das orientações e a necessidade de as adaptar à evolução em curso, as orientações técnicas elaboradas pelo administrador do Registo Suíço e pelo administrador central do Registo da União devem ser apresentadas ao Comité Misto para informação ou, se for caso disso, para aprovação,

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

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

São adotados os procedimentos operacionais comuns que constam do anexo da presente decisão.

Artigo 2.º

É criado um grupo de trabalho nos termos do artigo 12.º, n.º 5, do Acordo. Este grupo prestará assistência ao Comité Misto para assegurar a correta aplicação do Acordo, incluindo no que se refere à elaboração de orientações técnicas para a aplicação dos procedimentos operacionais comuns.

O grupo de trabalho incluirá, pelo menos, o administrador do Registo Suíço e o administrador central do Registo da União.

Artigo 3.º

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

Feito em língua inglesa, em Bruxelas, em XX de XX de 2020.

Pelo Comité Misto

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

APÊNDICE

ANEXO

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 relativos à solução provisória –

1. GLOSSÁRIO

Quadro 1-1 Acrónimos e definições

Acrónimo/Termo	Definição
Autoridade de Certificação (AC)	Entidade que emite certificados digitais
CH	Confederação Suíça
RCLE	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 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 que a ligação entre o CELE e o RCLE da Suíça se torne operacional, deve ser adotada uma solução provisória até maio de 2020 ou o mais rapidamente possível após essa data. As Partes devem cooperar para substituir, o mais rapidamente possível, a solução provisória pela ligação permanente entre registos (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 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, tal como constam do presente documento, deverão ser adotados pelo Comité Misto através da sua Decisão n.º 1/2020. Em conformidade com a presente decisão, o Comité Misto deve solicitar ao administrador do Registo Suíço e ao administrador central do Registo da União que elaborem novas orientações técnicas para operacionalizar a ligação e 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 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 (NTL), 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 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 solução provisória acordada, 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

Com a implantação da ligação permanente entre registos numa data posterior, os procedimentos operacionais comuns devem ser adaptados e complementados, quando necessário.

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 3). As práticas desta norma são reutilizadas e adaptadas às necessidades específicas relacionadas com a solução provisória.
- 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 CH
2.º nível	Gestor de operações da UE	Gestor de aplicações do Registo da CH
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 eletrónico.
- 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 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 CH) 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 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 pertinente que registou o incidente, que 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 fase.

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.

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 resolvido, 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 DE ALTERAÇÕES

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 na fase 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 única 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 EGI 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 os possíveis pontos fracos identificados;
- Dependendo da gravidade do incidente de segurança, remetê-lo oportunamente ao nível adequado para efeitos 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 RCLE SENSÍVEL.

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 RCLE CRÍTICO.

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 EGI.

9.4. Análise de incidentes de segurança

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

9.6. Comunicação da resposta de segurança

A EGI 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 EGI 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 EGI envia, em tempo útil, o relatório final do incidente de segurança da informação.

9.7. Monitorização, reforço da capacidade e melhoria contínua

A EGI 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 mais 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 NTL), são necessários os procedimentos operacionais comuns a seguir apresentados para cumprir os requisitos de segurança estabelecidos para a solução provisória.

10.1. Identificação de informações sensíveis

A sensibilidade das informações é avaliada através 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 as informações 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 RCLE CRÍTICO;
- A identificação de, pelo menos, um nível de confidencialidade, integridade ou disponibilidade MÉDIO classifica o ativo como RCLE SENSÍVEL;
- A identificação apenas de níveis de confidencialidade, integridade ou disponibilidade BAIXOS classifica o ativo como RCLE LIMITADO.

10.3. Atribuição de proprietários aos ativos de informação

Todos os ativos de informação devem ter um proprietário atribuído. Os ativos de informação do RCLE, 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 RCLE 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.

A antiguidade do proprietário deve ser adequada ao valor do(s) ativo(s) atribuído(s). A responsabilidade do proprietário pelo(s) ativo(s) e a 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 uma única informação deve ser tida em conta e registada na LIS (por exemplo, um conjunto de informações armazenadas na base de dados do sistema).

A LIS 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 LIS deve ser revista regularmente, devendo qualquer nova informação identificada como sensível ser imediatamente registada na LIS.

A LIS 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 solução provisória 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 intitulado «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 (NTL), 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.