

Status UPU: 2

Data de adoção deste status: **16 de fevereiro de 2016**

Data da aprovação desta versão: **16 de fevereiro de 2016**

Segurança postal – Medidas gerais de segurança

As normas de segurança da UPU estão atualizadas na íntegra. **Cada atualização dá lugar a uma nova versão, cujo número segue o da norma. Antes de utilizar este documento, assegure-se da sua validade consultando o Catálogo das normas da UPU, disponível gratuitamente no Website da UPU (www.upu.int).**

Cláusula de não-responsabilidade

O presente documento contém as informações mais recentes disponíveis no momento da publicação. A UPU não oferece qualquer garantia, expressa ou implícita, relativamente à exatidão, ao carácter suficiente, ao valor comercial ou à adequação das informações contidas no presente documento. Qualquer utilização é inteiramente da responsabilidade do utilizador.

Aviso – Propriedade intelectual

A UPU sublinha que a implementação desta norma poderá dar lugar à utilização de um direito de propriedade intelectual reivindicado. Os destinatários do presente documento estão convidados a apresentar, com os seus comentários, qualquer informação relativa aos direitos de propriedade intelectual que tenham conhecimento, e a fornecer justificações.

À data de aprovação da norma, a UPU não tinha qualquer informação sobre tais direitos de propriedade intelectual, à exceção das indicações fornecidas na presente publicação. Contudo, a UPU rejeita qualquer responsabilidade decorrente da existência de direitos de propriedade intelectual detidos por terceiros e materializados na sua totalidade ou em parte nas normas da UPU.

Aviso relativo aos direitos autorais

© UPU 2016. Todos os direitos reservados.

Os direitos autorais relativos ao presente documento estão protegidos pela UPU. Apesar de a reprodução do presente documento para fins de utilização pelos participantes no processo de desenvolvimento das normas da UPU ser permitida sem o acordo prévio da UPU, este documento, na sua totalidade ou em parte, não será nem reproduzido nem registado, nem transmitido sob qualquer forma e para qualquer fim sem a permissão prévia escrita da UPU.

Os pedidos de autorização relativos à reprodução do presente documento devem ser enviados para o seguinte endereço:

União Postal Universal
Programa «Normalização»
Case postale 312
3000 BERNE 15
SUIÇA

Telefone: (+41 31) 350 31 11

Fax: (+41 31) 350 31 10

Endereço eletrónico: standards@upu.int

Qualquer reprodução para fins comerciais pode ser sujeita a pagamento de direitos ou a um contrato de licença.

Índice	Página
Prefácio	4
Introdução	5
1. Campo de aplicação	6
2. Referências normativas	6
3. Termos e definições	6
3.1 Controlo de acesso	6
3.2 Instalação principal	6
3.3 Operador designado	6
3.4 Exigência mínima em matéria de segurança	7
3.5 Inspeção	7
3.6 Sistema de acesso único	7
4. Siglas e abreviaturas	7
5. Normas de segurança das instalações principais	7
5.1 Informações gerais relativas às medidas de segurança física	7
5.2 Medidas de controlo de acesso	9
6. Segurança e formação do pessoal	11
6.1 Informações gerais	11
6.2 Segurança do pessoal e procedimentos de recrutamento	11
6.3 Exigências em matéria de segurança relativas aos contratantes	11
6.4 Medidas de sensibilização e de formação	11
7. Transporte e informações de segurança para os operadores designados e os contratantes postais	11
8. Programa de verificação da conformidade e controlo	12
9. Unidade de segurança postal para a prevenção e o controlo	13
9.1 Unidade de segurança postal para a prevenção e o controlo (exigência mínima em segurança)	13
9.2 Recuperação após sinistro, preparação para situações de urgência e planeamento da continuidade das operações	13
Bibliografia	14

Prefácio

Os serviços postais fazem parte do quotidiano dos habitantes de todo o mundo. A União Postal Universal (UPU) é a instituição especializada das Nações Unidas responsável por regulamentar o serviço postal universal. Os serviços postais dos seus 192 Países-membros constituem a mais vasta rede de distribuição física do mundo. Mais de 5 milhões de empregados postais, que trabalham em mais de 660 000 estações de correio em todo o mundo, tratam um total de 434 mil milhões de objetos de correspondência ao nível nacional e mais de 5 mil milhões destes objetos ao nível internacional anualmente. Por outro lado, mais de 6 mil milhões de encomendas são expedidas pelo correio todos os anos. Seguindo o ritmo das alterações no mercado das comunicações, os operadores designados utilizam cada vez mais as novas tecnologias da informação e da comunicação além do que consideramos tradicionalmente como o seu setor essencial de atividade. Respondem às exigências crescentes dos clientes com uma gama alargada de produtos e de serviços de valor acrescentado.

A normalização é uma importante condição prévia para uma exploração postal eficaz e para uma interligação da rede postal universal. O grupo “Normalização” da UPU elabora e gera um número crescente de normas para melhorar as permutas de informações entre os operadores designados. Garante igualmente a compatibilidade das iniciativas da UPU e das outras entidades postais internacionais. Trabalha em estrita colaboração com os correios, os clientes, os fornecedores e outros parceiros, incluindo diferentes organizações internacionais. O Grupo «Normalização» zela pela implementação de normas coerentes em áreas tais como a permuta de dados informatizada (EDI), a codificação do correio, os formulários postais e a obliteração.

As normas da UPU são redigidas de acordo com as regras enunciadas na parte Y do documento «Informações gerais sobre as normas da UPU» e são publicadas pela Secretaria Internacional de acordo com a parte VII deste documento.

A UPU reconhece que a segurança do setor postal é essencial para permitir o comércio, as comunicações e a segurança dos transportes ao nível internacional. A fim de facilitar a elaboração de normas de segurança e de práticas recomendadas para adoção pelos operadores designados, a UPU criou o Grupo «Segurança postal» (GSP).

Este grupo reúne especialistas em matéria de segurança provenientes de alguns Países-membros da UPU e é responsável pela elaboração das estratégias em matéria de segurança mundiais e regionais para ajudar os operadores designados a cumprirem a sua missão na matéria. O GSP esforça-se, através de ações de formação, de missões de conselho e de programas de prevenção, por proteger os empregados e os haveres os operadores designados, assim como por prevenir qualquer forma de fraude, espoliação ou utilização abusiva do correio.

Trata-se da terceira versão do documento. A alteração introduzida na versão anterior, que está indicada por uma barra vertical na margem, diz respeito a uma alteração estrutural do ponto 5.2.2 (Sistemas de controlo de acesso para os funcionários, os visitantes, os prestadores de serviços e os fornecedores).

Introdução

Um dos objetivos do grupo «Segurança Postal» (GSP) é melhorar a segurança de todas as operações do setor postal. O GSP, em colaboração com outros interlocutores da UPU, definiu um conjunto mínimo de exigências em matéria de segurança aplicáveis a todos os aspetos do setor. O facto de elaborar normas de segurança quantificáveis para o setor postal contribui para a proteção dos funcionários, dos bens e dos objetos postais em geral, participa na segurança do transporte utilizado para encaminhar os objetos e permite às autoridades nacionais e internacionais utilizarem instrumentos de avaliação dos riscos

As normas de segurança física e de segurança das operações elaboradas no quadro do GSP são aplicáveis às instalações principais da rede postal. Segundo a publicação deste documento, as normas são as seguintes:

- Norma S58 (Normas de segurança postal – Medidas de segurança geral) (presente documento): define as exigências mínimas em matéria de segurança física e de segurança das operações aplicáveis às instalações principais da rede postal.
- Norma S59 (Normas de segurança postal – Segurança das estações de permuta e do correio-avião internacional): define as exigências mínimas relativas às operações de segurança para o transporte do correio-avião internacional.

Observação: para que a aplicação da norma S59 seja obrigatória, a norma S58 deve ser igualmente implementada. Apenas os agentes habilitados, dentro da Organização da Aviação Civil Internacional (OACI) no anexo 17 da Convenção relativa à aviação civil internacional, podem proceder às inspeções.

Normas de segurança postal – Segurança postal - Medidas gerais de segurança**1. Campo de aplicação**

O presente documento define as exigências mínimas em matéria de segurança física e de segurança das operações aplicáveis às instalações principais da rede postal.

Observação: os operadores designados deverão verificar a conformidade com toda a legislação nacional, regulamentação, etc.

Os operadores designados e as partes da cadeia logística podem fazer prova do respeito pelo Programa nacional de segurança da aviação civil ou pelos programas de certificação de segurança reconhecidos à escala internacional, que devem respeitar as exigências das normas S58 e S59 da UPU.

2. Referências normativas

Os documentos referenciados abaixo são indispensáveis à aplicação dos presentes. Para as referências que incluam uma data ou um número de versão, aplica-se apenas a edição citada. Para as referências sem data e que não incluam número de versão, aplica-se a última edição do documento referenciado (incluindo as suas eventuais modificações).

Organização da aviação civil internacional, Instruções técnicas para a segurança do transporte aéreo das mercadorias perigosas (Doc 9284).

Observação: os pedidos de cópias das publicações da OACI devem ser endereçados diretamente ao Grupo da venda dos documentos da OACI: sales@icao.int.

3. Termos e definições

Alguns termos comumente utilizados no presente documento encontram-se definidos no glossário das normas da UPU e dos documentos citados nas normas de referência e na bibliografia. As definições dos termos frequentemente utilizados ou particularmente importantes, assim como as de outros termos que se encontram no presente documento, encontram-se indicados a seguir.

3.1 Controlo de acesso

Em matéria de segurança física, o termo “controlo de acesso” faz referência à prática que consiste em limitar a entrada numa propriedade, um edifício ou de uma sala a um certo número de pessoas autorizadas.

Observação: o controlo do acesso físico pode efetuar-se através de uma pessoa (um agente de segurança ou um rececionista), por meios mecânicos (fechaduras e chaves) ou através de meios tecnológicos (sistema de cartão).

3.2 Instalação principal

Estação de permuta; centro aerpostal; instalações postais onde têm lugar os controlos de segurança aérea; última instalação postal pela qual transitaram os objetos postais antes de serem expedidos por via aérea.

3.3 Operador designado

Qualquer entidade governamental ou não governamental designada oficialmente pelo País-membro para garantir a exploração dos serviços postais e cumprir as obrigações inerentes decorrentes dos Atos da União no seu território.

3.4 Exigência mínima em matéria de segurança

Técnica, método, processo ou atividade compostos por medidas mínimas a tomar para tornar seguras as operações dentro da instalação principal no que respeita à legislação local, às políticas internas e aos procedimentos.

3.5 Inspeção

Análise do correio através de meios eletrónicos ou de outros meios não intrusivos a fim de identificar ou desativar explosivos.

3.6 Sistema de acesso único

Características físicas dos sistemas de controlo de acessos limitando a entrada de pessoas não autorizadas permitindo o acesso de uma única pessoa à zona controlada antes do encerramento das portas. Este sistema deve permitir evitar o acesso por usurpação de identidade assim como a passagem dos empregados não autorizados, e sem intervenção humana.

Observação: para ser colocado em prática, geralmente utilizam-se torniquetes, ou ainda portas com batentes duplos ou sensores especializados.

4. Siglas e abreviaturas

CCTV	Sistema de televisão em circuito fechado
OD	Operador designado
OACI	Organização da Aviação Civil Internacional
PNSAC	Programa nacional de segurança da aviação civil
GSP	Grupo «Segurança Postal»

5. Normas de segurança das instalações principais

5.1 Informações gerais relativas às medidas de segurança física

As medidas de segurança física relativas às instalações postais principais devem incluir, de acordo com o caso, uma combinação de diferentes medidas de segurança (barreiras perimetrais, iluminação, dispositivos de bloqueio e sistemas de controlo as chaves, agentes de segurança de uniforme e reconhecíveis, sistema de televisão em circuito fechado e sistemas de alarme/de deteção de intrusos).

5.1.1 Avaliação dos riscos e planos de segurança das instalações

Deve realizar-se uma avaliação dos riscos todos os anos para identificar cada instalação principal. Esta avaliação deve ter em conta os haveres do correio, as operações efetuadas da instalação em causa, a taxa de criminalidade geral na zona considerada e outros fatores suscetíveis de reforçar as possibilidades de delito.

Para cada instalação principal, deve ser redigido e atualizado um plano de segurança pormenorizado. O plano de segurança de uma instalação contém todas as medidas de controlo a seguir:

- Normas de conceção da instalação principal.
- Barreiras perimetrais.
- Janelas, portas e outras aberturas perimetrais.
- Iluminação.
- Dispositivos de bloqueio.
- Medidas de controlo de acesso.

S58-3

5.1.2 Normas de conceção da instalação principal

Todas as instalações devem ser construídas segundo as normas nacionais de segurança relativas à conceção dos edifícios. Devem ser utilizados materiais resilientes a fim de impedir qualquer acesso não autorizado.

Deve ser implementado um programa especial de inspeção e de reparações anuais para garantir a integridade das estruturas; deve incluir os prazos de realização das eventuais reparações. A inspeção anual deve igualmente incluir uma avaliação dos riscos dos ambientes, o perfil do produto postal tratado na instalação, assim como eventuais outras modificações de funcionamento que possam ter consequências na segurança do edifício e dos seus funcionários.

As zonas reservadas devem ser facilmente identificáveis, devidamente assinaladas e com segurança através das medidas de controlo de acesso que se impõem.

5.1.3 Barreiras perimetrais

Barreiras físicas, por exemplo as grades, os muros e os portões para os veículos, devem ser instalados para impedir o acesso de pessoas ou de veículos não autorizados nas zonas reservadas da instalação principal.

As vedações ou os muros de separação devem ser instalados a uma certa distância da instalação para permitir a vigilância de intrusos que tentem entrar nas zonas reservadas.

As zonas adjacentes às vedações não devem estar encobertas por detritos, arbustos e arvoredo, dado que estes elementos podem ser utilizados para penetrar na zona sujeita a segurança.

Devem realizar-se inspeções semanais às vedações para garantir a sua integridade.

5.1.4 Janelas, portas ou outras aberturas perimetrais

Todas as portas exteriores devem ser suficientemente sólidas para impedir ou atrasar um acesso á força com a ajuda de instrumentos manuais ou de outros meios de agressão.

Devem existir o mínimo possível de portas para garantir um acesso adequado às zonas com segurança da instalação, sem esquecer as saídas de emergência.

Devem ser colocados sinais e letreiros nas portas exteriores a fim de indicar quais são as zonas reservadas, exceto se tal representar uma obstrução visível ou se a regulamentação local o não permitir. Se necessário, devem estar bem visíveis sinais a descrever as responsabilidades e os procedimentos de informação das autoridades quando forem cometidos atos criminosos na instalação.

Todas as janelas, portas e outras aberturas exteriores devem estar seguras com a ajuda de mecanismos de bloqueio apropriados.

A avaliação dos riscos de instalação pode revelar a necessidade de medidas de segurança suplementares, por exemplo de janelas equipadas de barreiras, de grades ou de qualquer outro dispositivo com vista a reforçar a segurança do ponto de acesso contra qualquer entrada não autorizada.

5.1.5 Iluminação

Devem ser instalados sistemas de iluminação adequados em todas as zonas pedestres, nas zonas de entrada/saída de veículos, nas áreas externas de trabalho, nos parques de estacionamento e ao longo das vedações ou muros. A iluminação deve ser suficiente para identificar as pessoas ou os veículos situados nas proximidades. A instalação de dispositivos de iluminação nas zonas situadas na proximidade dos aeroportos ou das vias de circulação deve respeitar as normas da aviação civil/aeroporto.

Se for utilizado um sistema de televisão em circuito fechado, é conveniente iluminar bem as zonas interiores, nomeadamente os locais de armazenamento operacional.

Deve ser instalada uma iluminação nas zonas operacionais essenciais.

5.1.6 Dispositivos de bloqueio e sistemas de controlo das chaves

Todos os dispositivos de bloqueio para os pontos de entrada/saída de peões ou de veículos devem ser concebidos a partir de materiais reforçados, a fim de impedir o acesso de pessoas não autorizadas.

Deve ser implementado um sistema de controlo das chaves para garantir uma responsabilização dos detentores das chaves.

O sistema deve permitir registar os dados relativos à distribuição das chaves e proteger o acesso às chaves não distribuídas.

Este sistema deve ser gerado pela unidade encarregada da segurança postal ou pelos responsáveis dos estabelecimentos postais em questão.

5.2 Medidas de controlo de acesso

5.2.1 Informações gerais

As medidas de controlo de acesso que impeçam o acesso não autorizado ao correio e aos veículos utilizados para o encaminhamento do correio nas instalações principais. O controlo do acesso a todas as instalações principais deve ser de um nível absolutamente adequado a fim de proteger os pertences dos correios.

Observação: as medidas de controlo de acesso podem ser manuais, com agentes de segurança fixos colocados nos pontos de entrada/saída para verificar a identidade das pessoas ou dos veículos que entram nas zonas sujeitas a segurança. As medidas de controlo de acesso podem igualmente basear-se em sistemas eletrónicos simples ou complexos utilizados para efetuar verificações e permitir o acesso às zonas sujeitas a segurança. Independentemente dos aspetos tecnológicos ligados aos métodos utilizados, o sistema deve ser capaz de filtrar adequadamente os indivíduos em todos os pontos de entrada e de diferenciar os diversos tipos de acesso privilegiado de acordo com o tipo de pessoas em questão: funcionários, visitantes, prestadores de serviços ou fornecedores. O sistema de controlo de acesso de uma instalação principal deve ser segmentado de modo a garantir que os funcionários, os visitantes, os fornecedores de serviços e os vendedores beneficiem unicamente de um acesso às zonas necessárias no quadro das suas funções e das suas atividades.

5.2.2 Sistemas de controlo de acesso para os funcionários, os visitantes, os prestadores de serviços e os fornecedores

Deve ser implementado um procedimento adequado de controlo de acesso nas zonas sujeitas a segurança (interditas aos clientes) de todas as instalações principais. Pelo menos um dos elementos a seguir deve ser aplicado:

- 1º Sistema de controlo de acessos manual:
 - a) Agentes de segurança em uniforme, um rececionista ou qualquer outro membro do pessoal devem ser colocados nos pontos de entrada/saída a fim de verificar os privilégios de acesso de cada pessoa.
 - b) O processo manual deve estar documentado sob a forma de um procedimento operacional normalizado.
 - c) Há que assegurar uma formação e dar instruções ao pessoal encarregado de gerir o sistema e aos funcionários colocados nos pontos fixos de controlo de acessos.
 - d) Deve ser utilizado um sistema de registo para conservar os dados relativos ao acesso de pessoas para além dos funcionários às zonas sujeitas a segurança na instalação principal.
- 2º Sistema de controlo de acessos automatizado (eletrónico).

Observação 1: convém limitar os objetos pessoais e implementar procedimentos de busca.

O sistema deve ser concebido de forma a impedir o acesso não autorizado de pessoas pelos pontos de entrada/saída, graças a um sistema ou a um procedimento de acesso único. Deve tratar-se de um sistema que deixe passar unicamente o detentor do cartão que ativa o ponto de acesso.

Observação 2: o sistema de acesso único pode ser igualmente implementado pela colocação num ponto fixo de um agente de segurança com uniforme ou de um outro funcionário responsável por controlar as entradas/saídas no ponto de acesso. Se o ponto de entrada/saída não estiver sob vigilância, deve ser utilizado um sistema de controlo de acesso físico (torniquetes, portas e portadas de acesso), ativado por leitores de cartões ou de chaves automáticas.

Deve ser implementado um sistema de registo dos visitantes para conservar os dados relativos ao acesso de pessoas para além dos funcionários às zonas sujeitas a segurança na instalação principal.

5.2.3 Sistemas de controlo dos acessos para os veículos

Apenas os veículos oficiais e os veículos aprovados dos contratantes devem estar autorizados nas zonas utilizadas para o carregamento/transporte do correio ou às outras zonas exteriores sujeitas a segurança.

O acesso a estas zonas deve estar indicado de forma clara, nomeadamente graças a sinalização, para fazer conhecer os limites da zona reservada.

Deve ser utilizado um sistema de controlo de acesso manual ou automatizado para os veículos não autorizados que não possam aceder à zona exterior sujeita a segurança.

Se um veículo não oficial ou de terceiros entrar na zona exterior sujeita a segurança, há que aplicar um procedimento a fim de verificar a identidade do motorista e, se necessário, inspecionar o veículo antes que entre na zona sujeita a segurança.

Os lugares de estacionamento dos funcionários devem situar-se numa zona à parte da zona reservada aos veículos oficiais.

Os lugares de estacionamento reservados aos visitantes devem estar separados das zonas sujeitas a segurança reservadas aos veículos oficiais.

5.2.4 Sistemas de identificação

Deve ser implementado um sistema de identificação dos funcionários e dos visitantes para conhecer com exatidão a identidade dos funcionários e dos visitantes que entram na instalação principal.

O pessoal postal (fixo, temporário ou a contrato) deve receber um cartão que permita uma identificação fácil, indicando o nome jurídico da pessoa tal como está registado no sistema dos recursos humanos, uma fotografia e uma data de validade. Outras informações, como o nível de acesso, o departamento ou a unidade podem ser acrescentados em função da regulamentação e da legislação locais.

A unidade responsável pela segurança postal ou outros responsáveis postais devem garantir o controlo, a emissão e a renovação dos cartões de identificação destinados aos funcionários, aos visitantes e aos contratantes. Deve ser seguido um procedimento para a declaração e a comunicação das informações sobre os empregados.

Deve ser utilizado um sistema para inspecionar e identificar todos os veículos antes da sua entrada nas zonas exteriores protegidas.

6. Segurança e formação do pessoal

6.1 Informações gerais

Os funcionários são indispensáveis às operações postais; é assim fundamental para os operadores minimizarem eventuais riscos para a segurança que representam novos funcionários ou prestadores de serviços, assim como os que resultam da recolocação dos funcionários postais que necessitem de um controlo ou de uma formação diferentes. A segurança e a formação do pessoal devem estar organizadas de forma a reduzir e minimizar os riscos para a segurança das operações, dos clientes e dos funcionários.

6.2 Segurança do pessoal e procedimentos de recrutamento

A política de seleção e de recrutamento do pessoal deve estar documentada para todos os funcionários que trabalham nas instalações do OD ou que se ocupam do tratamento do correio em locais externos.

A política de recrutamento deve estar conforme a legislação nacional a fim de zelar para que os funcionários e os contratantes atuais e futuros sejam suficientemente qualificados para cumprir as suas tarefas postais de forma integrada.

Os funcionários fixos devem ser sujeitos a uma entrevista de fundo (verificação dos antecedentes criminais ou policiais), de acordo com as disposições da legislação nacional.

Deve ser seguido um procedimento de acompanhamento para a declaração e comunicação dos desempenhos e das faltas dos funcionários.

O processo de contratação inclui entrevistas, uma verificação de dados antes da entrevista e outras medidas de controlo, em função do posto ou das funções em questão.

A rescisão do contrato de um funcionário ou de um contratante deve estar bem documentada.

O processo de rescisão deve garantir a devolução atempada dos documentos de identificação, dos dispositivos de controlo de acesso, das chaves, dos uniformes e de outras informações sensíveis.

Deve ser alimentado um sistema de registo a fim de impedir a reintegração de um funcionário ou de um contratante despedido por falta.

6.3 Exigências em matéria de segurança relativamente aos contratantes

Os contratantes habituados a efetuar operações de tratamento/transporte do correio ou a exercer outras funções delicadas devem implementar medidas de segurança do pessoal semelhantes às do OD, de acordo com o conteúdo da secção 6.2.

O contratante deve comunicar ao OD as eventuais conclusões ou decisões relativas aos funcionários que podem potencialmente representar um risco para a segurança das operações.

6.4 Medidas de sensibilização e de formação

Deve estar documentado um programa de formação e de sensibilização para as questões de segurança, transversal a todos os funcionários e contratantes.

7. Transporte e instruções de segurança para os operadores designados e os contratantes postais

O OD e os contratantes autorizados devem apoiar-se em procedimentos bem documentados que permitam proteger a segurança do correio, independentemente do seu meio de transporte (avião, estrada, via marítima e caminho de ferro). O OD deve respeitar todas as disposições aplicáveis à legislação nacional relativas às normas de transporte.

S58-3

O acesso ao correio deve ser limitado, em função das necessidades, aos funcionários dos correios e aos contratantes encarregados de tratar o correio.

Os veículos de transporte do correio devem ser concebidos com materiais resilientes e possuir algumas características como um teto sólido, paredes sólidas ou paredes leves reforçadas, assim como portas de carregamento que possam ser bloqueadas. Os veículos devem ser inspecionados antes do carregamento, e os eventuais sinais de alteração devem estar bem visíveis.

Quando os veículos que transportam correio estão em trânsito ou são deixados sem vigilância fora dos locais sujeitos a segurança dos correios ou dos contratantes, devem ser bloqueados em todos os pontos de acesso ao correio.

Os veículos ou os meios de transporte devem, se possível, ter uma menção clara indicando que se trata de veículos postais autorizados ou de veículos contratados pelos correios.

Os operadores responsáveis pelo transporte (quer se trate de OD ou de contratantes) devem, se possível, envergar um uniforme dos correios e/ou possuir e expor de forma clara uma identificação postal ou do contratante válida, seja de que forma for.

A cabine do veículo e as chaves de contacto de todos os meios de transporte devem estar protegidos para evitar qualquer acesso não autorizado.

Deve ser implementado um processo de responsabilização.

Os itinerários, os horários e as paragens previstas devem ser sujeitas a uma avaliação dos riscos e, se necessário, devem ser tomadas medidas de segurança suplementares.

Os veículos, os meios de transporte ou os contentores devem ser corretamente esvaziados.

8. Programa de verificação da conformidade e controlo

Deve ser efetuada uma verificação da conformidade todos os anos pelo pessoal externo à equipa de gestão de uma instalação principal.

Estas pessoas devem dispor da autoridade necessária para obter as informações úteis e para implementar as medidas corretivas.

O programa de verificação da conformidade cobre todo o programa de segurança do correio para garantir o respeito pelas exigências em matéria de segurança. Este programa deve sublinhar, entre outros os seguintes elementos:

- Segurança das instalações.
- Segurança do pessoal.
- Segurança do transporte.

O OD deve garantir que a gestão do programa de verificação da conformidade é confiada a pessoas que não têm qualquer responsabilidade na aplicação das exigências de segurança.

É conveniente ter as pastas das verificações da conformidade e das recomendações.

Os resultados das verificações de conformidade devem ser transmitidos à direção executiva do OD. As ações devem ser vigiadas e documentadas.

9. Unidade da segurança postal para a prevenção e o controlo

9.1 *Unidade de segurança postal para a prevenção e o controlo (exigência mínima em matéria de segurança)*

O OD deve dispor de um programa de segurança documentado que cubra todas as áreas da prevenção e dos processos relativos à proteção do correio, dos funcionários, dos parceiros, dos clientes e dos haveres postais. Este programa deve ser comunicado a todos os funcionários.

Exemplo: equipamento, veículos, uniformes, tecnologias da informação, etc.

O OD deve poder contar com uma unidade de segurança postal ou com funcionários especificamente encarregados de tomarem medidas de segurança. O número de funcionários que cumprem estas funções deve ser proporcional à dimensão e às operações do OD.

A Unidade de segurança postal ou os funcionários especificamente responsáveis pela segurança devem efetuar análises periódicas à segurança das instalações e dos processos.

9.2 *Retomada da atividade pós-sinistro, preparação para situações de emergência e planeamento da continuidade das operações*

Os elementos a seguir devem ser documentados pelo OD e comunicados aos funcionários em questão:

- Um plano de gestão das crises com vista a garantir a segurança do correio, dos funcionários, dos clientes e dos haveres postais em caso de catástrofe de origem natural ou humana suscetível de afetar as permutas de correio ou as operações postais.
- Um plano para prosseguir com as atividades a fim de minimizar as interrupções dos serviços postais em caso de incidente maior suscetível de afetar as as operações postais nacionais ou internacionais.

Bibliografia

Esta bibliografia apresenta referências e indicações completas relativamente à fonte de todas as normas e de todos os outros documentos citados no texto do presente documento. Para as referências com uma data ou um número de versão particulares, as modificações ou revisões posteriores destas publicações podem não ser pertinentes. Contudo, os utilizadores do presente documento estão convidados a informar-se sobre a existência e a aplicabilidade de edições mais recentes. Para as referências sem data ou sem número de versão, aplica-se a última edição do documento citado. Lembramos que apenas os documentos mencionados no texto se encontram indicados a seguir.

1. Organização da Aviação Civil Internacional, Anexo 17 à Convenção relativa à aviação civil internacional: Segurança – Proteção da aviação civil internacional contra os atos de intervenção ilícita.

Observação: os pedidos de cópias das publicações da OACI devem ser endereçados diretamente ao Grupo de venda dos documentos da OACI: sales@icao.int.