



FSR 2026

TAPA Global Standard



TAPA Americas

1353 Riverstone Pkwy,
Ste 120-320
Canton, GA 30114 USA

www.tapaonline.org

TAPA Asia Pacific

10 Anson Rd, #33-15
International Plaza,
Singapore 079903

www.tapa-apac.org

TAPA EMEA

Kanaalpark 140
2321 JV Leiden
The Netherlands

www.tapaemea.org

Sumário

1.0	Introdução	4
1.1	Objetivo deste Documento FSR.....	4
1.2	Recursos para implementar o TAPA FSR.....	4
1.3	Proteção das Políticas e Procedimentos do LSP.....	4
2.0	Sobre a TAPA.....	5
2.1	Finalidade da TAPA	5
2.2	Missão da TAPA	5
3.0	Requisitos TAPA.....	6
3.1	Requisitos de Segurança TAPA.....	6
3.2	Implementação	6
4.0	Orientação Legal	7
4.1	Escopo	7
4.2	Tradução	7
4.3	A Marca “TAPA”	7
4.4	Limitação de Responsabilidade.....	7
5.0	Contratos e Subcontratação.....	8
5.1	Contratos	8
5.2	Subcontratação	8
5.3	Investigação e Resolução de Reclamações da TAPA	8
6.0	Dispensas.....	9
7.0	Requisitos de Segurança da Instalação	10
S1.	Requisitos Gerais.....	10
S2.	Perímetro	12
2.1	Área Externa de Manuseio de Carga, Expedição e Recebimento do Armazém	12
2.2	Barreiras Físicas.....	12
2.3	Áreas Externas de Cais.....	13
2.4	Acesso de Veículos Pessoais	14
S3.	Paredes Externas, Telhado e Portas	15
3.1	Lados Externos da Instalação: CCTV/VSS	15
3.2	Paredes Externas e Telhado	15
S4.	Pontos de Entrada e Saída do Escritório e Armazém.....	18
4.1	Ponto(s) de Entrada de Visitantes na Área de Escritório	18
4.2	Ponto(s) de Entrada da Força de Trabalho.....	19
4.3	Driver and Vehicle Identification.....	19
S5.	Interior do Armazém e Escritório.....	21
5.1	Área do Armazém: Paredes Multiusuário	21
5.2	Áreas Internas do Armazém.....	21

5.3	Portas de Cais Internas e Áreas de Cais	22
5.4	Controle de Acesso entre Escritório e Cais/Armazém	22
5.5	Área de Carga de Alto Valor (HVC)	23
5.6	Inspeção de Resíduos do Armazém	24
5.7	Pré-Carregamento e Área de Preparação (Staging).....	24
5.8	Contêineres Pessoais e Inspeções na Saída	25
5.9	Controle de Equipamentos de Manuseio de Carga	25
5.10	Integridade de Contêineres ou Reboques: Inspeção de 7 Pontos.....	26
5.11	Processo de Entrega de Carga; Lacres de Segurança.....	26
5.12	Integridade da Carga; Processo de Validação de Carregamento/Descarregamento	27
5.13	Fraudulent Pick-Ups	27
S6.	Sistemas de Segurança: Projeto, Monitoramento e Resposta	28
6.1	Posto de Monitoramento	28
6.2	Sistema de Detecção de Intrusão (IDS).....	28
6.3	Sistema Automático de Controle de Acesso (AACs).....	29
6.4	CCTV/ VSS.....	30
6.5	Iluminação Externa e Interna	30
S7.	Treinamento e Procedimentos	31
7.1	Procedimentos de Escalonamento.....	31
7.2	Compromisso da Gestão.....	31
7.3	Treinamento	31
7.4	Acesso aos Ativos do Comprador	32
7.5	Controle de Informação.....	32
7.6	Relato de Incidentes de Segurança	32
7.7	Programas de Manutenção	32
7.8	Integração de Contratados.....	33
7.9	Registros de Expedição e Recebimento.....	33
7.10	Processo de Pré-Alerta Implementado.....	34
S8.	Integridade da Força de Trabalho.....	35
8.1	Triagem / Verificação / Verificação de Antecedentes (conforme permitido pela legislação local) 35	
8.2	Desligamento ou Recontratação da Força de Trabalho	35
S9.	Requisitos da Função Central (aplicável apenas para Certificação Multi-site).....	37
9.1	Geral.....	37
9.2	Políticas e Procedimentos.....	38
9.3	Relatório de Auditoria de Autoavaliação realizado para todos os sites	38
9.4	Registros de inspeções, logs (registros de visitantes/motoristas), inspeções de 7 pontos	38
9.5	Avaliação de Risco de todos os sites.....	39
9.6	Layout de CCTV/VSS e alarmes do site	39
9.7	Registros de Alarmes e Controle de Acesso	39
9.8	Registros de Treinamento	39
9.9	Registros de Triagem/Verificação	40
9.10	Revisão da Gestão para avaliar autoauditorias; SCARs geradas; perdas, roubos; Avaliações de Risco40	
8.0	Ameaças de TI e Cibersegurança – Opção Avançada.....	41
E8.	E8 Requisitos Obrigatórios	41

1.0 Introdução

1.1 Objetivo deste Documento FSR

Este documento de Requisitos de Segurança de Instalações (FSR) é o normativo oficial da TAPA para o processo logístico de mercadorias e armazenamento seguros. Trata-se de um normativo global comum que pode ser utilizada em acordos comerciais na dimensão da segurança entre Clientes e Fornecedores de serviços logísticos (LSP) e/ou outros Requerentes que pretendam a Certificação.

No desenvolvimento deste normativo, a TAPA reconhece as múltiplas diferenças na forma como os serviços de armazenamento são fornecidos globalmente, regionalmente e até mesmo dentro das empresas, e que o FSR pode ser aplicado a todos ou a parte dos serviços fornecidos por um LSP/Requerente. Dependendo da complexidade e do tamanho da cadeia de abastecimento, a conformidade com os requisitos da TAPA pode ser alcançada por meio de um único LSP/Requerente ou de múltiplos LSPs/Requerentes e subcontratados qualificados.

Âmbito da Certificação

A TAPA desenvolveu três opções para apoiar a certificação:

- Certificação de uma única instalação pelo Organismo de Auditoria Independente (IAB).
- Certificação de múltiplas instalações pelo IAB.
- Certificação de autoauditoria por Auditores Autorizados (AA) pelo LSP/Requerente ou IAB (a executar uma autoauditoria em nome do LSP/Requerente).

Público-alvo

Os utilizadores típicos dos Requisitos TAPA incluem:

- Clientes
- LSPs/Requerentes
- Autoridades Policiais ou outras Organizações Governamentais
- Organizações Profissionais da Cadeia de Abastecimento
- Seguradoras

1.2 Recursos para implementar o FSR da TAPA

Os recursos para cumprir os requisitos da norma FSR serão da responsabilidade do LSP/Requerente assim como os custos associados ao seu cumprimento, exceto se negociados ou acordados de outra forma pelo Cliente e pelo LSP/Requerente.

1.3 Proteção das Políticas e Procedimentos do LSP

Cópias de documentos de políticas e procedimentos de segurança só serão transmitidas ao Cliente em conformidade com os acordos de divulgação assinados entre o LSP/Requerente e o Cliente, e serão obrigatoriamente tratadas como informações confidenciais.

2.0 Sobre a TAPA

2.1 Finalidade da TAPA

O crime contra a carga é um dos maiores desafios da cadeia de abastecimento para os fabricantes de produtos de valor elevado e de alto risco e para os seus fornecedores de serviços de logística.

A ameaça já não vem apenas de criminosos oportunistas. Atualmente, as redes de crime organizado operam globalmente e utilizam ataques cada vez mais sofisticados a veículos, instalações e pessoal para alcançarem os seus objetivos.

A TAPA é um fórum único que une fabricantes globais, prestadores de serviços logísticos, transportadoras, autoridades policiais e outras partes interessadas com o objetivo comum de reduzir as perdas das cadeias de abastecimento internacionais. O foco principal da TAPA é a prevenção de roubos através do uso de inteligência em tempo real e as mais recentes medidas preventivas.

2.2 Missão da TAPA

A missão da TAPA é ajudar a proteger os ativos dos membros, minimizando as perdas de carga da cadeia de abastecimento. A TAPA alcança isso através do desenvolvimento e aplicação de Requisitos de Segurança globais, práticas reconhecidas do setor, tecnologia, educação, *benchmarking*, colaboração regulatória e identificação proativa de tendências de crime e ameaças à segurança da cadeia de abastecimento.

3.0 Normas TAPA

3.1 Normas de segurança TAPA

Os seguintes Requisitos de Segurança TAPA globais foram criados para garantir o transporte e armazenagem seguros de mercadorias de alto valor, alvos de roubo:

- Os Requisitos de Segurança das Instalações (FSR) representam normas mínimas de *armazenamento seguro, seja em armazém seja em trânsito*, dentro de uma cadeia de abastecimento.
- Os Requisitos de Segurança do Transporte Rodoviário (TSR) centram-se exclusivamente no transporte por camião e representam os requisitos mínimos específicos para o *transporte rodoviário de produtos* dentro de uma cadeia de abastecimento.
- Os Requisitos de Cibersegurança (CSS) têm como objetivo disponibilizar uma ferramenta que permita às empresas compreender os requisitos mínimos de gestão de TI nas operações da cadeia de abastecimento, com vista à proteção dos ativos digitais contra ciberataques e falhas operacionais.

Os Requisitos de Segurança Globais da TAPA são analisados e revistos conforme necessário a cada três anos.

Este documento aborda apenas os requisitos do FSR!

- O processo de certificação para TAPA FSR está documentado no documento TAPA FSR Certification Framework.
- Ambas as versões atuais do TAPA FSR e do documento TAPA FSR Certification Framework devem ser seguidas para alcançar a certificação TAPA FSR.

3.2 Implementação

A implementação bem-sucedida dos Requisitos de Segurança TAPA depende do trabalho conjunto dos LSP's (Prestadores de Serviços Logísticos)/ Requerentes, Clientes (proprietários da carga) e Auditores Autorizados TAPA.

4.0 Orientação Jurídica

4.1 Âmbito da Certificação

O FSR é um normativo global, e todas as seções do normativo são obrigatórias, salvo quando uma exceção é concedida por meio do processo oficial de dispensa (consulte a Seção 6 do Normativo FSR e a Seção 7 do documento TAPA FSR Certification Framework).

4.2 Tradução

Em áreas geográficas onde o inglês não é o idioma principal, e onde a tradução é necessária e aplicável, é responsabilidade do LSP/Requerente e de seus agentes garantir que qualquer tradução do FSR, ou de qualquer de suas partes, reflita com precisão as intenções da TAPA no desenvolvimento e publicação destes Requisitos.

4.3 A Marca “TAPA”

“TAPA” é uma marca registrada da *Transported Asset Protection Association* e não pode ser utilizada sem a permissão expressa por escrito da TAPA, através das suas regiões oficialmente reconhecidas. Os normativos TAPA e o material associado são publicados pela TAPA, e não podem ser revistos, editados ou alterados por qualquer parte sem a permissão expressa por escrito da TAPA. O uso indevido da marca TAPA pode resultar na remoção da certificação ou em ação legal.

4.4 Limites de Responsabilidade

Com a publicação dos Requisitos, a TAPA não assegura nem fornece nenhuma garantia de que se evitarão todos os eventos de roubo de carga, independentemente de os normativos terem sido completamente e adequadamente implementados. Qualquer responsabilidade que possa resultar de um roubo de carga armazenada, ou qualquer outra perda de carga armazenada ao abrigo dos normativos FSR será responsabilidade do LSP/Requerente e/ou do Cliente de acordo com os termos e condições do contrato entre ambos e quaisquer leis ou estatutos que possam ser aplicáveis dentro da jurisdição em causa.

5.0 Contratos e Subcontratação

5.1 Contratos

A segurança no transporte, armazenagem e manuseamento seguro dos ativos do Cliente são da responsabilidade do LSP/Requerente, dos seus agentes e subcontratados durante todo o processo de receção, transporte, armazenagem e expedição, conforme especificado no contrato ou numa liberação logística.

Quando o normativo FSR é mencionado ou incluído no contrato entre LSP/Requerente e o Cliente, também deverá fazer-se referência ao programa de segurança do LSP/Requerente.

O LSP fornecerá ao Cliente evidência da Certificação FSR e, quando apropriado, evidências de que os requisitos FSR foram cumpridos. Além disso, qualquer falha alegada do LSP/Requerente em implementar os requisitos do FSR será resolvida de acordo com os termos do contrato negociado entre o Cliente e o LSP/Requerente.

5.2 Subcontratação

Ao recorrer a subcontratados, deve existir uma exigência contratual que assegure o cumprimento de todos os requisitos do FSR aplicáveis. Os Auditores Internos Autorizados do LSP devem verificar e confirmar que o subcontratado cumpre esses requisitos ao mesmo nível.

5.3 Investigação e Resolução de Reclamações da TAPA

Se a TAPA receber uma reclamação formal relativa ao desempenho de um LSP/Requerente certificado, a TAPA (sujeita a validação) pode exigir que o LSP/Requerente solicite uma nova auditoria, sendo o LSP/Requerente responsável pelas despesas. Se o LSP/Requerente falhar na auditoria, ou se recusar a cumprir este processo, o seu certificado pode ser retirado.

6.0 Processo Oficial de Dispensa

Uma dispensa é uma aprovação por escrito concedida para isentar uma instalação de um requisito específico da TAPA e aceitar uma solução alternativa de conformidade. Uma dispensa pode ser solicitada se um LSP/Requerente não puder cumprir com um requisito específico no FSR e puder justificar medidas alternativas. As dispensas são válidas durante o período da certificação.

TAPA Copyright © Do Not Copy

7.0 Requisitos de Segurança das Instalações

S1. Requisitos Gerais

Req. No.	Requisitos / Controlos	Nível Aplicável		
1.1.1	Todos os procedimentos ou políticas exigidos por este normativo devem ser documentados e atualizados pelo menos a cada dois anos.	Ⓐ	Ⓑ	Ⓒ
1.1.2	A Gestão deve ter nomeado formalmente uma pessoa (AA) para a segurança no local que seja responsável pela manutenção dos TAPA FSR, pelo encerramento de SCARs, pela avaliação de riscos, relatório de gestão e requisitos de segurança da cadeia de abastecimento da empresa. Outra pessoa (pode ser a mesma) também será responsável pela monitorização do programa FSR. Isso inclui agendamento de verificações de conformidade, comunicações com AAs, recertificação, alterações à norma FSR, etc. Estas pessoas podem ser colaboradores ou profissionais subcontratados para desempenhar esta função.	Ⓐ	Ⓑ	Ⓒ
1.1.3	Auditorias internas (realizadas por uma equipa multifuncional) ao sistema de gestão de segurança, relatórios de autoavaliação pelo AA interno e o encerramento de SCARS devem ser concluídos e documentados.	Ⓐ	Ⓑ	Ⓒ
1.1.4	É necessário um procedimento, registo e/ou plano de chaves para fechaduras físicas, cartões de acesso e/ou chaves, que assegure a gestão e controlo dos acessos físicos e eletrónicos. O procedimento deve incluir processos para duplicação, armazenamento e atuação em caso de chaves extraviadas ou perdidas.	Ⓐ	Ⓑ	Ⓒ

Req. No.	Requisitos / Controlos	Nível Aplicável		
1.1.5	Deve ser realizada e atualizada, pelo menos anualmente, uma avaliação de risco documentada que considere a probabilidade e o impacto de ameaças relacionadas com a segurança. A gestão deve rever e reconhecer que os riscos identificados foram avaliados e que foram implementados controlos adequados para os mitigar ou eliminar até um nível aceitável. No mínimo, devem ser avaliados os seguintes eventos internos/externos comuns: furto de carga ou informação, acessos não autorizados a instalações ou carga, adulteração ou destruição de sistemas de segurança, recolhas fictícias de mercadoria, continuidade da segurança em situações de escassez de mão de obra, desastres naturais, bem como a necessidade de instalação de barreiras anti-ram em janelas ou portas de cais acessíveis ao nível do solo, etc. Podem ainda ser consideradas ameaças adicionais com base nos riscos locais ou específicos do país.	Ⓐ	Ⓑ	Ⓒ
1.1.6	A pessoa que realiza auditorias internas ou anuais para o Requerente / LSP (chamado de LSP AA) deve receber formação. Essa pessoa pode ser a mesma pessoa mencionada no req. 1.1.2 ou pode ser uma pessoa subcontratada para desempenhar essa função.	Ⓐ	Ⓑ	Ⓒ
1.1.7	Para compreender o FSR e ser capaz de implementar todos os seus requisitos, todos os Requerentes / LSP AAs devem ter realizado e passado no exame aplicável para a Norma TAPA da versão que eles são obrigados a auditar.	Ⓐ	Ⓑ	Ⓒ

S2. Perímetro

2.1 Área de manuseamento, expedição e receção de carga externa do armazém

Req. No.	Requisitos / Controlos	Nível Aplicável		
2.1.1	CCTV (Circuito Fechado de Televisão) / VSS (Sistema de Videovigilância) capaz de visualizar todo o tráfego na área de manuseamento, expedição e receção de carga externa (incluindo pontos de acesso, entrada e saída), garantindo que todos os veículos e indivíduos sejam reconhecíveis em todos os momentos, a menos que haja obstrução temporária devido a necessidades operacionais (ou seja, carga e descarga de camiões em tempo real).	Ⓐ	Ⓑ	
2.1.2	Iluminação adequada nas áreas de carga e descarga, de forma a atuar como fator dissuasor básico da criminalidade e a garantir visibilidade das operações durante o período noturno. <i>Nota: A iluminação pode ser constante, ativada por alarme, movimento, deteção de som, etc., com iluminação imediata fornecida.</i>	Ⓐ	Ⓑ	Ⓒ
2.1.3	Procedimento que descreva a forma de gestão de veículos e pessoas não autorizados nas áreas externas de manuseamento, expedição e receção de carga externa. As respetivas instruções do procedimento devem ser comunicadas aos colaboradores relevantes, incluindo os vigilantes.	Ⓐ	Ⓑ	Ⓒ
2.1.4	A área de manuseamento, expedição e receção de carga deve ser adequadamente controlada para evitar acessos não autorizados.		Ⓑ	Ⓒ
2.1.5	No caso das janelas ou portas de cais acessíveis ao nível do solo, a avaliação anual dos riscos deve considerar a necessidade de barreiras anti-ram. Adicionalmente, deve incluir a avaliação da utilização de coberturas de janelas para prevenir a visualização não autorizada dos espaços interiores (ver Avaliação de Riscos, req. 1.1.5)	Ⓐ		

2.2 Barreiras Físicas

Req. No.	Requisitos / Controlos	Nível Aplicável		
2.2.1	Barreira física encerra a área de manuseamento, expedição e receção de carga.	Ⓐ		

Req. No.	Requisitos / Controlos	Nível Aplicável		
2.2.2	Barreira física ao redor da área de manuseamento, expedição e recepção de carga tem uma altura mínima de 1,80 metros. <i>Nota: A barreira física, concebida para impedir o acesso não autorizado, deve ter uma altura de 1,80 metros ao longo de toda a sua extensão, incluindo áreas onde o nível do solo muda, ou seja, é mais baixo.</i>	Ⓐ		
2.2.3	Barreira física ao redor da área de manuseamento, expedição e recepção de carga mantida em boas condições.	Ⓐ		
2.2.4	Portão(ões) integrados nas barreiras da área de manuseamento, expedição e recepção de carga, controlados física e/ou eletronicamente por pessoal autorizado.	Ⓐ		
2.2.5	Barreira física em torno área de manuseamento, expedição e recepção de carga é inspecionada quanto à integridade e danos pelo menos uma vez por semana..	Ⓐ		

2.3 Áreas Externas dos Cais

Req. No.	Requirements / Controls	Nível Aplicável		
2.3.1	Áreas externas de cais cobertas por CCTV/VSS com câmaras a cores ou com capacidade "dia/noite".	Ⓐ	Ⓑ	Ⓒ
2.3.2	Câmaras CCTV/VSS montadas de modo a ser possível visualizar todas as operações e movimento em torno da área externa de cais em todos os momentos, exceto se houver obstrução temporária devido a necessidades operacionais (ou seja, carga e descarga de caminhão em tempo real).	Ⓐ	Ⓑ	Ⓒ
2.3.3	Todos os veículos e indivíduos ao redor das áreas externas de cais devem estar cobertos por câmaras de CCTV/VSS que possam mostrar claramente as informações de identificação do veículo e capaz de discernir as características faciais dos intervenientes.	Ⓐ		
2.3.4	Veículos e indivíduos ao redor das áreas externas dos cais devem estar cobertos e visíveis por câmaras CCTV/VSS em pelo menos 75% dos casos durante um dia.		Ⓑ	Ⓒ
2.3.5	Todas as áreas externas ao redor das portas dos cais estão totalmente iluminadas.	Ⓐ	Ⓑ	Ⓒ

2.4 Acesso de Veículos Pessoais

Req. No.	Requisitos / Controlos	Nível Aplicável		
2.4.1	Veículos pessoais apenas são permitidos nas áreas de manuseamento, expedição e receção de carga quando previamente autorizados, de acordo com uma política documentada.	Ⓐ	Ⓑ	Ⓒ
2.4.2	Não são permitidas áreas de estacionamento pessoal a menos de 25 metros de distância a pé das áreas externas dos cais.	Ⓐ	Ⓑ	Ⓒ

S3. Paredes exteriores, cobertura e portas

3.1 Exterior da Instalação: CCTV/VSS

Req. No.	Requisitos / Controlos	Nível Aplicável		
3.1.1	Sistema CCTV/VSS com câmaras exteriores a cores ou com capacidade “dia/noite”, cobrindo todos os lados exteriores da instalação.	Ⓐ		
3.1.2	Sistema de CCTV/VSS com câmaras exteriores a cores ou com capacidade “dia/noite”, cobrindo os lados exteriores da instalação com portas, janelas ou outras aberturas.		Ⓑ	
3.1.3	Todas as vistas do sistema de CCTV/VSS exterior devem estar nítidas e totalmente desobstruídas em todos os momentos, a menos que haja obstrução temporária devido a necessidades operacionais (ou seja, carga e descarga de camião em tempo real).	Ⓐ		
3.1.4	Todos os veículos e indivíduos ao redor dos lados externos das instalações devem estar cobertos por câmaras de CCTV/VSS, devem mostrar claramente as informações de identificação do veículo com capacidade de discernir características faciais dos intervenientes.	Ⓐ		
3.1.5	Veículos e indivíduos visíveis em pelo menos 75% das gravações ao longo de um dia pelas câmaras CCTV/VSS externas.		Ⓑ	

3.2 Paredes Exteriores e Cobertura

Req. No.	Requisitos / Controlos	Nível Aplicável		
3.2.1	As paredes exteriores e a cobertura devem ser construídas e mantidas de forma a resistir à intrusão, <i>garantindo uma proteção física robusta. Os materiais utilizados devem apresentar resistência e durabilidade suficientes para impedir tentativas de entrada forçada (por exemplo: tijolo, blocos de betão, painéis de betão pré-moldado ou painéis tipo “sandwich” de alta resistência com pelo menos 7 mm de espessura).</i> <i>Nota: Quando forem utilizados materiais leves ou não estruturais, devem ser implementadas medidas de mitigação adicionais (como malha de aço no interior ou sistemas de deteção de intrusão), de forma a assegurar um nível de segurança equivalente.</i>	Ⓐ	Ⓑ	Ⓒ

Req. No.	Requisitos / Controlos	Nível Aplicável		
3.2.2	Qualquer janela, respiradouro, ventilação ou outra abertura nas paredes exteriores da instalação, ou qualquer janela selada instalada a menos de 3 metros do piso de trabalho nas paredes exteriores da instalação, deve ter uma barreira física ou ser alarmada e ligada ao sistema de alarme principal.	Ⓐ	Ⓑ	
3.2.3	Todas as janelas, claraboias, aberturas, portinholas de acesso ou outros vãos do teto da instalação que possam ser abertos devem ser protegidas por: (a) uma barreira física robusta (por exemplo, barras de segurança, grades ou coberturas reforçadas), ou (b) um dispositivo de detecção de intrusão integrado ao sistema de alarme principal da instalação. <i>Nota: As barreiras físicas devem ser concebidas de forma a impedir a sua remoção ou adulteração, e as aberturas com alarme devem gerar alertas imediatos em caso de acesso não autorizado.</i>	Ⓐ		
3.2.4	O acesso externo à cobertura (escada ou escadote) deve ser: Fisicamente trancado e coberto por CCTV/VSS (câmaras a cores ou com capacidade “dia/noite”), ou Fisicamente trancado e alarmado.	Ⓐ		
3.2.5	O acesso externo à cobertura (escada ou escadote) deve estar fisicamente trancado.		Ⓑ	Ⓒ
3.2.6	Todas as portas exteriores pedonais do armazém e portas de escritório são alarmadas para detetar abertura não autorizada e ligadas ao sistema de alarme principal. <i>Nota: As portas de cais não estão abrangidas por este requisito, consultar o req. 3.2.12 para os requisitos de alarme das portas de cais.</i>	Ⓐ	Ⓑ	Ⓒ
3.2.7	Cada porta externa do armazém, porta de escritório ou outra abertura deve ser identificada exclusivamente por porta ou por zona no sistema de alarme principal.	Ⓐ		
3.2.8	Todas as portas externas do armazém devem estar sempre fechadas e seguras quando não estão em uso ativo. Quando aplicável, chaves/códigos controlados.	Ⓐ	Ⓑ	

Req. No.	Requisitos / Controlos	Nível Aplicável		
3.2.9	As portas e caixilhos pedonais exteriores do armazém não podem ser facilmente penetrados. Se as dobradiças estiverem no exterior, devem ser fixadas ou soldadas por pontos. As portas total ou parcialmente de vidro no armazém são inaceitáveis, a menos que detetores de quebra de vidro estejam instalados, ou outro dispositivo de deteção local forneça cobertura (por exemplo, Infravermelho Passivo) com alarme direto para o centro de monitorização OU o vidro ser protegido por barras / rede. A TAPA permitirá que os atuais detentores de certificação que não tenham capacidade de cumprir este requisito continuem com sua configuração atual até a próxima revisão. Novos detentores de certificação ou novas instalações devem cumprir com o novo requisito.	Ⓐ	Ⓑ	Ⓒ
3.2.10	Saídas de emergência, destinadas exclusivamente a situações de emergência (Ex: saídas de incêndio), são sempre alarmadas com um dispositivo sonoro individual ou por zona.	Ⓐ	Ⓑ	
3.2.11	Todas as portas de cais devem ter resistência suficiente para dissuadir e/ou atrasar a entrada forçada através da utilização de pequenas ferramentas manuais elétricas ou a bateria.	Ⓐ	Ⓑ	Ⓒ
3.2.12	Portas de Cais Horário não operacional: Portas de cais fechadas e protegidas (ou seja, desativadas eletronicamente ou fisicamente trancadas). Portas de cais alarmadas para detetar intrusão não autorizada e gerar um alarme ligado ao sistema de alarme principal. Horário operacional: As portas das cais devem estar fechadas quando não estiverem em uso ativo. Os portões tesoura, se utilizados, devem ser protegidos por um fecho mecânico de correr/trinco e ter uma altura mínima de 2,40 metros de altura.	Ⓐ	Ⓑ	Ⓒ

S4. Pontos de Entrada e Saída de Escritório e Armazém

4.1 Ponto(s) de Entrada de Visitantes na Área de Escritório

Req. No.	Requisitos / Controlos	Nível Aplicável		
4.1.1	O(s) ponto(s) de entrada de visitantes são controlados por um colaborador / vigilante / rececionista formado em emissão de credenciais, controlo de acessos, registo de acessos, visitas, necessidade de acompanhamento, etc. (processo definido para quando colaboradores registram os seus próprios visitantes e para visitas fora do horário operacional).	Ⓐ	Ⓑ	Ⓒ
4.1.2	Ponto(s) de entrada de visitantes na área de escritório coberto(s) por CCTV (Câmaras a cores ou "dia / noite") indivíduos claramente reconhecíveis em todos os momentos.	Ⓐ	Ⓑ	
4.1.3	Alarme de emergência presente no(s) ponto(s) de entrada de visitantes da área de escritório e testado semanalmente.	Ⓐ	Ⓑ	
4.1.4	Todos os visitantes da área do escritório devem ser identificados tendo na sua posse um documento de identificação com fotografia emitido pelo governo (por exemplo, carta de condução, passaporte ou cartão de identificação nacional, etc.). Caso sejam aceites identificações digitais pela instalação e permitidas pela legislação local, deve existir um processo de verificação robusto (incluindo toda a infraestrutura técnica necessária).	Ⓐ	Ⓑ	Ⓒ
4.1.5	Todos os visitantes da área de escritórios devem ser registados, sendo mantido um registo por um período mínimo de 30 dias. Os detalhes da visita, tais como a pessoa visitada e o motivo da visita, devem ser rastreáveis através da informação inserida no registo de visitantes.	Ⓐ	Ⓑ	Ⓒ
4.1.6	Todas as credenciais de visitante devem ser desabilitadas e recolhidas assim que o visitante sai das instalações e todo o registo verificado diariamente.	Ⓐ	Ⓑ	
4.1.7	Todos os visitantes devem exibir visivelmente as suas credenciais e devem ser acompanhados por colaboradores da empresa.	Ⓐ	Ⓑ	

4.2 Ponto(s) de Entrada de Colaboradores

Req. No.	Requisitos / Controlos	Nível Aplicável		
4.2.1	Todos os ponto(s) de entrada de Colaboradores controlado(s) 24 horas por dia, 7 dias por semana.		Ⓑ	Ⓒ
4.2.2	Todos os ponto(s) de entrada de Colaboradores controlado(s) através de um dispositivo eletrónico de controlo de acesso 24 horas por dia, 7 dias por semana. Acesso registado.	Ⓐ		
4.2.3	Ponto(s) de entrada dos colaboradores coberto(s) por CCTV / VSS. (Câmaras a cores com funcionalidade “dia/noite”).	Ⓐ	Ⓑ	
4.2.4	Após a verificação, todos os colaboradores devem receber cartões de identificação com foto da empresa.	Ⓐ	Ⓑ	
4.2.5	Todos os colaboradores devem receber um cartão de identificação da empresa para torná-los reconhecíveis dentro das instalações.	Ⓐ	Ⓑ	
4.2.6	Todos os cartões dos Colaboradores devem ser claramente exibidos.	Ⓐ	Ⓑ	
4.2.7	Os cartões dos Colaboradores não devem ser partilhados em nenhuma circunstância e uma política de emissão de cartões deve estar em vigor.	Ⓐ	Ⓑ	

4.3 Identificação do Motorista e do Veículo

Req. No.	Requisitos / Controlos	Nível Aplicável		
4.3.1	Todos os motoristas devem ser identificados através de um documento de identificação com fotografia emitido pelo governo (por exemplo, carta de condução; passaporte ou cartão de identificação nacional, etc.) e um registo de motorista mantido. Caso sejam aceites identificações digitais pela instalação e permitidas pela legislação local, deve existir um processo de verificação robusto (incluindo toda a infraestrutura técnica necessária).	Ⓐ	Ⓑ	Ⓒ

Req. No.	Requisitos / Controlos	Nível Aplicável		
4.3.2	Verificação de que a carta de condução é válida, o documento de identificação com foto não expirou e que ambos correspondem ao motorista. Caso sejam aceites cartas de condução digitais pela instalação e permitidas pela legislação local, deve existir um processo de verificação robusto(incluindo toda a infraestrutura técnica necessária).	Ⓐ	Ⓑ	Ⓒ
4.3.3	Os dados dos veículos devem ser registados manualmente (ou seja, escritos) ou com câmaras. Deve incluir no mínimo a matrícula e o tipo de veículo.	Ⓐ		

S5. Interior do Armazém e Escritório

5.1 Área do Armazém: Paredes Multi-Inquilino

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.1.1	Cobertura e paredes interiores multi-inquilino do chão ao teto devem ser construídos/projetados e mantidos para resistir à penetração (Exemplo: tijolo, bloco, laje de concreto inclinável, paredes de painel sanduíche com espessura mínima de 7 milímetros).	Ⓐ	Ⓑ	Ⓒ
5.1.2	Se as paredes interiores multi-inquilino do chão ao teto forem construídas com rede metálica de segurança ou outra barreira segura reconhecida pela indústria, então também devem ser alarmadas para detetar intrusões. <i>Nota 1: Redes, vedações de baixo grau ou malha não classificada como segurança não são aceitáveis.</i> <i>Nota 2: Se as paredes multi-inquilino estão construídas com material sólido do chão ao teto, este requisito não se aplica (N/A).</i>	Ⓐ	Ⓑ	Ⓒ

5.2 Áreas Internas do Armazém

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.2.1	A detecção de intrusão (por exemplo, infravermelho, movimento, som ou vibração) é obrigatória para monitorar as áreas internas do armazém. Os alarmes devem estar ativados e conectados ao sistema de alarme principal durante períodos não operacionais (ou seja, quando o armazém estiver fechado) <i>Nota 1: Se o armazém operar verdadeiramente 24/7/366, este requisito pode ser considerado não aplicável (N/A), desde que os riscos e as medidas de mitigação estejam documentados na Avaliação de Riscos local (ver req. 1.1.5)</i> <i>Nota 2: Independentemente do horário de operação, a detecção de intrusão perimetral ou barreiras físicas são sempre obrigatórias em portas externas e janelas ao nível do solo no escritório e armazém (ver req. 3.2.2 e 3.2.6).</i>	Ⓐ		

5.3 Portas e Áreas de Cais Internas

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.3.1	Todas as áreas de cais e portas de cais interiores devem estar cobertas por CCTV / VSS (Câmaras a cores com funcionalidade “dia/noite”).	(A)	(B)	(C)
5.3.2	Vistas da carga a ser carregada/descarregada em todas as portas e áreas de cais interiores, sempre desobstruídas, a menos que haja obstrução temporária devido a necessidades operacionais (ou seja, carga e descarga de camiões em tempo real).	(A)	(B)	(C)
5.3.3	Ativos do Cliente sobre vigilância CCTV 100% em áreas de movimentação de carga ou preparação (ou seja, áreas de preparação / arrumação de paletes, rotas de armazenagem de e para racks / estanteria, cais, corredores de trânsito).	(A)	(B)	
5.3.4	A análise de pontos cegos para assegurar a cobertura CCTV a 100% das áreas de movimentação de carga deve ser realizada, no mínimo, anualmente, salvo quando ocorram alterações operacionais e/ou estruturais no armazém.	(A)		

5.4 Controlo de Acesso entre Escritório e Cais/Armazém

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.4.1	Acesso controlado entre escritório e cais/armazém.	(A)	(B)	
5.4.2	Os alarmes de porta de acesso por cartão ou intercomunicador, para portas entre o escritório e cais/armazém, são localmente audíveis e geram um alarme de resposta quando mantidas abertas por mais de 60 segundos ou imediatamente se as portas forem forçadas.	(A)		
5.4.3	Os alarmes de porta para as portas entre o escritório e o cais/ armazém são localmente audíveis ou enviam alarme quando mantidas abertas por mais de 60 segundos ou forem abertas forçadamente.		(B)	
5.4.4	O acesso à área de cais/armazém é concedido aos Colaboradores autorizados pelo LSP e aos visitantes acompanhados com base no estritamente necessário para desempenho das suas funções.	(A)	(B)	(C)
5.4.5	Lista de acesso às áreas de cais/armazém revista pelo menos trimestralmente para limitar/verificar se a permissão de acesso só é concedida a pessoal designado/autorizado.	(A)	(B)	

5.5 Área / Compartimento estanque de Alto Valor (HVC)

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.5.1	O tamanho e o uso da HVC podem ser definidos por acordo entre Cliente/LSP/Requerente. Caso não exista um acordo, a HVC deve ser capaz de armazenar no mínimo 6 metros cúbicos de produto.	Ⓐ	Ⓑ	
5.5.2	O perímetro da HVC deve ser estanque e estar segregado (Gaiola/Jaula) ou ter paredes duras em todos os lados, incluindo topo/cobertura.	Ⓐ	Ⓑ	
5.5.3	As portas/portões na HVC devem ter um dispositivo de bloqueio.	Ⓐ	Ⓑ	
5.5.4	Cobertura completa por CCTV/VSS (câmeras a cores ou com funcionalidade "dia/noite") na entrada e no interior da HVC. <i>Nota: Se a HVC for demasiado pequena para colocar uma câmara no interior, a cobertura da câmara da entrada é suficiente.</i>	Ⓐ		
5.5.5	Cobertura por CCTV/VSS (câmaras a cores ou com funcionalidade "dia/noite") na entrada da HVC.		Ⓑ	
5.5.6	Se o acesso ao HVC for necessário para mais de 10 pessoas, então o acesso deve ser controlado eletronicamente por cartão / credencial. Se o acesso for necessário por 10 ou menos pessoas, pode ser utilizado um sistema de fechadura ou cadeado resistente apoiado por um sistema de emissão de chaves controlado. As chaves podem ser entregues a indivíduos para cobrir um turno, mas não podem ser transferidas sem aprovação e devem ser obrigatoriamente registados os seus movimentos. Todas as chaves devem ser devolvidas e contabilizadas quando não estiverem a ser utilizadas.	Ⓐ		
5.5.7	As portas/portões da HVC devem estar alarmados para detetar entrada forçada. Os alarmes podem ser gerados por contactos magnéticos e/ou uso de deteção de movimento CCTV/VSS para detetar o acesso não autorizado.	Ⓐ		
5.5.8	O Perímetro da HVC mantido em bom estado e inspecionado mensalmente quanto à sua integridade e danos.	Ⓐ		

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.5.9	O LSP/Requerente deve garantir que o acesso à HVC seja concedido apenas a pessoal designado/autorizado.			
	A lista de acessos autorizados à HVC deve ser revista mensalmente e atualizada em tempo real quando um colaborador deixa a empresa ou não necessita mais de acesso.	Ⓐ	Ⓑ	
	Deve existir um procedimento para acesso à HVC.			

5.6 Inspeção de Resíduos do Armazém

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.6.1	Os recipientes de resíduos internos e/ou externos do armazém principal / áreas de compactação são monitorizadas por CCTV/VSS.	Ⓐ		
5.6.2	Quando utilizados, os sacos de resíduos dentro do armazém devem ser transparentes.		Ⓑ	Ⓒ

5.7 Pré-carregamento e preparação

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.7.1	Não é permitido o pré-carregamento ou estacionamento de camiões FTL/dedicados do Cliente, no exterior da instalação do armazém fora das horas de funcionamento, salvo acordo mútuo entre o Cliente e o LSP/Requerente.			
	Devem ser implementadas medidas de segurança alternativas (por exemplo, dispositivos de segurança adicionais em veículos / compartimentos de carga).	Ⓐ	Ⓑ	Ⓒ
	Nota: "No exterior da instalação do armazém" são aquelas áreas separadas, afastadas da instalação, mas ainda dentro da vedação/perímetro do LSP.			

5.8 Recipientes Pessoais e Revistas à Saída

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.8.1	Os procedimentos de segurança escritos definem a forma como os "recipientes pessoais" são controlados no interior do armazém. Os recipientes pessoais incluem lancheiras, mochilas, sacos térmicos, bolsas, etc.	Ⓐ	Ⓑ	
5.8.2	Sempre que permitido pela legislação local, o Prestador de Serviços Logísticos (LSP)/ Requerente deve desenvolver e manter um procedimento documentado para a realização de revistas à saída. A ativação deste procedimento fica ao critério do LSP/ Requerente e/ou de acordo com o definido entre o Cliente e o LSP/ Requerente. No mínimo, o procedimento deve contemplar o direito do LSP/ Requerente de implementar revistas sempre que exista necessidade de introduzir este controlo, mesmo que normalmente não seja aplicado (por exemplo, quando há suspeita de furto interno por colaboradores). Colaboradores, Trabalhadores Temporários, Subcontratados e Visitantes devem ser informados sobre esta política antes da sua entrada no armazém.	Ⓐ		

5.9 Controlo dos Equipamentos de Movimentação de Carga

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.9.1	Procedimento que exige que todas os empilhadores e outros equipamentos de movimentação de carga motorizados sejam desativados fora das horas de atividade operacional. Nota: Isto não inclui empilhadores manuais e porta paletes.	Ⓐ	Ⓑ	

5.10 Integridade do Contentor ou Reboque: Inspeção de 7 pontos

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.10.1	Inspeção física de 7 pontos realizada, na expedição em todos os contentores ou reboques dedicados do Cliente: parede frontal, lado esquerdo, lado direito, pavimento carga, teto/cobertura, portas interiores/exteriores e mecanismo de bloqueio, e carroçaria. <i>Nota: Isto aplica-se a todos os tipos de reboques e contentores trancados e/ou selados (ou seja, não se limita a contentores de carga marítima).</i>	Ⓐ	Ⓑ	Ⓒ

5.11 Processo de Transferência de carga; Selos de Segurança

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.11.1	A menos que especificamente isentos pelo Cliente, selos de segurança invioláveis são usados em todas as entregas diretas e contínuas. Os selos devem ser certificados de acordo com a norma ISO 17712 (classificação I, S ou H). <i>Nota: Os selos não são necessários em entregas com várias paragens, devido à complexidade e ao risco associados aos motoristas transportarem vários selos.</i>	Ⓐ	Ⓑ	Ⓒ
5.11.2	O LSP/Requerente deve dispor de procedimentos documentados e em vigor para a gestão e controlo de selos de segurança, trancas das portas da galera/contentor, <i>pin locks</i> , outros equipamentos de segurança.	Ⓐ	Ⓑ	Ⓒ
5.11.3	Os selos de segurança apenas devem ser colocados ou removidos por pessoal autorizado, ou seja, pessoal do armazém, que é instruído para reconhecer e comunicar a existência selos comprometidos. Os selos nunca devem ser afixados ou removidos pelo condutor, a menos que haja dispensa Cliente.	Ⓐ	Ⓑ	Ⓒ
5.11.4	Devem existir procedimentos em vigor para reconhecer e comunicar selos de segurança comprometidos.	Ⓐ	Ⓑ	Ⓒ

5.12 Integridade da Carga; Processo de Validação de Carga/Descarga

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.12.1	Procedimentos robustos em vigor que garantam que todos os ativos do Cliente enviados e recebidos sejam validados no ponto de entrega através da realização de uma contagem manual e/ou eletrônica da carga. O processo deve garantir que as anomalias sejam consistentemente reconhecidas, documentadas e relatadas ao LSP/Requerente e/ou Cliente.			
	Os registos manuais e/ou eletrónicos devem ser de qualidade evidente. Se os motoristas não estiverem presentes para testemunhar esta atividade, o Cliente / LSP/Requerente deve garantir a verificação de contagem alternativa, como digitalizações e/ou imagens de CCTV/VSS, recolhidas e retidas especificamente para este fim. <i>Nota: Além de carga em falta, as anomalias podem incluir danos, falta de correias ou fita, cortes ou outras aberturas óbvias, indicando um possível roubo ou furto.</i>	Ⓐ	Ⓑ	Ⓒ

5.13 Recolhas fraudulentas

Req. No.	Requisitos / Controlos	Nível Aplicável		
5.13.1	A identificação do motorista do camião, a documentação de recolha da carga e os detalhes de pré-alerta aplicáveis especificados pelo Cliente devem ser validados antes do carregamento. O procedimento deve estar em vigor.			
	Caso sejam aceites identificações digitais pela instalação e permitidas pela legislação local, deve existir um processo de verificação robusto (incluindo toda a infraestrutura técnica necessária).	Ⓐ	Ⓑ	Ⓒ

S6. Sistemas de Segurança; Conceção, Monitorização e Respostas

6.1 Posto de Monitorização

Req. No.	Requisitos / Controlos	Nível Aplicável		
6.1.1	Monitorização de eventos de alarme 24x7x366 deve ser realizada através de um posto de monitorização interno ou subcontratação, protegido contra acesso não autorizado. <i>Nota: Os postos de monitorização podem estar localizados dentro ou fora do local e podem ser propriedade da empresa ou de terceiros. Em todos os casos, o acesso deve ser controlado através do uso de um sistema eletrónico de controlo de acesso (cartões), fechaduras ou scanners biométricos.</i>	(A)	(B)	(C)
6.1.2	Deve existir um posto de monitorização para responder a todos os alarmes do sistema de segurança em tempo real 24x7x366.	(A)	(B)	(C)
6.1.3	O posto de monitorização reconhece o evento que despoletou o alarme e responde em menos de 3 minutos.	(A)	(B)	(C)
6.1.4	Devem estar disponíveis relatórios de monitorização de alarmes.	(A)	(B)	(C)
6.1.5	Procedimentos de resposta do posto de monitorização em vigor.	(A)	(B)	(C)

6.2 Sistema de Detecção de Intrusão (IDS)

Req. No.	Requisitos / Controlos	Nível Aplicável		
6.2.1	Todos os IDS ativados durante as horas não operacionais e ligados ao sistema de alarme principal.	(A)	(B)	(C)
6.2.2	Mantidos 90 dias os registos de alarme IDS.	(A)	(B)	
6.2.3	Registos de alarme IDS devem ser armazenados em segurança e copiados (<i>backup</i>) pelo menos semanalmente.	(A)	(B)	

Req. No.	Requisitos / Controlos	Nível Aplicável		
6.2.4	Deve existir um procedimento de forma a garantir que o acesso ao IDS seja restrito a indivíduos autorizados ou administradores de sistema. Isso inclui servidores, consolas, controladores, painéis, redes e dados. Os privilégios de acesso ao IDS devem ser prontamente atualizados quando os indivíduos terminam as suas funções na organização ou mudam de função, não necessitando mais de acesso.	(A)	(B)	(C)
6.2.5	Alarme transmitido em caso de falha de energia / perda do IDS. <i>Nota: Para sistemas com Fonte de Alimentação Ininterrupta (UPS), o alarme é transmitido quando a bateria da UPS falha.</i>	(A)	(B)	(C)
6.2.6	Verificação do sistema de alarme IDS em vigor. <i>Nota: Procedimentos que validam que os alarmes estão armados durante as horas não operacionais.</i>	(A)	(B)	(C)
6.2.7	Alarme IDS transmitido através de linha fixa ou sem fio e/ou falha do modo de comunicação.	(A)	(B)	
6.2.8	Sistema de comunicação de recurso (<i>backup</i>) em vigor em caso de falha do dispositivo IDS e/ou da linha.	(A)	(B)	

6.3 Sistema de Controlo de Acesso Automático (AACS)

Req. No.	Requisitos / Controlos	Nível Aplicável		
6.3.1	90 dias de registos de transações AACS disponíveis. Registos armazenados de forma segura; necessária cópia de segurança (<i>backup</i>).	(A)	(B)	
6.3.2	Deve estar em vigor um procedimento que garanta que o acesso ao AACS é restrito a indivíduos autorizados ou a administradores de sistema. Os privilégios de acesso devem ser prontamente atualizados quando os indivíduos terminam as suas funções na organização ou mudam de função, não necessitando mais de acesso.	(A)	(B)	
6.3.3	Os relatórios do sistema de acesso devem ser revistos pelo menos trimestralmente para identificar irregularidades ou uso indevido (ou seja, várias tentativas mal sucedidas, leituras falsas (por exemplo, cartão desativado), evidências de partilha de cartão para permitir acesso não autorizado, etc.). Processo em vigor.	(A)	(B)	

6.4 CCTV/ VSS

Req. No.	Requisitos / Controlos	Nível Aplicável		
6.4.1	Gravação digital de CCTV/VSS em vigor.	(A)	(B)	(C)
6.4.2	Velocidade de gravação para CCTV/VSS deve estar definida como um mínimo de 8 fotogramas por segundo (fps) por câmara.	(A)	(B)	(C)
6.4.3	A funcionalidade de gravação digital verificada diariamente, em dias de operação, de acordo com procedimento. Registos disponíveis.	(A)	(B)	(C)
6.4.4	Gravações CCTV/VSS armazenadas por um mínimo de 30 dias, quando permitido pela lei local. LSP/Requerente deve fornecer provas de quaisquer leis locais que proíbam o uso de CCTV e/ou limitem a armazenagem de dados de vídeo a menos de 30 dias.	(A)	(B)	(C)
6.4.5	Acesso ao sistema CCTV/VSS rigorosamente controlado, incluindo hardware, software e armazenagem de dados / vídeo. Esta sala deve ser trancada se o sistema de armazenagem CCTV/VSS estiver na instalação com controlos de acesso em vigor.	(A)	(B)	(C)
6.4.6	As imagens de CCTV/VSS, para fins de segurança, devem ser visualizadas apenas por pessoal autorizado.	(A)	(B)	(C)
6.4.7	Procedimentos em vigor a detalhar a política de proteção de dados CCTV/VSS em relação ao uso de imagens em tempo real e arquivadas de acordo com a legislação local.	(A)	(B)	

6.5 Iluminação Exterior e Interior

Req. No.	Requisitos / Controlos	Nível Aplicável		
6.5.1	Os níveis de iluminação externa e interna devem ser suficientes para suportar imagens de CCTV/VSS que permitam investigação e gravação de imagens com qualidade evidente / probatória.	(A)	(B)	
6.5.2	Os níveis de iluminação externa e interna devem ser suficientes para reconhecer claramente todos os veículos e indivíduos.	(A)		

S7. Formação e Procedimentos

7.1 Procedimentos de Escalonamento

Req. No.	Requisitos / Controlos	Nível Aplicável		
7.1.1	Procedimentos locais em vigor para lidar com os ativos do Cliente, incluindo o processo para a comunicação atempada de ativos perdidos, extraviados ou roubados do Cliente. Incidentes a serem reportados pelo LSP/Requerente ao Cliente no prazo de 24 horas. Atos ilícitos óbvios (roubo/furto) devem ser reportados imediatamente. Processo cumprido de forma consistente.	Ⓐ	Ⓑ	Ⓒ
7.1.2	No caso de incidentes de segurança, devem estar registados e disponíveis os contactos de emergência do Cliente e da gestão das instalações do LSP/Requerente. Lista atualizada a cada 6 meses e inclui contactos de emergência das autoridades policiais.	Ⓐ	Ⓑ	Ⓒ

7.2 Compromisso da Gestão

Req. No.	Requisitos / Controlos	Nível Aplicável		
7.2.1	A Gestão deve desenvolver, comunicar e manter uma política de segurança para garantir que todas as pessoas relevantes (ou seja, funcionários e contratados) estejam claramente cientes das expectativas de segurança do fornecedor.	Ⓐ	Ⓑ	Ⓒ

7.3 Formação

Req. No.	Requisitos / Controlos	Nível Aplicável		
7.3.1	Formação de Segurança/Sensibilização para Ameaças, a ministrar a todos os Colaboradores nos primeiros 60 dias após a admissão na empresa e, posteriormente, de 2 em 2 anos.	Ⓐ	Ⓑ	Ⓒ
7.3.2	Formação de sensibilização sobre segurança da informação focado na proteção dos dados de envio eletrónicos e físicos do Cliente fornecidos aos Colaboradores que tem acesso às informações do Cliente e, posteriormente, pelo menos a cada 2 anos, ou de acordo com a legislação local, caso seja definido um período mais curto.	Ⓐ	Ⓑ	Ⓒ

7.4 Acesso aos Ativos do Cliente

Req. No.	Requisitos / Controlos	Nível Aplicável		
7.4.1	Procedimento(s) em vigor para proteger os ativos do Cliente (ou seja, carga) de acesso não autorizado por parte dos Colaboradores, visitantes, etc.	Ⓐ	Ⓑ	Ⓒ

7.5 Controlo de Informação

Req. No.	Requisitos / Controlos	Nível Aplicável		
7.5.1	Acesso a documentos de transporte e informações sobre os ativos do Cliente controlados com base no "estritamente necessário". Deve existir um processo para garantir a proteção das informações do Cliente.	Ⓐ	Ⓑ	Ⓒ
7.5.2	Acesso a documentos de envio e informações sobre os ativos do Cliente monitorizados e registados. Devem existir processos e registros relacionados.	Ⓐ	Ⓑ	Ⓒ
7.5.3	Os documentos de transporte e quaisquer outros documentos que contenham informações sobre os ativos do Cliente devem ser protegidos até à sua destruição.	Ⓐ	Ⓑ	Ⓒ

7.6 Relatório de Incidentes de Segurança

Req. No.	Requisitos / Controlos	Nível Aplicável		
7.6.1	Deve existir um sistema de reporte e acompanhamento de incidentes de segurança, utilizado para implementar medidas proativas.	Ⓐ	Ⓑ	

7.7 Programas de Manutenção

Req. No.	Requisitos / Controlos	Nível Aplicável		
7.7.1	Devem existir programas de manutenção para todas as instalações técnicas (físicas) / sistemas de segurança, para garantir a sua funcionalidade em todos os momentos (por exemplo, CCTV/VSS, Controlos de acesso, Detecção de Intrusão e Iluminação).	Ⓐ	Ⓑ	Ⓒ

Req. No.	Requisitos / Controlos	Nível Aplicável		
7.7.2	Manutenção preventiva realizada uma vez por ano, ou de acordo com as especificações do fabricante.	Ⓐ	Ⓑ	Ⓒ
7.7.3	Verificações de funcionalidade de todos os sistemas a serem realizadas uma vez por semana e documentadas, exceto se as falhas do sistema sejam imediatamente/automaticamente relatadas ou alarmadas.	Ⓐ	Ⓑ	
7.7.4	Uma ordem de reparação deve ser iniciada no prazo de 48 horas após a descoberta da falha. Devem ser implementadas mitigações alternativas para quaisquer reparações previstas para além de 24 horas.	Ⓐ	Ⓑ	

7.8 Orientação do Subcontratado

Req. No.	Requisitos / Controlos	Nível Aplicável		
7.8.1	LSP/Requerente deve garantir que todos os subcontratados/fornecedores estão cientes e cumprem os programas de segurança relevantes do LSP/Requerente.	Ⓐ	Ⓑ	Ⓒ

7.9 Registos de Expedição e Receção

Req. No.	Requisitos / Controlos	Nível Aplicável		
7.9.1	Documentos de expedição e receção legíveis, completos e precisos (ou seja, hora, data, assinaturas, motorista, pessoal de expedição e receção, detalhes e quantidade do envio, etc.). Os nomes do motorista e do expedidor devem ser sempre claramente legíveis.	Ⓐ	Ⓑ	Ⓒ
7.9.2	O LSP/Requerente deve manter registos de todas as recolhas e comprovativos de entregas, por um período não inferior a dois anos, e disponibilizá-los para investigações de perdas, conforme necessário.	Ⓐ	Ⓑ	Ⓒ
7.9.3	A prova de entrega deve ser fornecida em conformidade com o acordo escrito entre o Cliente e o LSP/Requerente e onde o Cliente exige, o destino deve notificar a origem dentro do prazo acordado da receção da carga, conciliando detalhes de envio de pré-alerta.	Ⓐ	Ⓑ	Ⓒ

7.10 Processo de Pré-Alerta em vigor

Req. No.	Requisitos / Controlos	Nível Aplicável		
7.10.1	Quando o Cliente exigir, o processo de pré-alerta aplicado a entregas e/ou receções de carga está em vigor. Os detalhes do pré-alerta devem ser acordados entre o Cliente e o LSP/Requerente. Os detalhes sugeridos incluem: hora de partida, hora prevista de chegada, transportadora, nome do motorista, detalhes da matrícula, informações de envio (contagem de peças, peso, número do conhecimento de embarque, etc.) e números de selo do transporte.	Ⓐ	Ⓑ	Ⓒ

S8. Integridade dos Trabalhadores

8.1 Triagem/ Verificação de antecedentes/Rescisão (conforme permitido pela legislação local)

Req. No.	Requisitos / Controlos	Nível Aplicável		
8.1.1	O LSP/Requerente deve possuir um processo de triagem/verificação de antecedentes que inclua, no mínimo, os últimos 5 anos de histórico de empregos anteriores e antecedentes criminais. A seleção/verificação aplica-se a todos os candidatos, incluindo colaboradores e contratados. O LSP/Requerente também deve ter acordado contratualmente que um processo equivalente seja aplicado pelas empresas contratadas que fornecem trabalhadores temporários (TAS).	Ⓐ	Ⓑ	Ⓒ
8.1.2	LSP/Requerente terá acordos em vigor para obter as informações exigidas de triagem/verificação/antecedentes por parte da agência e/ou subcontratado que fornece trabalhadores TAS ou deverá realizar essa triagem por conta própria. A triagem deve incluir verificação de antecedentes criminais e verificações de empregos anteriores.	Ⓐ	Ⓑ	Ⓒ
8.1.3	Procedimento para lidar com a falsa declaração do trabalhador do LSP/Requerente antes ou pós contratação.	Ⓐ	Ⓑ	Ⓒ

8.2 Rescisão ou Recontratação da Trabalhadores

Nota: A rescisão contratual inclui tanto separações voluntárias quanto involuntárias — trabalhadores demitidos ou que pediram demissão.

Req. No.	Requisitos / Controlos	Nível Aplicável		
8.2.1	Recuperar os ativos físicos dos Trabalhadores que terminam as suas funções na empresa, incluindo: IDs da empresa, cartões de acesso, chaves, equipamentos, ativos de TI e informações confidenciais. Necessário procedimento documentado.	Ⓐ	Ⓑ	Ⓒ
8.2.2	Proteger os dados do Cliente: Desabilitar o acesso dos Trabalhadores que terminam as suas funções na empresa a sistemas físicos ou eletrônicos, incluindo aqueles que contêm dados do Cliente (inventário ou cronogramas). Procedimento necessário.	Ⓐ	Ⓑ	Ⓒ
8.2.3	Lista de controlo da admissão e término de funções dos Trabalhadores em vigor para verificação.	Ⓐ	Ⓑ	Ⓒ

Req. No.	Requisitos / Controlos	Nível Aplicável		
8.2.4	Recontratação: Estão em vigor procedimentos para prevenir que o LSP/Requerente recontrate Trabalhadores se os critérios de rescisão ainda forem válidos. Nota: Os registos são revistos antes da recontratação (Ex: antecedentes de pessoal anteriormente despedido ou – candidatos rejeitados (emprego anteriormente negado).	Ⓐ	Ⓑ	Ⓒ

S9. Requisitos da Função Central (aplicável apenas para Certificação Multi-site)

9.1 Geral

Req. No.	Requisitos / Controlos	Nível Aplicável		
9.1.1	Existe uma função central para gerir o sistema de gestão de segurança de todas as instalações tal como definido no âmbito da certificação Multi-instalação.	Ⓐ	Ⓑ	Ⓒ
9.1.2	Todas as instalações devem ter uma relação legal ou contratual com a função central. Este requisito não se estende a instalações de subcontratados incluídos no âmbito de certificação, conforme a cláusula 4.2.2 do CFD.	Ⓐ	Ⓑ	Ⓒ
9.1.3	Um único sistema de gestão de segurança é estabelecido para garantir que todas as instalações inseridas no sistema estão em conformidade com os requisitos do Normativo de Segurança TAPA aplicável.	Ⓐ	Ⓑ	Ⓒ
9.1.4	A função central e o seu sistema de gestão devem ser sujeitos a auditorias internas para assegurar conformidade permanente das normas TAPA.	Ⓐ	Ⓑ	Ⓒ
9.1.5	A função central deve realizar auditorias às instalações abrangidas para garantir que cada instalação cumpre os requisitos aplicáveis do FSR da TAPA. As auditorias devem ser realizadas com os modelos de auditoria TAPA apropriados. Todas as auditorias anuais individuais da instalação devem ser concluídas e devem estar disponíveis para o auditor antes do processo de certificação.	Ⓐ	Ⓑ	Ⓒ
9.1.6	A função central deve ter autoridade e direitos para exigir que todas as instalações cumpram os Requisitos de Segurança TAPA e para implementar ações corretivas e preventivas conforme necessário. <i>Nota: Quando aplicável, isso deve estar definido em acordo formal entre a função central e as instalações.</i>	Ⓐ	Ⓑ	Ⓒ

9.2 Políticas e Procedimentos

Req. No.	Requisitos / Controlos	Nível Aplicável		
9.2.1	A função central deve manter políticas e procedimentos documentados para os seus sistemas de gestão de segurança, aplicáveis a todos as suas instalações.	(A)	(B)	(C)
9.2.2	A função central deve assegurar que as políticas e os procedimentos adequados são atualizados, comunicados, implementados e aplicados em todas as instalações, conforme necessário.	(A)	(B)	(C)
9.2.3	As políticas e procedimentos devem ser mantidos e estar facilmente acessíveis a todos os sites, conforme necessário.	(A)	(B)	(C)

9.3 Relatório de Auditoria Interna realizada para todas as Instalações

Req. No.	Requisitos / Controlos	Nível Aplicável		
9.3.1	A função central deve solicitar a todas as instalações que efetuem auditorias internas, e todos os relatórios de auditoria interna devem ser apresentados à função central para registo e análise. Os registos devem ser mantidos durante, pelo menos, dois (2) anos.	(A)	(B)	(C)
9.3.2	A função central deve assegurar que todos os SCARs resultantes das auditorias internas sejam devidamente encerrados, a fim de melhorar os seus sistemas de gestão da segurança.	(A)	(B)	(C)
9.3.3	Todos as instalações devem apresentar à função central atualizações dos progressos realizados e relatórios sobre todos os SCAR pendentes. A função central deve escalar para a gestão do LSP/Requerente se os SCARs não forem concluídos antes das datas previstas. Os registos devem ser mantidos durante, pelo menos, dois (2) anos.	(A)	(B)	(C)

9.4 Registos de inspeções, visitantes / motoristas, Inspeções de 7 pontos

Req. No.	Requisitos / Controlos	Nível Aplicável		
9.4.1	A função central deve dispor de procedimentos para garantir que todas as instalações mantêm registos das inspeções, dos registos de visitantes, dos registos dos motoristas, das inspeções de 7 pontos, etc.	(A)	(B)	(C)

9.5 Avaliação de Risco de todas as instalações

Req. No.	Requisitos / Controlos	Nível Aplicável		
9.5.1	A função central deve dispor de procedimentos que garantam a realização de avaliações de riscos e respetiva gestão adequada em todas as instalações e os seus registos são mantidos durante, pelo menos, dois (2) anos.	Ⓐ	Ⓑ	Ⓒ

9.6 Layout de CCTV/VSS e alarmes da instalação

Req. No.	Requisitos / Controlos	Nível Aplicável		
9.6.1	A função central deve possuir procedimentos que garantam que todas as instalações revejam e mantenham documentos de todos os sistemas de segurança física, como o layout de CCTV e alarmes.	Ⓐ	Ⓑ	Ⓒ

9.7 Registos de Alarmes e Controlo de Acessos

Req. No.	Requisitos / Controlos	Nível Aplicável		
9.7.1	A função central deve possuir procedimentos que garantam que todos os sistemas de alarme e controlo de acessos sejam mantidos e testados para assegurar sua eficácia operacional.	Ⓐ	Ⓑ	Ⓒ
9.7.2	A função central deve possuir procedimentos que garantam que todos as instalações mantenham registos de todos os testes e incidentes relacionados à deteção de intrusão e controlo de acessos.	Ⓐ	Ⓑ	Ⓒ

9.8 Registos de Formação

Req. No.	Requisitos / Controlos	Nível Aplicável		
9.8.1	A função central deve possuir procedimentos para garantir que todos as instalações mantenham registos de formação de gestão de segurança dos seus trabalhadores.	Ⓐ	Ⓑ	Ⓒ
9.8.2	A função central deve possuir procedimentos para garantir que todos as instalações mantenham registos de formação de segurança de todo os trabalhadores. Os registos devem ser mantidos por pelo menos dois (2) anos.	Ⓐ	Ⓑ	Ⓒ

9.9 Registos de Triagem / Verificação

Req. No.	Requisitos / Controlos	Nível Aplicável		
9.9.1	A função central deve possuir procedimentos para garantir que todos as instalações realizem revisões periódicas dos registos de triagem e verificação, a fim de assegurar a integridade e a eficácia dos sistemas de gestão de segurança.	(A)	(B)	(C)
9.9.2	A função central deve possuir procedimentos para garantir que os registos das revisões, incluindo suas conclusões e ações corretivas/preventivas (ver 9.1.6), sejam mantidos. Os registos devem ser mantidos por pelo menos dois (2) anos.	(A)	(B)	(C)

9.10 Revisão por parte da Gestão para avaliar as auditorias internas; SCARs verificadas; perdas, roubos; Avaliações de Risco

Req. No.	Requisitos / Controlos	Nível Aplicável		
9.10.1	A função central deve, no mínimo, realizar revisões regulares da gestão para garantir a conformidade, eficácia e melhoria dos seus sistemas de gestão de segurança	(A)	(B)	(C)
9.10.2	As revisões por parte da gestão devem, entre outros aspetos, abranger a eficácia das auditorias internas, o encerramento das SCARs, as avaliações de risco, os incidentes e as ações de melhoria.	(A)	(B)	(C)
9.10.3	A função central deve manter registos de todas as revisões por parte gestão por pelo menos dois (2) anos	(A)	(B)	(C)

8.0 Ameaças de TI e Cibersegurança – Opção Adicional

O FSR inclui melhorias opcionais para Ameaças de TI e Cibersegurança que são considerados um nível mais alto de proteção e podem ser utilizadas em conjunto para além dos módulos. Esta melhoria opcional destina-se a ser selecionada pelo LSP/Requerente e/ou pelo seu Cliente como requisitos adicionais para as necessidades de segurança operacional. Quando na avaliação da pré-certificação esta melhoria opcional é selecionada, faz parte da auditoria de certificação e todos os requisitos se tornam obrigatórios.

A Opção Adicional no TAPA FSR fornece um nível básico de Controlos de TI e Cibersegurança no nível da instalação. Os membros são fortemente incentivados a adotar os Requisitos de Cibersegurança (CSS) para alcançar uma estrutura de Cibersegurança mais abrangente e robusta.

E8. Requisitos Obrigatórios

Req. No.	Requisitos / Controlos
E8.1.1	O LSP/Requerente deve possuir políticas de segurança para ameaças TI e Cibersegurança. As políticas podem ser separadas ou combinadas em um único documento. As políticas devem explicar: 1. As ações do LSP/Requerente para identificar e responder a ameaças. 2. As políticas e procedimentos existentes para proteger, detectar, testar e responder a eventos de segurança. 3. Os métodos para recuperação de sistemas de TI e/ou dados. 4. O protocolo de comunicação com Clientes para mitigar impactos na cadeia de abastecimento dentro de 24 horas após o conhecimento do incidente. 5. Como as políticas são revisadas anualmente e atualizadas conforme apropriado.
E8.1.2	O LSP/Requerente deve fornecer formação de sensibilização em segurança da informação a todos os colaboradores. Esta formação deve: 1. Abranger as funções e responsabilidades dos utilizadores de computador na manutenção da segurança e os benefícios associados. 2. Possuir um sistema que garanta que os registos das pessoas que receberam formação sejam mantidos e retidos por um período mínimo de 2 anos.

E8.1.3	O LSP/Requerente deve possuir uma política escrita para garantir que medidas de Cibersegurança estejam implementadas com subcontratados e/ou fornecedores, assegurando que: 1. Os requisitos de Cibersegurança do LSP/Requerente sejam comunicados aos subcontratados e/ou fornecedores e incorporados nos acordos contratuais. 2. Caso os subcontratados e/ou fornecedores não reconheçam ou se recusem a adotar os requisitos de Cibersegurança do LSP/Requerente, medidas devem ser documentadas e implementadas para mitigar os riscos aos requisitos de Cibersegurança do LSP/Requerente e de seus Clientes.
E8.1.4	O LSP/Requerente deve possuir um plano de mitigação de interrupção de energia (por exemplo, fonte de energia alternativa ou gerador de reserva / <i>backup</i>), que garanta o fornecimento de energia para sistemas críticos de TI (identificados na avaliação de risco da instalação) por um período mínimo de 48 horas.
E8.1.5	Os sistemas de informação do LSP/Requerente devem possuir software antivírus e antimalware licenciado e instalado. O software deve conter as atualizações mais recentes.
E8.1.6	O LSP/Requerente deve possuir um Plano de Recuperação de Desastres de TI (DRP) apropriado para recuperação de ataques que comprometam os sistemas, incluindo, entre outros, todos os arranjos necessários de backup e recuperação de dados e software.
E8.1.7	Os sistemas de informação do LSP/Requerente devem ser submetidos a backup. Esses backups devem ser testados regularmente, e os dados de backup devem ser criptografados e transferidos para um local secundário fora da instalação.
E8.1.8	O LSP/Requerente deve implementar uma política para todas as contas de utilizador de forma a gerir e controlar o acesso aos Sistemas de Informação, utilizando identificadores individuais exclusivos e palavras-passe fortes. Procedimentos em vigor têm de assegurar que: 1. Programa de auditoria de conformidade de palavra-passe em vigor. 2. Uma palavra-passe inicial exclusiva deve ser atribuída a cada nova conta no momento da criação. 3. As palavra-passe iniciais não podem conter o nome do utilizador, número de identificação ou seguir um padrão com base nas informações do utilizador. 4. As palavras-passe serão comunicadas aos utilizadores de forma segura e apenas após a validação da identidade do utilizador. 5. Os utilizadores devem ser obrigados a alterar a palavra-passe no login inicial. 6. As palavras-passe devem ser alteradas pelo menos a cada 90 dias.

A título informativo: a tradução da Norma para o idioma nacional disponibilizada a V. Exas. tem como objetivo facilitar a compreensão dos requisitos da TAPA 2026. A tradução da Norma foi elaborada e validada de boa-fé, com base no melhor conhecimento disponível e tendo em consideração os fundamentos necessários. No entanto, para efeitos de auditoria, a versão original em inglês da respetiva Norma é e continuará a ser a versão oficial e vinculativa.

Informações de Publicação e Direitos de Autor

Este documento é publicado pela Transported Asset Protection Association (TAPA).

© TAPA 2026–2029

Todos os direitos reservados. Nenhuma parte desta publicação pode ser reproduzida, armazenada em um sistema de recuperação, transmitida em qualquer forma ou por qualquer meio — eletrônico, mecânico, fotocópia, gravação ou outro — sem autorização prévia por escrito da TAPA, exceto conforme permitido pela legislação de direitos autorais aplicável.

O aviso de direitos autorais exibido neste documento indica o ano em que o documento foi emitido pela última vez.

Histórico de Publicação

Primeira publicação: setembro de 2026

Edição atual publicada em: setembro de 2026

Esta Especificação Publicamente Disponível (PAS) entra em vigor em 15 de setembro de 2026.

Estado deste Documento

Este documento representa os Requisitos de Segurança de Instalações da TAPA (FSR) – Revisão 2026 e estabelece os requisitos básicos para segurança de instalações dentro da estrutura de certificação da TAPA.

O documento permanece válido até que seja substituído, revisto ou retirado pela TAPA.

A TAPA poderá emitir futuras revisões, atualizações ou alterações para refletir a evolução das ameaças de segurança, práticas do setor e desenvolvimentos tecnológicos.

Uso deste Documento

A conformidade com esta especificação pode ser utilizada como parte do processo de certificação TAPA para instalações que lidam com cargas de alto valor suscetíveis a roubo.

As organizações que implementam esta especificação são responsáveis por garantir que todos os requisitos legais, regulatórios e operacionais aplicáveis sejam atendidos, além dos requisitos descritos neste documento.