FACILITY SECURITY REQUIREMENTS

TAPA

Transported Asset Protection Association

Requisitos de segurança das instalações
FSR 2023

Padrões TAPA

TAPA Américas

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

www.tapaonline.org
Telefone: (561) 617-0096

TAPA Ásia-Pacífico

1 Paya Lebar Link, #04-01,
Bairro Paya Lebar,
Singapura 408533

www.tapa-apac.org
Telefone: (65) 6514 0892

TAPA EMEA

Pastoor Ohllaan 393451 CB
VleutenPaíses Baixos

www.tapaemea.org
Telefone: +31 19573461

Índice FSR

1. Introdução 6
1.1 Finalidade deste Documento FSR 6
1.2 Recursos para implementar o FSR da TAPA 7
1.3 Protegendo políticas e procedimentos de LSP 7
2. Sobre a TAPA 8
2.1 Finalidade da TAPA 8
2.2 Missão da TAPA 8
3. Normas TAPA 9
3.1 Normas de Segurança TAPA 9
3.2 Execução 9
4. Orientação jurídica 10
4.1 Âmbito de aplicação 10
4.2 Tradução 10
4.3 A Marca "TAPA" 10
4.4 Limites de Responsabilidade 10
5. Contratos e Subcontratação 11
5.1 Contratos 11
5.2 Subcontratação 11
5.3 Investigação e Resolução de Reclamações TAPA 11
6. Renúncias 12
6. 1 Visão geral 12
6. 2 Processo de Negócio de Renúncia 12
6. 3 Derrogações para barreiras físicas (na secção 1) e para gaiolas de elevado valor 13
(HVC, ponto 4.5) 13
7. Requisitos de segurança das instalações 15
7.1 Armazém Externo de Movimentação de Carga, Expedição e Estaleiro de Recebimento (Geral) 16
7.2 Lados exteriores da instalação: CCTV 18
7.3 Ponto de Entrada de Visitantes da Área de Escritório 19
7.4 Área do Armazém: Paredes Multi-Inquilino 21
7.5 Posto de Monitorização 25
7.6 Procedimentos de escalonamento 27
7.7 Triagem/Verificação/Verificação de antecedentes (conforme permitido pela legislação local) 28
8. Requisitos da função central 29
8.1 Generalidades 29
8.2 Políticas e Procedimentos 30
8.3 Relatório de auditoria de autoavaliação realizado em todos os locais 30
8.4 Registos das inspeções, registos (registos de visitantes, registo do condutor), inspeções de 7 pontos 30
8.5 Avaliações de risco de todos os locais 30
8.6 CCTV e layout de alarme dos sites 30
8.7 Registos de alarme e controlo de acessos 31
8.8 Registos de formação 31
8.9 Rastreio/verificação de registos 31

8.10 Revisão gerencial para avaliar as autoauditorias; SCARs levantados; quaisquer perdas, roubos; Avaliações de Risco. 31
9.0. Ameaça à segurança informática e à cibersegurança – opção reforçada 31
9. Requisitos obrigatórios 32

1. Introdução

1.1 Finalidade deste Documento FSR

Este documento de Requisitos de Segurança de Instalações (FSR) é o padrão oficial da TAPA para armazenamento e armazenamento seguros. É uma norma global comum que pode ser usada em acordos de negócios/segurança entre compradores e prestadores de serviços logísticos (LSPs) e/ou outros candidatos que buscam certificação.

No desenvolvimento desta Norma, 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 aplicar-se a todos ou parte dos serviços prestados por um LSP/Requerente. Dependendo da complexidade e do tamanho da cadeia de suprimentos, a conformidade com os Padrões TAPA pode ser alcançada por meio de um único LSP/Requerente ou vários LSPs/Candidatos e subcontratados qualificados.

Âmbito de aplicação

A TAPA desenvolveu três opções para apoiar a certificação:

- Certificação de local único pelo Organismo de Auditoria Independente (IAB).
- Certificação Multi-site pelo IAB.
- Certificação de autoauditoria por Auditores Autorizados (AA) pelo LSP/Requerente ou IAB.

Público-alvo

Os usuários típicos dos Padrões TAPA incluem:

- Compradores
- LSPs/ Requerentes
- Aplicação da lei ou outras organizações governamentais
- Organizações Profissionais da Cadeia de Suprimentos
- Seguradoras

1. Introdução

1.2 Recursos para implementar o FSR da TAPA

Os recursos para atender aos requisitos do FSR serão de responsabilidade do LSP/Requerente e às custas do LSP/Candidato, a menos que conforme negociado ou acordado de outra forma pelo Comprador e pelo LSP/Requerente.

1.3 Protegendo políticas e procedimentos de LSP

Cópias de documentos de políticas e procedimentos de segurança só serão enviadas ao Comprador de acordo com os acordos de divulgação assinados entre o LSP / Requerente e o Comprador e serão tratadas como informações confidenciais.

2. Sobre a TAPA

2.1 Finalidade da TAPA

O crime de carga é um dos maiores desafios da cadeia de suprimentos para os fabricantes de produtos valiosos e de alto risco e seus prestadores de serviços logísticos.

A ameaça já não vem apenas de criminosos oportunistas. Hoje, as redes de crime organizado estão operando globalmente e usando ataques cada vez mais sofisticados a veículos, instalações e pessoal para alcançar seus objetivos.

A TAPA é um fórum único que une fabricantes globais, fornecedores de logística, transportadoras de carga, agências de aplicação da lei 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 suprimentos. A TAPA alcança isso através do desenvolvimento e aplicação de Padrões 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 suprimentos.

3. Normas TAPA

3.1 Normas de Segurança TAPA

Os seguintes Padrões de Segurança TAPA globais foram criados para garantir o transporte e armazenamento seguros de cargas direcionadas a roubo de alto valor:

- Os Requisitos de Segurança das Instalações (FSR) representam padrões mínimos especificamente para *armazenamento seguro, ou armazenamento em trânsito,* dentro de uma cadeia de suprimentos.
- Os Requisitos de Segurança para Camiões (TSR) centram-se exclusivamente no transporte por camião e representam normas mínimas específicas para *o transporte rodoviário de produtos* dentro de uma cadeia de abastecimento.

Os Padrões de Segurança Globais da TAPA são revisados e revisados 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 documento TAPA FSR e TAPA FSR Certification Framework devem ser seguidas para alcançar o status de certificação TAPA FSR.

3.2 Execução

A implementação bem-sucedida dos Padrões de Segurança da TAPA depende do trabalho conjunto dos LSPs (Prestadores de Serviços Logísticos)/Requerentes, Compradores (proprietários da carga) e Auditores Autorizados TAPA.

4. Orientação jurídica

4.1 Âmbito de aplicação

O FSR é um Padrão Global e todas as seções do Padrão são obrigatórias, a menos que uma exceção seja concedida através do processo oficial de isenção. (Ver secção 6).

4.2 Tradução

Em áreas geográficas onde o inglês não é a primeira língua, e onde a tradução é necessária e aplicável, é da responsabilidade do LSP/ Requerente e seus agentes garantir que qualquer tradução do FSR, ou qualquer uma das suas partes, reflita com precisão as intenções da TAPA no desenvolvimento e publicação destas Normas.

4.3 A Marca "TAPA"

"TAPA" é uma marca registada da Associação de Proteção de Bens Transportados e não pode ser utilizada sem a autorização expressa por escrito da TAPA através das suas regiões oficialmente reconhecidas. Os Padrões TAPA e o material associado são publicados através e 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 ações legais.

4.4 Limites de Responsabilidade

Com a publicação destas Normas, a TAPA não fornece nenhuma garantia ou garantia de que todos os eventos de roubo de carga serão evitados, quer as Normas sejam ou não totalmente implantadas e devidamente implementadas. Qualquer responsabilidade que possa resultar de um roubo de carga em armazenamento, ou qualquer outra perda de carga em armazenamento sob os Padrões FSR será por conta do LSP / Requerente e/ou do Comprador de acordo com os termos e condições em seu contrato uns com os outros e quaisquer leis ou estatutos que possam ser aplicáveis dentro da jurisdição do assunto.

5. Contratos e Subcontratação

5.1 Contratos

O transporte, armazenamento e manuseio seguros dos ativos do Comprador são de responsabilidade do LSP/Requerente, seus agentes e subcontratados durante toda a coleta, trânsito, armazenamento e entrega, conforme especificado em uma liberação ou contrato.

Quando o FSR é referenciado ou incluído no contrato entre o LSP/Requerente e o Comprador, também deve ser referenciado no programa de segurança do LSP/Candidato.

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

5.2 Subcontratação

Os subcontratados de armazenamento incluem um requisito contratual de que o LSP/Requerente subcontratado cumpra todas as Normas FSR mencionadas.

5.3 Investigação e Resolução de Reclamações 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 contrate uma nova auditoria a expensas do LSP/Candidato. Se o LSP/Requerente falhar na auditoria, ou se recusar a cumprir este processo, o seu certificado pode ser retirado.

6. Renúncias

6. 1 Visão geral

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

Todos os pedidos de renúncia para um requisito de segurança específico (parcial ou totalmente) devem ser submetidos através de um formulário de Pedido de Renúncia TAPA ao Órgão de Auditoria Independente (IAB)/ Auditor Autorizado (AA) pelo LSP/ Requerente (disponível no site da TAPA). O LSP/Requerente requerente assume total responsabilidade pela exatidão das informações fornecidas no pedido de renúncia.

Cada pedido de renúncia deve então ser submetido através do IAB/AA ao Comité Regional de Renúncia da TAPA para aprovação. É da responsabilidade do IAB/AA decidir se o pedido está completo e justifica o tratamento pela TAPA; Tal inclui a verificação do(s) fator(es) atenuante(s) e/ou controlos de segurança alternativos.

Caso os funcionários e/ou Compradores da TAPA contestem que as condições de renúncia mudaram, a TAPA concluirá uma investigação formal e o LSP/Requerente entende que a renúncia pode ser revogada pela TAPA.

6. 2 Processo de Negócio de Renúncia

Se um LSP não puder atender a um requisito específico no FSR, o processo de renúncia abaixo será implementado.

Tabela 1: Responsabilidades: Pedido de Dispensa / Avaliação

Passo	Responsabilidade	Ação
1.	LSP/ Requerente	Estabelece e verifica medidas de mitigação.
2.	LSP/ Requerente	Preenche o formulário de Pedido de Renúncia TAPA e submete-se ao IAB/AA.
3.	IAB/ AA	Analisa e verifica a integridade das informações contidas no formulário de Pedido de Renúncia da TAPA.
4.	IAB/ AA	Submete o formulário de Pedido de Renúncia de TAPA ao Comité Regional de Renúncia de TAPA.
5.	Comité Regional de Renúncia da TAPA	Revisa o pedido e concede ou nega a renúncia.

6. Renúncias

Se a renúncia for negada

Se o Comitê Regional de Renúncia da TAPA não aprovar o pedido de isenção, o LSP/Requerente é obrigado a implementar todos os requisitos de segurança do FSR.

Se a renúncia for concedida

Se o Comitê Regional de Renúncia da TAPA aprovar o pedido de isenção, as seguintes ações serão tomadas:

Tabela 2: Aprovação de renúncia

Passo	Responsabilidade	Ação
1.	Comité Regional de Renúncia da TAPA	Documenta e assina os detalhes da renúncia.
2.	Comité Regional de Renúncia da TAPA	Especifica o tempo de vida da renúncia (até um máximo de três anos) e envia uma cópia para o AA.
3.	AA	Notifica o LSP/ Requerente do resultado do Pedido de Renúncia.
4.	LSP/ Requerente	Cumpre com os requisitos de renúncia. Caso contrário, a aprovação de renúncia será anulada.

6. 3 Derrogações para barreiras físicas (na secção 1) e para gaiolas de elevado valor (HVC, ponto 4.5)

A TAPA considerará uma renúncia a todos ou parte dos requisitos de barreira perimetral e/ou para o HVC se todas as seguintes condições prévias forem atendidas:

Geral:

- O pedido de renúncia é submetido através do processo oficial do formulário de Pedido de Renúncia TAPA e é endossado pelo IAB/AA.
- O pedido de dispensa inclui pormenores sobre quaisquer medidas atenuantes destinadas a assegurar que os bens vulneráveis não correm riscos desnecessários de roubo ou perda.

- Uma avaliação de risco deve ser concluída e apresentada juntamente com o pedido de isenção. Quaisquer vulnerabilidades significativas identificadas na avaliação dos riscos devem ser enumeradas separadamente na derrogação e as medidas tomadas para reduzir o risco para um nível aceitável.

6. Renúncias

Medidas de mitigação a serem implementadas e documentadas no envio do pedido de isenção:

- **Barreiras perimetrais:**
  - Equipamentos, recursos e procedimentos adicionais introduzidos para ajudar na deteção oportuna de pessoas ou veículos não autorizados, podem incluir, mas não estão limitados a iluminação adicional, cobertura de CFTV, pessoas aprimoradas e procedimentos de aplicação de identificação de veículos, colete LSP ou uniforme apenas áreas restritas.
  - Os sinais de perímetro visíveis devem ser instalados no idioma local indicando "Sem acesso não autorizado", "Sem estacionamento não autorizado".
  - Devem ser instalados sinais visíveis nas portas ou paredes externas das docas instruindo os motoristas, visitantes, etc., a procederem ao lobby apropriado, ao controlo de segurança.
  - Confirmação de que existem procedimentos que garantem que as áreas do estaleiro de movimentação, expedição e receção de carga são inspecionadas e cumprem as condições de dispensa pelo menos semanalmente.

- **HVC:**
  - Para as isenções de HVC, as ações de mitigação apropriadas para minimizar o risco (quando um HVC não está disponível) devem ser consideradas e documentadas na Avaliação de Risco anual.
  - O pedido de renúncia inclui uma declaração anexa assinada pelo LSP/ Requerente estipulando que nenhum Comprador necessita de um HVC.

7. Requisitos de segurança das instalações

Secção	Requisitos gerais:	Um	B	C
7.0				
7.0.1	Todos os procedimentos ou políticas exigidos por esta Norma devem ser documentados.	✔	✔	✔
7.0.2	A gerência deve ter nomeado formalmente uma pessoa (AA) para a segurança no local que seja responsável pela manutenção dos requisitos de segurança da TAPA FSR, SCARS closure, avaliação de risco, relatório de gestão e requisitos de segurança da cadeia de abastecimento da empresa. Outra pessoa (pode ser a mesma) também será responsável pelo monitoramento do programa FSR. Isso inclui agendamento de verificações de conformidade, comunicações com AAs, recertificação, alterações no padrão FSR, etc. *Nota: Estas pessoas podem ser um empregado ou pessoa terceirizada sob contrato para desempenhar esta função.*	✔	✔	✔
7.0.3	Auditorias internas (por uma equipe multifuncional) no sistema de gestão de segurança, relatórios de autoavaliação pelo AA interno e fechamento SCARS devem ser concluídos e documentados.	✔	✔	✔
7.0.4	É necessário um procedimento, registo e/ou plano de chaves para fechaduras físicas, cartões de acesso e/ou chaves que gerem e controlam as chaves físicas e eletrónicas. O procedimento deve incluir processos de duplicação, armazenamento e resposta a chaves perdidas/perdidas.	✔	✔	✔
7.0.5	Uma avaliação de risco que reconheça a probabilidade e o impacto de eventos relacionados à segurança deve ser conduzida e atualizada pelo menos anualmente. A administração deve reconhecer que os riscos identificados foram avaliados e que foram implementados controlos adequados para mitigar ou eliminar os riscos para um nível aceitável. No mínimo, devem ser avaliados os seguintes eventos internos e externos comuns: roubo de carga ou informação, acesso não autorizado a instalações ou carga, adulteração/destruição de sistemas de segurança, recolhas fictícias de carga, continuidade da segurança durante escassez de mão de obra ou desastres naturais, necessidade de barreiras anti-carneiro para janelas	✔	✔	✔

	acessíveis ao nível do solo ou portas de doca, etc. Eventos adicionais podem ser considerados com base nos riscos locais/nacionais.			
7.0.6	A pessoa que realiza auditorias internas ou anuais para o candidato / LSP (chamado de LSP AA) deve ser treinada. Essa pessoa pode ser a mesma pessoa mencionada no ponto 7.0.2 ou pode ser uma pessoa terceirizada sob contrato para desempenhar essa função.	✔	✔	✔
7.0.7	Para entender o FSR e ser capaz de implementar todos os seus requisitos, todos os candidatos / LSP AAs devem ter feito e passado no exame aplicável para o Padrão TAPA e versão que eles são obrigados a auditar.	✔	✔	✔

Secção	Perímetro	Um	B	C
7.1				
Armazém Externo de Movimentação de Carga, Expedição e Estaleiro de Recebimento (Geral)				
7.1.1	CCTV (Circuito Fechado de Televisão) / VSS (Sistema de Videovigilância) capaz de visualizar todo o tráfego no pátio externo de movimentação, expedição e receção de carga (incluindo pontos de 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 caminhões em tempo real).	✔	✔	
7.1.2	Iluminação adequada nas áreas de carga e descarga. *Nota: A iluminação pode ser constante, ativada por alarme, movimento, deteção de som, etc., com iluminação imediata fornecida.*	✔	✔	✔
7.1.3	Procedimento que descreve a forma como os veículos e pessoas não autorizados devem ser geridos no estaleiro externo de movimentação, expedição e receção de carga. As instruções sobre o procedimento devem ser dadas aos membros relevantes da força de trabalho, incluindo os guardas.	✔	✔	✔
7.1.4	O manuseio, o transporte e o pátio de receção de carga são adequadamente controlados para evitar o acesso não autorizado.		✔	✔
7.1.5	No caso das janelas ou portas de doca acessíveis ao nível do solo, a Avaliação de Risco anual deve avaliar a necessidade de barreiras anti-carneiro. Além disso, deve incluir a avaliação da utilização de tampas de janelas para impedir a visualização não autorizada dos espaços interiores (ver Avaliação de Riscos, Secção 7.0.5.).	✔		
Barreiras físicas				
7.1.6	A barreira física envolve a movimentação de carga, o transporte e o pátio de receção.	✔		

Secção	Perímetro	Um	B	C
7.1.7	A barreira física ao redor do pátio de movimentação, embarque e recebimento de cargas tem uma altura mínima de 6 pés / 1,8 metros. *Nota: A barreira física, concebida para impedir o acesso não autorizado, deve ter uma altura de 6 pés / 1,8 metros ao longo de toda a sua extensão, incluindo áreas onde o nível do solo muda, ou seja, é mais baixo.*	✔		
7.1.8	Barreira física em torno do pátio de movimentação de carga, expedição e recebimento mantida em boas condições.	✔		
7.1.9	Portão(s) dentro das barreiras do pátio de movimentação, expedição e receção de cargas, tripulado ou controlado eletronicamente.	✔		
7.1.10	A barreira física em torno do manuseio de carga, transporte e pátio de recebimento é inspecionada quanto à integridade e danos pelo menos semanalmente.	✔		
Áreas Externas de Docas				
7.1.11	Áreas de doca externas cobertas via cor ou "dia / noite" exterior CCTV / VSS câmaras.	✔	✔	✔
7.1.12	CCTV / VSS câmeras montadas para ser capaz de visualizar todas as operações e movimento em torno da área de doca externa em todos os momentos, a menos obstrução temporária devido a necessidades operacionais (ou seja, carga e descarga de caminhão em tempo real).	✔	✔	✔
7.1.13	Todos os veículos e indivíduos em torno de áreas de doca externa deve ser coberto por câmeras de CFTV / VSS. que pode mostrar claramente as informações de identificação do veículo e capaz de discernir as características faciais do pessoal. *Nota: A TAPA permitirá que os detentores de certificação existentes sem a capacidade de atualizar para a resolução da câmera, continuem com sua resolução atual até a revisão de 2026. Novos titulares de certificados ou novos locais devem atender ao novo requisito.*	✔		
7.1.14	Veículos e indivíduos em torno de áreas de doca externa devem ser cobertos e visíveis por câmeras de CFTV / VSS na maioria dos casos.		✔	✔
7.1.15	Todas as áreas externas ao redor das portas das docas totalmente iluminadas.	✔	✔	✔
Acesso a Veículos Pessoais				
7.1.16	Veículos pessoais só são permitidos para áreas de movimentação, expedição e receção de carga se pré-aprovados e restritos a áreas de estacionamento assinadas/designadas. Não há estacionamento pessoal a menos de 25 m a pé das áreas de doca externas. Os processos para a pré-aprovação e restrições em vigor.	✔	✔	✔

Secção	Paredes exteriores, telhado e portas	Um	B	C
7.2				

Secção	Paredes exteriores, telhado e portas	Um	B	C
Lados exteriores da instalação: CCTV				
7.2.1	Cor ou "dia / noite" exterior CCTV / VSS câmera no lugar cobrindo todos os lados externos da instalação.	✔		
7.2.2	Cor ou "dia / noite" exterior CCTV / VSS sistema de câmera no lugar cobrindo os lados externos da instalação com portas, janelas ou outras aberturas.		✔	
7.2.3	Todas as vistas do exterior CCTV / VSS sistema de câmera clara em todos os momentos, a menos que obstrução temporária devido a necessidades operacionais (ou seja, carga e descarga de caminhão em tempo real).	✔		
7.2.4	Todos os veículos e indivíduos ao redor dos lados externos das instalações ser coberto por câmeras de CFTV / VSS, que pode mostrar claramente as informações de identificação do veículo e capaz de discernir características faciais do pessoal.	✔		
7.2.5	Veículos e indivíduos visíveis na maioria dos casos pelo exterior CCTV / VSS câmaras.		✔	
Paredes Exteriores e Telhado				
7.2.6	Paredes exteriores e telhado concebidos e mantidos para resistir à penetração (Exemplo: tijolo, bloco, laje de betão inclinável, paredes de painel sanduíche).	✔	✔	✔
7.2.7	Qualquer janela, 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.	✔	✔	
7.2.8	Todas as janelas, claraboias, aberturas, portinholas de acesso ou outros vãos do teto da instalação que possam ser abertos devem possuir uma barreira física **ou** estar alarmadas e ligadas ao sistema de alarme principal.	✔		
7.2.9	O acesso externo ao telhado (escada ou escada) deve ser: Fisicamente bloqueado e coberto por CCTV / VSS (cores ou "dia / noite" câmaras). quer Fisicamente bloqueado e alarmado.	✔		
7.2.10	Acesso externo ao telhado (escada ou escadas) fisicamente trancado.		✔	✔
7.2.11	Todas as portas externas do armazém e portas do escritório são alarmadas para detetar aberturas não autorizadas e ligadas ao sistema de alarme principal. *Nota: As portas das docas não são abrangidas por este requisito, ver ponto 7.2.17 para os requisitos de alarme das portas das docas.*	✔	✔	✔
7.2.12	Cada porta de armazém externa da instalação, porta de escritório ou outra abertura deve ser identificada exclusivamente por porta ou por zona dentro do sistema de alarme principal.	✔		
7.2.13	Todas as portas externas do armazém sempre fechadas e seguras quando não estão em uso ativo. Quando aplicável, chaves/códigos controlados.	✔	✔	

Secção	Paredes exteriores, telhado e portas	Um	B	C
7.2.14	As portas e caixilhos pedonais dos armazéns não podem ser facilmente penetrados. Se as dobradiças estiverem no exterior, devem ser fixadas ou soldadas por pontos. Portas de vidro são inaceitáveis, a menos que detetores de quebra de vidro estejam instalados, ou outro dispositivo de deteção local esteja fornecendo cobertura (por exemplo, PIR) e alarme diretamente para o centro de monitoramento ou vidro é protegido por barras / malha.	✔	✔	✔
7.2.15	As saídas de emergência que são utilizadas apenas para fins de emergência (Ex: saídas de incêndio), são sempre alarmadas com uma sonda audível individual ou zoneada.	✔	✔	
7.2.16	Todas as portas de doca de resistência suficiente para dissuadir e/ou atrasar a entrada forçada através da utilização de pequenas ferramentas manuais portáteis.	✔	✔	✔
7.2.17	**Portas Docas** **Horário de funcionamento:** Portas de doca fechadas, seguras (ou seja, incapacitadas eletronicamente ou fisicamente trancadas). Portas de doca alarmadas para detetar intrusão não autorizada e gerar um alarme ligado ao sistema de alarme principal. **Horário de funcionamento:** As portas das docas devem ser fechadas quando não estiverem em uso ativo. Os portões tesoura, se utilizados, devem ser fixados por corrediça/fecho mecânico e ter um mínimo de 8 pés/2,4 metros de altura.	✔	✔	✔

Secção	Pontos de entrada e saída de escritórios e armazéns	Um	B	C
7.3				
Ponto de Entrada de Visitantes da Área de Escritório				
7.3.1	O(s) ponto(s) de entrada de visitantes são controlados por um funcionário/guarda/rececionista que foi treinado na emissão de crachás, controles, registros, visitantes, requisitos de escolta, etc. (processo em vigor para visitas fora do horário operacional).	✔	✔	✔
7.3.2	Ponto(s) de entrada de visitantes da área de escritório coberto(s) por CCTV; (Cores ou "dia / noite" câmeras) indivíduos claramente reconhecíveis em todos os momentos.	✔	✔	
7.3.3	Alarme de Duress presente no(s) ponto(s) de entrada de visitantes da área de escritório e testado semanalmente.	✔	✔	

Secção	Pontos de entrada e saída de escritórios e armazéns	Um	B	C
7.3.4	Todos os visitantes da área do escritório identificados usando um documento de identificação com foto emitido pelo governo (por exemplo, carteira de motorista; passaporte ou carteira de identidade nacional, etc.).	✔	✔	✔
7.3.5	Todos os visitantes da área do escritório cadastrados e registrados são mantidos por um período mínimo de 30 dias.	✔	✔	✔
7.3.6	Todos os crachás de visitante devem ser reconciliados à medida que o visitante sai das instalações e o registro completo verificado diariamente.	✔	✔	
7.3.7	Todos os visitantes exibem visivelmente crachás ou passes e são escoltados por funcionários da empresa.	✔	✔	
Ponto(s) de entrada da força de trabalho				
7.3.8	Acesso controlado(s) ao(s) ponto(s) de entrada da força de trabalho 24 horas por dia, 7 dias por semana.		✔	✔
7.3.9	Ponto(s) de entrada da força de trabalho controlado(s) através de um dispositivo eletrónico de controlo de acesso 24 horas por dia, 7 dias por semana. Acesso registado.	✔		
7.3.10	Ponto(s) de entrada na mão de obra coberto(s) por CCTV. (Câmeras coloridas ou "dia/noite").	✔	✔	
7.3.11	Após a verificação, todos os funcionários devem receber crachás de identificação com foto da empresa.	✔	✔	
7.3.12	Todos os outros funcionários devem receber um crachá de identificação da empresa para torná-los reconhecíveis dentro da instalação.	✔	✔	
7.3.13	Todos os crachás da força de trabalho são claramente exibidos.	✔	✔	
7.3.14	Os crachás da força de trabalho não devem ser compartilhados em nenhuma circunstância e uma política de emissão de crachás deve estar em vigor.	✔	✔	
Identificação do condutor e do veículo				
7.3.15	Todos os condutores identificados através de um documento de identificação com fotografia emitido pelo governo (por exemplo, carta de condução; passaporte ou bilhete de identidade nacional, etc.) e um registo de condutor mantido.	✔	✔	✔
7.3.16	Verificação de que a carteira de motorista é válida, o documento de identificação com foto do motorista não expirou e corresponde ao motorista.	✔	✔	✔
7.3.17	Os identificadores dos veículos são registados manualmente (ou seja, escritos) ou com câmaras. Inclua no mínimo placa e tipo de veículo.	✔		

Secção	Interior do Armazém e Escritório	Um	B	C
7.4				

Secção	Interior do Armazém e Escritório	Um	B	C
Área do Armazém: Paredes Multi-Inquilino				
7.4.1	Paredes interiores do chão ao teto multi-inquilino e telhado construído/projetado e mantido para resistir à penetração (Exemplo: tijolo, bloco, laje de concreto inclinável, paredes de painel sanduíche).	✔	✔	✔
7.4.2	Se as paredes interiores do chão ao teto multi-inquilino são construídas de malha de arame de grau de segurança ou outra barreira segura reconhecida pela indústria, então também é para ser alarmado para detetar intrusão. *Nota: Não é aceitável a rede, a vedação de baixa qualidade ou a malha de grau não relacionado com a segurança.*	✔	✔	✔
Áreas de Almoxarifado Interno				
7.4.3	A deteção de intrusão (por exemplo, deteção de infravermelho, movimento, som ou vibração) é necessária para monitorar as áreas internas do armazém . Os alarmes devem ser ativados e ligados ao sistema de alarme principal durante as horas de inoperância (ou seja, quando o armazém está fechado). *Nota: Se o armazém for uma verdadeira operação 24/7/366, este requisito pode ser N/A se os riscos e mitigações estiverem documentados na Avaliação de Risco local. (Ver ponto 7.0.5)* *Independentemente do horário de funcionamento, a deteção de intrusão perimetral ou barreiras físicas são sempre necessárias em portas externas e janelas do térreo em escritórios e armazéns. (Ver secção 7.2.11).*	✔		
Portas e Áreas de Docas Internas				
7.4.4	Todas as portas de doca internas e áreas de doca cobertas por CCTV. (Câmeras coloridas ou "dia/noite").	✔	✔	✔
7.4.5	Vistas da carga a ser carregada/descarregada em todas as portas e áreas das docas internas, desimpedidas em todos os momentos, a menos que haja obstrução temporária devido a necessidades operacionais (ou seja, carga e descarga de camiões em tempo real).	✔	✔	✔
7.4.6	Ativos do comprador sob vigilância 100% CCTV em áreas de movimentação de carga ou preparação (ou seja, áreas de quebra / construção de paletes, rotas de e para racks de armazenamento, doca, corredores de trânsito).	✔	✔	
Controlo de Acesso entre o Escritório e a Doca/Armazém				
7.4.7	Acesso controlado entre escritório e doca/armazém.	✔	✔	
7.4.8	Os alarmes de porta de acesso por cartão ou interfone, para portas entre o escritório e a doca / armazém, são localmente audíveis e geram um alarme de resposta quando mantidos abertos por mais de 60 segundos ou imediatamente se forçados a abrir.	✔		
7.4.9	Os alarmes de porta para portas entre o escritório e a doca / armazém são localmente audíveis ou **enviam alarme para resposta** quando mantidos abertos por mais de 60 segundos ou abertos forçadamente.		✔	
7.4.10	A força de trabalho autorizada do LSP/Requerente e os visitantes escoltados permitiam o acesso às áreas de doca/armazém com base em uma necessidade comercial e restrita.	✔	✔	✔

Secção	Interior do Armazém e Escritório	Um	B	C
7.4.11	Lista de acesso às áreas de doca/armazém revisada pelo menos trimestralmente para limitar/verificar se a permissão de acesso só é concedida a pessoal designado/autorizado.	✔	✔	
Gaiola de Alto Valor (HVC) /Área				
7.4.12	O tamanho e o uso do HVC podem ser ditados pelo contrato do Comprador/LSP/Requerente. Se não houver acordo, o HVC deve ser capaz de armazenar um mínimo de 6 metros cúbicos de produto.	✔	✔	
7.4.13	HVC/ Perímetro de área enjaulado ou paredes duras em todos os lados, incluindo topo/telhado.	✔	✔	
7.4.14	HVC/ Dispositivo de bloqueio de área na porta/portão.	✔	✔	
7.4.15	Cobertura completa CCTV / VSS (cores ou "dia / noite") cobertura na entrada HVC e área interna. *Nota: Se o HVC for demasiado pequeno para localizar uma câmara no interior, a cobertura da câmara da entrada é suficiente.*	✔		
7.4.16	CCTV (cores ou "dia / noite" câmeras) cobertura na entrada HVC.		✔	
7.4.17	Se o acesso ao HVC for necessário para mais de 10 pessoas, então o acesso deve ser controlado eletronicamente por cartão / fob. Se o acesso for requerido por 10 ou menos pessoas, sistema de cadeado ou cadeado para serviço pesado suportado por um sistema de emissão de chaves controladas. As chaves podem ser desconectadas para indivíduos para cobrir um turno, mas não devem ser transferidas sem aprovação e registradas no registro de chaves. Todas as chaves a serem devolvidas e contabilizadas quando não estiverem em uso.	✔		
7.4.18	As portas/portões HVC são alarmados para detetar a entrada forçada. Os alarmes podem ser gerados por contatos de porta e / ou uso de CCTV / VSS deteção de movimento para detetar o acesso não autorizado.	✔		
7.4.19	Perímetro de HVC mantido em bom estado e inspecionado mensalmente quanto à integridade e danos.	✔		
7.4.20	LSP/ Requerente para garantir que o acesso ao HVC só é concedido a pessoal designado/autorizado. Lista de acesso aprovada ao HVC revisada mensalmente e atualizada em tempo real quando o funcionário deixa o emprego ou não precisa mais de acesso. Procedimento para acesso HVC no local.	✔	✔	
Inspeção de lixo do armazém				
7.4.21	As lixeiras internas e/ou externas do armazém principal / áreas de compactação são monitoradas por CFTV / VSS.	✔		
7.4.22	Quando utilizados, os sacos de lixo utilizados dentro do armazém são transparentes.		✔	✔

Pré-carregamento e preparo				
7.4.23	Nenhum pré-carregamento ou estacionamento de caminhões FTL / dedicado do Comprador externamente da instalação do armazém durante as horas não operacionais, a menos que mutuamente acordado entre o Comprador e o LSP / Requerente. Devem ser implementadas medidas de segurança alternativas (por exemplo, dispositivos de segurança adicionais no contentor). *Nota: "Externamente à instalação do armazém" são as áreas separadas, afastadas da instalação, mas ainda dentro da vedação do LSP/pátio do requerente/perímetro.*	✔	✔	✔
Contentores Pessoais e Pesquisas de Saída				
7.4.24	Procedimentos de segurança escritos definem a forma como os "contentores pessoais" são controlados no interior do armazém. Os recipientes pessoais incluem marmitas, mochilas, refrigeradores, bolsas, etc.	✔	✔	
7.4.25	Se permitido pela lei local, o LSP / Requerente deve desenvolver e manter um procedimento documentado para pesquisas de saída. A ativação do procedimento fica a critério do LSP/ Requerente e/ou conforme o contrato do Comprador/LSP/Candidato. No mínimo, o procedimento deve abordar os critérios de pesquisa do direito do LSP/Requerente a pesquisar, caso seja necessário introduzir buscas quando normalmente não são exigidas (por exemplo, quando há suspeita de roubo de mão de obra).	✔		
Controlo dos equipamentos de movimentação de carga				
7.4.26	Procedimento que exige que todas as empilhadeiras e outros equipamentos de movimentação de carga motorizados sejam desativados durante as horas não operacionais. *Nota: Isto não inclui hand-jacks/pallet-jacks.*	✔	✔	
integridade do contentor ou reboque; Inspeção de 7 pontos				
7.4.27	Inspeção física de 7 pontos realizada em todos os contentores ou reboques dedicados ao comprador de saída: parede frontal, lado esquerdo, lado direito, chão, teto/telhado, portas interiores/exteriores e mecanismo de bloqueio, exterior/material rodante. *Nota: Isto aplica-se a todos os tipos de reboques e contentores fechados e/ou fechados (ou seja, Não limitado a contentores de carga marítima).*	✔	✔	✔
Processo de Transferência de Frete; Selos de Segurança				

7.4.28	A menos que especificamente isento pelo Comprador, selos de segurança invioláveis são usados em todas as remessas diretas e contínuas. Os selos devem ser certificados de acordo com a norma ISO 17712 (classificação I, S ou H). *Nota: Os selos não são necessários em remessas com várias paradas, devido à complexidade e ao risco associados aos motoristas que transportam vários selos.*	✔	✔	✔
7.4.29	O LSP/Requerente deve dispor de procedimentos documentados para a gestão e controlo de selos de segurança, fechaduras das portas do reboque (contentor), fechaduras dos pinos e outro equipamento de segurança.	✔	✔	✔
7.4.30	Os selos de segurança só são afixados ou removidos por pessoal autorizado, ou seja, pessoal do armazém, que é instruído a reconhecer e comunicar selos comprometidos. Os selos nunca devem ser afixados ou removidos pelo condutor, a menos que haja isenção do Comprador.	✔	✔	✔
7.4.31	Procedimentos em vigor para reconhecer e comunicar selos de segurança comprometidos.	✔	✔	✔
Integridade da Carga; Processo de validação de carga/descarga				
7.4.32	Procedimentos robustos em vigor garantindo que todos os ativos do Comprador enviados e recebidos sejam validados no ponto de entrega através da realização de uma contagem manual e/ou eletrônica de peças. O processo deve garantir que as anormalidades sejam consistentemente reconhecidas, documentadas e relatadas ao LSP / Requerente e/ou Comprador. Os registos manuais e/ou eletrónicos devem ter qualidade probatória. Se os motoristas não estiverem presentes para testemunhar esta atividade, o Comprador / LSP / Requerente deve garantir a verificação de contagem alternativa, como digitalizações e/ou imagens de CFTV / VSS, coletadas e retidas especificamente para este fim. *Nota: Além das peças em falta, as anomalias podem incluir danos, falta de correias ou fita, cortes ou outras aberturas óbvias, indicando um possível roubo ou furto.*	✔	✔	✔
Retiradas fraudulentas				
7.4.33	A identificação do motorista do caminhão, a documentação de coleta de carga e os detalhes de pré-alerta especificados pelo comprador aplicáveis são validados antes do carregamento. O procedimento deve estar em vigor.	✔	✔	✔

Secção	Sistemas de Segurança; Conceção, Monitorização e Respostas.	Um	B	C
7.5				

Secção	Sistemas de Segurança; Conceção, Monitorização e Respostas.	Um	B	C
Posto de Monitorização				
7.5.1	Monitorização de eventos de alarme 24x7x366 através de um posto de monitorização interno ou 3rd party externo, protegido contra acesso não autorizado. *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 eletrônico de controle de acesso (crachás), fechaduras ou scanners biométricos.*	✔	✔	✔
7.5.2	Post de monitoramento para responder em todos os alarmes do sistema de segurança em tempo real 24x7x366.	✔	✔	✔
7.5.3	O posto de monitoramento reconhece a ativação do alarme e aumenta em menos de 3 minutos.	✔	✔	✔
7.5.4	Relatórios de monitorização de alarmes disponíveis.	✔	✔	✔
7.5.5	Monitorizar os procedimentos pós-resposta em vigor.	✔	✔	✔
Sistema de Deteção de Intrusão (IDS)				
7.5.6	Todos os IDS ativados durante as horas não operacionais e ligados ao sistema de alarme principal.	✔	✔	✔
7.5.7	60 dias de registros de alarme IDS mantidos.	✔	✔	
7.5.8	Registros de alarme IDS armazenados e copiados com segurança.	✔		
7.5.9	Registos de alarme IDS armazenados de forma segura.		✔	
7.5.10	Procedimento para garantir que o acesso ao IDS seja restrito a indivíduos autorizados ou administradores de sistema. Isso inclui servidores, consoles, controladores, painéis, redes e dados. Os privilégios de acesso devem ser prontamente atualizados quando os indivíduos saem da organização ou mudam de função, não necessitando mais de acesso.	✔	✔	✔
7.5.11	Alarme transmitido em falha de energia / perda do IDS. *Nota: Para sistemas com Fonte de Alimentação Ininterrupta (UPS), o alarme é transmitido quando a bateria da UPS falha.*	✔	✔	✔
7.5.12	Verificação do conjunto de alarme IDS no local. *Nota: Procedimentos que validam que os alarmes estão armados durante as horas não operacionais.*	✔	✔	✔
7.5.13	Alarme IDS transmitido através de linha fixa ou sem fio e/ou falha do modo de comunicação.	✔	✔	
7.5.14	Sistema de comunicação de backup em vigor no dispositivo IDS e/ou falha de linha.	✔	✔	

Secção	Sistemas de Segurança; Conceção, Monitorização e Respostas.	Um	B	C
Sistema de Controle de Acesso Automático (AACS)				
7.5.15	90 dias de registros de transações AACS disponíveis. Registos armazenados de forma segura; Cópia de segurança.	✔	✔	
7.5.16	Procedimento para garantir que o acesso ao AACS seja restrito a indivíduos autorizados ou administradores de sistema. Os privilégios de acesso devem ser prontamente atualizados quando os indivíduos saem da organização ou mudam de função, não necessitando mais de acesso.	✔	✔	
7.5.17	Relatórios do sistema de acesso revisados pelo menos trimestralmente para identificar irregularidades ou uso indevido (ou seja, várias tentativas malsucedidas, leituras falsas (por exemplo, cartão desativado), evidências de compartilhamento de cartão para permitir acesso não autorizado, etc.). Processo em vigor.	✔	✔	
CCTV				
7.5.18	Gravação digital de CFTV / VSS no lugar.	✔	✔	✔
7.5.19	Velocidade de gravação para CCTV / VSS é definido como um mínimo para 8 quadros por segundo (fps) por câmera.	✔	✔	✔
7.5.20	Funcionalidade de gravação digital verificada diariamente em dias operacionais através de procedimento. Registos disponíveis.	✔	✔	✔
7.5.21	CCTV / VSS gravações armazenadas por um mínimo de 30 dias, quando permitido pela lei local. LSP/Candidato deve fornecer provas de quaisquer leis locais que proíbam o uso de CFTV e/ou limitem o armazenamento de dados de vídeo a menos de 30 dias.	✔	✔	✔
7.5.22	Acesso rigorosamente controlado ao sistema CCTV / VSS, incluindo hardware, software e armazenamento de dados / vídeo. Esta sala deve ser trancada se o sistema de armazenamento CCTV / VSS estiver no local com controles de acesso no lugar.	✔	✔	✔
7.5.23	As imagens CCTV / VSS, por motivos de segurança, só são visualizadas por pessoal autorizado.	✔	✔	✔
7.5.24	Procedimentos em vigor detalhando a política de proteção de dados CCTV / VSS em relação ao uso de imagens em tempo real e arquivo de acordo com a legislação local.	✔	✔	
Iluminação Exterior e Interior				
7.5.25	Os níveis de iluminação exterior e interior são suficientes para suportar imagens de CCTV que permitem a investigação e gravação de imagem de qualidade probatória.	✔	✔	
7.5.26	Os níveis de iluminação exterior e interior são suficientes para reconhecer claramente todos os veículos e indivíduos.	✔		

Secção	Formação e Procedimentos	Um	B	C
7.6				
	Procedimentos de escalonamento			
7.6.1	Procedimentos locais em vigor para lidar com os ativos do Comprador, incluindo o processo para a comunicação atempada de ativos perdidos, perdidos ou roubados do Comprador. Incidentes a serem reportados pelo LSP/Requerente ao Comprador no prazo de 24 horas. Roubos óbvios relatados imediatamente. Processo seguido de forma consistente.	✔	✔	✔
7.6.2	Contatos de gerenciamento de instalações do Comprador de Emergência e LSP/Requerente para incidentes de segurança listados e disponíveis. Lista atualizada a cada 6 meses e inclui contactos de emergência das autoridades policiais	✔	✔	✔
Compromisso da Gestão				
7.6.3	A gerência 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 provedor.	✔	✔	✔
Formação				
7.6.4	Formação de Segurança/Sensibilização para Ameaças, a ministrar a todos os membros da força de trabalho nos primeiros 60 dias de emprego e, posteriormente, de 2 em 2 anos.	✔	✔	✔
7.6.5	Treinamento de conscientização sobre segurança da informação focado na proteção dos dados de envio eletrônicos e físicos do Comprador fornecidos à força de trabalho que tem acesso às informações do Comprador.	✔	✔	✔
Acesso aos Ativos do Comprador				
7.6.6	Procedimento(s) em vigor para proteger os ativos do Comprador (ou seja, carga) contra o acesso não autorizado por parte da força de trabalho, visitantes, etc.	✔	✔	
Controlo de Informação				
7.6.7	Acesso a documentos de envio e informações sobre os ativos do Comprador controlados com base na "necessidade de saber".	✔	✔	✔
7.6.8	Acesso a documentos de envio e informações sobre os ativos do Comprador monitorados e registrados.	✔	✔	✔
7.6.9	Documentos de Envio e informações sobre os bens do Comprador salvaguardados até à destruição.	✔	✔	✔
Relatório de incidentes de segurança				
7.6.10	Sistema de notificação e rastreamento de incidentes de segurança em vigor, usado para implementar medidas proativas.	✔	✔	
Programas de Manutenção				
7.6.11	Programas de manutenção em vigor para todas as instalações / sistemas de segurança técnica (física) para garantir a funcionalidade em todos os momentos (por exemplo, CCTV / VSS, Controles de Acesso, Deteção de Intrusão e Iluminação).	✔	✔	✔

Secção	Formação e Procedimentos	Um	B	C
7.6.12	Manutenção preventiva realizada uma vez por ano, ou de acordo com as especificações do fabricante.	✔	✔	✔
7.6.13	Verificações de funcionalidade de todos os sistemas uma vez por semana e documentadas, a menos que a falha do sistema seja imediatamente / automaticamente relatada ou alarmada.	✔	✔	
7.6.14	Uma ordem de reparação deve ser iniciada no prazo de 48 horas após a descoberta da falha. Para quaisquer reparações previstas para além de 24 horas, devem ser implementadas mitigações alternativas.	✔	✔	
Orientação ao Empreiteiro				
7.6.15	LSP/ Candidato para garantir que todos os subcontratados/fornecedores estejam cientes e cumpram os programas de segurança relevantes do LSP/ Candidato.	✔	✔	✔
Registos de Expedição e Receção				
7.6.16	Documentos de Envio e Receção legíveis, completos e precisos (ou seja, hora, data, assinaturas, motorista, pessoal de expedição e receção, detalhes e quantidade do envio, etc.).	✔	✔	✔
7.6.17	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.	✔	✔	✔
7.6.18	A prova de entrega deve ser fornecida de acordo com o acordo escrito entre o Comprador e o LSP / Requerente, onde o Comprador exige, o destino para notificar a origem dentro do prazo acordado de recebimento da remessa, conciliando detalhes de envio pré-alerta.	✔	✔	✔
Processo de pré-alerta em vigor				
7.6.19	Quando o Comprador exigir, o processo de pré-alerta aplicado a remessas de entrada e/ou saída está em vigor. Os detalhes do pré-alerta devem ser acordados entre o Comprador e o LSP/Requerente. Os detalhes sugeridos incluem: hora de partida, hora prevista de chegada, empresa de camionagem, nome do motorista, detalhes da matrícula, informações de envio (contagem de peças, peso, número do conhecimento de embarque, etc.) e números de selo do reboque.	✔	✔	✔

Secção	Integridade da força de trabalho	Um	B	C
7.7				
7.1	**Rastreio/Verificação/Verificação de antecedentes (conforme permitido pela legislação local)**			
7.7.1	O LSP/ Candidato deve ter um processo de triagem/verificação/antecedentes que inclua, no mínimo, verificações de antecedentes criminais e de emprego. A triagem/verificação aplica-se a todos os candidatos, incluindo funcionários e contratados. O LSP/Requerente também exigirá que um processo equivalente seja aplicado nas empresas contratantes fornecedoras de trabalhadores do TAS.	✔	✔	✔

Secção	Integridade da força de trabalho	Um	B	C
7.7.2	O trabalhador do TAS é obrigado a assinar uma declaração de que não tem condenações criminais atuais e cumprirá os procedimentos de segurança do LSP/Requerente.	✔	✔	✔
7.7.3	LSP/ O candidato terá acordos em vigor para ter informações de triagem/verificação/antecedentes exigidas fornecidas pela agência e/ou subcontratada que fornece trabalhadores do TAS ou deve realizar essa triagem por conta própria. A triagem deve incluir verificação de antecedentes criminais e verificações de emprego.	✔	✔	✔
7.7.4	Procedimento para lidar com a declaração falsa do candidato/força de trabalho antes ou após a contratação.	✔	✔	✔
Rescisão ou Recontratação de Mão de obra *Nota: A rescisão inclui separações voluntárias e involuntárias — membros da força de trabalho demitidos e demitidos.*				
7.7.5	Recupere ativos físicos da força de trabalho encerrada para incluir IDs da empresa, crachás de acesso, chaves, equipamentos, ativos de TI e informações confidenciais. Procedimento documentado necessário.	✔	✔	✔
7.7.6	Proteger os dados do Comprador: Encerrar o acesso da força de trabalho encerrada a sistemas físicos ou eletrônicos, incluindo aqueles que contêm dados do Comprador (inventário ou cronogramas) Procedimento necessário.	✔	✔	✔
7.7.7	Lista de verificação da força de trabalho para onboarding e off boarding no local para verificação.	✔	✔	✔
7.7.8	Recontratação: Estão em vigor procedimentos para impedir que o LSP/Candidato recontrate força de trabalho se os critérios de recusa/rescisão ainda forem válidos. *Nota: Os registos são revistos antes da recontratação (Ex: antecedentes de pessoal anteriormente despedido ou – candidatos rejeitados (emprego anteriormente negado).*	✔	✔	✔

8. Requisitos da função central (aplicável apenas à certificação multi-site)

Secção	Função central	Um	B	C
8.1	**Generalidades**			
8.1.1	Existe uma função central para gerir o sistema de gestão da segurança de todos os sítios, tal como definido no âmbito da certificação Multi-site.	✔	✔	✔
8.1.2	Todos os sítios devem ter uma relação jurídica ou contratual com a função central.	✔	✔	✔
8.1.3	Um único sistema de gerenciamento de segurança é estabelecido para garantir que todos os seus sites dentro do sistema estejam atendendo aos requisitos da Norma de Segurança TAPA aplicável.	✔	✔	✔

Secção	Função central	Um	B	C
8.1.4	A função central e o seu sistema de gestão devem ser sujeitos a auditorias internas para assegurar o cumprimento permanente das normas TAPA.	✔	✔	✔
8.1.5	A função central deve realizar auditorias aos locais abrangidos para garantir que cada local cumpre os requisitos aplicáveis do FSR da TAPA. As auditorias devem ser feitas com os modelos de auditoria TAPA apropriados. Todas as auditorias anuais individuais do local devem ser concluídas e devem estar disponíveis para o auditor antes do processo de certificação.	✔	✔	✔
8.1.6	A função central deve ter a autoridade e os direitos necessários para exigir que todos os locais cumpram as normas de segurança da TAPA e para aplicar medidas corretivas e preventivas, conforme necessário. *Nota: Se for caso disso, tal deve ser estabelecido no acordo formal entre a função central e os sítios.*	✔	✔	✔
8.2	**8.2 Políticas e Procedimentos**			
8.2.1	A função central deve manter políticas e procedimentos documentados para os seus sistemas de gestão da segurança, aplicáveis a todas as suas instalações.	✔	✔	✔
8.2.2	A função central deve assegurar que as políticas e os procedimentos adequados são atualizados, comunicados, implantados e aplicados por todos os sítios, conforme necessário.	✔	✔	✔
8.2.3	As políticas e os procedimentos devem ser mantidos e facilmente acessíveis por todos os sítios, conforme necessário.	✔	✔	✔
8.3	**8.3 Relatório de auditoria de autoavaliação realizado em todos os locais**			
8.3.1	A função central deve mandatar todas as instalações para efetuarem autoavaliações e todos os relatórios de autoavaliação devem ser apresentados à função central para registos e análises. Os registos devem ser mantidos durante, pelo menos, dois (2) anos.	✔	✔	✔
8.3.2	A função central deve assegurar que todos os CCAR resultantes da autoavaliação e das auditorias sejam devidamente encerrados, a fim de melhorar os seus sistemas de gestão da segurança.	✔	✔	✔
8.3.3	Todos os sítios devem apresentar à função central atualizações dos progressos realizados e relatórios sobre todos os CCAR pendentes. A função central será transferida 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.	✔	✔	✔
8.4	**8.4 Registos das inspeções, registos (registos de visitantes, registo do condutor), inspeções de 7 pontos**			
8.4.1	A função central deve dispor de procedimentos para garantir que todos os locais mantêm registos das inspeções, dos registos de visitantes, dos registos dos condutores, das inspeções de 7 pontos, etc.	✔	✔	✔
8.5	**8.5 Avaliações de risco de todos os locais**			
8.5.1	A função central deve dispor de procedimentos que garantam a realização de avaliações e a gestão de riscos adequadas em todos os sítios e a manutenção dos seus registos durante, pelo menos, dois (2) anos.	✔	✔	✔
8.6	**CCTV e layout de alarme dos sites**			

Secção	Função central	Um	B	C
8.6.1	A função central deve dispor de procedimentos que garantam que todos os locais analisam e mantêm documentos em todos os sistemas de segurança física, como CCTV e configuração de alarmes.	✔	✔	✔
8.7	**Registos de alarme e controlo de acessos**			
8.7.1	A função central deve dispor de procedimentos que garantam a manutenção e o ensaio de todos os sistemas de alarme e de controlo de acessos, a fim de garantir a sua eficácia operacional.	✔	✔	✔
8.7.2	A função central deve dispor de procedimentos que permitam que todos os locais mantenham registos de todos os ensaios e incidentes de deteção de intrusão e de controlo do acesso.	✔	✔	✔
8.8	**Registos de formação**			
8.8.1	A função central deve dispor de procedimentos que garantam que todas as instalações mantenham registos de formação adequados sobre a formação em gestão da segurança dos seus trabalhadores.	✔	✔	✔
8.8.2	A função central deve dispor de procedimentos que garantam que todos os locais mantêm registos da formação em segurança de todo o seu pessoal. Os registos devem ser mantidos durante, pelo menos, dois (2) anos.	✔	✔	✔
8.9	**8.9 Rastreio/verificação de registos**			
8.9.1	A função central deve dispor de procedimentos que garantam que todas as instalações efetuam o rastreio e a verificação dos registos a intervalos regulares, a fim de garantir a integridade e a eficácia dos sistemas de gestão da segurança.	✔	✔	✔
8.9.2	A função central deve dispor de procedimentos que garantam a manutenção dos registos das revisões, incluindo as suas constatações, e das ações corretivas/preventivas do ponto 8.1.6. Os registos serão mantidos durante, pelo menos, 2 (dois) anos.	✔	✔	✔
8.10	**8.10 Revisão gerencial para avaliar as autoauditorias; SCARs levantados; quaisquer perdas, roubos; Avaliações de Risco.**			
8.10.1	A função central deve, no mínimo, proceder a revisões periódicas da gestão, a fim de assegurar a conformidade, a eficácia e a melhoria dos seus sistemas de gestão da segurança.	✔	✔	✔
8.10.2	As revisões da gestão devem abranger, nomeadamente, a eficácia das autoauditorias, os encerramentos de SCAR, as avaliações de risco, os incidentes e as medidas de melhoria.	✔	✔	✔
8.10.3	A função central deve manter registos de todas as análises da gestão durante, pelo menos, dois (2) anos.	✔	✔	✔

9.0. Ameaça à segurança informática e à cibersegurança – opção reforçada

O FSR inclui aprimoramentos opcionais de ameaças de segurança cibernética que são considerados um nível mais alto de proteção e podem ser usados além dos módulos. Esta

melhoria opcional destina-se a ser selecionada pelo LSP/Requerente e/ou pelo seu Comprador como requisitos adicionais para as suas necessidades de segurança operacional. Quando esta melhoria opcional é selecionada na avaliação de pré-certificação para fazer parte da auditoria de certificação, todos os requisitos se tornam obrigatórios.

Secção	Ameaça à TI e à cibersegurança – Opção melhorada
9.	**Requisitos obrigatórios**
9.1	O LSP / Candidato deve ter políticas de segurança para TI e ameaças cibernéticas. As políticas podem ser separadas ou em um documento combinado. As políticas devem explicar: - 1. As ações do LSP/ Requerente para identificar e responder a ameaças. 2. As políticas e procedimentos em vigor para proteger, detetar, testar e responder a eventos de segurança. 3. Os métodos de recuperação de sistemas e/ou dados informáticos. 4. O protocolo de comunicação aos Compradores/Clientes para mitigar o impacto na cadeia de abastecimento no prazo de 24 horas após o conhecimento do incidente. 5. Como as políticas são revistas anualmente e atualizadas conforme apropriado.
9.2	O LSP/Candidato deve ministrar formação de sensibilização para a informação a todos os colaboradores. Esta formação deve: - 1. Cobrir as funções e responsabilidades que os usuários de computador têm na manutenção da segurança e os benefícios associados. 2. Dispor de um sistema que garanta que os registos das pessoas que recebem formação são mantidos e conservados por um período mínimo de 2 anos.
9.3	O LSP / Candidato deve ter uma política escrita em vigor para garantir que as medidas de Segurança Cibernética estejam em vigor com subcontratados e/ou fornecedores que garantam: 1. Os requisitos de Segurança Cibernética da LSP/Requerente são comunicados a subcontratados e/ou fornecedores e incorporados em contratos. 2. Quando os subcontratados e/ou fornecedores não reconhecem ou se recusam a adotar os requisitos de Segurança Cibernética do LSP/Candidato, são documentadas e implementadas medidas que mitigam os riscos para os requisitos de Segurança Cibernética do LSP/Requerente e seus clientes.
9.4	O LSP/Requerente deve ter um plano de Mitigação da Interrupção de Energia (por exemplo, fonte de alimentação alternativa ou gerador de reserva), que garanta que a energia é encaminhada para sistemas de TI críticos (identificados na avaliação de risco local) por um período mínimo de 48 horas.
9.5	Os Sistemas de Informação do LSP/Candidato devem ter instalado software antivírus e antimalware licenciado. O software antivírus e antimalware deve conter as atualizações mais recentes.
9.6	O LSP/ Candidato deve ter um Plano de Recuperação de Desastres de TI (DRP) apropriado para a recuperação de ataques comprometidos ao sistema, incluindo, mas não limitado a, todos os dados necessários e arranjos de backup e recuperação de software.
9.7	Os sistemas de informação do LSP/candidato 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 do local.

Secção	Ameaça à TI e à cibersegurança – Opção melhorada
9.8	O LSP/ Candidato deve implementar uma política para todas as contas de usuário para gerenciar e controlar o acesso aos Sistemas de Informação usando identificadores individuais exclusivos e senhas fortes. Procedimentos em vigor para assegurar: 1. Programa de auditoria de conformidade de senha em vigor. 2. Uma senha inicial exclusiva deve ser atribuída a cada nova conta no momento da criação. 3. As senhas iniciais não podem conter o nome do usuário, número de identificação ou seguir um padrão padrão com base nas informações do usuário. 4. As palavras-passe serão comunicadas aos utilizadores de forma segura e apenas após a validação da identidade do utilizador. 5. Os usuários devem ser obrigados a alterar as senhas no login inicial. 6. As senhas devem ser alteradas pelo menos a cada 90 dias.

Publicação e informações sobre direitos de autor

Historial da publicação

Publicado pela primeira vez em agosto de 2023

Primeira edição (presente) publicada em agosto de 2023

Esta especificação publicamente disponível entra em vigor em 15 de setembro de 2023