Transported Asset Protection Association

Requisitos de segurança das instalações FSR 2023

Requisitos 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

FACILITY SECURITY REQUIREMENTS

Transported Asset Protection Association

Índice FSR

1. Introdução

1.1 Finalidade deste Documento FSR

Este documento de Requisitos de Segurança das Instalações (FSR) é a norma oficial da TAPA para o processo logístico de mercadorias e armazenamento seguros. Trata-se de uma norma 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 um padrão de certificação.

No desenvolvimento desta norma, a TAPA reconhece as múltiplas diferenças na forma como os serviços de armazenagem são fornecidos globalmente, regionalmente e até mesmo dentro das empresas, e que o FSR pode aplicar-se a todos ou a parte dos serviços prestados por um LSP/Requerente. Dependendo da complexidade e do tamanho da cadeia de abastecimento, a conformidade com os requisitos TAPA pode ser alcançada por meio de um único ou vários LSPs/Fornecedor(es) 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.

Público-alvo

Os utilizadores típicos dos Requisitos TAPA incluem:

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

1. Introdução

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 de 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. 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. 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 para Camiões (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 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 documento TAPA FSR e 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) / Fornecedores, Clientes (proprietários da carga) e Auditores credenciados TAPA.

4. Orientação jurídica

4.1 Âmbito da Certificação

O FSR é uma Norma Global e todas as seções da Norma são obrigatórias, a menos que uma exceção seja concedida através do processo oficial de dispensa. (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 dos seus colaboradores, garantir que qualquer tradução do FSR, ou qualquer uma das suas partes, reflita com precisão as intenções da TAPA no desenvolvimento e publicação destes normativos.

4.3 A Marca "TAPA"

"TAPA" é uma marca registada 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 ações legais.

4.4 Limites de Responsabilidade

Com a publicação da Norma, 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. 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 provas da Certificação FSR e, quando apropriado, provas 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

Os subcontratantes de armazenagem 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 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. Processo de Negociação de Dispensa

6.1 Visão geral

Uma dispensa é uma aprovação por escrito concedida para eximir uma instalação sobre um requisito específico de TAPA ou para 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.

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

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

Caso os funcionários e/ou Clientes da TAPA contestem que as condições de dispensa mudaram, a TAPA efetuará uma investigação formal e o LSP/Requerente deve estar ciente que a dispensa pode ser revogada pela TAPA.

6.2 Processo de Negociação de Dispensa

Se um LSP não estiver conforme com um requisito específico no FSR, o processo de dispensa 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 Dispensa TAPA e submete ao IAB/AA.
3.	IAB/ AA	Analisa e verifica a integridade das informações contidas no formulário de Pedido de Dispensa da TAPA.
4.	IAB/ AA	Submete o formulário de Pedido de Dispensa da TAPA ao Comité Regional de Dispensa da TAPA.
5.	Comité Regional de Dispensa da TAPA	Revê o pedido e concede ou nega a dispensa.

6. Dispensas

Se a dispensa for negada

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

Se a dispensa for concedida

Se o Comité Regional de Dispensa da TAPA aprovar o pedido de dispensa, as seguintes ações serão tomadas:

Tabela 2: Aprovação de dispensa

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

6.3 Dispensas para barreiras físicas (na secção 1) e para Jaula Alto Valor (HVC - High Value Cage)

A TAPA considerará um pedido de dispensa a todos ou parte dos requisitos de barreiras físicas no perímetro e/ou para o HVC se todas as seguintes condições prévias forem cumpridas:

Geral:

- O pedido de dispensa é submetido através do processo oficial do formulário de Pedido de Dispensa TAPA e é aprovado pelo IAB/AA.
- O pedido de dispensa inclui pormenores sobre quaisquer ações mitigatórias destinadas a assegurar que os bens vulneráveis não correm riscos desnecessários de roubo ou perda.
- Deve ser preenchida uma avaliação dos riscos e apresentada juntamente com o pedido. Quaisquer vulnerabilidades significativas identificadas na avaliação dos riscos devem ser enumeradas separadamente no pedido de dispensa e as ações mitigatórias tomadas para reduzir o risco a um nível aceitável.

6. Dispensas

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

- **Barreiras perimétricas:**
  - Equipamentos, recursos e procedimentos adicionais introduzidos para ajudar na deteção atempada de pessoas ou veículos não autorizados, podem incluir, mas não estão limitados a iluminação adicional, cobertura de CCTV, procedimentos reforçados de controlo da identificação de pessoas e veículos em zonas de acesso restrito, uso de colete identificativo do LSP ou uniforme em áreas restritas.
  - Devem ser instalados sinais visíveis no perímetro no idioma local indicando: "Acesso não autorizado", "Estacionamento não autorizado".
  - Devem ser instalados sinais visíveis nas portas ou paredes externas dos cais instruindo os motoristas, visitantes, etc., a procederem à receção apropriada, para controlo de segurança.
  - Confirmação de que existem procedimentos que garantem que as áreas de movimentação de carga, expedição e receção de carga são inspecionadas e cumprem as condições do pedido de dispensa pelo menos semanalmente.

- **HVC:**
  - Para as dispensas da 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 dispensa inclui uma declaração em anexo assinada pelo LSP/Requerente estipulando que nenhum Cliente necessita de um HVC.

7. Requisitos de segurança das instalações

Secção	Requisitos gerais:	A	B	C
7.0				
7.0.1	Todos os procedimentos ou políticas exigidas por esta Norma devem ser documentados.	✔	✔	✔
7.0.2	O responsável pelas operações deve ter nomeado formalmente uma pessoa (AA) para a segurança no local que seja responsável pela manutenção dos requisitos de segurança 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. *Nota: Estas pessoas podem ser um colaborador ou uma pessoa subcontratada para desempenhar essa função.*	✔	✔	✔
7.0.3	Auditorias internas (realizadas por uma equipa multifuncional) no sistema de gestão de segurança, relatórios de autoavaliação pelo AA interno e encerramento de SCARS devem ser concluídos e documentados.	✔	✔	✔
7.0.4	É necessário um procedimento de gestão de chaveiro e/ou um registo da movimentação 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 para duplicação, armazenagem e resposta a chaves perdidas/desaparecidas.	✔	✔	✔
7.0.5	É necessário realizar uma avaliação de risco que reconheça a probabilidade e o impacto de eventos relacionados com a segurança, deve ser conduzida e atualizada pelo menos anualmente. O responsável das operações deve reconhecer que os riscos identificados foram avaliados e que foram implementados controlos adequados para mitigar ou eliminar os riscos a 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 dificultadoras de acesso (anti-ram) para janelas ou portas de cais acessíveis ao nível do solo ou portas de cais, etc. Podem ser considerados eventos adicionais com base nos riscos locais/nacionais. Eventos adicionais podem ser considerados com base nos riscos locais/nacionais.	✔	✔	✔
7.0.6	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 ponto 7.6.3 ou pode ser uma pessoa subcontratada para desempenhar essa função.	✔	✔	✔
7.0.7	Para compreender o FSR e ser capaz de implementar todos os seus requisitos, todos os Requerentes / LSP AAs devem ter feito e passado no exame aplicável para a Norma TAPA da versão que eles são obrigados a auditar.	✔	✔	✔

Secção	Perímetro	A	B	C
7.1				
Movimentação de Carga no Exterior do Armazém, Expedição e Área de Receção (Geral)				
7.1.1	CCTV (Circuito Fechado de Televisão) / VSS (Sistema de Videovigilância) capaz de visualizar todo o tráfego no parque 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 camiões 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 na área exterior de movimentação de carga, expedição e receção de carga. As instruções sobre o procedimento devem ser comunicadas aos membros relevantes da força de trabalho, incluindo os vigilantes.	✔	✔	✔
7.1.4	O manuseio, o transporte e a área de receção de carga são adequadamente controlados para evitar o acesso não autorizado.		✔	✔
7.1.5	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. Além disso, deve incluir a avaliação da utilização de coberturas 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 encerra a zona de movimentação de carga, a expedição e a zona de receção de carga.	✔		
7.1.7	A barreira física ao redor da zona de movimentação, expedição e receção 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 da zona de movimentação de carga, expedição e receção mantida em boas condições.	✔		
7.1.9	Portão(ões) dentro das barreiras da zona de receção, movimentação e expedição de cargas, controlados física e/ou eletronicamente por pessoal autorizado.	✔		
7.1.10	A barreira física em torno da zona da movimentação de carga, transporte e zona de receção é inspecionada quanto à integridade e danos pelo menos uma vez por semana.	✔		
Áreas Externas dos Cais				
7.1.11	Áreas externas dos cais cobertas por câmaras CCTV/ VSS para exterior a cores ou "dia/noite".	✔	✔	✔
7.1.12	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 camião em tempo real).	✔	✔	✔

Secção	Perímetro	A	B	C
7.1.13	Todos os veículos e indivíduos em torno 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. *Nota: A TAPA permitirá que os detentores de certificação existentes sem a capacidade de atualizar para a resolução da câmara, continuem com sua resolução atual até a revisão de 2026. Novos titulares de certificados ou novas instalações devem estar conformes com o novo requisito.*	✔		
7.1.14	Veículos e indivíduos em torno da área externa dos cais devem ser cobertos e visíveis por câmaras de CCTV/VSS na maioria dos casos.		✔	✔
7.1.15	Todas as áreas externas ao redor das portas dos cais são totalmente iluminadas.	✔	✔	✔
Acesso a Veículos Pessoais				
7.1.16	Só é permitida a entrada de veículos pessoais nas zonas de movimentação, expedição e receção de carga se pré-aprovados e restritos às áreas de estacionamento sinalizadas/designadas. Não é permitido o estacionamento pessoal a menos de 25 m a pé das áreas externas dos cais. Os processos para a pré-aprovação e restrições devem estar em vigor.	✔	✔	✔

Secção	Paredes exteriores, cobertura e portas	A	B	C
7.2				
Exterior das instalações: CCTV				
7.2.1	Sistema de câmaras CCTV/ VSS exteriores, a cores ou "dia/noite", que cubra todos os lados exteriores da instalação.	✔		
7.2.2	Sistemas de CCTV/VSS a cor ou "dia / noite" que cubram os lados exteriores da instalação com portas, janelas ou outras aberturas.		✔	
7.2.3	Todas as vistas do sistema de câmaras exteriores CCTV/VSS são claras em todos os momentos, a menos que haja obstrução temporária devido a necessidades operacionais (ou seja, carga e descarga de camião em tempo real).	✔		
7.2.4	Todos os veículos e indivíduos ao redor dos lados externos das instalações devem ser cobertos por câmaras de CCTV/VSS, que devem mostrar claramente as informações de identificação do veículo com capacidade de discernir características faciais dos intervenientes.	✔		
7.2.5	Veículos e indivíduos visíveis na maioria dos casos pelo sistema de câmaras exterior CCTV/VSS.		✔	
Paredes Exteriores e Cobertura				
7.2.6	Paredes exteriores e telhado/cobertura concebidos e mantidos de forma a resistir à penetração (Exemplo: tijolo, bloco, laje de betão inclinável, paredes de painel sanduíche).	✔	✔	✔
7.2.7	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.	✔	✔	

Secção	Paredes exteriores, cobertura e portas	A	B	C
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 à cobertura (escadote ou escadas) deve ser: Fisicamente bloqueado e coberto por CCTV/VSS (a cores ou câmaras "dia / noite"). ou Fisicamente bloqueado e alarmado.	✔		
7.2.10	Acesso externo à cobertura (escadote 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 estão conectadas ao sistema de alarme principal. *Nota: As portas das cais não são abrangidas por este requisito, ver ponto 7.2.17 para os requisitos de alarme das portas dos Cais.*	✔	✔	✔
7.2.12	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.	✔		
7.2.13	Todas as portas externas do armazém devem estar sempre fechadas e seguras quando não estão em uso ativo. Quando aplicável, chaves/códigos controlados.	✔	✔	
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 forneça cobertura (por exemplo, PIR) e alarme diretamente para o centro de monitorização ou o vidro ser protegido por barras / rede.	✔	✔	✔
7.2.15	As saídas de emergência só devem ser utilizadas para fins de emergência (Ex: saídas de incêndio), são sempre alarmadas com um dispositivo sonoro individual ou por zona.	✔	✔	
7.2.16	Todas as portas de cais devem ter resistência suficiente para dissuadir e/ou atrasar a entrada forçada através da utilização de pequenas ferramentas manuais portáteis.	✔	✔	✔
7.2.17	**Portas de Cais** **Horário de funcionamento:** Portas de cais fechadas e protegidas (ou seja, incapacitadas eletronicamente ou fisicamente trancadas). Portas de cais alarmadas para detetar intrusão não autorizada e gerar um alarme ligado ao sistema de alarme principal. **Horário de funcionamento:** As portas das cais devem ser 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 8 pés/2,4 metros de altura.	✔	✔	✔

Secção	Pontos de entrada e saída de escritórios e armazéns	A	B	C
7.3				
Ponto de Entrada de Visitantes na Área de Escritório				
7.3.1	O(s) ponto(s) de entrada de visitantes são controlados por um funcionário/guarda/rececionista que foi capacitado na emissão de cartões, controlo, registo, entrada de visitantes, requisitos de escolta, etc. (processo em vigor para visitas fora do horário de funcionamento).	✔	✔	✔
7.3.2	Ponto(s) de entrada de visitantes da área de escritório coberto(s) por CCTV; (Câmaras a cores ou "dia / noite") indivíduos claramente reconhecíveis em todos os momentos.	✔	✔	
7.3.3	Alarme de emergência presente no(s) ponto(s) de entrada de visitantes da área de escritório e testado semanalmente.	✔	✔	
7.3.4	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.).	✔	✔	✔
7.3.5	Todos os visitantes da área do escritório registados são mantidos por um período mínimo de 30 dias.	✔	✔	✔
7.3.6	Todos os cartões de visitante devem ser desabilitados assim que o visitante sai das instalações e o registo verificado diariamente.	✔	✔	
7.3.7	Todos os visitantes devem exibir visivelmente os seus cartões e devem ser acompanhados por Colaboradores da empresa.	✔	✔	
Ponto(s) de entrada de Colaboradores				
7.3.8	Ponto(s) de entrada de Colaboradores controlado(s) 24 horas por dia, 7 dias por semana.		✔	✔
7.3.9	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.	✔		
7.3.10	Ponto(s) de entrada da mão de obra coberto(s) por CCTV. (Câmaras coloridas ou "dia/noite").	✔	✔	
7.3.11	Após a verificação, todos os funcionários devem receber cartões de identificação com foto da empresa.	✔	✔	
7.3.12	Todos os funcionários devem receber um cartão de identificação da empresa para torná-los reconhecíveis dentro das instalações.	✔	✔	
7.3.13	Todos os cartões dos Colaboradores devem ser claramente exibidos.	✔	✔	
7.3.14	Os cartões dos Colaboradores não devem ser partilhados em nenhuma circunstância e uma política de emissão de cartões deve estar em vigor.	✔	✔	
Identificação do condutor e do veículo				
7.3.15	Todos os condutores 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 condutor mantido.	✔	✔	✔

Secção	Pontos de entrada e saída de escritórios e armazéns	A	B	C
7.3.16	Verificação de que a carta de condução é válida, o documento de identificação com foto não expirou e que ambos correspondem ao motorista.	✔	✔	✔
7.3.17	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.	✔		

Secção	Interior do Armazém e Escritório	A	B	C
7.4				
	do Armazém: Paredes Multi-Inquilino			
7.4.1	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).	✔	✔	✔
7.4.2	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. *Nota: Não é aceitável rede, vedação de baixa qualidade ou malhas que não garantam segurança.*	✔	✔	✔
Áreas de Almoxarifado Interno				
7.4.3	A deteção de intrusão (por exemplo, deteção de infravermelho, movimento, som ou vibração) é necessária para monitorizar as áreas internas do armazém. Os alarmes devem ser ativados e ligados ao sistema de alarme principal fora das horas de atividade (nas horas em que não decorre a operação) (ou seja, quando não existe operação e 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 do perímetro ou barreiras físicas são sempre necessárias em portas externas e janelas térreas e em escritórios e armazéns. (Ver secção 7.2.11).*	✔		
Portas e Áreas de Cais Internas				
7.4.4	Todas as portas interiores de cais e áreas de cais devem ser cobertas por CCTV. (Câmaras coloridas ou "dia/noite").	✔	✔	✔
7.4.5	Vistas da carga a ser carregada/descarregada em todas as portas e áreas das cais internas, sempre desimpedidas, 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 Cliente 100% sobre vigilância CCTV em áreas de movimentação de carga ou preparação (ou seja, áreas de receção / arrumação de paletes, rotas de armazenagem de e para racks, cais, corredores de trânsito).	✔	✔	
Controlo de Acesso entre o Escritório e a Cais/Armazém				
7.4.7	Acesso controlado entre escritório e cais/armazém.	✔	✔	

Secção	Interior do Armazém e Escritório	A	B	C
7.4.8	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.	✔		
7.4.9	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.		✔	
7.4.10	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 comerciais.	✔	✔	✔
7.4.11	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.	✔	✔	
Compartimento estanque de Alto Valor (HVC) /Área				
7.4.12	O tamanho e o uso do HVC podem ser ditados pelo acordo/contrato do Cliente/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 do compartimento de Alto Valor deve ser estanque e estar segregado (Gaiola/Jaula) ou ter paredes duras em todos os lados, incluindo topo/cobertura.	✔	✔	
7.4.14	HVC/ Área da porta/portão deve ter um dispositivo de bloqueio.	✔	✔	
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 colocar uma câmara no interior, a cobertura da câmara da entrada é suficiente.*	✔		
7.4.16	Cobertura CCTV (câmaras a cores ou "dia / noite") na entrada da 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 / controlo portátil. Se o acesso for necessário por 10 ou menos pessoas, deve ser utilizado um sistema de fechadura ou cadeado resistente apoiado por um sistema de emissão de chaves controladas. As chaves podem ser entregues a indivíduos para cobrir um turno, mas não devem 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.	✔		
7.4.18	As portas/portões HVC são alarmados para detetar a entrada forçada. Os alarmes podem ser gerados por contactos de porta e/ou utilização de deteção de movimento CCTV/VSS para detetar acesso não autorizado. (Os alarmes podem ser gerados por contactos magnéticos e/ou uso de deteção de movimento CCTV/VSS para detetar o acesso não autorizado.)	✔		
7.4.19	Perímetro de HVC mantido em bom estado e inspecionado mensalmente quanto à sua integridade e danos.	✔		

Secção	Interior do Armazém e Escritório	A	B	C
7.4.20	LSP/Requerente tem de garantir que o acesso ao HVC só é concedido a pessoal designado/autorizado. Lista de acesso aprovada do HVC revista mensalmente e atualizada em tempo real quando o funcionário termina as suas funções na empresa ou não necessita mais de acesso. Procedimento para acesso HVC em vigor.	✔	✔	
Inspeção de lixo do armazém				
7.4.21	Os recipientes de lixo internos e/ou externos do armazém principal / áreas de compactação são monitorizadas por CCTV/VSS.	✔		
7.4.22	Quando utilizados, os sacos de lixo dentro do armazém devem ser transparentes.		✔	✔
Pré-carregamento e preparação				
7.4.23	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 no contentor). *Nota: "No exterior da instalação do armazém" são aquelas áreas separadas, afastadas da instalação, mas ainda dentro da vedação/perímetro do LSP.*	✔	✔	✔
Recipientes Pessoais e Revistas à Saída				
7.4.24	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.	✔	✔	
7.4.25	Se permitido pela lei local, o LSP/Requerente deve desenvolver e manter um procedimento documentado para revistas à saída. A ativação do procedimento fica ao critério do LSP/Requerente e/ou conforme o contrato do Cliente/LSP/Requerente. No mínimo, o procedimento deve abordar o direito e os critérios da revista por parte do LSP/Requerente, principalmente em casos que normalmente não estavam exigidas (por exemplo, quando há suspeita de furto por parte dos funcionários).	✔		
Controlo dos equipamentos de movimentação de carga				
7.4.26	Procedimento que exige que todas os empilhadores e outros equipamentos de movimentação de carga motorizados sejam desativados fora das horas de atividade operacional. N*ota: Isto não inclui empilhadores manuais e porta paletes.*	✔	✔	
Integridade do contentor ou reboque; Inspeção de 7 pontos				
7.4.27	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. *Nota: Isto aplica-se a todos os tipos de galeras e contentores fechados e/ou selados (ou seja, não se limita a contentores de carga marítima).*	✔	✔	✔

Secção	Interior do Armazém e Escritório	A	B	C
Processo de Transferência de carga; Selos de Segurança				
7.4.28	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). *Nota: Os selos não são necessários em entregas com várias paragens, devido à complexidade e ao risco associados aos motoristas que transportam vários selos.*	✔	✔	✔
7.4.29	O LSP/Requerente deve dispor de procedimentos documentados e em vigor para a gestão e controlo de selos de segurança, fechaduras das portas da galera/contentor, fechadura de passadores, outros equipamentos de segurança.	✔	✔	✔
7.4.30	Os selos de segurança apenas devem ser colocados ou removidos por pessoal autorizado, ou seja, pessoal do armazém, que é instruído a reconhecer e comunicar a existência selos comprometidos. Os selos nunca devem ser afixados ou removidos pelo condutor, a menos que haja dispensado Cliente.	✔	✔	✔
7.4.31	Devem existir 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 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 eletrónica 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. *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.*	✔	✔	✔
Recolhas fraudulentas				
7.4.33	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.	✔	✔	✔

Secção	Sistemas de Segurança; Conceção, Monitorização e Respostas.	A	B	C
7.5				
	Posto de Monitorização			
7.5.1	Monitorização de eventos de alarme 24x7x366 deve ser realizada através de um posto de monitorização interno ou subcontratação, 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 eletrónico de controlo de acesso (cartões), fechaduras ou scanners biométricos.*	✔	✔	✔
7.5.2	Deve existir um posto de monitorização para responder a todos os alarmes do sistema de segurança em tempo real 24x7x366.	✔	✔	✔
7.5.3	O posto de monitorização reconhece o evento que despoletou o alarme e responde em menos de 3 minutos.	✔	✔	✔
7.5.4	Devem estar disponíveis relatórios de monitorização de alarmes.	✔	✔	✔
7.5.5	Procedimentos de resposta do posto de monitorização 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	Mantidos 60 dias os registos de alarme IDS.	✔	✔	
7.5.8	Registos de alarme IDS devem ser armazenados e copiados (backup) em segurança.	✔		
7.5.9	Registos de alarme IDS devem ser armazenados em segurança.		✔	
7.5.10	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 devem ser prontamente atualizados quando os indivíduos terminam as suas funções na organização ou mudam de função, não necessitando mais de acesso.	✔	✔	✔
7.5.11	Alarme transmitido em caso de 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 sistema de alarme IDS em vigor. *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.	✔	✔	

Secção	Sistemas de Segurança; Conceção, Monitorização e Respostas.	A	B	C
7.5.14	Sistema de comunicação de recurso em vigor em caso de falha do dispositivo IDS e/ou da linha.	✔	✔	
Sistema de Controlo de Acesso Automático (AACS)				
7.5.15	90 dias de registos de transações AACS disponíveis. Registos armazenados de forma segura; necessária cópia de segurança.	✔	✔	
7.5.16	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.	✔	✔	
7.5.17	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.	✔	✔	
CCTV				
7.5.18	Gravação digital de CCTV/VSS em vigor.	✔	✔	✔
7.5.19	Velocidade de gravação para CCTV/VSS deve estar definida como um mínimo de 8 fotogramas por segundo (fps) por câmara.	✔	✔	✔
7.5.20	A funcionalidade de gravação digital verificada diariamente, em dias de operação, de acordo com procedimento. Registos disponíveis.	✔	✔	✔
7.5.21	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.	✔	✔	✔
7.5.22	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 no local com controlos de acesso acessíveis.	✔	✔	✔
7.5.23	Por motivos de segurança, as imagens CCTV/VSS, só podem ser visualizadas por pessoal autorizado.	✔	✔	✔
7.5.24	Procedimentos em vigor a detalhar 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 evidente.	✔	✔	
7.5.26	Os níveis de iluminação exterior e interior são suficientes para reconhecer claramente todos os veículos e indivíduos.	✔		

Secção	Formação e Procedimentos	A	B	C
7.6				
	Procedimentos de escalonamento			
7.6.1	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.	✔	✔	✔
7.6.2	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	✔	✔	✔
Compromisso da Gestão				
7.6.3	A direção 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.	✔	✔	✔
Formação				
7.6.4	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.	✔	✔	✔
7.6.5	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.	✔	✔	✔
Acesso aos Ativos do Cliente				
7.6.6	Procedimento(s) em vigor para proteger os ativos do Cliente (ou seja, carga) contra o acesso não autorizado por parte dos Colaboradores, visitantes, etc.	✔	✔	
Controlo de Informação				
7.6.7	Acesso a documentos de transporte e informações sobre os ativos do Cliente controlados com base no "estritamente necessário".	✔	✔	✔
7.6.8	Acesso a documentos de envio e informações sobre os ativos do Cliente monitorizados e registados.	✔	✔	✔
7.6.9	Documentos de envio e informações sobre os bens do Cliente salvaguardados até à destruição.	✔	✔	✔
Relatório de incidentes de segurança				
7.6.10	Sistema de notificação e rastreamento de incidentes de segurança em vigor, devendo ser utilizado 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	A	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 a serem realizadas uma vez por semana e documentadas, exceto se as falhas do sistema sejam imediatamente/automaticamente relatadas ou alarmadas.	✔	✔	
7.6.14	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.	✔	✔	
Orientação do Contratante				
7.6.15	LSP/Requerente tem de garantir que todos os subcontratados/fornecedores estão cientes e cumprem os programas de segurança relevantes do LSP/Requerente.	✔	✔	✔
Registos de Expedição e Receção				
7.6.16	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.).	✔	✔	✔
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 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.	✔	✔	✔
Processo de pré-alerta em vigor				
7.6.19	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.	✔	✔	✔

Secção	Integridade dos Colaboradores	A	B	C
7.7				
7.1	**Triagem/ Verificação de antecedentes/Rescisão (conforme permitido pela legislação local)**			
7.7.1	O LSP/Requerente deve ter um processo de triagem/verificação que inclui, empregos anteriores e antecedentes criminais. A seleção/verificação aplica-se a todos os candidatos, incluindo funcionários e contratados. O LSP/Requerente também exigirá que um processo equivalente seja aplicado nas empresas contratadas fornecedoras de trabalhadores temporários (TAS).	✔	✔	✔
7.7.2	Os trabalhadores temporários são obrigados a assinar uma declaração em como não possuem atuais condenações criminais e cumprirão os procedimentos de segurança do LSP/Requerente.	✔	✔	✔
7.7.3	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.	✔	✔	✔
7.7.4	Procedimento para lidar com a falsa declaração do trabalhador do LSP/ Requerente antes ou pós contratação.	✔	✔	✔
Rescisão ou Recontratação de Mão de obra *Nota: A rescisão contratual pode ser voluntária ou involuntárias — Colaboradores que foram demitidos e que se demitiram.*				
7.7.5	Recuperar os ativos físicos dos Colaboradores 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.	✔	✔	✔
7.7.6	Proteger os dados do Cliente: Desabilitar o acesso dos Colaboradores que terminam as suas funções na empresa a sistemas físicos ou eletrónicos, incluindo aqueles que contêm dados do Cliente (inventário ou cronogramas). Procedimento necessário.	✔	✔	✔
7.7.7	Lista de controlo da admissão e término de funções dos Colaboradores em vigor para verificação.	✔	✔	✔
7.7.8	Recontratação: Estão em vigor procedimentos para prevenir que o LSP/Requerente recontrate Colaboradores 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).*	✔	✔	✔

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

Secção	Função central	A	B	C
8.1	**Geral**			
8.1.1	Existe uma função central para gerir o sistema de gestão de segurança de todos as instalações tal como definido no âmbito da certificação Multi-instalação	✔	✔	✔
8.1.2	Todos as instalações devem ter uma relação jurídica ou contratual com a função central.	✔	✔	✔
8.1.3	Um único sistema de gestão de segurança é estabelecido para garantir que todos os suas instalações s inseridas no sistema estão conformes com os requisitos do Normativo de Segurança TAPA aplicável.	✔	✔	✔
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 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.	✔	✔	✔
8.1.6	A função central deve ter a autoridade e os direitos necessários para exigir que todas as instalações cumpram os normativos de segurança da TAPA e para aplicar medidas corretivas e preventivas, conforme se mostrar necessário. *Nota: Caso seja necessário, tal deve ser estabelecido no acordo formal entre a função central e as instalações.*	✔	✔	✔
8.2	**Políticas e Procedimentos**			
8.2.1	A função central deve manter políticas e procedimentos documentados para os seus sistemas de gestão de 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, implementados e aplicados em todas as instalações, conforme necessário.	✔	✔	✔
8.2.3	As políticas e os procedimentos devem ser mantidos e facilmente acessíveis por todas as instalações, conforme necessário.	✔	✔	✔
8.3	**Relatório de auditoria de autoavaliação realizado em todos os locais**			
8.3.1	A função central deve solicitar a todas as instalações que efetuem autoavaliações, e todos os relatórios de autoavaliação devem ser apresentados à função central para registo e análise. Os registos devem ser mantidos durante, pelo menos, dois (2) anos.	✔	✔	✔
8.3.2	A função central deve assegurar que todos os SCARs resultantes da autoavaliação e das auditorias sejam devidamente encerrados, a fim de melhorar os seus sistemas de gestão da segurança.	✔	✔	✔
8.3.3	Todos as instalações devem apresentar à função central atualizações dos progressos realizados e relatórios sobre todos os SCAR 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.	✔	✔	✔

Secção	Função central	A	B	C
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 todas as instalações mantêm registos das inspeções, dos registos de visitantes, dos registos dos condutores, das inspeções de 7 pontos, etc.	✔	✔	✔
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 as instalações e a manutenção dos seus registos durante, pelo menos, dois (2) anos.	✔	✔	✔
8.6	**CCTV e layout de alarme das instalações**			
8.6.1	A função central deve dispor de procedimentos que garantam que todas as instalações 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 ter procedimentos que garantam que todos os sistemas de alarme e de controlo de acesso são mantidos e testados para assegurar a sua eficácia operacional.	✔	✔	✔
8.7.2	A função central deve dispor de procedimentos que permitam que todas as instalações mantenham registos de todas as testagens 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 de segurança dos seus Colaboradores.	✔	✔	✔
8.8.2	A função central deve dispor de procedimentos que garantam que todas as instalações mantêm registos da formação em segurança de todo o seu pessoal. Os registos devem ser mantidos durante, pelo menos, dois (2) anos.	✔	✔	✔
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 em 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 para garantir a conservação dos registos das análises, incluindo as suas conclusões e as ações corretivas/preventivas 8.1.6. Os registos serão mantidos durante, pelo menos, dois (2) anos.	✔	✔	✔
8.10	**Revisão da gestão para avaliar as autoauditorias; SCARs identificados; quaisquer perdas, roubos; Avaliações de Risco.**			
8.10.1	A função central deve, no mínimo, efetuar uma análise regular da gestão para garantir a conformidade, a eficácia e a melhoria dos seus sistemas de gestão da segurança.	✔	✔	✔
8.10.2	As análises da direção devem abranger, entre outros aspetos, a eficácia das autoauditorias, o encerramento de SCARs, as avaliações de risco, os incidentes e as ações de melhoria.	✔	✔	✔

Secção	Função central	A	B	C
8.10.3	A função central deve manter registos de todas as análises de gestão durante, pelo menos, dois (2) anos.	✔	✔	✔

9.0 Ameaça à segurança informática e à cibersegurança – opção reforçada

O FSR inclui melhorias opcionais para ameaças de 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.

Secção	Ameaça à TI e à cibersegurança – Opção adicional
9.	**Requisitos obrigatórios**
9.1	O LSP/Requerente deve ter políticas de segurança para TI (Tecnologias de Informação) e ameaças de cibersegurança. As políticas podem ser separadas ou num 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. A forma como as políticas são revistas anualmente e atualizadas, se necessário.
9.2	O LSP/Requerente deve fornecer formação de sensibilização para a segurança da informação a todos os colaboradores. Esta formação deve: - 1. Abranger as funções e responsabilidades que os utilizadores de computadores 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/Requerente deve ter uma política escrita de forma a garantir que as medidas de cibersegurança estão em vigor com subcontratados e/ou fornecedores, que garantem que: 1. Os requisitos de cibersegurança do 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 cibersegurança do LSP/Requerente, são documentadas e implementadas medidas que mitigam os riscos para os requisitos de cibersegurança 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/Requerente devem ter instalado um software antivírus e *antimalware* licenciado. O software antivírus e o *antimalware* deve conter as atualizações mais recentes.
9.6	O LSP/Requerente deve ter um Plano de Recuperação de Desastres de TI (DRP) adequado à recuperação de ataques a sistemas comprometidos, incluindo, mas não se limitando a, todas as disposições necessárias de cópias de segurança e recuperação de dados e software.

Secção	Ameaça à TI e à cibersegurança – Opção adicional
9.7	Os sistemas de informação do LSP/Requerente devem ser objeto de cópias de segurança. Essas cópias de segurança devem ser testadas regularmente e os dados das cópias de segurança devem ser encriptados e transferidos para uma localização secundária, fora das instalações.
9.8	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.

Para sua informação: a tradução da norma para o idioma local fornecida a você visa melhorar a compreensão dos requisitos da TAPA 2023. A tradução da norma foi iniciada e validada com o melhor do nosso conhecimento e crença e com conhecimento dos fundamentos necessários. No entanto, a versão original em inglês da respetiva norma é e continua a ser decisiva para o exame.

Publicação e informações sobre direitos de autor

O aviso de direitos autorais da TAPA exibido neste documento indica quando o documento foi emitido pela última vez.

Histórico 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