FSR 2020

REQUISITOS DE SEGURANÇA DA INSTALAÇÃO

Transported Asset Protection Association

Requisitos de segurança da instalação FSR 2020

Padrões TAPA

TAPA Américas
5030 Champion Blvd,
G-11 #266 Boca Raton,
Flórida 33496
EUA
www.tapaonline.org
Tel. (561) 617-0096

TAPA Ásia Pacífico
1 Gateway Drive, Westgate
Tower #07-01,
Singapura 608531

www.tapa-apac.org
Tel. (65) 6514 9648

TAPA EMEA
Rhijngeesterstraatweg 40D
2341 BV Oegstgeest
Países Baixos

www.tapaemea.org
Tel. +44 1633 251325

Índice de FSR

Índice de FSR (continuação)

□□□

1. Introdução

1.1 Finalidade deste documento FSR

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

No desenvolvimento deste padrão, a TAPA reconhece as diferenças de como os serviços de armazenamento são prestados globalmente, regionalmente e até mesmo dentro das empresas, e que o TSR pode se aplicar a todos ou parte dos serviços prestados por um LSP/Candidato. Dependendo da complexidade e do tamanho da cadeia de suprimentos, a conformidade com os padrões TAPA pode ser obtida por meio de um único LSP/Candidato ou múltiplos LSPs/Candidatos e subcontratados qualificados.

Escopo

A TAPA desenvolveu três opções para suporte à certificação:

- Certificação de um único local por órgão de auditoria independente (IAB).
- Certificação de vários locais pelo IAB.
- Certificação de autoauditoria por auditores autorizados (AA) pelo LSP/Candidato ou IAB.

Público-alvo

Os usuários típicos dos padrões TAPA incluem:

- Compradores;
- LSPs/Candidatos;
- forças policiais ou outras organizações governamentais;
- organizações profissionais da cadeia de suprimentos; e
- seguradoras.

1. Introdução

1.2 Recursos para implementar o TAPA FSR

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

1.3 Proteção das políticas e procedimentos do LSP

Cópias das políticas de segurança e documentos de procedimentos serão enviados ao Comprador de acordo com os acordos de divulgação assinados entre o LSP/Candidato e Comprador e devem ser tratados como informações confidenciais.

2. Sobre a TAPA

2.1 Propósito da TAPA

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

A ameaça não é mais apenas de criminosos oportunistas. Hoje, os círculos do crime organizado operam globalmente e usam ataques cada vez mais sofisticados a veículos, instalações e pessoal para atingir seus objetivos.

TAPA é um fórum exclusivo que une fabricantes, fornecedores de logística, transportadoras de carga, agências de aplicação da lei e outras partes interessadas pelo mundo com o objetivo comum de reduzir perdas de cadeias de suprimentos internacionais. O foco principal da TAPA é a prevenção contra roubo através do uso de inteligência em tempo real e das 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, testes comparativos, colaboração regulatória e a identificação proativa de tendências de crimes e ameaças à segurança da cadeia de suprimentos.

3. Padrões TAPA

3.1 Segurança TAPA Padrões

Os seguintes padrões globais de segurança TAPA foram criados para garantir o transporte e armazenamento seguros de carga de alto valor com risco de roubo:

- Os Requisitos de Segurança da Instalação (FSR) representam padrões mínimos especificamente para *armazenamento seguro ou em trânsito,* dentro de uma cadeia de suprimentos.
- Os Requisitos de Segurança de Transporte (TSR) se concentram exclusivamente no transporte por caminhão e representam Padrões mínimos especificamente para *transpor produtos via estrada* dentro de uma cadeia de suprimentos.

Os padrões de segurança globais TAPA são revisados e alterados conforme necessário a cada três anos.

Este documento aborda apenas os requisitos FSR.

- O processo de certificação para TAPA FSR é documentado na estrutura de certificação de requisitos de segurança da instalação TAPA FSR.
- As versões atuais dos requisitos TAPA FSR e da estrutura de certificação TAPA FSR devem ser seguidas para conseguir o status de certificação TAPA FSR.

3.2 Implementação

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

4. Orientação jurídica

4.1 Escopo

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

4.2 Tradução

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

4.3 A marca "TAPA"

"TAPA" é uma marca registrada da Transported Asset Protection Association (Associação de Proteção de Ativos Transportados) e não pode ser usada sem a permissão expressa por escrito da TAPA através de suas regiões oficialmente reconhecidas. Os Padrões TAPA e material associado são publicados pela TAPA, e não podem ser revisados, editados ou alterados em qualquer parte sem a permissão expressa, por escrito, da TAPA. O uso indevido da marca TAPA pode resultar na remoção da certificação ou ação legal.

4.4 Limites de Responsabilidade

Pela publicação destes Padrões, a TAPA não garante nem afirma que todos os eventos de roubo de carga serão evitados se os Padrões estiverem ou não totalmente empregados e devidamente implementados. Qualquer responsabilidade que possa resultar de roubo de carga em armazenamento, ou qualquer outra perda de carga em armazenamento nos termos dos Padrões FSR será por conta do LSP/Candidato e/ou Comprador de acordo com os termos e condições em seu contrato entre as partes 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 e protegido dos ativos do Comprador é de responsabilidade do LSP/Candidato, seus agentes e subcontratados durante a coleta, trânsito, armazenamento e entrega, conforme especificado em uma liberação ou contrato.

Quando o FSR for referenciado ou incluído no contrato entre o LSP/Candidato e o Comprador, ele também deverá ser referenciado no programa de segurança do LSP/Candidato.

O LSP fornecerá ao Comprador evidências da Certificação FSR e, quando apropriado, evidência de que os requisitos do FSR foram atendidos. Além disso, qualquer suposta falha pelo LSP/Candidato de implementar os requisitos da FSR deverá ser resolvida de acordo com os termos do contrato negociado entre o Comprador e o LSP/Candidato.

5.2 Subcontratação

Os subcontratados de armazenamento incluem uma exigência contratual de que o subcontratante do LSP/Candidato atende a todos os Padrões FSR observados.

5.3 Investigação e solução de reclamações da TAPA

Se a TAPA receber uma reclamação formal referente ao desempenho de um LSP/Candidato certificado, a TAPA (sujeita à validação) pode exigir que o contrato LSP/Candidato passe por uma nova auditoria com despesas por conta do LSP/Candidato. Se o LSP/Candidato não cumprir a auditoria ou se recusar a cumprir este processo, seu certificado poderá ser revogado.

6. Isenções

6.1 Visão geral

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

Todos os pedidos de isenção para um requisito de segurança específico (em parte ou inteiro) devem ser enviados por meio de um formulário de Pedido de isenção da TAPA para o órgão de auditoria independente (IAB)/Auditor autorizado (AA) pelo LSP/Candidato (encontrado no site da TAPA). O LSP/Candidato solicitante assume total responsabilidade pela precisão das informações fornecidas no pedido de isenção.

Cada pedido de isenção deve ser enviado através do IAB/AA para o Comitê Regional de Isenção da TAPA para aprovação. É responsabilidade do IAB/AA decidir se o pedido está completo e justificar o processamento pela TAPA; isso inclui a verificação de fatores de mitigação e/ou controles de segurança alternativos.

Caso os funcionários da TAPA e/ou Compradores suspeitem que as condições de isenção mudaram, a TAPA executará uma investigação formal e o LSP/Candidato entende que a isenção pode ser revogada pela TAPA.

6.2 Processo de isenção de negócios

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

Tabela 1: Responsabilidades: Pedido de isenção / avaliação

Etapa	Responsabilidade	Ação
1.	LSP/Candidato	Estabelece e verifica medidas de mitigação.
2.	LSP/Candidato	Preenche o formulário de pedido de isenção da TAPA e o envia para o IAB/AA.
3.	IAB AA	Analisa e verifica a integridade das informações contidas no formulário de pedido de isenção da TAPA.
4.	IAB AA	Envia o formulário de pedido de isenção da TAPA ao Comitê Regional de Isenção da TAPA.
5.	Comitê Regional de Isenção da TAPA	Analisa o pedido e concede ou recusa a isenção.

6. Isenções

Se a isenção for negada

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

Se a isenção for concedida

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

Tabela 2: Aprovação de isenção

Etapa	Responsabilidade	Ação
1.	Comitê Regional de Isenção da TAPA	Documenta e assina as especificidades de isenção.
2.	Comitê Regional de Isenção da TAPA	Especifica a duração da isenção (até no máximo três anos) e envia uma cópia para o AA.
3.	AA	Notifica o LSP/Candidato sobre o resultado do Pedido de isenção.
4.	LSP/Candidato	Cumpre os requisitos de isenção. O não cumprimento do contrato anulará a aprovação da isenção.

6.3 Isenções para barreiras físicas (na seção 1) e para gaiola de proteção para valores altos (HVC) (HVC, na seção 4.5)

A TAPA considerará uma isenção a todo ou parte dos requisitos da barreira perimetral e/ou ao HVC se todas as seguintes pré-condições forem atendidas:

Geral:

- O pedido de isenção é enviado através do formulário oficial de pedido de isenção da TAPA e endossado pelo IAB/AA.
- O pedido de isenção inclui informações de quaisquer medidas de mitigação para garantir que as mercadorias vulneráveis não estejam em risco desnecessário de roubo ou perda.
- Uma avaliação de risco deve ser feita e enviada com o pedido de isenção. Quaisquer vulnerabilidades significativas identificadas na avaliação de risco devem ser listadas separadamente na isenção e devem ser tomadas ações para reduzir o risco em um nível aceitável.

6. Isenções

Medidas de mitigação que devem estar em vigor e documentadas no envio do pedido de isenção:

- **Barreiras de perímetro:**
  - Equipamentos, recursos e procedimentos adicionais introduzidos para auxiliar na detecção em tempo hábil de pessoas ou veículos não autorizados que podem incluir, entre outros, iluminação adicional, cobertura de CFTV, melhores procedimentos de aplicação de identificação de pessoas e de veículos, áreas de restrição que apenas exijam ou colete ou uniforme do LSP.
  - Sinais de perímetro visíveis devem ser instalados no idioma local indicando “Proibido o acesso não autorizado”, “Proibido estacionar sem autorização”.
  - Placas visíveis em portas ou paredes externas das docas devem ser instaladas instruindo condutores, visitantes etc. para prosseguir para a entrada apropriada, controle de segurança.
  - Confirmação de que procedimentos em vigor garantem que as áreas de manuseio, transporte e recebimento de carga sejam inspecionadas e estejam em conformidade com as condições de isenção pelo menos semanalmente.

- **HVC (Gaiolas de proteção para altos valores):**
  - Para isenções de HVC, deve-se considerar e documentar ações de mitigação adequadas para minimizar o risco (onde uma HVC não estiver disponível) na avaliação de risco anual.
  - O pedido de isenção inclui uma declaração anexada assinada pelo LSP/Candidato estipulando que nenhum Comprador exige uma HVC.

7. Requisitos de segurança da instalação

Seção	Requisitos gerais:	A	B	C
7.0				
7.0.1	Todos os procedimentos ou políticas exigidos por este Padrão devem ser documentados.	✔	✔	✔
7.0.2	Um procedimento, registro e/ou plano-chave é necessário para bloqueios físicos, cartões de acesso e/ou chaves que gerenciam e controlam as chaves físicas e eletrônicas.	✔	✔	✔

Seção	Perímetro	A	B	C
7.1				
Pátio de manuseio, transporte e recebimento (geral) para carga fora do depósito				
7.1.1	CFTV capaz de visualizar todo o tráfego em um pátio externo de manuseio, transporte e recebimento de carga (incluindo pontos de entrada e saída), garantindo que todos os veículos e indivíduos sejam reconhecíveis em todos os momentos, a menos que ocorra obstrução temporária devido às necessidades operacionais (ou seja, carga e descarga de caminhões em tempo real).	✔	✔	
7.1.2	Iluminação adequada nas áreas de carga e descarga. *Observação: A iluminação pode ser constante, ativada por alarme, movimento, detecção de som, etc., com iluminação imediata.*	✔	✔	✔
7.1.3	Procedimento descrevendo como veículos e pessoas não autorizadas devem ser gerenciados dentro do pátio externo de manuseio, transporte e recebimento de cargas. Instruções sobre o procedimento devem ser entregue aos respectivos funcionários, incluindo guardas.	✔	✔	✔
7.1.4	O pátio de manuseio, transporte e recebimento deve ser adequadamente controlado para evitar acesso não autorizado.		✔	✔
7.1.5	Para janelas acessíveis pelo nível térreo ou portas das docas, a Avaliação de risco anual deve avaliar a necessidade de barreiras contra invasão de veículos. (Consulte Avaliação de risco, Seção 7.6.5.).	✔		
Barreiras físicas				
7.1.6	A barreira física protege o pátio de manuseio, transporte e recebimento de cargas.	✔		
7.1.7	A barreira física ao redor do pátio de manuseio, transporte e recebimento de carga tem uma altura mínima de 6 pés/1,8 metro. *Observação: A barreira física, projetada para impedir o acesso não autorizado, deve ser uma altura de 6 pés/1,8 metro ao longo de todo o seu comprimento, incluindo áreas onde há mudanças no nível do solo para menos.*	✔		
7.1.8	Barreira física ao redor do pátio de manuseio, transporte e recebimento de cargas mantida em boas condições.	✔		

Seção	Perímetro	A	B	C
7.1.9	Portões dentro do pátio de manuseio, transporte e recebimento de cargas controláveis ou controlados eletronicamente.	✔		
7.1.10	Barreira física ao redor do pátio de manuseio, transporte e recepção de cargas inspecionadas quanto à integridade e danos pelo menos semanalmente.	✔		
Áreas de docas externas				
7.1.11	Áreas de docas externas cobertas por câmeras externas coloridas ou "dia/noite".	✔	✔	✔
7.1.12	Câmeras montadas para poder visualizar todas as operações e movimentos em torno da área externa de doca em todos os momentos, a menos que ocorra obstrução temporária devido às necessidades operacionais (como, carga e descarga de caminhões em tempo real).	✔	✔	✔
7.1.13	Todos os veículos e pessoas em torno das áreas externas de doca claramente reconhecíveis.	✔		
7.1.14	Veículos e pessoas em torno de áreas externas de doca visíveis na maioria dos casos.		✔	✔
7.1.15	Todas as áreas externas ao redor das portas da doca totalmente iluminadas.	✔	✔	✔
Acesso a veículos pessoais				
7.1.16	Veículos pessoais só são permitidos em áreas de manuseio, transporte e recebimento de carga, se pré-aprovadas e restritas a áreas de estacionamento atribuídas/designadas. Não há estacionamento pessoal a uma distância de 25 m a pé das áreas de docas externas. Processos para aprovação prévia e restrições em vigor.	✔	✔	✔

Seção	Paredes externas, telhado e portas	A	B	C
7.2				
Lados externos da instalação: CFTV				
7.2.1	Sistema de câmera externa colorido ou “dia/noite” que cubra todos os lados externos da instalação.	✔		
7.2.2	Sistema de câmera externa colorido ou “dia/noite” que cubra os lados externos da instalação com portas, janelas ou outras aberturas.		✔	
7.2.3	Todas as visualizações do sistema de câmera externa limpas o tempo todo, a menos que ocorra obstrução temporária devido às necessidades operacionais (como carga e descarga de caminhões em tempo real).	✔		
7.2.4	Todos os veículos e indivíduos reconhecíveis claramente pelo sistema de câmera externa.	✔		
7.2.5	Veículos e pessoas visíveis na maioria dos casos pelo sistema de câmera externa.		✔	
Paredes externas e telhado				
7.2.6	Paredes externas e telhado projetados e mantidos para resistir à penetração (Exemplo: tijolos, bloco, parede inclinada de concreto, paredes sanduíche).	✔	✔	✔

Seção	Paredes externas, telhado e portas	A	B	C
7.2.7	Qualquer janela, ventilação ou outra abertura nas paredes externas da instalação, ou qualquer janela vedada instalada a menos de 3 metros do piso de trabalho nas paredes externas da instalação, deve ter uma barreira física **ou** alarme e deve ser ligada ao sistema de alarme principal.	✔	✔	
7.2.8	Qualquer janela, claraboia, ventilação, escotilha ou outra abertura no telhado da instalação, deve ter uma barreira física **ou** alarme e deve ser ligada ao sistema de alarme principal.	✔		
7.2.9	O acesso externo ao telhado (escada ou escadas) deve ser: Fisicamente trancado e coberto por CFTV (câmeras coloridas ou “dia/noite”). ou Fisicamente trancado e com alarme.	✔		
7.2.10	Acesso externo ao telhado (escada ou escadas) fisicamente trancado.		✔	✔
7.2.11	Todas as portas de depósito da instalação e portas de escritório com alarme para detectar abertura não autorizada, ligado ao sistema de alarme principal. *Observação: As portas da doca não são cobertas por este requisito, consulte a seção 7.2.17 para requisitos de alarme de porta de doca.*	✔	✔	✔
7.2.12	Cada porta externa do depósito da instalação, porta de escritório ou outra abertura deve ser identificada de forma exclusiva, por porta ou por zona, dentro do sistema de alarme principal.	✔		
7.2.13	Todas as portas externas do depósito sempre fechadas e protegidas quando não estiverem em uso ativo. Chaves/códigos controlados.	✔	✔	
7.2.14	As portas e portais de pedestres do depósito não podem ser facilmente penetrados. Se as dobradiças estiverem do lado de fora, devem ser rebitadas ou soldadas. Portas de vidro são inaceitáveis, a menos que sejam equipadas com detectores de quebra de vidro ou outro dispositivo de detecção local forneça cobertura (por exemplo, PIR [sensor infravermelho passivo] e haja um alarme diretamente ligado ao centro de monitoramento, ou o vidro seja protegido por barras/telas.	✔	✔	✔
7.2.15	Saídas de emergência usadas apenas para fins de emergência (ex.: saídas de incêndio), com alarmes em todos os momentos com um som sonoro individual ou por zona.	✔	✔	
7.2.16	Todas as portas da doca com resistência suficiente para impedir e/ou retardar a entrada forçada pelo uso de pequenas ferramentas portáteis.	✔	✔	✔

Seção	Paredes externas, telhado e portas	A	B	C
7.2.17	**Portas da doca** **Horas não operacionais:** Portas da doca fechadas, protegidas (ou seja, eletronicamente desativadas ou fisicamente travadas). Portas de doca com alarme de intrusão não autorizada ligado ao sistema de alarme principal. **Horas operacionais:** As portas da doca devem ser fechadas quando não estiverem em uso ativo. Os portões tipo tesoura (scissor gates), se usados, devem ser fixados por corrediça/trava mecânica e devem ter no mínimo 8 pés/2,4 metros de altura.	✔	✔	✔

Seção	Pontos de entrada e saída de escritório e depósito	A	B	C
7.3				
Pontos de entrada de visitantes à área de escritório				
7.3.1	Acesso aos pontos de entrada de visitante na área do escritório controlados por um funcionário/guarda/recepcionista treinado na emissão de crachás, controles, registro, visitantes, requisito de escolta etc. (processo em vigor para visitas fora do horário operacional).	✔	✔	✔
7.3.2	Pontos de entrada de visitante na área do escritório cobertos por CFTV; (câmeras coloridas ou “dia/noite”) com reconhecimento claro de indivíduos o tempo todo.	✔	✔	
7.3.3	Alarme de coação presente nos pontos de entrada de visitante na área de escritório, testado semanalmente.	✔	✔	
7.3.4	Todos os visitantes na área de escritório identificados com identidade com foto emitida pelo governo (por exemplo, carteira de motorista, passaporte ou carteira de identidade nacional, etc.).	✔	✔	✔
7.3.5	Registro de todos os visitantes na a área do escritório e registro mantido por no mínimo 30 dias.	✔	✔	✔
7.3.6	Todos os crachás de visitantes devem ser recolhidos quando o visitante deixa as instalações e o registro completo verificado diariamente.	✔	✔	
7.3.7	Todos os visitantes devem exibir visivelmente crachás ou passes e ser acompanhados pelo pessoal da empresa.	✔	✔	
Pontos de entrada de funcionários				
7.3.8	Acessos de pontos de entrada de funcionários controlados 24 horas por dia, 7 dias por semana.		✔	✔
7.3.9	Pontos de entrada de funcionários controlados através do dispositivo eletrônico de controle de acesso 24 horas por dia, 7 dias por semana. Acesso registrado.	✔		
7.3.10	Pontos de entrada de funcionários cobertos por CFTV. (Câmeras coloridas ou “dia/noite”).	✔	✔	
7.3.11	Após a verificação, todos os funcionários devem receber crachás de identificação da empresa com foto.	✔	✔	
7.3.12	Todos os outros funcionários devem receber um crachá de identificação da empresa para reconhecimento dentro da instalação.	✔	✔	
7.3.13	Todos os crachás dos funcionários claramente visíveis.	✔	✔	
7.3.14	Os crachás de funcionários não devem ser compartilhados em nenhuma circunstância e deve haver uma política de emissão de crachás em vigor.	✔	✔	
Identificação de motorista e veículo				
7.3.15	Todos os motoristas identificados através de identidade com foto emitida pelo governo (por exemplo, carteira de motorista, passaporte ou carteira de identidade nacional, etc.) e um registro de motorista em vigor.	✔	✔	✔

Seção	Pontos de entrada e saída de escritório e depósito	A	B	C
7.3.16	Verificação de que a carteira de motorista é válida, e que a identificação de motorista com foto não esteja vencida.	✔	✔	✔
7.3.17	Os identificadores de veículo são registrados manualmente (por exemplo, por escrito) ou com câmeras. Incluir, pelo menos, o número da placa e tipo do veículo.	✔		

Seção	Dentro do depósito e escritório	A	B	C
7.4				
Área do depósito: Paredes divisórias				
7.4.1	Paredes divisórias do chão ao teto e telhado projetados/construídos e mantidos para resistir à penetração (Exemplo: tijolos, bloco, parede inclinada de concreto, paredes tipo sanduíche).	✔	✔	✔
7.4.2	Se paredes divisórias internas do chão ao teto forem construídas de telas com malha com grau de segurança ou outra barreira segura reconhecida pelo setor, então também deve- haver um alarme para detectar a intrusão. *Observação: Cerca de tela de baixa qualidade ou tela/grade não segura não são aceitáveis.*	✔	✔	✔
Áreas internas do depósito				
7.4.3	É necessária a detecção de intrusão (por exemplo, detecção de infravermelho, movimento, som ou vibração) para monitorar áreas internas do depósito. Os alarmes devem ser ativados e vinculados ao sistema de alarme principal durante horas não operacionais (ou seja, quando o depósito estiver fechado). *Observação: Se o depósito operar efetivamente 24 horas por dia, 7 dias por semana, 365 dias por ano, este requisito pode ser N/A se os riscos e mitigações forem documentados na Avaliação de risco local.* *Independente das horas operacionais, a detecção de intrusão de perímetro ou barreiras físicas sempre é necessária em portas externas e janelas de andares térreos em escritórios e depósitos. (Consulte a seção 7.2.11).*	✔		
Portas e áreas de docas internas				
7.4.4	Todas as portas e áreas internas de docas cobertas por CFTV. (Câmeras coloridas ou “dia/noite”).	✔	✔	✔
7.4.5	Visualizações claras o tempo todo do frete que é carregado/descarregado, em todas as portas e áreas de doca internas, a menos que ocorra obstrução temporária devido às necessidades operacionais (ou seja, carga e descarga de caminhões em tempo real).	✔	✔	✔
7.4.6	Ativos do comprador sob vigilância de CFTV todo o tempo em áreas de movimentação de carga ou de preparação (ou seja, áreas de desmontagem/montagem de palete, rotas de e para os racks de armazenamento, docas, corredores de trânsito).	✔	✔	
Controle de acesso entre escritório e doca/depósito				
7.4.7	Controle de acesso entre escritório e doca/depósito.	✔	✔	
7.4.8	Alarmes para portas com cartões de acesso ou interfone para portas entre escritório e doca/depósito, localmente audíveis **e** que geram um alarme de resposta quando mantidas abertas por mais de 60 segundos, ou imediatamente, se forem forçadas.	✔		

Seção	Dentro do depósito e escritório	A	B	C
7.4.9	Alarmes para as portas entre escritório e doca/depósito localmente audíveis **ou** que enviam um alarme de resposta quando mantidas abertas por mais de 60 segundos, ou imediatamente, se forem forçadas.		✔	
7.4.10	Os funcionários autorizados do LSP/Candidato e os visitantes acompanhados devem ter permissão de acesso às áreas de docas/armazéns com base necessidades comerciais e restritas.	✔	✔	✔
7.4.11	Lista de acesso para áreas de doca/depósito revisada pelo menos trimestralmente para limitar/verificar se a permissão de acesso é concedida apenas ao pessoal designado/autorizado.	✔	✔	
Gaiola de proteção (HVC)/área para valores altos				
7.4.12	O tamanho e o uso da HVC podem ser ditados pelo contrato do Comprador/LSP/Candidato. Se um acordo não estiver em vigor, a HVC deve ser capaz de armazenar no mínimo 6 metros cúbicos de produtos.	✔	✔	
7.4.13	O perímetro da HVC/área é coberto ou murado em todos os lados, incluindo o topo/telhado.	✔	✔	
7.4.14	Dispositivo de bloqueio da HVC/área na porta/portão.	✔	✔	
7.4.15	Cobertura completa de CFTV (câmeras coloridas ou “dia/noite”) na entrada e dentro da HVC. *Observação: Se a HVC for muito pequena para suportar uma câmera interna, a cobertura da câmera da entrada é suficiente.*	✔		
7.4.16	Cobertura de CFTV (câmeras coloridas ou “dia/noite”) na entrada da HVC .		✔	
7.4.17	Se o acesso à HVC for necessário a mais de 10 pessoas, este deverá ser controlado eletronicamente por cartão/token. Se o acesso for necessário a 10 ou menos pessoas, sistema de trava ou cadeado para serviço pesado com sistema de emissão controlado por chaves. As chaves podem ser designadas a indivíduos para cobrir um turno, mas não devem ser transferidas sem aprovação e devem ser registradas no registro de chaves. Todas as chaves devem ser devolvidas e contabilizadas quando não estiverem em uso.	✔		
7.4.18	Portas/portas de HVC devem possuir alarmes para detectar entrada forçada. Os alarmes podem ser gerados por contatos da porta e/ou uso de detecção de movimento do CFTV para detectar acesso não autorizado.	✔		
7.4.19	Perímetro da HVC mantido em boas condições e inspecionado mensalmente quanto à integridade e danos.	✔		
7.4.20	LSP/Candidato deve garantir que o acesso à HVC só é concedido ao pessoal designado/autorizado. Lista de acesso aprovada para a HVC revisada mensalmente e atualizada em tempo real quando o funcionário deixar o emprego ou não necessitar mais de acesso. Procedimento para acesso da HVC em vigor.	✔	✔	

Seção	Dentro do depósito e escritório	A	B	C
Inspeção de lixo do depósito				
7.4.21	As lixeiras principais e/ou internas do depósito de coleta de lixo/áreas de compactação devem ser monitoradas pelo CFTV.	✔		
7.4.22	Quando utilizados, sacos de lixo usados dentro do depósito devem ser transparentes.		✔	✔

Pré-carregamento e preparação				
7.4.23	Não é autorizado o pré-carregamento ou estacionamento de caminhões de FTL/Comprador dedicado na parte externa do depósito durante horas não operacionais, a menos que mutuamente acordado entre o Comprador e o LSP/Candidato. Medidas de segurança alternativas devem ser implementadas (por exemplo, dispositivos de segurança adicionais no contêiner). *Observação: "Parte externa do depósito" são aquelas áreas separadas ou afastadas da instalação, mas ainda dentro da cerca/perímetro do pátio do LSP/Candidato.*	✔	✔	✔
Recipientes pessoais e buscas na saída				
7.4.24	Procedimentos de segurança escritos definem como "recipientes pessoais" são controlados dentro do depósito. Os recipientes pessoais incluem lancheiras, mochilas, coolers, bolsas, etc.	✔	✔	
7.4.25	Se permitido pela lei local, o LSP/Candidato deve desenvolver e manter um procedimento documentado para as buscas de saída. A ativação do procedimento fica a critério do LSP/Candidato e/ou de acordo com o contrato do Comprador/LSP/Candidato. No mínimo, o procedimento deve abordar o direito do LSP/Candidato sobre os critérios de busca, caso surja uma necessidade de apresentar buscas quando normalmente não forem necessárias (por exemplo, quando houver suspeita de roubo por funcionário).	✔		
Controle de equipamentos de manuseio de carga				
7.4.26	Procedimento que exige que todas as empilhadeiras e outros equipamentos motorizados de manuseio de carga sejam desativados durante horas não operacionais. *Observação: Isso não inclui macacos manuais/macacos para palete.*	✔	✔	
Integridade do contêiner ou carroceria; inspeção de 7 pontos				
7.4.27	Inspeção física de 7 pontos realizada na saída em todos os contêineres ou carrocerias exclusivos do Comprador: Parede frontal, lado esquerdo, lado direito, piso, teto/cobertura, portas internas/externas e mecanismo de travamento, exterior/inferior. *Observação: Isso se aplica a todos os tipos de carrocerias e contêineres travados e/ou lacrados (ou seja, não limitado a contêineres de frete marítimo).*	✔	✔	✔
Processo de entrega de frete; lacres de segurança				
7.4.28	A menos que especificamente isentado pelo Comprador, os lacres de segurança invioláveis são usados em todos os transportes diretos e ininterruptos. Os lacres devem ser certificados com ISO 17712 (classificação I, S ou H). *Observação: Não são necessárias lacres em transporte de múltiplas paradas devido à complexidade e risco associados com condutores que transportam vários lacres.*	✔	✔	✔

7.4.29	O LSP/Candidato deve ter procedimentos documentados em vigor para a gestão e controle de lacres de segurança, travas de porta de carroceria (contêiner), travas de pino e outros equipamentos de segurança.	✔	✔	✔
7.4.30	Os lacres de segurança são afixados ou removidos por pessoal autorizado, ou seja, a equipe do depósito, instruídos a reconhecer e relatar lacres comprometidos. Os lacres nunca devem ser afixados ou removidos pelo motorista, a menos que isentado pelo Comprador.	✔	✔	✔
7.4.31	Procedimentos em vigor para reconhecer e relatar lacres de segurança comprometidos.	✔	✔	✔
Integridade da carga, processo de validação de carga/descarga				
7.4.32	Procedimentos robustos em vigor, assegurando que todos os ativos transportados e recebidos do comprador sejam validados no ponto de entrega através da realização de uma contagem manual e/ou eletrônica. O processo deve garantir que as anormalidades sejam consistentemente reconhecidas, documentadas e relatadas ao LSP/Candidato e/ou Comprador. Registros manuais e/ou eletrônicos devem ter qualidade comprovada. Se os motoristas não estiverem presentes para testemunhar esta atividade, o comprador/LSP/Candidato deve garantir uma verificação de contagem alternativa, como varreduras e/ou imagens de CFTV, coletadas e retidas especificamente para esta finalidade. *Observação: Além de peças faltantes, as anormalidades podem incluir danos, tiras ou fitas ausentes, cortes ou outras aberturas óbvias, indicando um possível furto ou roubo.*	✔	✔	✔
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 são validados antes do carregamento. O procedimento deve estar em vigor.	✔	✔	✔

Seção	**Sistemas de segurança, projeto, monitoramento e respostas.**	**A**	**B**	**C**
7.5				
Posto de monitoramento				

Seção	Sistemas de segurança, projeto, monitoramento e respostas.	A	B	C
7.5.1	Monitoramento dos eventos de alarme 24 horas por dia, 7 dias por semana e 365 dias por ano por meio de posto de monitoramento interno ou externo terceirizado, protegido contra acesso não autorizado. *Observação: Os postos de monitoramento podem estar localizados dentro ou fora do local e podem ser de 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), travas ou leitores biométricos.*	✔	✔	✔
7.5.2	O posto de monitoramento deve responder a todos os alarmes do sistema de segurança em tempo real, 24 horas por dia, 7 dias por semana, 365 dias por ano.	✔	✔	✔
7.5.3	O posto de monitoramento reconhece a ativação do alarme e é expandido em menos de 3 minutos.	✔	✔	✔
7.5.4	Relatórios de monitoramento de alarme disponíveis.	✔	✔	✔
7.5.5	Procedimentos de resposta do posto de monitoramento em vigor.	✔	✔	✔
Sistema de detecção de intrusão (IDS)				
7.5.6	Todos os IDS ativados durante horas não operacionais e ligados ao sistema de alarme principal.	✔	✔	✔
7.5.7	Registros de alarme IDS mantidos por 60 dias.	✔	✔	
7.5.8	Registros de alarme IDS armazenados com segurança e backup.	✔		
7.5.9	Registros de alarme IDS armazenados com segurança.		✔	
7.5.10	Procedimento para garantir que o acesso ao IDS seja restrito a pessoas autorizadas ou administradores de sistema. Isso inclui servidores, consoles, controladores, painéis, redes e dados. Os privilégios de acesso devem ser atualizados imediatamente quando indivíduos se desligam da empresa ou mudam de função, não mais necessitando o acesso.	✔	✔	✔
7.5.11	Alarme transmitido em caso de falha/perda de energia do IDS. *Observação: Para sistemas com fonte de alimentação ininterrupta (UPS), o alarme é transmitido quando a bateria UPS falhar.*	✔	✔	✔
7.5.12	Verificação do conjunto de alarme IDS no lugar. *Observação: Procedimentos que validam que os alarmes ficam armados durante horas não operacionais.*	✔	✔	✔
7.5.13	Alarme IDS transmitido via linha fixa em caso de falha do dispositivo e/ou linha.	✔	✔	
7.5.14	Sistema de comunicação de backup instalado em caso de falha do dispositivo IDS e/ou linha.	✔	✔	
Sistema de controle de acesso automático (AACS)				

Seção	Sistemas de segurança, projeto, monitoramento e respostas.	A	B	C
7.5.15	Disponibilização de registros de transações do AACS por 90 dias. Registros armazenados com segurança e com backup.	✔	✔	
7.5.16	Procedimento para garantir que o acesso ao AACS seja restrito a pessoas autorizadas ou administradores do sistema. Os privilégios de acesso devem ser atualizados imediatamente quando indivíduos se desligam da empresa ou mudam de função, não mais necessitando o acesso.	✔	✔	
7.5.17	Acessar relatórios do sistema revisados pelo menos trimestralmente para identificar irregularidades ou mau uso (ou seja, múltiplas tentativas malsucedidas, leituras falsas - ou seja, cartão desativado, evidência de compartilhamento de cartão para permitir acesso não autorizado, etc). Processo em vigor.	✔	✔	
CFTV				
7.5.18	Gravação digital do CFTV funcionando.	✔	✔	✔
7.5.19	A velocidade de gravação do CFTV é definida como um mínimo de 8 quadros por segundo (fps) por câmera. *Observação: A TAPA permitirá que detentores de certificação sem capacidade de atualização para 8 fpds continuem com sua capacidade atual de 3fps até a revisão de 2023. Novos detentores de certificados devem atender ao novo requisito.*	✔	✔	✔
7.5.20	Funcionalidade da gravação digital verificada diariamente nos dias operacionais por procedimento. Registros disponíveis.	✔	✔	✔
7.5.21	Registros do CFTV armazenados por no mínimo 30 dias, quando permitido pela lei local. O LSP/Candidato deve fornecer evidência de qualquer lei local que proíba o uso de CFTV e/ou limite o armazenamento de dados de vídeo por menos de 30 dias.	✔	✔	✔
7.5.22	Acesso firmemente controlado ao sistema de CFTV, incluindo hardware, software e armazenamento de dados/vídeo.	✔	✔	✔
7.5.23	Imagens de CFTV, para fins de segurança, visualizadas apenas por pessoal autorizado.	✔	✔	✔
7.5.24	Procedimentos em vigor detalhando a política de proteção de dados do CFTV sobre o uso de imagens em tempo real e de arquivamento de acordo com a lei local.	✔	✔	
Iluminação exterior e interior				
7.5.25	Níveis de iluminação externa e interna suficientes para favorecer as imagens do CFTV que permitam a investigação, com gravação de imagens de qualidade.	✔	✔	
7.5.26	Níveis de iluminação externa e interna suficientes para reconhecer claramente todos os veículos e indivíduos.	✔		

Seção	Treinamento e procedimentos	A	B	C
7.6				
Procedimentos de escalonamento				
7.6.1	Procedimentos locais em vigor para lidar com os ativos do comprador, incluindo o processo de relato oportuno de perda, falta ou roubo de ativos do comprador. Incidentes devem ser relatados pelo LSP/Candidato ao Comprador dentro de 24 horas. Roubos óbvios, relatados imediatamente. Processo seguido de forma consistente.	✔	✔	✔
7.6.2	Contatos da administração de emergência do Comprador e LSP/Candidato para incidentes de segurança listados e disponíveis. Listagem atualizada a cada 6 meses que inclui contatos de emergência da polícia	✔	✔	✔
Compromisso da administração				
7.6.3	A administração do fornecedor deve ter nomeado formalmente uma pessoa para segurança no local que seja responsável por manter os requisitos de segurança da cadeia de suprimentos da TAPA FSR e da empresa. O fornecedor também deve ter uma pessoa (pode ser a mesma) responsável por monitorar o programa FSR. Isso inclui programar verificações de conformidade, comunicações com AAs, recertificação, alterações no padrão FSR, etc. *Observação: Essas pessoas podem ser um funcionário ou uma pessoa terceirizada sob contrato para desempenhar esta função.*	✔	✔	✔
7.6.4	A administração deve desenvolver, comunicar e manter uma política de segurança para garantir que todas as pessoas relevantes (ou seja, funcionários e contratados) estejam claramente cientes das expectativas de segurança do fornecedor.	✔	✔	✔
7.6.5	Uma avaliação de risco da instalação que reconhece a probabilidade e o impacto de eventos relacionados à segurança deve ser conduzida/atualizada pelo menos anualmente. O processo de Avaliação de risco deve exigir que a administração tome decisões informadas sobre vulnerabilidades e se a mitigação é suficiente. No mínimo, os seguintes eventos internos/externos comuns devem ser avaliados: roubo de carga ou informações, acesso não autorizado a instalações ou carga, adulteração/destruição de sistemas de segurança, coletas fictícias de carga, continuidade de segurança durante escassez de mão de obra, desastres naturais, etc. Eventos adicionais podem ser considerados com base nos riscos locais/do país.	✔	✔	✔
Treinamento				
7.6.6	Treinamento de conscientização sobre segurança/ameaças deve ser fornecido a todos os funcionários nos primeiros 60 dias de emprego e depois a cada 2 anos.	✔	✔	✔
7.6.7	Treinamento de conscientização sobre segurança da informação focado na proteção dos dados de transporte eletrônicos e físicos do comprador fornecidos aos funcionários que tenham acesso às informações do comprador.	✔	✔	
Acesso aos ativos do comprador				
7.6.8	Procedimentos em vigor para proteger os ativos do comprador (ou seja, a carga) de acesso não autorizado pelos funcionários, visitantes, etc.	✔	✔	

Seção	Treinamento e procedimentos	A	B	C
Controle de informações				
7.6.9	Acesso aos documentos de transporte e informações sobre os ativos do Comprador controlados com base na “necessidade de saber”.	✔	✔	✔
7.6.10	Acesso aos documentos de transporte e informações sobre os ativos monitorados e registrados do Comprador, com base na “necessidade de saber”.	✔	✔	✔
7.6.11	Documentos de transporte e informações sobre os ativos do Comprador protegidos até a destruição.	✔	✔	✔
Relatório de incidentes de segurança				
7.6.12	Sistema de rastreamento e relatório de incidentes de segurança em vigor para implementar medidas proativas.	✔	✔	
Programas de manutenção				
7.6.13	Programas de manutenção em vigor para todas as instalações/sistemas de segurança técnica (física) para garantir a funcionalidade em todos os momentos (por exemplo, CFTV, controles de acesso, detecção de intrusos e iluminação).	✔	✔	✔
7.6.14	Manutenção preventiva realizada uma vez por ano ou de acordo com as especificações do fabricante.	✔	✔	✔
7.6.15	Verificações documentadas de funcionalidade de todos os sistemas uma vez por semana, a menos que falhas do sistema sejam imediata/automaticamente relatadas ou alarmadas.	✔	✔	
7.6.16	Um pedido de reparo deve ser iniciado dentro de 48 horas após a falha ser descoberta. Deve-se implementar mitigações alternativas para qualquer reparo que tenha previsão de exceder 24 horas.	✔	✔	
Orientação do contratado				
7.6.17	O LSP/Candidato deve garantir que todos os subcontratados/fornecedores estejam cientes e cumpram os programas de segurança relevantes do LSP/Candidato.	✔	✔	✔
Registros de transporte e recebimento				
7.6.18	Documentos legíveis, completos e precisos de transporte e recebimento (ou seja, hora, data, assinaturas, motorista, equipe de transporte e recebimento, detalhes e quantidades da remessa, etc.).	✔	✔	✔
7.6.19	O LSP/Candidato deve manter registros de todas as cobranças e comprovantes de entregas por um período não inferior a dois anos e mantê-los disponíveis para investigações de perda, se necessário.	✔	✔	✔
7.6.20	O comprovante de entrega deve ser fornecido de acordo com o contrato por escrito entre o comprador e o LSP/Candidato, quando o comprador exigir, o destino deve notificar a origem dentro do prazo acordado do recebimento da remessa, conferindo os detalhes de pré-alerta da remessa.	✔	✔	✔
Processo de pré-alerta em vigor				

Seção	Treinamento e procedimentos	A	B	C
7.6.21	Quando o Comprador exigir, deve haver processo de pré-alerta aplicado às remessas de entrada e/ou saída em vigor. .As informações de pré-alerta devem ser acordadas pelo Comprador e pelo LSP/Candidato. Os detalhes sugeridos incluem: horário de partida, horário de chegada estimado, empresa de transporte, nome do motorista, detalhes da placa do veículo, informações da remessa (contagem de peças, peso, número do conhecimento de embarque, etc.) e números dos lacres da carroceria.	✔	✔	✔

Seção	Integridade dos funcionários	A	B	C
7.7				
7.1	Verificações de triagem/verificação/antecedentes (conforme permitido pela lei local)			
7.7.1	O LSP/Candidato deve ter um processo de triagem/verificação/ histórico que inclua, no mínimo, verificações de histórico criminal e emprego anterior. A triagem/verificação se aplica a todos os candidatos, incluindo funcionários e contratados. O LSP/Candidato também exigirá um processo equivalente, sendo aplicado em empresas contratadas que forneçam trabalhadores TAS (Lei de compensação e reabilitação de trabalhadores 1988).	✔	✔	✔
7.7.2	O funcionário da TAS deve assinar a declaração de que não tem condenações criminais atuais e cumprirá os procedimentos de segurança do LSP/Candidato.	✔	✔	✔
7.7.3	O LSP/Candidato terá contratos em vigor para ter as informações necessárias de triagem/verificação/antecedentes fornecidas pela agência e/ou subcontratado que tenha trabalhadores TAS ou conduzirá a própria triagem. A triagem deve incluir verificação de antecedente criminal e verificações de emprego.	✔	✔	✔
7.7.4	Procedimento para lidar com a declaração falsa de candidatos/funcionários antes e depois da contratação.	✔	✔	✔
Rescisão ou recontratação de funcionários *Observação: A rescisão inclui desligamentos voluntários e involuntários, funcionários desligados e aposentados.*				
7.7.5	Recuperar ativos físicos do funcionário demitido, incluindo identificações da empresa, crachás de acesso, chaves, equipamentos ou informações confidenciais. Um procedimento documentado é necessário.	✔	✔	✔
7.7.6	Proteger os dados do comprador: Encerrar o acesso de funcionários desligados a sistemas físicos ou eletrônicos que contenham dados do Comprador (inventário ou programações).	✔	✔	✔
7.7.7	Lista de verificação de funcionários implementada para verificação.	✔	✔	✔

Seção	Integridade dos funcionários	A	B	C
7.7.8	Recontratação: Existem procedimentos para evitar que LSP/Candidato recontrate funcionários se critérios de negação/rescisão ainda estiverem válidos. *Observação: Os registros são analisados antes da recontratação (ex.: histórico de pessoal desligado anteriormente ou – candidatos rejeitados (emprego negado anteriormente).*	✔	✔	✔

8. Requisitos da função central (aplicável apenas para certificação de vários locais)

Seção	Função central	A	B	C
8.1	**Geral**			
8.1.1	Há uma função central para gerenciar o sistema de gestão de segurança para todos os locais, conforme definido no escopo da certificação de vários locais.	✔	✔	✔
8.1.2	Todos os locais devem ter uma relação legal ou contratual com a função central.	✔	✔	✔
8.1.3	Um único sistema de gestão de segurança é estabelecido para garantir que todos os seus locais dentro do sistema atendam aos requisitos do Padrão de Segurança da TAPA aplicável.	✔	✔	✔
8.1.4	A função central e seu sistema de gestão devem estar sujeitos a auditorias internas para garantir a conformidade contínua com os padrões TAPA.	✔	✔	✔
8.1.5	A função central deve realizar auditorias dos vários locais para fornecer a confiança e a garantia de que o sistema de gestão de segurança em todos os locais do sistema atende aos requisitos do Padrão aplicável e é capaz de atingir seus resultados pretendidos em todos os locais envolvidos. As auditorias devem ser feitas com os modelos de auditoria apropriados da TAPA.	✔	✔	✔
8.1.6	A função central deve ter a autoridade e os direitos necessários para exigir que todos os locais cumpram os Padrões de segurança da TAPA e implementem ações corretivas e preventivas conforme necessário. *Observação: Quando aplicável, isso deve ser estabelecido no acordo formal entre a função central e os locais.*	✔	✔	✔
8.2	**Políticas e procedimentos**			
8.2.1	A função central deve manter políticas e procedimentos documentados para seus sistemas de gestão de segurança que sejam aplicáveis para todos os seus locais.	✔	✔	✔
8.2.2	A função central deve garantir que as políticas e procedimentos adequados sejam atualizados, comunicados, implementados e colocados em funcionamento por todos os locais, conforme necessário.	✔	✔	✔
8.2.3	As políticas e procedimentos devem ser mantidos e facilmente acessíveis por todos os locais, conforme necessário.	✔	✔	✔
8.3	**Relatório de auditoria de autoavaliação realizada para todos os locais**			

Seção	Função central	A	B	C
8.3.1	A função central deve obrigar todos os locais a realizar a autoavaliação e todos os relatórios de autoavaliação devem ser enviados à função central para registros e revisões.	✔	✔	✔
8.3.2	A função central deve garantir que todos os SCARs da autoavaliação e auditorias estejam devidamente encerrados para melhorar seus sistemas de gestão de segurança.	✔	✔	✔
8.3.3	Todos os locais devem enviar atualizações de progresso e relatórios sobre todos os SCARs pendentes para a função central. A função central deverá encaminhar para a administração do LSP/Candidato caso os SCARs não sejam concluídos antes de suas datas de vencimento.	✔	✔	✔
8.4	**Registros de inspeções, registros (registros de visitantes, registro de motorista), inspeções de 7 pontos**			
8.4.1	A função central deve ter procedimentos para garantir que todos os locais mantenham registros de inspeções, registros de visitantes, registros de motoristas e inspeção de 7 pontos, etc.	✔	✔	✔
8.5	**Avaliações de risco de todos os locais**			
8.5.1	A função central deve ter procedimentos em vigor para garantir que as avaliações e a gestão de risco adequadas sejam feitas em todos os locais e seus registros sejam mantidos.	✔	✔	✔
8.6	**Disposição do CFTV e alarme dos locais**			
8.6.1	A função central deve ter procedimentos em vigor que garantam que todos os locais revisem e mantenham documentos em todos os sistemas de segurança física, como o CFTV e o layout do alarme.	✔	✔	✔
8.7	**Registros de controle de acesso e alarme**			
8.7.1	A função central deve ter procedimentos em vigor que garantam que todos os sistemas de controle de alarme e acesso sejam mantidos e testados para garantir sua eficácia operacional.	✔	✔	✔
8.7.2	A função central deve ter procedimentos para que todos os locais mantenham registros de todos os testes e incidentes de detecção de intrusão e controle de acesso.	✔	✔	✔
8.8	**Registros de treinamento**			
8.8.1	A função central deve ter procedimentos para garantir que todos os locais mantenham registros de treinamento adequados sobre o treinamento de gerenciamento de segurança de seus funcionários.	✔	✔	✔
8.8.2	A função central deve ter procedimentos para garantir que todos os locais mantenham registros de treinamento em segurança de todos os funcionários da instalação.	✔	✔	✔
8.9	**Registros de triagem/verificação**			

Seção	Função central	A	B	C
8.9.1	A função central deve ter procedimentos em vigor para garantir que todos os locais realizem a triagem e a verificação dos registros em intervalos regulares para garantir a integridade e a eficácia dos sistemas de gestão de segurança.	✔	✔	✔
8.9.2	A função central deve ter procedimentos para garantir que os registros de revisões, incluindo suas descobertas e ações corretivas/preventivas 8.1.6 sejam mantidos.	✔	✔	✔
8.10	**Revisão de gestão para avaliar as autoauditorias, SCARs abertos, quaisquer perdas, roubos, avaliações de risco.**			
8.10.1	A função central deve conduzir uma revisão regular da administração para garantir a conformidade, eficácia e melhoria aos seus sistemas de gestão de segurança.	✔	✔	✔
8.10.2	As revisões de gestão devem, entre outras coisas, cobrir a eficácia de autoauditorias, fechamentos de SCARs, avaliações de risco, incidentes e ações de melhoria.	✔	✔	✔
8.10.3	A função central deve manter registros de todas as revisões da administração.	✔	✔	✔

9.0. Ameaça à segurança cibernética e TI – Opção aprimorada

O FSR inclui melhorias opcionais contra ameaças à segurança cibernética que são consideradas um nível mais alto de proteção e podem ser usados além dos módulos. Essa melhoria opcional deve ser selecionada pelo LSP/Candidato e/ou pelo Comprador como requisito adicional para suas necessidades de segurança operacionais. Quando este aprimoramento opcional for selecionado na avaliação de pré-certificação para fazer parte da auditoria de certificação, todos os requisitos se tornam obrigatórios.

Seção	Ameaça à segurança cibernética e TI – Opção aprimorada
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/Candidato para identificar e responder a ameaças. 2. As políticas e procedimentos implementados para proteger, detectar, testar e responder a eventos de segurança. 3. Os métodos para a recuperação de sistemas e/ou dados de TI. 4. O protocolo de comunicação para Compradores/Clientes para mitigar o impacto na cadeia de suprimentos em até 24 horas após o conhecimento do incidente. 5. Como as políticas são revisadas anualmente e atualizadas conforme apropriado.
9.2	O LSP/Candidato deve fornecer treinamento de conscientização de informações para todos os funcionários. Este treinamento deve: - 1. Cobrir as funções e responsabilidades que os usuários do computador têm na manutenção da segurança e benefícios relacionados. 2. Ter um sistema em vigor que garanta que os registros de pessoas que recebem treinamento sejam mantidos por pelo menos dois anos.

Seção	Ameaça à segurança cibernética e TI – Opção aprimorada
9.3	O LSP/Candidato deve ter uma política por escrito em vigor para garantir que as medidas de Segurança Cibernética estejam em vigor com subcontratados e/ou fornecedores que garanta: 1. Os requisitos de segurança cibernética da LSP/Candidato são comunicados a subcontratados e/ou fornecedores e incorporados em acordos. 2. Quando subcontratados e/ou fornecedores não reconhecerem ou recusarem adotar os requisitos de segurança cibernética da LSP/Candidato, as medidas serão documentadas e implementadas para mitigar os riscos aos requisitos de Segurança Cibernética da LSP/Candidato e seus clientes.
9.4	O LSP/Candidato deve ter um plano de Mitigação de interrupção de energia (por exemplo, fonte de alimentação alternativa ou gerador de reserva), que garanta que a energia seja direcionada para sistemas críticos de TI (identificados na avaliação de risco local) por no mínimo 48 horas.
9.5	Os sistemas de informação do LSP/Candidato devem ter software antivírus e antimalware licenciado instalado. O software antivírus e antimalware deve conter as últimas atualizações.
9.6	O LSP/Candidato deve ter o Plano de Recuperação de Desastres de TI (Disaster Recovery Plan, DRP) apropriado para recuperação de ataques que comprometam o sistema, incluindo, entre outros, todos os dados necessários e sistemas de recuperação de software.
9.7	Os sistemas de informação LSP/Candidato devem ter back-up. Esses backups devem ser testados regularmente e os dados de backup devem ser criptografados e transferidos para um local secundário, fora da instalação.
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 únicos e senhas fortes. Procedimentos em vigor para garantir: 1. Programa de auditoria de conformidade de senha. 2. Uma senha original inicial deve ser atribuída a cada nova conta no momento da criação. 3. As senhas iniciais não podem conter o nome do usuário, o número de identificação ou seguir um padrão com base nas informações do usuário. 4. As senhas serão comunicadas aos usuários de forma segura e somente depois de validar a identidade do usuário. 5. Os usuários devem ser obrigados a alterar senhas no login inicial. 6. As senhas devem ser alteradas pelo menos a cada 90 dias.

Informações de publicação e direitos autorais

Histórico de publicação

Publicado pela primeira vez em janeiro de 2020

Primeira edição (presente) publicada em janeiro de 2020

Esta especificação disponível publicamente entra em vigor em 1.º de julho de 2020