Critérios Mínimos de Segurança – Fabricantes Estrangeiros

Marco 2020

Obs.: Os números de identificação dos critérios não estão em sequência. Os números de ID não listados não se aplicam aos fabricantes estrangeiros.

Primeira Área de Enfoque: Segurança Corporativa

1. **Visão e responsabilidade com a segurança** — Para que um programa de segurança da cadeia de abastecimento dos membros da CTPAT (Parceria da Alfândega-Comércio contra o Terrorismo) se torne eficaz e assim continue, é necessário que tenha o apoio da alta administração da empresa. Inculcar a segurança como parte integral da cultura corporativa e garantir que seja prioridade na empresa como um todo é, em grande parte, responsabilidade da sua liderança.

ID	Critérios	Diretrizes para implementação	Obrigatório /Recomen-dado
1.1	Ao promover uma cultura de segurança, os membros da CTPAT devem demonstrar o seu compromisso com a cadeia de abastecimento e com o Programa da CTPAT mediante uma declaração de apoio. Essa declaração deve ser assinada por um responsável de nível sênior da empresa e exibida em locais adequados da mesma.	A declaração de apoio deve destacar a importância da proteção da cadeia de abastecimento contra atividades criminosas, como tráfico de drogas, terrorismo, tráfico de pessoas e contrabando. Entre os responsáveis de nível sênior da empresa que podem apoiar e assinar a declaração estão o presidente, CEO, gerente geral ou diretor de segurança. As áreas onde a declaração de segurança deve ser exibida incluem o website da empresa, cartazes em áreas-chave (recepção, embalagem, armazém, etc.), e/ou devem fazer parte de seminários sobre segurança da empresa, etc.	Recomen-dado
1.2	Para preparar um programa robusto de segurança da cadeia de abastecimento, a empresa deve incorporar representantes de todos os departamentos pertinentes em uma equipe multidisciplinar.	A segurança da cadeia de abastecimento tem um âmbito muito mais amplo que os programas tradicionais de segurança. Está interligada à segurança em vários departamentos, como Recursos Humanos, Tecnologia da Informação, e escritório de Importação/Exportação.	Recomen-dado

ID	Critérios	Diretrizes para implementação	Obrigatório /Recomen-dado
	Essas novas medidas de segurança devem ser incluídas nos procedimentos existentes da empresa, o que cria uma estrutura mais sustentável e enfatiza que a segurança da cadeia de abastecimento é responsabilidade de todos.	Os programas de segurança da cadeia de abastecimento ancorados em modelos mais tradicionais com base em departamentos de segurança podem se tornar menos viáveis a longo prazo, porque a responsabilidade de executar medidas de segurança acaba se concentrando em um número menor de funcionários, ficando mais suscetível à perda de funcionários-chave.	
1.3	O programa de segurança da cadeia de abastecimento deve ser projetado, apoiado e implementado por meio de um componente adequado de revisão por escrito. O objetivo do componente de revisão é documentar a existência de um sistema em que os funcionários sejam responsabilizados e todos os procedimentos de segurança descritos no programa de segurança estejam sendo cumpridos como esperado. O plano de revisão deve ser atualizado conforme necessário, segundo modificações pertinentes nas operações da empresa e no nível de risco.	O objetivo da revisão para os propósitos da CTPAT é garantir que os seus funcionários estejam seguindo os procedimentos de segurança da empresa. O processo de revisão não precisa ser complexo. O membro decide o escopo das revisões e o seu nível de profundidade — com base em seu papel na cadeia de abastecimento, modelo de negócios, nível de risco e variações entre localidades/sítios específicos. Empresas menores podem criar uma metodologia simples de revisão, enquanto um grande conglomerado multinacional pode precisar de um processo mais amplo, tendo que considerar vários fatores, como os requisitos jurídicos locais, etc. Algumas grandes empresas talvez já tenham uma equipe de auditores que pode ser acionada para ajudar com as revisões de segurança. O membro pode escolher o uso de revisões direcionadas menores, voltadas a procedimentos específicos. Áreas especializadas que são fundamentais para a segurança da cadeia de abastecimento, como inspeção e controle de lacres, podem passar por revisões específicas. No entanto, é útil realizar uma revisão periódica geral para garantir que todas as áreas de segurança do programa estejam funcionando de maneira adequada. Se o membro já estiver realizando revisões como parte do seu programa anual, esse processo pode ser suficiente para atender a esse critério. Para membros com cadeias de abastecimento de alto risco (determinadas pela sua avaliação de risco), uma simulação ou exercícios teóricos podem ser incluídos no programa de revisão para	Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório /Recomen-dado
		garantir que os funcionários saibam como reagir no caso de um incidente real de segurança.	
1.4	Os pontos de contato da empresa com a CTPAT devem estar cientes dos requisitos do programa da CTPAT. Esses indivíduos precisam fornecer atualizações frequentes à alta gerência sobre questões relativas ao programa, incluindo o progresso ou resultado de auditorias, exercícios relativos à segurança e validações da CTPAT.	A CTPAT espera que os pontos de contato sejam indivíduos proativos que trabalhem com o especialista em segurança da cadeia de abastecimento e sigam as suas orientações. Os membros podem identificar indivíduos adicionais dispostos a apoiar essa função, listando-os como contatos no portal da CTPAT.	Obrigatório

2. **Avaliação de riscos —** A ameaça contínua de grupos terroristas e de organizações criminosas que visam as cadeias de abastecimento enfatiza a necessidade de que os membros avaliem a exposição existente ou potencial a essas ameaças crescentes. A CTPAT reconhece que, quando a empresa possui várias cadeias de abastecimento com um grande número de parceiros comerciais, enfrenta uma maior complexidade para garantir a segurança dessas cadeias. Quando uma empresa possui inúmeras cadeias de abastecimento, ela deve se concentrar nas áreas geográficas/cadeias de abastecimento em que o risco seja mais alto.

   Ao determinar o risco às suas cadeias de abastecimento, os membros devem considerar fatores como o modelo de negócios, a localização geográfica dos fornecedores e outros aspectos que podem ser característicos de uma cadeia de abastecimento especifica.

   Definição-chave: risco — Medida de um dano potencial devido a um evento indesejável que abrange ameaça, vulnerabilidade e consequências. O que determina o nível de risco é a probabilidade de que uma ameaça ocorra. Uma alta probabilidade de ocorrência geralmente se adequa a um alto nível de risco. O risco pode não ser eliminado, mas pode ser mitigado ao ser gerenciado — diminuindo a vulnerabilidade ou o impacto geral para a empresa.

ID	Critérios	Diretrizes para implementação	Obrigatório/Reco-mendado
2.1	Os membros da CTPAT devem verificar e documentar o montante de risco na sua cadeia de abastecimento. Os membros da	A avaliação de riscos (AR) geral é composta de duas partes-chave. A primeira é uma auto-avaliação do membro quanto às práticas de segurança, procedimentos e políticas da cadeia de abastecimento dentro das instalações que controla para verificar a sua adesão aos critérios mínimos de segurança da CTPAT, e uma análise geral da gerência sobre como o risco está sendo	Obriga-tório

ID	Critérios	Diretrizes para implementação	Obrigatório/Recomendado
	CTPAT devem realizar uma avaliação de riscos (AR) geral para identificar onde possam existir vulnerabilidades. A AR deve identificar ameaças, avaliar riscos e incorporar medidas sustentáveis para mitigar vulnerabilidades. Os membros devem levar em consideração requisitos da CTPAT específicos ao seu papel na cadeia de abastecimento.	gerenciado. A segunda parte da AR é a avaliação internacional de riscos. Essa parte da AR inclui a identificação de ameaça(s) geográfica(s) com base no modelo de negócios do membro e seu papel na cadeia de abastecimento. Ao considerar o possível impacto de cada ameaça à segurança da sua cadeia de abastecimento, o membro precisa de um método para avaliar ou diferenciar os níveis de risco. Um método simples é atribuir níveis de risco baixo, médio e alto. A CTPAT desenvolveu um guia de Avaliação de Risco em Cinco Etapas como ferramenta para a realização da parte internacional da avaliação de riscos que compreende a avaliação geral de riscos do membro. O guia pode ser encontrado no site do Serviço de Alfândega e Proteção de Fronteiras dos EUA: https://www.cbp.gov/sites/default/files/documents/C-TPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf. Para membros com uma extensa cadeia de abastecimento, o enfoque principal deve ser na área de maior risco.	
2.2	A parte internacional da avaliação de riscos deve documentar ou mapear a movimentação da carga do membro ao longo de toda a cadeia de abastecimento, do ponto de origem ao centro de distribuição do importador. O mapeamento deve incluir todos os parceiros comerciais envolvidos, tanto direta quanto indiretamente, na exportação/ movimentação das mercadorias. Conforme for aplicável, o mapeamento deve incluir documentação de como a carga entra e sai das instalações de transporte/ terminais de carga,	Ao desenvolver um processo para mapear cadeias de abastecimento, as áreas de alto risco devem ser as primeiras a ser consideradas. Ao documentar a movimentação de todas as cargas, o membro deve considerar todas as partes envolvidas relevantes — inclusive aquelas que se limitam a lidar com os documentos de importação/ exportação, como despachantes, e outros que talvez não lidem diretamente com a carga, mas possam ter controle operacional, como carregadores não operadores de navio (sigla em inglês, NVOCCs) ou fornecedores de logística terceirizados (3PLs). Caso alguma parte do transporte seja terceirizada, precisará também ser considerada porque, quanto mais níveis de partes indiretas, maior o risco envolvido. O exercício de mapeamento implica a consideração mais aprofundada de como a sua cadeia de abastecimento funciona. Além de identificar os riscos, ele pode servir também para encontrar áreas em que a cadeia de abastecimento é ineficiente, o que pode resultar em formas de diminuir os custos ou o ciclo de recepção do produto.	Recomendado

ID	Critérios	Diretrizes para implementação	Obrigatório/Recomendado
	observando se a carga está “em repouso” em algum desses locais por um período de tempo prolongado. A carga fica mais vulnerável quando está “em repouso”, aguardando a próxima etapa da sua jornada.		
2.3	A avaliação de riscos deve ser examinada anualmente ou com mais frequência de acordo com os fatores de risco.	Entre as circunstâncias que possam requerer que a análise da avaliação de riscos seja mais frequente do que uma vez ao ano estão o aumento no nível de ameaça de um país específico, períodos de alerta elevado, em seguida a uma falha ou incidente de segurança, mudança nos parceiros comerciais, e/ou modificações na estrutura corporativa ou em sua propriedade devido a fusões e aquisições, etc.	Obrigatório
2.4	Os membros da CTPAT devem ter procedimentos por escrito que tratem de gestão de crise, continuidade dos negócios, planos para recuperação da segurança e retomada dos negócios.	Uma crise pode incluir a interrupção da movimentação de dados comerciais devido a um ciberataque, incêndio ou sequestro de um transportador por indivíduos armados. Com base nos riscos e no local de operação do membro ou das suas fontes, os planos de contingência podem incluir notificações ou suporte adicionais de segurança, e como recuperar o que foi destruído ou roubado, retomando assim as condições normais de operação.	Recomendado

3. **Parceiros comerciais —** Os membros da CTPAT trabalham com vários parceiros comerciais, doméstica ou internacionalmente. Para os parceiros comerciais que têm contato direto com a carga e/ou documentação de importação/exportação, é essencial que os membros se assegurem de que esses parceiros adotem medidas adequadas para garantir a segurança das mercadorias em toda a cadeia internacional de abastecimento. Quando os parceiros comerciais terceirizam certas funções, um nível adicional de complexidade é acrescentado à equação, o que deve ser considerado ao se realizar uma análise de riscos da cadeia de abastecimento.

Definição-chave: parceiro comercial — Parceiro comercial é qualquer individuo ou empresa que possa afetar a cadeia de custódia de segurança dos bens importados para os Estados Unidos ou exportados pelo país por meio da cadeia de abastecimento de um membro da CTPAT. Parceiro comercial pode ser qualquer parte que preste serviços para atender uma necessidade dentro da cadeia internacional de abastecimento de uma empresa. Isso inclui todas as partes envolvidas (direta ou indiretamente) na compra, preparação de documentos, facilitação, manuseio, armazenamento, e/ou movimentação de carga para, ou em nome de, um

membro importador ou exportador da CTPAT. Dois exemplos de parceiros indiretos são transportadoras terceirizadas ou armazéns de consolidação no exterior — organizados por um agente/fornecedor de logística.

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomendado
3.1	Os membros da CTPAT devem ter um processo por escrito, com base em riscos, para averiguar novos parceiros comerciais e monitorar os parceiros atuais. Um fator a ser incluído nesse processo é a verificação de atividades relacionadas a lavagem de dinheiro e financiamento de terrorismo. Para auxiliar nesse processo, consulte os Indicadores de Alerta da CTPAT para Lavagem de Dinheiro com Base em Comércio e Atividades de Financiamento do Terrorismo.	Os seguintes são exemplos de alguns elementos de verificação que podem ajudar a determinar se uma empresa é legítima: • Verificar o endereço comercial da empresa e há quanto tempo ela está nesse endereço; • Pesquisar na internet tanto a empresa quanto seus diretores; • Verificar as referências comerciais; e • Solicitar um relatório de crédito. Entre os parceiros comerciais que precisam ser averiguados estão parceiros comerciais diretos, como fabricantes, fornecedores de produtos, vendedores/prestadores de serviços pertinentes, e fornecedores de transporte/logística. Qualquer fornecedor/prestador de serviço que esteja diretamente ligado à cadeia de abastecimento da empresa ou lide com informações/equipamentos sensíveis está incluído na lista de averiguação; isso inclui despachantes ou fornecedores terceirizados de serviços de TI. A profundidade da averiguação depende do nível de risco na cadeia de abastecimento.	Obrigatório
3.4	O processo de averiguação de um parceiro comercial deve levar em consideração se o parceiro é membro da CTPAT ou de um programa aprovado de Operador Econômico Autorizado (OEA), com um Acordo de Reconhecimento Mútuo (sigla em inglês MRA) com os Estados Unidos (ou um MRA aprovado). A certificação da CTPAT ou de um OEA é uma prova aceitável de conformidade com as exigências do programa para parceiros comerciais; os membros precisam obter evidências da certificação e continuar a monitorar esses parceiros comerciais para verificar se estão mantendo a sua certificação.	A certificação da CTPAT dos parceiros comerciais pode ser verificada no sistema de Interface de Verificação de Status do portal da CTPAT. Se o certificado do parceiro comercial for de um programa de um OEA estrangeiro segundo um MRA com os Estados Unidos, a certificação do OEA estrangeiro incluirá o componente de segurança. Os membros podem visitar o site da administração alfandegária estrangeira onde os nomes dos OEAs daquela administração alfandegária estão listados, ou solicitar a certificação diretamente aos seus parceiros comerciais. Os MRA atuais dos Estados Unidos incluem: Nova Zelândia, Canadá, Jordânia, Japão, Coreia do Sul, União Europeia (28 Estados membros), Taiwan, Israel, México, Cingapura, República Dominicana e Peru.	Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomendado
3.5	Quando um membro da CTPAT terceiriza ou subcontrata elementos da sua cadeia de abastecimento, deve exercer devida diligência (mediante visitas, questionários, etc.) para garantir que as medidas de segurança adotadas pelos parceiros comerciais atendam ou excedam os critérios mínimos de segurança (sigla em inglês MSC) da CTPAT.	Importadores e exportadores tendem a subcontratar uma grande parte das atividades da cadeia de abastecimento. Os importadores (e alguns exportadores) são as partes nessas transações que geralmente têm influência sobre seus parceiros comerciais e podem requerer a implementação de medidas de segurança em toda a cadeia de abastecimento, conforme necessário. Para os parceiros comerciais que não são membros da CTPAT ou aceitos em MRA, o membro da CTPAT exercerá devida diligência para garantir (quando tiver influência para tanto) que esses parceiros comerciais atendam os critérios de segurança aplicáveis do programa. Para verificar a adesão aos requisitos de segurança, os importadores realizam avaliações de segurança dos seus parceiros comerciais. O processo para determinar o quanto de informações deve ser levantado sobre o programa de segurança de um parceiro comercial está baseado na avaliação de riscos do membro e, no caso de cadeias de abastecimento numerosas, as áreas de alto risco são prioritárias. Pode-se determinar de várias maneiras se um parceiro comercial está em conformidade com os MSC. Com base nos riscos, a empresa pode fazer uma auditoria nas instalações, contratar empreiteira/fornecedor de serviços para realizar uma auditoria nas instalações, ou usar um questionário de segurança. Se forem usados questionários de segurança, o nível de risco determinará a quantidade de detalhes ou evidências necessária a ser levantada. Pode ser necessário um detalhamento maior no caso de empresas localizadas em áreas de alto risco. Se um membro estiver enviando um questionário de segurança aos seus parceiros comerciais, deve considerar a solicitação dos seguintes itens: •Nome e título da(s) pessoa(s) que o estejam preenchendo; •Data do preenchimento; •Assinatura do(s) indivíduo(s) que preencheram o documento; •*Assinatura de um funcionário de nível sênior da empresa, supervisor	Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomendado
		de segurança, ou representante autorizado da empresa que comprove a precisão das respostas ao questionário; •Dar detalhes suficientes nas respostas para determinar conformidade; e •Com base nos riscos e se assim for permitido pelos protocolos de segurança locais, incluir evidências fotográficas, cópias de políticas/procedimentos, e cópias de formulários preenchidos, como listas de verificação e/ou registros de guardas da inspeção dos instrumentos de tráfego internacional. *As assinaturas podem ser eletrônicas. Se for difícil obter/verificar uma assinatura, o responsável pela resposta pode confirmar a validade do questionário por e-mail, e que as respostas e todas as evidências que as apoiam foram aprovadas por um supervisor/gerente (nome e título são necessários).	
3.6	Se forem identificados pontos fracos durante as avaliações de segurança dos parceiros comerciais, é preciso resolvê-los o quanto antes, e as correções devem ser implementadas em tempo hábil. Os membros precisam confirmar, mediante evidências documentais, que as deficiências foram mitigadas.	A CTPAT reconhece que haverá cronogramas diferentes para a realização das correções com base no que for necessário para tanto. A instalação de equipamentos físicos geralmente leva mais tempo do que uma modificação de processos, mas a brecha na segurança deve ser resolvida assim que for descoberta. Por exemplo, se a questão for a substituição de uma cerca danificada, o processo de compra de uma nova cerca deve começar imediatamente (tratar da deficiência) e a instalação da nova cerca (ação corretiva) precisa ocorrer o quanto antes. Com base no nível de risco envolvido e na importância do ponto fraco identificado, algumas questões exigem atenção imediata. Se for uma deficiência que possa comprometer a segurança de um contêiner, por exemplo, deve ser tratada o quanto antes. Entre os exemplos de evidências documentais estão cópias de contratos de mais guardas de segurança, fotografias de câmeras de segurança ou de alarme contra intrusos recém-instaladas, ou cópias de listas de verificação de inspeção, etc.	Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomendado
3.7	Para garantir que seus parceiros comerciais continuem em conformidade com os critérios de segurança da CTPAT, os membros devem atualizar as avaliações de segurança dos seus parceiros comerciais com frequência, ou conforme as necessidades determinadas por circunstâncias/riscos.	A análise periódica das avaliações de segurança dos parceiros comerciais é importante para garantir que programas robustos de segurança continuem a ser utilizados e estejam funcionando de maneira adequada. Se o membro nunca solicitar atualizações dos planos de segurança dos seus parceiros comerciais, jamais tomará conhecimento de quando um programa outrora eficaz se tornou obsoleto, colocando em risco a sua cadeia de abastecimento. A decisão sobre a frequência da análise da avaliação de segurança de um parceiro se baseia no processo de avaliação de risco do membro. Cadeias de abastecimento de risco mais alto deveriam passar por avaliações mais frequentes do que as de risco mais baixo. Se um membro estiver avaliando a segurança do seu parceiro comercial por meio de visitas em pessoa, poderá considerar necessário outros tipos de visitas. Por exemplo, treinar pessoal que testa controle de qualidade para realizar também verificações de segurança. As circunstâncias podem exigir que uma auto-avaliação seja feita com mais frequência, entre elas níveis mais altos de ameaça de um país de origem, mudanças no local de origem, novos parceiros comerciais críticos (aqueles que de fato manuseiam a carga, fornecem serviços de segurança para instalações, etc.).	Recomendado

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomendado
3.8	No caso de envios para os Estados Unidos, se um membro subcontratar os serviços de transporte de outra transportadora viária, deverá usar uma que seja certificada pela CTPAT ou que trabalhe diretamente para o membro, conforme estipulado por meio de contrato por escrito. O contrato deve estipular a adesão a todos os critérios mínimos de segurança (MSC).	A transportadora deve fornecer às instalações onde a carga é apanhada e entregue uma lista dos carregadores e motoristas subcontratados. Qualquer modificação à lista da transportadora subcontratada deve ser imediatamente transmitida aos parceiros relevantes. Ao examinar o cumprimento dos prestadores de serviço, os membros devem verificar se a empresa subcontratada é de fato a empresa que está transportando a carga — e que não foram feitas subcontratações adicionais sem aprovação. Os membros devem limitar a subcontratação de serviços de transporte a um único nível. Caso sejam permitidas exceções para subcontratos adicionais, o membro da CTPAT e o expedidor devem ser notificados sobre o subcontrato adicional da carga.	Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomendado
3.9	Os membros da CTPAT devem ter um programa de conformidade social documentado, estipulando no mínimo que mercadorias importadas pelos Estados Unidos não tenham sido extraídas, produzidas ou fabricadas, em sua totalidade ou em parte, mediante formas de trabalho proibidas, ou seja, trabalho forçado, escravo, servil, ou trabalho infantil forçado.	Os esforços do setor privado na proteção dos direitos trabalhistas nas suas operações e cadeias de abastecimento podem promover um entendimento maior sobre leis e padrões trabalhistas que mitigam práticas laborais inadequadas. Esses esforços criam também um ambiente para melhores relações entre empregador e trabalhador e contribuem para os rendimentos da empresa. A seção 307 da Lei Tarifária de 1930 (19 U.S.C. § 1307) proíbe a importação de mercadorias extraídas, produzidas ou fabricadas, em sua totalidade ou em parte, em países estrangeiros mediante trabalho forçado ou trabalho infantil servil, incluindo trabalho infantil forçado. O trabalho forçado é definido pela Convenção nº 29 da Organização Mundial do Trabalho como todo trabalho ou serviço executado por um indivíduo sob ameaça de castigo e para o qual tal indivíduo não tenha se disponibilizado de maneira voluntária. O programa de conformidade social é o conjunto de políticas e práticas pelo qual uma empresa procura garantir a adesão máxima aos elementos do seu código de conduta que cobre questões sociais e trabalhistas. A conformidade social diz respeito a como uma empresa lida com suas responsabilidades quanto à proteção do meio-ambiente, saúde, segurança e direitos dos seus funcionários, da comunidade onde atua, e da vida e das comunidades dos funcionários ao longo da cadeia de abastecimento.	Recomendado

4. **<u>Cibersegurança</u>** — No mundo digital atual, a cibersegurança é essencial na proteção de alguns dos bens mais preciosos de uma empresa — propriedade intelectual, informações sobre clientes, dados financeiros e comerciais e registros dos funcionários, entre outros. Com uma conectividade cada vez maior à internet, existe o risco de falhas na segurança dos sistemas de informação de uma empresa. Essa ameaça diz respeito a empresas de todos os tipos e portes. Medidas para proteger a tecnologia da informação (TI) e os dados são de extrema importância, e os critérios listados oferecem uma base para um programa geral de cibersegurança para os membros.

   Definições-chave: cibersegurança — A cibersegurança é uma atividade ou um processo centrado na proteção de computadores, redes, programas e dados contra acesso, modificação ou destruição não intencionais ou não autorizados. É o processo de identificação, análise, avaliação e comunicação de um risco cibernético para que tal risco seja admitido, evitado, transferido ou mitigado a um nível aceitável, considerando-se custos e benefícios.

   Tecnologia da informação (TI) — A TI inclui computadores, armazenamento, rede e outros dispositivos físicos, infraestrutura e processos de criação, processamento, armazenamento, proteção e troca de todo tipo de dados eletrônicos.

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomen-dado
4.1	Os membros da CTPAT devem ter políticas e/ou procedimentos abrangentes por escrito de cibersegurança para proteção dos sistemas de tecnologia da informação (TI). Essas políticas para TI, no mínimo, devem cobrir todos os critérios individuais de cibersegurança.	Espera-se que os membros sigam protocolos de cibersegurança baseados em modelos/padrões reconhecidos da indústria. O *Instituto Nacional de Padrões e Tecnologia (sigla em inglês NIST) é uma das organizações que oferecem um modelo de cibersegurança (https://www.nist.gov/cyberframework) que oferece orientação voluntária baseada em padrões, diretrizes e práticas existentes que ajudam a gerir e reduzir o risco à cibersegurança, tanto interna quanto externamente. O modelo pode ser usado para ajudar a identificar e priorizar ações para reduzir riscos cibernéticos, e é uma ferramenta para alinhar políticas, negócios e abordagens tecnológicas para a gestão de risco. Ele complementa o processo de gestão de risco de uma empresa e o seu programa de cibersegurança. Por outro lado, a organização que não tenha um programa de cibersegurança pode usar o modelo como referência para estabelecê-lo. *O NIST é uma agência federal não reguladora do Departamento de Comércio que promove e mantém padrões métricos, e é responsável pelo desenvolvimento de padrões tecnológicos para o governo federal.	Obrigatório
4.2	Para defender os sistemas de tecnologia da informação (TI) contra ameaças à cibersegurança, a empresa deve instalar suficiente proteção de software/hardware contra malware (vírus, spyware, worms, cavalos de troia, etc.) e contra intrusões internas/externas (firewalls) nos sistemas de informática dos membros. Os membros precisam garantir que seu software de segurança esteja atualizado e receba atualizações frequentes. Os membros devem ter políticas e procedimentos para evitar ataques por meio de engenharia social. Caso ocorra uma violação de dados ou outro evento imprevisto que resulte na perda de dados e/ou equipamentos, os procedimentos devem incluir a recuperação (ou substituição) dos sistemas e/ou dados de TI.		Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomen-dado
4.3	Os membros da CTPAT que usam sistemas em rede devem testar com frequência a segurança da sua infraestrutura de TI. Caso sejam encontradas vulnerabilidades, devem ser implementadas correções o quanto antes.	Uma rede de computadores segura é essencial para uma empresa, e garantir a sua proteção exige testes frequentes. Isso pode ser feito por meio de verificações programadas de vulnerabilidades. Da mesma forma que um guarda de segurança verifica se há portas ou janelas abertas em uma empresa, a verificação de segurança (VS) identifica brechas nos computadores (portos e endereços de IP abertos), sistemas operacionais e software, pelos quais um hacker poderia acessar o sistema de TI da empresa. A VS faz isso mediante a comparação dos resultados da sua verificação com um banco de dados de vulnerabilidades conhecidas, e produz um relatório de correção com o qual a empresa pode trabalhar. Há várias versões grátis e comercialmente disponíveis de verificação de vulnerabilidades. A frequência dos testes dependerá de vários fatores, incluindo o modelo de negócios da empresa e o nível de risco. Por exemplo, as empresas devem fazer esses testes sempre que houver modificações na infraestrutura da sua rede. No entanto, os ciberataques estão aumentando em empresas de todos os portes, e isso precisa ser considerado ao se projetar um plano para testes.	Obrigatório
4.4	As políticas de cibersegurança devem considerar a forma pela qual o membro compartilha informações sobre ameaças à cibersegurança com governos e outros parceiros comerciais.	Espera-se que os membros compartilhem informações sobre ameaças à cibersegurança com governos e outros parceiros comerciais na sua cadeia de abastecimento. A troca de informações é uma parte-chave da missão do Departamento de Segurança Interna para gerar conhecimento situacional sobre atividades cibernéticas maliciosas. Os membros da CTPAT devem considerar a participação no Centro Nacional de Integração de Cibersegurança e Comunicações (sigla em inglês NCCIC - https://www.us-cert.gov/nccic). O NCCIC compartilha informações entre parceiros dos setores público e privado para aumentar o conhecimento sobre vulnerabilidades, incidentes e mitigação. Usuários de sistemas de controle cibernético e industrial podem receber produtos de informações, *feeds* e serviços sem nenhum custo.	Reco-mendado

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomen-dado
4.5	Deve-se implementar um sistema para identificar o acesso não autorizado a sistemas/dados de TI ou o abuso de políticas e procedimentos, inclusive o acesso impróprio a sistemas internos ou websites externos, ou a violação ou adulteração de dados da empresa por parte de funcionários ou contratados. Todos os infratores devem estar sujeitos a ações disciplinares adequadas.		Obrigatório
4.6	Políticas e procedimentos de cibersegurança devem ser revistos anualmente ou com maior frequência, conforme as exigências de riscos ou circunstâncias. Depois da revisão, as políticas e procedimentos devem ser atualizados, se necessário.	Um exemplo de circunstância que exigiria a atualização das políticas antes do prazo de um ano seria um ciberataque. O uso das lições aprendidas com o ataque ajudaria a fortalecer a política de cibersegurança do membro.	Obrigatório
4.7	O acesso do usuário deve ser restringido com base na descrição do cargo ou deveres que lhe são atribuídos, e a autorização para tanto deve ser revista com frequência para garantir que o acesso a sistemas sensíveis seja baseado nas necessidades do cargo. O acesso a computadores e redes deve ser interrompido assim que o funcionário sair da empresa.		Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomen-dado
4.8	Indivíduos com acesso a sistemas de tecnologia da informação (TI) devem usar contas individualmente atribuídas. O acesso a sistemas de TI deve estar protegido contra infiltrações por meio de uso de palavras-senha, frases-senha, ou outras formas de autenticação, e o acesso do usuário aos sistemas de TI precisa ser protegido. As palavras-senha e/ou frases-senha devem ser mudadas o quanto antes se houver evidência ou suspeita razoável de comprometimento.	Para proteger os sistemas de TI contra infiltrações, o acesso do usuário deve ser salvaguardado mediante um processo de autenticação. Palavras-senha ou frases-senha complexas para o login, tecnologias biométricas e cartões de ID eletrônicos são três tipos diferentes de processos de autenticação. Os processos que usam mais de uma medida são preferíveis. Estes são os processos de autenticação com dois fatores (2FA) ou a autenticação multifatorial (MFA). A MFA é a mais segura pois exige que um usuário apresente duas ou mais evidências (credenciais) para autenticar a identidade de uma pessoa durante o processo de logon. As MFA podem ajudar a impedir as intrusões em uma rede facilitadas por uma senha fraca ou credenciais roubadas. As MFA podem ajudar a impedir esses vetores de ataque exigindo que indivíduos fortaleçam as palavras-senha ou frases-senha (algo do conhecimento da pessoa) com um objeto em sua posse, como um token, ou por características físicas — biometria. Quando se usa uma senha, ela precisa ser complexa. A Publicação Especial 800-63B: Digital Identity Guidelines, (https://pages.nist.gov/800-63-3/sp800-63b.html) do Instituto Nacional de Padrões e Tecnologia (sigla em inglês NIST), inclui diretrizes para senhas. Recomenda o uso de frases-senha fáceis de serem lembradas em vez de palavras-senha com caracteres especiais. Essas frases-senha mais longas (o NIST recomenda permitir o uso de até 64 caracteres) são consideradas mais difíceis de ser decifradas pois são compostas por sentenças ou frases fáceis de serem lembradas.	Obrigatório
4.9	Os membros que permitem a conexão remota de usuários a uma rede devem usar tecnologias seguras, como redes privadas virtuais (VPN), para permitir o acesso seguro de funcionários à intranet da empresa quando estiverem fora do escritório. Os membros também devem contar com procedimentos projetados para evitar o acesso remoto de usuários não autorizados.	As VPN não são a única maneira de proteger o acesso a uma rede. A autenticação multifatorial (MFA) é um outro método. Um exemplo de autenticação multifatorial seria o uso de um token com um código de segurança dinâmico que o funcionário precisa digitar para entrar na rede.	Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomen-dado
4.10	Se os membros permitirem que seus funcionários utilizem dispositivos pessoais para o trabalho na empresa, todos esses dispositivos devem aderir a políticas e procedimentos de cibersegurança da empresa de modo a incluir atualizações de segurança frequentes e métodos para acessar com segurança a rede da empresa.	Dispositivos pessoais incluem dispositivos de armazenamento como CDs, DVDs e pendrive (USB). É preciso cautela caso os funcionários tenham permissão de conectar seus dispositivos pessoais a sistemas individuais, já que esses dispositivos de armazenamento de dados podem ser infectados por malware e se propagar usando a rede da empresa.	Obrigatório
4.11	Políticas e procedimentos de cibersegurança devem incluir medidas para evitar o uso de produtos tecnológicos falsificados ou com licença inadequada.	Software de informática é propriedade intelectual (PI) da entidade que o criou. Sem a permissão expressa do fabricante ou divulgador, a instalação do software é ilegal, não importando como tenha sido adquirido. Essa permissão quase sempre é expressa por uma licença do divulgador, que acompanha as cópias autorizadas do software. Software não licenciado tem mais chances de falhar devido à incapacidade de fazer atualizações. Está mais propenso a conter malware, inutilizando assim os computadores e suas informações. Não se pode esperar garantia ou assistência de softwares não licenciados, o que deixa a sua empresa descoberta para lidar com as falhas. Há consequências jurídicas para o uso de software não licenciado, incluindo penalidades civis rigorosas e processos penais. Os softwares piratas aumentam o custo para os usuários de softwares legitimamente autorizados e diminuem o capital disponível para investimento em pesquisa e desenvolvimento de novos softwares. Pode ser do interesse dos membros ter uma política exigindo que as principais etiquetas e os certificados de autenticidade sejam guardados ao se comprar novos produtos. CDs, DVDs, pendrives(USB) incluem recursos holográficos de segurança para ajudar a garantir a autenticidade dos produtos e proteger contra falsificações.	Reco-mendado

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomen-dado
4.12	O backup de dados deve ser feito uma vez por semana ou quando apropriado. Todos os dados sigilosos ou confidenciais devem ser armazenados em formato criptografado.	O backup de dados deve ser feito porque a perda de dados pode afetar de maneira diferente os indivíduos dentro da empresa. Backups diários também são recomendados caso a produção ou servidores compartilhados fiquem comprometidos ou percam dados. Sistemas individuais podem necessitar de backups menos frequentes, dependendo do tipo de informação que estiver envolvida. A mídia usada para armazenar os backups deve ser preferivelmente guardada em uma instalação fora da empresa. Os dispositivos usados para o backup de dados não devem estar na mesma rede que aquela utilizada para o trabalho de produção. O backup na nuvem é aceitável enquanto instalação “fora da empresa”.	Recomen-dado
4.13	Toda mídia, hardware ou outros equipamentos de TI que contenham informações sigilosas sobre o processo de importação/exportação precisam ser contabilizados em inventários frequentes. Ao serem descartados, precisam ser adequadamente limpos e/ou destruídos segundo as Diretrizes para Limpeza de Mídia do Instituto Nacional de Padrões e Tecnologia (NIST) ou outras diretrizes adequadas.	Alguns tipos de mídia computadorizada são discos rígidos, discos removíveis, CD-ROM ou discos CD-R, DVDs ou drives USB. O Instituto Nacional de Padrões e Tecnologia (NIST) desenvolveu padrões para a destruição de mídia de dados do governo. Os membros podem consultar os padrões do NIST para limpeza e destruição de equipamentos e mídia de TI. Limpeza de mídia: https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization	Obrigatório

Segunda Área de Enfoque: Segurança do Transporte

5. **<u>Segurança de veículos e instrumentos de tráfego internacional</u>** — Esquemas de contrabando geralmente envolvem a modificação de veículos ou instrumentos de tráfego internacional (sigla em inglês IIT), ou a ocultação de contrabando dentro dos IIT. Esta categoria de critérios abrange medidas de segurança cujo objetivo é evitar, detectar, e/ou deter a alteração da estrutura dos IIT ou a entrada clandestina nos mesmos, o que poderia permitir a introdução de materiais ou indivíduos não autorizados.

   Durante o empacotamento/carregamento, devem ser usados procedimentos adequados de inspeção de IIT e lacres. A carga em trânsito ou "em repouso" está sob menos controle ficando, portanto, mais vulnerável à infiltração. É por isso que os controles de lacre e os métodos para rastrear a carga ou o veículo em trânsito são critérios essenciais de segurança.

   As violações nas cadeias de abastecimento ocorrem com mais frequência durante o processo de transporte; por conseguinte, os membros devem permanecer atentos para que estes critérios-chave para cargas sejam respeitados em toda a cadeia de abastecimento.

   Definição-chave: instrumentos de tráfego internacional (IIT) — Os ITT compreendem contêineres, plataformas, dispositivos de cargas unitárias (sigla em inglês ULDs), *lift vans*, furgões de carga, tanques de transporte, caixotes, paletes, pás carregadeiras, *caul boards*, miolos para têxteis e outros contêineres especializados que chegam (carregados ou vazios), estão em uso ou serão usados no futuro para envio de mercadorias no comércio internacional.

ID	Critérios	Diretrizes para implementação	Obrigatório / Recomendado
5.1	Os veículos e os instrumentos de tráfego internacional (IIT) devem ser armazenados em uma área segura para evitar acesso não autorizado, o que poderia resultar na alteração da estrutura de um instrumento de tráfego internacional ou, se for o caso, permitir que um lacre ou porta sejam comprometidos.	O armazenamento seguro de veículos e instrumentos de tráfego internacional (vazios ou não) é importante para a proteção contra acesso não autorizado.	Obrigatório
5.2	O processo de inspeção da CTPAT deve contar com procedimentos por escrito para inspeções de segurança e agrícolas.	Com a prevalência de esquemas de contrabando que envolvem a modificação de veículos ou instrumentos de tráfego internacional, é essencial que os membros realizem inspeções de veículos e instrumentos de tráfego internacional para procurar pragas ou outras sérias deficiências estruturais. Da mesma	Obrigatório

ID	Critérios	Diretrizes para implementação	Obriga-tório / Reco-mendado
		maneira, a prevenção da contaminação por pragas por intermédio de veículos e IIT é uma grande preocupação; sendo assim, adicionou-se um componente agrícola ao processo de inspeção de segurança. A contaminação por pragas é definida como formas visíveis de animais, insetos ou outros invertebrados (vivos ou não, em qualquer estágio do ciclo de vida, incluindo cascas de ovos ou ovas), ou qualquer material orgânico de origem animal (incluindo sangue, ossos, pelos, carne, secreções, excreções); plantas viáveis ou não, ou produtos vegetais (incluindo frutas, sementes, folhas, gravetos, raízes, casca); ou outros materiais orgânicos, incluindo fungos; ou solo ou água; quando tais produtos não fizerem parte do manifesto de carga de instrumentos de tráfego internacional (ou seja, contêineres; dispositivos de carga unitária, etc.).	
5.3	Os membros da CTPAT devem garantir que sejam realizadas as seguintes inspeções de segurança e agrícolas sistemáticas da CTPAT. Os requisitos para essas inspeções variarão caso a cadeia de abastecimento seja terrestre (Canadá ou México) ou tenha origem estrangeira (modalidade marítima ou aérea). Antes da embalagem ou do empacotamento, todos os instrumentos de tráfego internacional (IIT) têm de ser inspecionados, e os veículos também precisam ser inspecionados ao cruzar a fronteira terrestre com os Estados Unidos. <u>Requisitos de inspeção para carregamentos da CTPAT via fronteiras marítimas, aéreas ou terrestres (quando aplicável), por ferrovias ou frete intermodal:</u> Uma inspeção de sete pontos deve ser realizada em todos os contêineres e dispositvos de carga unitária (ULD) vazios; e uma inspeção de oito pontos deve ser realizada em todos os contêineres e ULD refrigerados vazios:	As inspeções de segurança e agrícolas são realizadas em instrumentos de tráfego internacional (IIT) e veículos para garantir que suas estruturas não tenham sido modificadas para ocultar contrabando, nem tenham sido contaminadas com pragas agrícolas visíveis. Espera-se que as cadeias de abastecimento estrangeiras inspecionem todos os IIT no momento de embalagem ou empacotamento. No entanto, se uma cadeia de abastecimento marítima ou aérea apresentar um risco mais alto, pode-se justificar a inclusão de procedimentos de inspeção mais extensos que incluam veículos e/ou inspeções em terminais de portos marítimos ou instalações de logística aérea. Geralmente, há níveis de risco mais altos envolvidos em carregamentos que cruzam fronteiras terrestres e, por isso, tanto os veículos quanto os IIT passam por inspeções múltiplas.	Obriga-tório

ID	Critérios	Diretrizes para implementação	Obriga-tório / Reco-mendado
	1. Parede dianteira ; 2. Lado esquerdo; 3. Lado direito; 4. Base; 5. Teto/topo; 6. Portas internas/externas, inclusive a confiabilidade do mecanismo de trava das portas; 7. Dentro e debaixo do chassi; e 8. Caixa do ventilador em contêineres refrigerados. <u>Requisitos adicionais de inspeção para o cruzamento de fronteiras terrestres em transporte viário:</u> As inspeções de veículos e IIT têm de ser realizadas no pátio de armazenamento do veículo/IIT. Quando for viável, as inspeções devem ser realizadas na entrada e saída do pátio de armazenamento e no local de empacotamento/ embalagem. Essas inspeções sistemáticas devem incluir inspeções de 17 pontos: **<u>Tratores:</u>** 1. Para-choques/pneus/aros; 2. Portas, compartimentos de ferramentas e mecanismos de trava; 3. Caixa da bateria; 4. Respirador de ar; 5. Tanques de combustível; 6. Compartimentos da cabine anterior/beliche; e 7. Teto/topo.	Alguns exemplos de IIT para modalidades diferentes são contêineres oceânicos, contêineres/trailers refrigerados, trailers de estrada, trailers de plataforma, caminhões-tanque, vagões/vagões de carga fechados, vagões tremonhas e dispositivos de carga unitária (ULD). A Seção da Biblioteca Pública do Portal da CTPAT contém materiais de treinamento sobre inspeções de segurança e agrícolas de veículos e instrumentos de tráfego internacional.	

ID	Critérios	Diretrizes para implementação	Obrigatório / Recomendado
	Trailers: 1. Área da quinta roda – verificar o compartimento natural/placa de deslizamento; 2. Exterior – frente/lados; 3. Posterior – para-choques/portas; 4. Parede dianteira; 5. Lado esquerdo; 6. Lado direito; 7. Base; 8. Teto/topo; 9. Portas externas/internas e mecanismos de trava; e 10. Dentro e debaixo do chassi.		
5.4	Os veículos e instrumentos de tráfego internacional (quando for o caso) devem estar equipados com material externo que possa resistir bem a qualquer tentativa de remoção. Portas, maçanetas, varas, ferrolhos, rebites, suportes e todas as outras peças do mecanismo de trava de um contêiner devem ser inspecionados por completo para detectar adulterações e inconsistências do material antes de se acoplar dispositivos de lacre.	Considere o uso de contêineres/trailers com dobradiças resistentes a adulteração. Os membros também podem colocar placas ou pinos de proteção em pelo menos duas das dobradiças das portas e/ou lacres/fitas adesivas por cima de pelo menos uma dobradiça de cada lado.	Obrigatório
5.5	A inspeção de todos os veículos e instrumentos de tráfego internacional vazios deve ser registrada em uma lista de verificação, da qual devem constar os seguintes elementos: • Número do contêiner/trailer/instrumento de tráfego internacional; • Data da inspeção; • Hora da inspeção; • Nome do funcionário que realizou a inspeção; e • Áreas especificas dos instrumentos de tráfego internacional que foram inspecionadas. Se as inspeções forem supervisionadas, o supervisor também deve		Recomendado

ID	Critérios	Diretrizes para implementação	Obrigatório / Recomendado
	assinar a lista de verificação. A folha de inspeção preenchida dos contêineres/ instrumentos de tráfego internacional devem fazer parte do pacote de documentação do carregamento. O consignatário deve receber o pacote completo da documentação de transporte antes de receber a mercadoria.		
5.6	Todas as inspeções de segurança devem ser realizadas em uma área de acesso controlado e, quando disponível, ser monitoradas por um sistema de circuito fechado de televisão (sigla em inglês CCTV).		Recomendado
5.7	Se for encontrada contaminação visível por pragas durante a inspeção de veículos/instrumentos de tráfego internacional, deve-se lavar o local e usar um aspirador para remover a contaminação. A documentação deve ficar retida durante um ano para demonstrar conformidade com esses requisitos de inspeção.	Manter registros dos tipos de contaminantes encontrados, onde foram encontrados (local no veículo), e como a contaminação por pragas foi eliminada pode ajudar os membros a evitar ocorrências futuras.	Obrigatório
5.8	Com base nos riscos, a gerência deve realizar buscas aleatórias dos veículos depois que os funcionários de transporte tiverem realizado inspeções nos veículos/instrumentos de tráfego internacional. As buscas em veículos devem ser realizadas periodicamente, com maior frequência dependendo dos riscos. Devem ser realizadas de maneira aleatória, sem aviso prévio, para não se tornarem previsíveis. A inspeção deve ser realizada em vários locais onde o veículo estiver vulnerável: o pátio da transportadora, depois que o caminhão for carregado, e a caminho da fronteira dos Estados Unidos.	Buscas de supervisão de veículos são realizadas para combater conspirações internas. Para praticar, os supervisores podem esconder um objeto (um brinquedo ou caixa colorida) no veículo para determinar se o responsável pelo teste ou operador do veículo o encontra. O pessoal de supervisão pode ser o gerente de segurança, responsável perante a alta administração pela segurança, ou outro funcionário designado pela gerência.	Recomendado
5.14	Os membros da CTPAT devem trabalhar com seus provedores de transporte para rastrear veículos da origem até o destino final. Requisitos específicos para rastreio, relatórios e compartilhamento de dados devem ser incorporados aos termos do acordo de serviço com os prestadores de serviços.		Recomendado

ID	Critérios	Diretrizes para implementação	Obrigatório / Recomendado
5.15	Os expedidores devem ter acesso ao sistema GPS de monitoramento da frota da transportadora para que possam acompanhar o movimento do carregamento.		Recomendado
5.16	Para transportes por fronteiras terrestres próximas aos Estados Unidos, uma política de "parada negada" deve ser implementada em relação a paradas não programadas.	Carga em repouso é carga em risco. Paradas previstas não são cobertas por essa política, mas devem ser consideradas em um procedimento geral de rastreio e monitoramento.	Recomendado
5.24	Em áreas de alto risco, e imediatamente antes da chegada ao cruzamento da fronteira, os membros da CTPAT devem adicionar um processo de verificação de "última instância" para cargas a caminho dos EUA, a fim de verificar se há sinais de adulteração em veículos/instrumentos de tráfego internacional. Essa verificação deve incluir inspeção visual de veículos e processos de verificação de lacre VVPT (visualizar, verificar, puxar e torcer). Indivíduos com treinamento adequado devem realizar as inspeções. V – Visualizar o lacre e os mecanismos de trava do contêiner; verificar se estão OK; V – Verificar a numeração do lacre, comparando-a aos documentos de transporte para garantir precisão; P – Dar um puxão no lacre para garantir que esteja afixado de maneira adequada; T – Torcer e girar o lacre de barreira para garantir que os seus componentes não se desparafusem, separam-se uns dos outros, ou que nenhuma parte do lacre se solte.		Recomendado
5.29	Se uma ameaça crível (ou detectada) à segurança da carga ou do veículo for descoberta, o membro deve alertar (assim que possível) os parceiros comerciais na cadeia de abastecimento que possam ser afetados, e também as autoridades policiais, conforme apropriado.		Obrigatório

6. **<u>Segurança do lacre</u>** — O lacre de trailers e de contêineres, e a manutenção contínua da sua integridade, é elemento essencial em uma cadeia de abastecimento segura. A segurança do lacre inclui ter uma abrangente política por escrito que trate de todos os aspectos da segurança do lacre; usar os lacres corretos segundo os requisitos da CTPAT; colocar de modo adequado o lacre em um IIT; e verificar se o lacre foi afixado corretamente.

ID	Critérios	Diretrizes para implementação	Obrigatório / Recomendado
6.1	Os membros da CTPAT devem ter procedimentos por escrito de alta segurança para lacres que descrevam como o lacre é expedido e controlado nas instalações e durante o trânsito. Os procedimentos devem fornecer as etapas a serem cumpridas caso o lacre tenha sido alterado, manipulado, ou apresente a numeração incorreta, com documentação do evento, protocolos de comunicação a parceiros, e investigação do incidente. Os resultados da investigação devem ser documentados e qualquer medida corretiva deve ser implementada o quanto antes. Os procedimentos por escrito devem ser guardados no nível operacional local para serem de fácil acesso. Eles devem ser revistos pelo menos uma vez por ano e atualizados quando necessário. Os controles por escrito para lacres devem incluir os seguintes elementos: **Controle do acesso ao lacre**: • A administração dos lacres está restrita apenas a pessoal autorizado. • Armazenamento seguro. **Inventário, distribuição e rastreio (registro do lacre):** • Registro do recebimento de um novo lacre. • A entrega de lacres consignada no registro. • Rastreio do lacre por meio do registro. • Apenas funcionários treinados autorizados podem afixar o lacre a instrumentos de tráfego internacional (IIT). **Controle do lacre em trânsito**: • Ao se receber o IIT lacrado (ou depois da parada), verificar se o lacre		Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório / Recomendado
	está intacto e sem nenhum sinal de adulteração. • Confirmar se a numeração do lacre corresponde à anotação nos documentos de transporte. **Lacres rompidos em trânsito:** • Se a carga for examinada, registrar a numeração do lacre substituído. • O motorista deve notificar imediatamente o despacho se o lacre foi rompido, indicar quem o rompeu e fornecer o número do novo lacre. • A transportadora deve notificar imediatamente o expedidor, despachante e importador que o lacre foi trocado, informando a numeração do novo lacre. • O expedidor deve anotar o número do novo lacre no registro de lacres. **Discrepâncias nos lacres:** • Guardar os lacres alterados ou adulterados para auxiliar nas investigações. • Investigar as discrepâncias; a seguir, adotar medidas corretivas (quando for justificável). • Quando for o caso, informar o comprometimento dos lacres ao CBP e ao governo estrangeiro pertinente para auxiliar nas investigações.		

ID	Critérios	Diretrizes para implementação	Obrigatório / Recomendado
6.2	Todos os carregamentos da CTPAT que podem ser lacrados devem ser protegidos logo que forem carregados /embalados /empacotados pela parte responsável (ou seja, o expedidor ou embalador agindo em nome do expedidor) com um lacre de alta segurança que corresponda ou supere os padrões mais atualizados para lacres de alta segurança da Organização Internacional para Padronização (ISO) 17712. Lacres de metal e de barreira qualificados são ambos aceitáveis. Todos os lacres usados devem estar afixados de maneira segura e adequada aos instrumentos de tráfego internacional que transportam carga dos membros da CTPAT de/para os Estados Unidos.	O lacre de alta segurança utilizado deve ser colocado na posição segura do came, quando disponível, e não na maçaneta da porta à direita. O lacre deve ser posto na parte inferior do centro da barra mais vertical da porta direita do contêiner. Outra alternativa é colocar o lacre no centro da maçaneta de trava à extrema esquerda na porta direita do contêiner quando a posição segura do came não estiver disponível. Se um lacre de barreira estiver sendo utilizado, recomenda-se que ele seja inserido com a parte do cilindro voltada para cima acima do ferrolho.	Obrigatório
6.5	Os membros da CTPAT (que têm um inventário de lacres) devem ser capazes de provar que os lacres de alta segurança por eles usados estejam de acordo ou excedam os padrões ISO 17712 mais atuais.	Cópia de um certificado de teste em laboratório que demonstre a conformidade com os padrões para lacres de alta segurança da ISO são evidências aceitáveis de conformidade. Os membros da CTPAT devem estar cientes das características indicativas de adulteração dos lacres que compram.	Obrigatório
6.6	Se um membro tiver um inventário de lacres, a gerência ou o supervisor de segurança da empresa deve realizar uma auditoria que inclua inventário dos lacres armazenados e cotejo com inventário de lacres e documentação de transporte. Todas as auditorias devem ser documentadas. Como parte do processo geral de auditoria de lacres, os supervisores de doca e/ou gerentes de armazenamento devem verificar periodicamente a numeração dos lacres usados em veículos e em instrumentos de tráfego internacional.		Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório / Recomendado
6.7	O processo de verificação de lacre da CTPA deve ser seguido para garantir que todos os lacres de alta segurança (de barreira/cabos de metal) tenham sido afixados de maneira adequada aos instrumentos de tráfego internacional, e estejam funcionando da maneira esperada. O procedimento é conhecido como VVPT: V – Visualizar o lacre e os mecanismos de trava do contêiner; verificar se estão OK; V – Verificar a numeração do lacre, comparando-a aos documentos de transporte para garantir precisão; P – Dar um puxão no lacre para garantir que esteja afixado de maneira adequada; T – Torcer e girar o lacre de barreira para garantir que seus componentes não se desparafusem, separem-se uns dos outros, ou que nenhuma parte do lacre se solte.	Quando são utilizados lacres de cabo de metal, é necessário envolver a base retangular da ferragem das barras verticais a fim de eliminar qualquer movimento ascendente ou descendente do lacre. Uma vez que o lacre tenha sido colocado, assegurar-se de que foi removida qualquer folga dos dois lados do cabo. O processo VVPT para lacres com cabo de metal é usado para garantir que os cabos estejam esticados. Depois de afixado adequadamente, dar um puxão no cabo para detectar qualquer deslizamento dentro da caixa de trava.	Obrigatório

7. **<u>Procedimentos de segurança</u> —** Os procedimentos de segurança abrangem muitos aspectos do processo de importação-exportação, dos requisitos de documentação, armazenamento e manuseio de cargas. Outros critérios essenciais dos procedimentos dizem respeito a informes e notificações de incidentes às autoridades policiais pertinentes. Adicionalmente, a CTPAT costuma exigir que os procedimentos sejam escritos, o que ajuda a manter a uniformidade do processo ao longo do tempo. No entanto, o detalhamento necessário dos procedimentos escritos dependerá de vários elementos, como o modelo de negócios da empresa, ou do que está sendo abarcado pelo procedimento.

   A CTPAT reconhece que a tecnologia usada em cadeias de abastecimento continua a evoluir. A terminologia usada nos critérios diz respeito a procedimentos, documentos e formulários por escrito, mas isso não significa que eles precisem ser impressos em papel. Documentos e assinaturas eletrônicos e outras tecnologias digitais são aceitáveis para cumprir esses requisitos.

   O programa não é projetado para ser um modelo único que sirva para todos; cada empresa deve decidir (com base na sua avaliação de riscos) como implementar e manter os procedimentos. No entanto, é mais eficaz incorporar processos de segurança a procedimentos existentes do que criar um manual separado para protocolos de segurança. Isso cria uma estrutura mais sustentável e ajuda a enfatizar que a segurança da cadeia de abastecimento é responsabilidade de todos.

ID	Critérios	Diretrizes para implementação	Obrigatório /Recomendado
7.1	Quando a carga é preparada durante a noite ou por períodos de tempo extensos, devem ser adotadas medidas para protegê-la contra o acesso não autorizado.		Obrigatório
7.2	As áreas de preparação da carga e imediatamente ao seu redor devem ser inspecionadas com frequência para garantir que estejam livres de contaminação visível por pragas.	Medidas preventivas, como o uso de iscas, armadilhas e outras barreiras, podem ser usadas quando necessário. A remoção de ervas daninhas ou a redução de excesso de vegetação pode ajudar a eliminar o habitat das pragas nas áreas de preparação.	Obrigatório
7.4	O carregamento/colocação da carga em contêineres/IIT deve ser supervisionado por um responsável/gerente de segurança ou outro funcionário com essa atribuição.		Recomendado

ID	Critérios	Diretrizes para implementação	Obrigatório /Recomendado
7.5	Como evidência documentada da instalação adequada de lacres, deve-se tirar fotografias digitais no local de embarque da carga. Na medida do possível, essas imagens devem ser enviadas eletronicamente ao destino para serem verificadas.	As evidências fotográficas podem incluir fotografias tiradas no local do embarque para documentar as marcas da carga, o processo de carregamento, o local em que foi afixado o lacre e o lacre devidamente instalado.	Recomendado
7.6	É obrigatório haver procedimentos que garantam que todas as informações usadas na liberação da mercadoria/carga sejam legíveis, completas, precisas, e estejam protegidas contra mudanças, perda ou introdução de informações errôneas, e que sejam relatadas pontualmente.		Obrigatório
7.7	Se forem usados documentos em papel, os formulários e a documentação relativa a importação/exportação devem ser protegidos para evitar uso não autorizado.	Podem ser adotadas medidas como o uso de um fichário trancado para proteger o armazenamento de formulários que não estejam sendo usados, incluindo manifestos, para evitar o uso não autorizado da documentação.	Recomendado
7.8	O expedidor ou seus agentes devem garantir que o conhecimento de embarque (sigla em inglês BOL) e/ou os manifestos reflitam fielmente as informações enviadas à transportadora, as quais devem ser diligentes a fim de garantir que esses documentos sejam precisos. Os BOL e manifestos devem ser preenchidos junto ao Serviço de Alfândegas e Proteção de Fronteiras (CBP) dos EUA em tempo hábil. As informações sobre o BOL apresentadas ao CBP devem indicar a primeira localidade/instalação estrangeira em que a transportadora tomou posse da carga com destino aos Estados Unidos. É obrigatório que o peso e a contagem de peças sejam precisos.	Ao receber um instrumento de tráfego internacional lacrado, as transportadoras podem confiar nas informações fornecidas pelo expedidor nas instruções de transporte . A exigência de que a numeração do lacre seja impressa eletronicamente no conhecimento de embarque (BOL) ou em outros documentos de exportação protege contra modificações no lacre e alterações nos documentos pertinentes para que combinem com o número do novo lacre. No entanto, para algumas cadeias de abastecimento, as mercadorias poderão ser examinadas em trânsito por uma autoridade alfandegária estrangeira ou pelo CBP. Uma vez que o lacre tenha sido rompido por autoridades governamentais, deve haver um processo para registrar a numeração do novo lacre afixado ao IIT depois do exame da carga. Em alguns casos, isso pode ser escrito à mão.	Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório /Recomendado
7.23	Os membros da CTPAT devem ter procedimentos por escrito para relatar incidentes, o que inclui a descrição do processo de agravamento interno da instalação. Deve haver um protocolo de notificação para relatar atividades suspeitas ou incidentes de segurança (como apreensão de drogas, descoberta de um passageiro clandestino, etc.) que ocorram em qualquer lugar do mundo e afetem a segurança da cadeia de abastecimento do membro. Quando for aplicável, o membro deve relatar incidentes globais ao seu especialista em segurança de cadeia de abastecimento, ao porto de entrada mais próximo, às autoridades policiais relevantes, e aos parceiros comerciais que possam fazer parte da cadeia de abastecimento afetada. O CBP deve ser notificado assim que possível e antes que o veículo ou IIT cruze a fronteira. Os procedimentos de notificação devem incluir informações de contato precisas com nome e telefone do pessoal a ser notificado, assim como das autoridades policiais. Os procedimentos devem ser revistos periodicamente para garantir que as informações de contato estejam corretas.	Exemplos de incidentes que justificam uma notificação ao Serviço de Alfândegas e Proteção de Fronteiras dos EUA incluem (entre outros) os seguintes: • Descoberta de adulteração em um contêiner/IIT ou em um lacre de alta segurança; • Descoberta de um compartimento escondido em um veículo ou IIT; • Um novo lacre desconhecido foi colocado no IIT; • Contrabando, inclusive de pessoas ou passageiros clandestinos; • Entrada não autorizada em veículos, locomotivas, embarcações ou porta-aviões; • Extorsão, pagamento de proteção, ameaças e/ou intimidação; • Uso não autorizado da identificação de pessoa jurídica, como número de Importador de Registro (sigla em inglês IOR), código de Transportadora Padrão Alpha (sigla em inglês SCAC), etc.	Obrigatório
7.24	Deve haver procedimentos para identificar, questionar e lidar com pessoas não autorizadas/não identificadas. Os funcionários devem conhecer o protocolo para questionar pessoas não autorizadas/ não identificadas, como responder a esse tipo de situação, e familiarizar-se com os procedimentos de remoção de indivíduos não autorizados das instalações.		Obrigatório
7.25	Os membros da CTPAT devem estabelecer um mecanismo para relatar anonimamente questões relativas a segurança. Ao se receber uma alegação, esta deve ser investigada, e, quando for o caso, devem ser adotadas medidas corretivas.	Problemas internos, como roubo, fraude e conspirações internas, podem ser relatados com maior prontidão quando a parte que faz a denúncia sabe que tem anonimidade. Os membros podem estabelecer um programa de linha direta ou	Recomendado

ID	Critérios	Diretrizes para implementação	Obrigatório /Recomendado
		um mecanismo semelhante que permita manter a anonimidade das pessoas, caso temam represálias por suas ações. Recomenda-se que as denúncias sejam guardadas como evidência para documentar que cada item relatado foi investigado e que foram adotadas medidas corretivas.	
7.27	É obrigatório investigar e resolver todas as coisas que faltam, os excedentes e outras discrepâncias ou anomalias significativas, conforme for adequado.		Obrigatório
7.28	A carga de entrada deve ser comparada às informações no manifesto de carga. A carga de saída deve ser comparada às ordens de compra ou de entrega.		Recomendado
7.29	A numeração dos lacres designada a transportes específicos deve ser transmitida ao consignatário antes da saída.		Recomendado
7.30	A numeração dos lacres deve ser impressa eletronicamente no conhecimento de embarques ou em outros documentos de expedição.		Recomendado
7.37	Depois de um incidente significativo, os membros devem fazer uma análise pós-incidente assim que tomarem conhecimento do incidente para determinar se a cadeia de abastecimento não foi comprometida. Essa análise não pode impedir ou interferir em investigações conhecidas sendo realizadas por autoridades policiais do governo. As conclusões da análise pós-incidente da empresa devem ser documentadas, concluídas o quanto antes, e, caso seja permitido pelas autoridades policiais, estar disponível, ao ser solicitada, para especialistas em cadeias de abastecimento (sigla em inglês, SCSS).	Um incidente de segurança é uma violação na qual medidas de segurança foram contornadas, evitadas ou violadas, e que resultou ou resultará em um ato criminoso. Incidentes de segurança incluem terrorismo, contrabando (narcóticos, seres humanos, etc.) e a presença de passageiros clandestinos.	Obrigatório

8. <u>Segurança agrícola</u> — A a agricultura é a maior indústria e o maior setor de empregos dos EUA. Também é o setor mais ameaçado pela introdução de animais exóticos e contaminantes de plantas, como solo, esterco, sementes e material vegetal ou animal que pode abrigar pragas e doenças invasivas e destrutivas. A eliminação de contaminantes em todos os veículos e em todos os tipos de carga pode reduzir a retenção da carga pelo CBP, atrasos, ou devolução e tratamento de produtos. Garantir a conformidade com os requisitos da CTPAT para a agricultura também ajudará a proteger esse importante setor dos EUA e o abastecimento global de alimentos.

Definição-chave: contaminação por pragas — A Organização Marítima Internacional define a contaminação por pragas como formas visíveis de animais, insetos ou outros invertebrados (vivos ou não, em qualquer estágio do ciclo de vida, incluindo cascas de ovos ou ovas), ou qualquer material orgânico de origem animal (incluindo sangue, ossos, pelos, carne, secreções, excreções); plantas viáveis ou não, ou produtos vegetais (incluindo frutas, sementes, folhas, gravetos, raízes, casca de árvore); ou outros materiais orgânicos, incluindo fungos; ou solo ou água, quando tais produtos não fizerem parte do manifesto de carga encontrado dentro dos instrumentos de tráfego internacional (ou seja, contêineres, dispositivos de carga unitária, etc.).

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomendado
8.1	Os membros da CTPAT devem, de acordo com o seu modelo de negócios, contar com procedimentos por escrito destinados a evitar a contaminação visível por pragas, incluindo os regulamentos para Materiais de Embalagem de Madeira (sigla em inglês WPM). As medidas de prevenção contra pragas visíveis devem ser cumpridas em toda a cadeia de abastecimento. Medidas que dizem respeito a WPM devem respeitar os padrões internacionais de Medidas Fitossanitárias nº	Os WPM são definido como madeira ou produtos de madeira (excluídos produtos de papel) usados para o suporte, proteção, ou transporte de uma mercadoria. Os WPM incluem itens como paletes, caixotes, caixas, carretéis e calços de madeira. Esses produtos são feitos frequentemente de madeira *in natura,* que pode não ter passado por processamento ou tratamento suficiente para remover ou eliminar pragas, continuando a ser uma via de introdução e de disseminação de pragas, principalmente os calços de madeira, que costumam apresentar um alto risco de introdução e disseminação de pragas. A CIPV é um tratado multilateral supervisionado pela Organização das Nações Unidas para a Alimentação e Agricultura, cujo objetivo é garantir ações coordenadas e eficazes para evitar e controlar a introdução e disseminação de pragas e contaminantes. O ISPM 15 inclui medidas internacionalmente aceitas que podem ser aplicadas aos WPM para reduzir significativamente o risco de introdução e disseminação da maioria das pragas associadas a WPM. O ISPM 15 abrange todos os materiais de embalagem em madeira, exigindo que sejam desembarcados e a seguir sejam tratados termicamente ou fumigados com brometo de metila, e carimbados com a marca de conformidade da CIPV. Essa marca de conformidade é comumente conhecida como "*wheat stamp*". Produtos isentos de ISPM 15 são feitos de materiais alternativos como papel, metal, plástico ou painéis	Obrigatório

ID	Critérios	Diretrizes para implementação	Obriga-tório/ Reco-mendado
	15 (ISPM 15) da Convenção Internacional para a Proteção dos Vegetais (CIPV).	de madeira (como painéis de madeira orientada [sigla em inglês OSB], chapa de fibra de alta densidade e madeira compensada).	

Terceira Área de Enfoque: Segurança Pessoal e Física

9. <u>Segurança física</u> — É obrigatório que as instalações de armazenamentoo e manuseio de carga, áreas de armazenamento de instrumentos de tráfego internacional e instalações em que se prepare a documentação de importação/exportação em localidades domésticas ou internacionais disponham de barreiras físicas e obstáculos para proteção contra o acesso não autorizado.
A flexibilidade é um dos pilares da CTPAT, e os programas de segurança devem ser adaptados às circunstâncias de cada empresa. As necessidades de segurança física podem variar bastante dependendo do papel do membro na cadeia de abastecimento, do seu modelo de negócios e do nível de risco.
Os critérios de segurança física oferecem um número de barreiras ou obstáculos que ajudam a evitar o acesso não justificado a cargas, equipamentos sensíveis e/ou informações, e os membros devem usar essas medidas de segurança em toda a sua cadeia de abastecimento.

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomendado
9.1	É obrigatório que todas as instalações onde a carga seja manuseada ou armazenada, incluindo os pátios dos trailers e escritórios, tenham barreiras físicas e/ou obstáculos para evitar o acesso não autorizado.		Obrigatório
9.2	A cerca do perímetro deve encerrar as áreas em torno das instalações de manuseio e armazenamento de cargas. Se houver manuseio de carga em uma instalação, deve ser usada cerca interior para proteger a carga e as áreas de seu manuseio. Dependendo do risco, uma cerca adicional interior deve separar diferentes tipos de carga, como carga doméstica, internacional, de alto valor e/ou materiais perigosos. A cerca deve ser inspecionada com frequência por um funcionário escolhido para verificar a sua integridade ou a existência de danos. Caso haja danos na cerca, devem ser feitos reparos o quanto antes.	Outras barreiras aceitáveis podem ser usadas em vez de uma cerca, como uma parede divisória ou recursos naturais impenetráveis, tais como penhascos ou matagais fechados.	Recomendado
9.4	Os portões de entrada/saída de veículos e/ou funcionários (como também outros pontos de egresso) precisam ser vigiados ou monitorados. Indivíduos e veículos podem estar sujeitos a buscas de acordo com as leis locais e trabalhistas.	Recomenda-se que o número de portões seja o mínimo necessário para acesso e segurança adequados. Outros pontos de egresso seriam as entradas sem portões às instalações.	Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomendado
9.5	Deve ser proibido o estacionamento de veículos particulares de passageiros dentro ou perto da área de manuseio ou armazenamento de carga e dos veículos.	Os estacionamentos devem ser localizados fora das áreas cercadas e/ou operacionais — ou, ao menos, a uma distância razoável das áreas de manuseio ou armazenamento de carga.	Recomendado
9.6	É essencial haver iluminação adequada dentro e fora das instalações, inclusive, quando for o caso, nas seguintes áreas: entradas e saídas, áreas de manuseio e armazenamento de carga, perímetro da cerca e estacionamentos.	Temporizadores automáticos ou sensores de luz que acendam automaticamente as luzes de segurança são acessórios úteis em sistemas de iluminação.	Obrigatório
9.7	Devem ser utilizadas tecnologias de segurança para monitorar as instalações e evitar o acesso não autorizado a áreas sensíveis.	A tecnologia eletrônica de segurança usada para proteger/monitorar áreas sensíveis inclui: sistemas de alarme contra arrombamento (perímetro e interior), também conhecidos como sistemas de detecção de intrusos (sigla em inglês IDS); dispositivos para controle do acesso; e sistemas de vigilância por vídeo (VSS), incluindo câmeras de circuito fechado de televisão (CCTV). Um sistema CCTV/VSS pode incluir componentes como câmeras análogas (tipo coaxial), câmeras (tipo em rede) IP, dispositivos de gravação e software de gerenciamento de vídeo. Entre as áreas seguras ou sensíveis, que podem se beneficiar da vigilância por vídeo, estão: áreas de manuseio e armazenamento de carga; áreas de expedição ou recebimento em que são guardados documentos de importação; servidores de TI; pátios e áreas de armazenamento de instrumentos de tráfego internacional (IIT); áreas em que os IIT são inspecionados; e áreas de armazenamento de lacres.	Recomendado
9.8	Os membros que dependem de tecnologias de segurança para segurança física devem contar com políticas e procedimentos por escrito governando o uso, manutenção e proteção dessas tecnologias. É essencial que, no mínimo, essas políticas e procedimentos estipulem que: • O acesso às localidades onde a tecnologia é controlada ou	A tecnologia de segurança deve ser testada com regularidade para garantir o seu funcionamento adequado. Há diretrizes gerais a serem seguidas: • Teste os sistemas de segurança depois de serviços de manutenção e durante e depois de grandes reparos, modificações ou inclusão de anexos a um prédio ou instalação. Um componente do sistema pode ter sido comprometido, intencional ou acidentalmente.	Obrigatório

ID	Critérios	Diretrizes para implementação	Obriga-tório/ Reco-mendado
	administrada esteja limitado a funcionários autorizados; • Sejam implementados procedimentos para testar/inspecionar a tecnologia com regularidade; • As inspeções incluam verificações do funcionamento adequado do equipamento, e, quando for o caso, do seu posicionamento correto; • Os resultados das inspeções e dos testes de desempenho sejam documentados; •Quando correções são necessárias, sejam implementadas o quanto antes e sejam documentadas; • Os resultados documentados dessas inspeções sejam guardados durante tempo suficiente para auditorias. Caso seja usada uma central de monitoramento (externa) terceirizada, os membros da CTPAT devem contar com procedimentos por escrito que estipulem a funcionalidade de sistemas críticos e de protocolos de autenticação, como (entre outros) modificações em códigos de segurança, adição ou remoção de funcionários autorizados, revisões de senha e acesso ou recusa de acesso a sistemas. É obrigatório rever políticas e procedimentos de tecnologia de segurança anualmente, ou com mais frequência, conforme riscos e circunstâncias.	• Teste os sistemas de segurança depois de modificações de grande porte aos serviço de telefone ou internet. Qualquer coisa que possa afetar a capacidade do sistema de se comunicar com o centro de monitoramento deve ser duplamente verificada. • Assegure-se de que as configurações de vídeo, como gravações ativadas por movimento, alertas de detecção de movimento, imagens por segundo (IPS) e nível de qualidade, tenham sido configuradas de maneira adequada. • Assegure-se de que as lentes das câmeras (ou os domos que protegem as câmeras) estejam limpas e em foco. A visibilidade não pode ser limitada por obstáculos ou luzes brilhantes. • Realize teste para garantir que as câmeras de segurança estejam posicionadas corretamente e assim se mantenham (as câmeras podem ter sido movidas deliberada ou acidentalmente).	
9.9	Os membros da CTPAT devem utilizar recursos licenciados/certificados ao considerar o projeto e a instalação de tecnologia de segurança.	A atual tecnologia de segurança é complexa e muda rapidamente. Muitas vezes as empresas compram a tecnologia de segurança errada, que acaba sendo ineficaz quando precisam dela, e/ou pagam mais do que necessário. A procura de ajuda qualificada auxilia o	Reco-men-dado

ID	Critérios	Diretrizes para implementação	Obriga-tório/ Reco-mendado
		comprador a escolher a opção certa de tecnologia para suas necessidades e seu orçamento. Segundo a Associação Nacional de Prestadores de Serviços Elétricos (NECA, sigla em inglês), 33 estados dos EUA atualmente exigem licença para profissionais que trabalham com a instalação de sistemas de segurança e alarme.	
9.10	É essencial proteger fisicamente a infrastrutura de tecnologia de segurança contra acesso não autorizado.	A infraestrutura de tecnologia de segurança inclui computadores, software de segurança, painéis de controle eletrônico, vigilância por vídeo ou câmeras de televisão de circuito fechado, componentes elétricos e disco rígido para câmeras e gravação.	Obriga-tório
9.11	Os sistemas de tecnologia de segurança devem ser configurados com uma fonte de energia alternativa que permita a continuação do funcionamento do sistema caso haja uma interrupção inesperada da fonte direta.	Um criminoso que esteja tentando violar a sua segurança pode tentar cortar a eletricidade para os sistemas de tecnologia de segurança a fim de contorná-los. Sendo assim, é importante ter uma fonte de energia alternativa para eles, que pode ser um gerador auxiliar ou baterias sobressalentes. Geradores sobressalentes também podem ser usados para outros sistemas críticos, como a iluminação.	Reco-men-dado
9.12	Quando se usam sistemas de câmeras, elas devem monitorar as instalações e áreas sensíveis para coibir o acesso não autorizado. Alarmes devem ser usados para alertar uma empresa sobre o acesso não autorizado a áreas sensíveis.	Áreas sensíveis, quando for o caso, podem incluir áreas de manuseio e armazenamento de cargas, áreas de expedição/recebimento em que são guardados documentos importantes, servidores de TI, pátios e áreas de armazenamento de instrumentos de tráfego internacional (IIT), áreas em que os IIT são inspecionados, e áreas de armazenamento de lacres.	Reco-men-dado
9.13	Quando se usam sistemas de câmera , elas devem ser posicionadas de modo a cobrir as áreas-chave das instalações ligadas ao processo de importação/exportação. As câmeras devem ser programadas para gravação com a melhor qualidade possível de imagem disponível, configuradas para gravar vinte e quatro horas por dia, sete dias por semana.	O posicionamento correto das câmeras é importante para gravar o quanto possível a “cadeia de custódia” física dentro do controle das instalações. Segundo os riscos, as áreas ou processos mais importantes podem incluir o manuseio e armazenamento de carga; expedição/ recebimento; processo de carregamento; processo de lacre;	Obriga-tório

ID	Critérios	Diretrizes para implementação	Obriga-tório/ Reco-mendado
		chegada/saída de veículos; servidores de TI; inspeção de contêineres (de segurança e agrícola); armazenamento dos lacres; e qualquer outra área relativa à proteção de transportes internacionais.	
9.14	Quando se usam sistemas de câmeras, elas devem dispor de um recurso de alarme/notificação que indique se houver falha de operação ou de gravação.	Uma falha no sistema de vigilância por vídeo pode ocorrer quando alguém desativa o sistema a fim de violar uma cadeia de abastecimento sem deixar evidências do crime em vídeo. O recurso de falha de operação pode resultar no envio de uma notificação eletrônica a pessoa(s) pré-estabelecida(s), notificando-a(s) de que o dispositivo exige atenção imediata.	Reco-men-dado

ID	Critérios	Diretrizes para implementação	Obriga-tório/ Reco-mendado
9.15	Quando se usam sistemas de câmeras, devem ser realizadas revisões periódicas e aleatórias das gravações (pela gerência, segurança ou outro funcionário com essa atribuição) para verificar se os procedimentos de segurança da carga estão sendo adequadamente cumpridos de acordo com a lei. Os resultados das revisões devem ser resumidos por escrito de modo a incluir as correções realizadas. Os resultados devem ser guardados durante tempo suficiente para a realização de auditorias.	Se as gravações forem examinadas apenas quando houver razão para tanto (como parte de uma investigação depois de uma violação da segurança, etc.), o benefício pleno do uso das câmeras não será aproveitado. As câmeras não são meras ferramentas de investigação. Ao serem usadas de maneira proativa, podem ajudar a evitar que ocorra uma violação de segurança. Concentre a revisão aleatória nas gravações da cadeia de custódia física para verificar se o transporte permaneceu seguro e se todos os protocolos de segurança foram seguidos. Alguns exemplos de processos que podem ser revistos são os seguintes: • Atividades de manuseio da carga; • Inspeções dos contêineres; • Processo de carregamento; • Processo de lacre; • Chegada/saída de veículos; e • Saída da carga, etc. **Objetivo da revisão:** O objetivo da revisão é avaliar a adesão e eficácia gerais dos processos de segurança estabelecidos, identificar brechas ou pontos fracos, e estabelecer medidas corretivas que apoiem a melhoria dos processos de segurança. Com base nos riscos, (incidentes anteriores ou relatos anônimos sobre funcionários que não seguiram protocolos de segurança no cais de carga, etc.), o membro pode determinar revisões periódicas. **Itens a serem incluídos no resumo por escrito**: • Data da revisão; • Data das gravações que foram examinadas; • A partir de que câmeras/áreas estava sendo feita a gravação; • Breve descrição do que foi descoberto; e • Quando justificável, medidas corretivas.	Obriga-tório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomendado
9.16	Quando se usam câmeras, as gravações de áreas-chave dos processos de importação/exportação dos transportes monitorados devem ser guardadas durante tempo suficiente para que a investigação seja concluída.	Se ocorrer uma violação, deve-se realizar uma investigação, e é de suma importância que a gravação relativa ao empacotamento (para exportação) e os processos de carregamento/lacre seja guardada a fim de descobrir em que ponto a cadeia de abastecimento foi comprometida. Para o monitoramento, o programa da CTPAT recomenda a alocação de pelo menos 14 dias depois da chegada de uma carga no seu primeiro ponto de distribuição. É quando o contêiner é aberto pela primeira vez depois de ser liberado na alfândega.	Recomendado

10. **Controles do acesso físico —** O controle do acesso evita a entrada não autorizada em instalações/áreas, ajuda a manter o controle de funcionários e visitantes e protege os bens da empresa. O controle do acesso inclui a identificação positiva de todos os funcionários, visitantes, prestadores de serviço e vendedores em todos os pontos de entrada.

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomendado
10.1	Os membros da CTPAT devem ter procedimentos por escrito para determinar como os crachás de identificação e dispositivos de acesso são concedidos, modificados e removidos. Quando for o caso, um sistema de identificação de funcionários deve ser usado para identificação positiva e controles de acesso. O acesso a áreas sensíveis deve ser restringido com base na descrição do cargo ou deveres atribuídos. A remoção de dispositivos de acesso deve ocorrer quando um funcionário deixar a empresa.	Dispositivos de acesso incluem crachás de identificação de funcionários, crachás temporários para visitantes e vendedores, sistemas de identificação biométrica, cartões-chave de proximidade, códigos e chaves. Quando um funcionário deixa a empresa, o uso de listas de verificação de saída ajuda a garantir que todos os dispositivos de acesso tenham sido devolvidos e/ou desativados. No caso de empresas menores, onde todos se conhecem, não é necessário haver um sistema de identificação. Em geral, em uma empresa com mais de 50 funcionários, é necessário um sistema de identificação.	Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomendado
10.2	Visitantes, vendedores e prestadores de serviço devem apresentar um documento de identidade com foto ao chegar, devendo ser mantido um registro com os detalhes da visita. Todos os visitantes devem ser acompanhados. Além disso, todos os visitantes e prestadores de serviço devem receber uma identificação temporária. Quando usada, a identificação temporária deve permanecer visível o tempo todo durante a visita. O registro deve incluir o seguinte: • Data da visita; • Nome do visitante; • Verificação do documento de identidade com foto (como carteira de motorista ou carteira de identidade nacional). Frequentemente, visitantes conhecidos, como vendedores, podem passar sem a identificação por foto, mas, mesmo assim, ainda precisam ser registrados ao chegar e sair do local; • Hora de chegada; • Ponto de contato na empresa; e • Hora de saída.		Obrigatório
10.3	Motoristas que entregam ou recebem cargas devem ser positivamente identificados antes do recebimento ou liberação da carga. O motorista deve apresentar ao funcionário que lhe dará acesso um documento de identidade com foto emitido pelo governo para verificação da sua identidade. Se a apresentação de um documento de identidade com foto emitido pelo governo não for possível, o funcionário da empresa pode aceitar uma forma reconhecível de identificação com foto emitida pela transportadora viária que emprega o motorista.		Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomendado
10.4	Deve-se manter um registro de coleta da carga com anotações sobre o motorista e os detalhes do seu veículo quando a carga for entregue. Quando o motorista chega para receber a carga, um funcionário da empresa deve registrar sua chegada, fazendo o mesmo quando partir. O registro de cargas deve ser mantido em segurança, e os motoristas não podem ter acesso a ele. O registro de coleta da carga deve conter os seguintes itens: • Nome do motorista; • Data e hora de chegada; • Funcionário; • Número do caminhão; • Número do trailer; • Hora de partida; • Numeração do lacre afixado à carga na hora da partida.	O registro de visitantes pode funcionar como registro de cargas, contanto que as informações adicionais sejam anotadas.	Obrigatório
10.7	Antes da chegada, a transportadora deve notificar as instalações da empresa sobre o horário aproximado de chegada para a coleta agendada da carga, dando o nome do motorista e o número do caminhão. Quando for operacionalmente viável, os membros da CTPAT devem permitir apenas entregas e recepções agendadas.	Esse critério ajuda expedidores e transportadoras a evitar coletas fictícias. Coletas fictícias são esquemas criminosos que resultam em roubo de carga devido a embustes que incluem uso de identificação falsa pelo motorista e/ou empresas falsas criadas com o objetivo de roubar a carga. Quando uma transportadora usa os mesmos motoristas para pegar mercadorias em um empresa, é aconselhável que a empresa mantenha uma lista dos motoristas com fotos. Assim, quando não for possível avisar a empresa sobre o motorista que fará a coleta, a empresa tem como verificar se o motorista está aprovado para coletar carga nessas instalações.	Recomendado
10.8	Deve-se verificar periodicamente se não há contrabando nos pacotes e na correspondência antes de serem aceitos.	Exemplos de contrabando incluem, entre outros, explosivos, drogas ilícitas e dinheiro.	Recomendado

ID	Critérios	Diretrizes para implementação	Obriga-tório/ Reco-mendado
10.10	Quando se trabalha com guardas de segurança, as instruções que eles precisam seguir devem estar por escrito em políticas e procedimentos. A gerência deve verificar periodicamente o cumprimento e adequação desses procedimentos por meio de auditorias e revisões das políticas.	Embora se possa trabalhar com guardas em qualquer instalação, eles costumam ser empregados em fábricas, portos marítimos, centros de distribuição, pátios de armazenamento de instrumentos de tráfego internacional, consolidadores e locais de operação de despacho.	Obriga-tório

11. <u>Segurança dos funcionários</u> — Os recursos humanos de uma empresa são um dos seus bens mais importantes, mas também podem ser o elo mais frágil na segurança. Os critérios nesta categoria se concentram em questões como triagem de funcionários e verificação antes da contratação.

Muitas violações na segurança são causadas por conspirações internas, em que um ou mais funcionários se organizam para contornar procedimentos de segurança a fim de permitir infiltração na cadeia de abastecimento. Sendo assim, os membros devem ser diligentes na verificação da fidedignidade e confiabilidade de funcionários que ocupam cargos sensíveis. Os funcionários que ocupam esses cargos podem trabalhar diretamente com a carga ou sua documentação, bem como funcionários que controlam o acesso a áreas ou equipamentos sensíveis. Esses cargos incluem, entre outros, despacho, recebimento, pessoal de correspondência, motoristas, despachantes, guardas de segurança e qualquer indivíduo que trabalhe diretamente com distribuição de cargas, rastreio de veículos, e/ou controle de lacres.

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomen-dado
11.1	Deve haver processos escritos para a triagem de futuros funcionários e a verificação periódica dos funcionários atualmente contratados. Informações em solicitações de emprego, tais como histórico profissional e referências, devem ser verificadas antes da contratação, na medida do possível e dentro dos limites legais.	A CTPAT entende que as leis trabalhistas e de privacidade em certos países podem não permitir que todas as informações na solicitação de emprego sejam verificadas. No entanto, deve-se usar de devida diligência para verificar estas informações sempre que for permitido.	Obriga-tório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomen-dado
11.2	De acordo com os limites legais aplicáveis e a disponibilidade de bancos de dados de fichas criminais, deve-se averiguar os antecedentes do funcionário. Segundo o nível de segurança do cargo, as exigências de verificação em relação aos funcionários devem se estender também a trabalhadores temporários e empreiteiros. Depois de contratados, os funcionários devem passar por investigações periódicas quando houver motivos, e/ou devido ao nível de segurança do cargo. A averiguação dos antecedentes do funcionário deve incluir a sua identidade e ficha criminal, abrangendo bancos de dados municipais, estaduais e federais. Os membros da CTPAT e seus parceiros comerciais devem levar em consideração os resultados das averiguações de antecedentes, em conformidade com os estatutos locais, ao tomar decisões sobre contratações. As averiguações de antecedentes não se limitam à verificação da identidade e das fichas criminais. Em áreas de maior risco, investigações mais aprofundadas podem ser justificadas.		Reco-mendado
11.5	É essencial que os membros da CTPAT tenham um código de conduta dos funcionários que inclua expectativas e defina comportamentos aceitáveis. O código de conduta precisa incluir penalidades e processos disciplinares. Funcionários/ empreiteiros terceirizados devem confirmar que leram e entenderam o código de conduta por meio de assinatura, e essa confirmação deve ser guardada como documentação no arquivo sobre o funcionário.	O código de conduta ajuda a proteger a sua empresa e informa os funcionários sobre as suas expectativas. O seu objetivo é desenvolver e manter um padrão de conduta que seja aceitável para a empresa, ajudando-a a desenvolver uma imagem profissional e estabelecer uma cultura ética robusta. Até mesmo uma empresa de pequeno porte precisa de um código de conduta, que, no entanto, não precisa ser excessivamente elaborado nem conter informações complexas.	Obrigatório

12. <u>Formação, treinamento e conscientização</u> — Os critérios de segurança da CTPAT são elaborados de modo a formar a base de um sistema de segurança em várias etapas. Quando uma etapa é ultrapassada, uma outra deve prevenir uma violação da segurança, ou alertar a empresa sobre a violação. A implementação e manutenção de um programa de segurança em etapas exige a participação ativa e o apoio de vários departamentos e funcionários.

Um dos aspectos-chave para a manutenção de um programa de segurança é o treinamento. A educação dos funcionários sobre quais são as ameaças e sobre o quanto o seu papel é importante na proteção da cadeia de abastecimento da empresa é um aspecto significativo do êxito e da durabilidade de um programa de segurança da cadeia de abastecimento. Além do mais, quando o funcionário compreende a razão da existência dos procedimentos de segurança, a adesão a eles se torna muito mais fácil.

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomen-dado
12.1	Os membros devem estabelecer e manter um programa de treinamento e conscientização em segurança para reforçar o conhecimento sobre as vulnerabilidades da segurança em instalações, veículos e cargas em cada ponto da cadeia de abastecimento, as quais podem ser exploradas por terroristas ou contrabandistas. O programa de treinamento precisa ser abrangente e cobrir todos os requisitos de segurança da CTPAT. Funcionários em cargos sensíveis precisam fazer treinamento especializado adicional voltado para as responsabilidades de seus cargos. Um dos aspectos-chave do programa de segurança é o treinamento. A adesão dos funcionários às medidas de segurança é mais provável quando eles compreendem o porquê da sua existência. O treinamento em segurança deve ser oferecido com regularidade aos funcionários, conforme necessário, com base nas suas funções e cargos, e os funcionários recém-contratados precisam receber esse treinamento como parte da orientação/ habilitação para o trabalho. Os membros devem reter as evidências de treinamento, como os registros de treinamento, assinatura em folhas de chamada (lista),	Entre os tópicos de treinamento incluem-se proteção dos controles de acesso, reconhecimento de conspirações internas, e procedimentos para relatar atividades suspeitas e incidentes de segurança. Sempre que possível, o treinamento especializado deve incluir uma demonstração prática. Ao fazer uma demonstração prática, o instrutor deve dar tempo para que os alunos demonstrem o processo. Para os propósitos da CTPAT, cargos sensíveis incluem os dos funcionários que trabalham diretamente com carga de importação/exportação ou sua documentação, e os dos funcionários envolvidos no controle de acesso a áreas ou equipamento sensíveis. Esses cargos incluem, entre outros, despacho, recebimento, pessoal de correspondência, motoristas, despachantes, guardas de segurança e qualquer indivíduo que trabalhe diretamente com distribuição de cargas, rastreio de veículos, e/ou controle de lacres.	Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomen-dado
	ou registros eletrônicos de treinamento. Esses registros devem incluir a data, o nome dos participantes e os tópicos cobertos.		

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomen-dado
12.2	Os motoristas e outros funcionários que fazem inspeções de segurança e agrícolas de veículos e instrumentos de tráfego internacional (IIT) vazios devem ser treinados para fazer a inspeção dos veículos/IIT tendo em mente questões de segurança e agrícolas. Periodicamente, deve ser realizado treinamento de atualização, conforme necessário, depois de um incidente ou violação da segurança, ou quando houver modificações nos procedimentos da empresa. O treinamento para inspeções deve incluir os seguintes tópicos: • Sinais de compartimentos escondidos; • Contrabando escondido em compartimentos normais; e • Sinais de contaminação por pragas.		Obrigatório
12.4	Os membros da CTPAT devem contar com medidas para verificar se o treinamento oferecido atende todos os seus objetivos.	Compreender o treinamento e ser capaz de utilizá-lo no cargo específico (para funcionários em cargos sensíveis) é de extrema importância. Exames ou testes, exercícios/treinos simulados ou procedimentos regulares de auditoria, etc. são algumas das medidas que o membro pode implementar para determinar a eficácia do treinamento.	Reco-mendado
12.8	Quando for o caso, com base nos seus cargos e/ou funções, os funcionários devem receber treinamento sobre as políticas e procedimentos de cibersegurança da empresa. Este treinamento deve incluir a necessidade de o funcionário proteger as suas palavras-senha/frases-senha e o acesso ao computador.	Treinamento de qualidade é importante para reduzir a vulnerabilidade a ciberataques. Um programa robusto de treinamento em cibersegurança geralmente é fornecido aos funcionários relevantes em ambientes adequados e não simplesmente mediante e-mails ou memorandos.	Obrigatório

ID	Critérios	Diretrizes para implementação	Obrigatório/ Recomen-dado
12.9	Os funcionários que operam ou gerenciam sistemas de tecnologia de segurança precisam receber treinamento em operação e manutenção nas suas áreas específicas. Experiência anterior com sistemas semelhantes é aceitável. Auto-treinamento por meio de manuais operacionais e outros métodos é aceitável.		Obrigatório
12.10	Os funcionários devem ser treinados em como relatar incidentes de segurança e atividades suspeitas.	Procedimentos para relatar incidentes de segurança ou atividades suspeitas são aspectos extremamente importantes de um sistema de segurança. O treinamento em como relatar incidentes pode estar incluído no treinamento geral sobre segurança. Módulos de treinamento especializado (com base nos deveres do cargo) podem ser mais detalhados quanto aos procedimentos de relato, incluindo detalhes específicos sobre o processo, como, por exemplo, o que e a quem relatar o incidente, como relatá-lo, e o que fazer quando o relatório for concluído.	Obrigatório

Número de Publicação: 1077-0420