Transported Asset Protection Association

FSR 2026

TAPA Global Standard

Copyright © TAPA Not Copy

TAPA Americas

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

www.tapaonline.org

TAPA Asia Pacific

Oxley BizHub 2
62 Ubi Road 1, #06-11
Singapore 408734

www.tapa-apac.org

TAPA EMEA

Kanaalpark 140
2321 JV Leiden
The Netherlands

www.tapaemea.org

© TAPA 2026

Índice

1.0 Introducción 4

1.1 Finalidad de este documento FSR 4

1.2 Recursos para implementar el TAPA FSR 4

1.3 Protección de las políticas y procedimientos de los Proveedores de servicios logísticos(PSL) 4

2.0 Acerca de TAPA 5

2.1 Propósito de TAPA 5

2.2 La misión de TAPA 5

3.0 Normas TAPA 6

3.1 Normas de seguridad de TAPA 6

3.2 Implementación 6

4.0 Asesoramiento legal 7

4.1 Alcance 7

4.2 Traducción 7

4.3 La marca "TAPA" 7

4.4 Límites de responsabilidad 7

5.0 Contratos y subcontratación 8

5.1 Contratos 8

5.2 Subcontratación 8

5.3 Investigación y resolución de quejas de TAPA 8

6.0 Exenciones 9

7.0 Requisitos de seguridad de las instalaciones 10

S1. Requisitos generales 10

S2. Perímetro 12

2.1 Almacén, área de manipulación, envío y recepción de carga externa. 12
2.2 Barreras físicas 12
2.3 Áreas de muelle exteriores 13
2.4 Acceso para vehículos particulares 14

S3. Paredes exteriores, techo y puertas 15

3.1 Lados exteriores de la instalación: CCTV/VSS 15

3.2 Muros exteriores y techo 15

S4. Puntos de entrada y salida de oficinas y almacenes 18

4.1 Punto(s) de acceso para visitantes en la zona de oficinas 18
4.2 Punto(s) de entrada al mercado laboral 19
4.3 Identificación del conductor y del vehículo 19

S5. IDentro del almacén y la oficina 21

TAPA Copyright © Do Not Copy

5.1 Área de almacén: Paredes para múltiples inquilinos 21
5.2 Áreas internas del almacén 21
5.3 Puertas y áreas de muelle internas 22
5.4 Control de acceso entre la oficina y el muelle/almacén. 22
5.5 Área de carga de alto valor (HVC) 23
5.6 Inspección de basura del almacén 24
5.7 Precarga y preparación 24
5.8 Registros de contenedores personales y de salida 25
5.9 Control de equipos de manipulación de carga 25
5.10 Integridad del contenedor o remolque: inspección de 7 puntos 25
5.11 Proceso de entrega de mercancías; precintos de seguridad 26
5.12 Integridad de la carga; Proceso de validación de carga/descarga 27
5.13 Recogidas fraudulentas 27

S6. Sistemas de seguridad: diseño, monitoreo y respuesta 28
6.1 Puesto de vigilancia 28
6.2 Sistema de detección de intrusos (IDS) 28
6.3 Sistema de Control de Acceso Automático (AACS) 29
6.4 CCTV/VSS 30
6.5 Iluminación exterior e interior 31

S7. Capacitación y procedimientos 32
7.1 Procedimientos de escalamiento 32
7.2 Compromiso de la dirección 32
7.3 Capacitación 32
7.4 Acceso a los activos del comprador 33
7.5 Control de la información 33
7.6 Informe de incidentes de seguridad 33
7.7 Programas de mantenimiento 33
7.8 Orientación para contratistas 34
7.9 Registros de envío y recepción 34
7.10 Proceso de prealerta en marcha 35

S8. Integridad de la fuerza laboral 36
8.1 Selección/Verificación de antecedentes (según lo permita la legislación local) 36
8.2 Terminación o recontratación de la fuerza laboral 36

S9. Requisitos de la función central (solo aplicable para la certificación multisitio) .. 38
9.1 General 38
9.2 Políticas y procedimientos 39
9.3 Informe de auditoría de autoevaluación realizado para todos los sitios. 39
9.4 Registros de inspecciones, bitácoras (registros de visitantes/conductores), inspecciones de 7 puntos 40
9.5 Evaluación de riesgos de todos los sitios 40
9.6 Diseño del sistema de CCTV/VSS y alarma del sitio 40
9.7 Registros de alarmas y control de acceso 40
9.8 Registros de capacitación 41
9.9 Registros de selección/verificación 41
9.10 Revisión de la dirección para evaluar las autoauditorías; informes SCAR generados; pérdidas y robos; evaluaciones de riesgos. 41

8.0 Amenazas a la seguridad informática y cibernética: opción mejorada 43

E8. Requisitos obligatorios 43

TAPA Copyright © Do Not Copy

1.0 Introducción

1.1 Finalidad de este documento FSR

Este documento de Requisitos de Seguridad de Instalaciones (FSR, por sus siglas en inglés) es el estándar oficial de TAPA para el almacenamiento seguro. Se trata de un estándar global común que puede utilizarse en acuerdos comerciales y de seguridad entre compradores y proveedores de servicios logísticos (PSL) u otros solicitantes que busquen la certificación.

Al desarrollar este estándar, TAPA reconoce las múltiples diferencias en la prestación de servicios de almacenamiento a nivel global, regional e incluso dentro de las empresas, y que el FSR puede aplicarse a la totalidad o a parte de los servicios prestados por un PSL/solicitante. Dependiendo de la complejidad y el tamaño de la cadena de suministro, el cumplimiento de los estándares de TAPA puede lograrse mediante un único PSL/solicitante o mediante varios PSL/solicitantes y subcontratistas cualificados.

Alcance

TAPA ha desarrollado tres opciones para respaldar la certificación:

• Certificación de una sola sede por un organismo de auditoría independiente (IAB).

• Certificación de múltiples sedes por un IAB.

• Autocertificación por auditores autorizados (AA) por parte del proveedor de servicios lingüísticos (PSL)/solicitante o el IAB (realizando una autoauditoría en nombre del PSL/solicitante).

Audiencia

Entre los usuarios típicos de las Normas TAPA se incluyen:

• Compradores

• Proveedores de servicios logísticos(PSL)/Solicitantes

• Organismos encargados de la aplicación de la ley u otras organizaciones gubernamentales

• Organizaciones profesionales de la cadena de suministro

• Aseguradoras

1.2 Recursos para implementar el TAPA FSR

Los recursos necesarios para cumplir con los requisitos del FSR serán responsabilidad del PSL/Solicitante y correrán a cargo del PSL/Solicitante, a menos que el Comprador y el PSL/Solicitante negocien o acuerden lo contrario.

1.3 Protección de las políticas y procedimientos de los Proveedores de servicios logísticos (PSL)

Las copias de los documentos de políticas y procedimientos de seguridad solo se entregarán al Comprador de conformidad con los acuerdos de divulgación firmados entre el PSL/Solicitante y el Comprador, y se tratarán como información confidencial.

TAPA Copyright © Do Not Copy

2.0 Acerca de TAPA

2.1 Propósito de TAPA

El robo de mercancías es uno de los mayores desafíos para la cadena de suministro de los fabricantes de productos valiosos y de alto riesgo, así como para sus proveedores de servicios logísticos.

La amenaza ya no proviene únicamente de delincuentes oportunistas. Hoy en día, las redes de delincuencia organizada operan a nivel mundial y utilizan ataques cada vez más sofisticados contra vehículos, instalaciones y personal para lograr sus objetivos.

TAPA es un foro único que reúne a fabricantes globales, proveedores de logística, transportistas, organismos encargados de hacer cumplir la ley y otras partes interesadas con el objetivo común de reducir las pérdidas en las cadenas de suministro internacionales. El enfoque principal de TAPA es la prevención del robo mediante el uso de inteligencia en tiempo real y las medidas preventivas más avanzadas.

2.2 La misión de TAPA

La misión de TAPA es ayudar a proteger los activos de sus miembros minimizando las pérdidas de carga en la cadena de suministro. TAPA logra esto mediante el desarrollo y la aplicación de estándares de seguridad globales, prácticas reconocidas en la industria, tecnología, capacitación, análisis comparativo, colaboración regulatoria y la identificación proactiva de tendencias delictivas y amenazas a la seguridad de la cadena de suministro.

TAPA Copyright © Do Not Copy

3.0 Normas TAPA

3.1 Normas de seguridad de TAPA

Las siguientes Normas de Seguridad TAPA globales se han creado para garantizar el transporte y almacenamiento seguros de carga de alto valor susceptible de robo:

• Los Requisitos de Seguridad de Instalaciones (FSR) establecen las normas mínimas específicas para el almacenamiento seguro, o el almacenamiento en tránsito, dentro de una cadena de suministro.

• Los Requisitos de Seguridad para el Transporte por Carretera (TSR) se centran exclusivamente en el transporte por carretera y establecen las normas mínimas específicas para el transporte de productos por carretera dentro de una cadena de suministro.

• Las Normas de Ciberseguridad (CSS) tienen como objetivo proporcionar a las empresas una herramienta para comprender los requisitos mínimos de gestión de TI en las operaciones de su cadena de suministro, a fin de proteger los activos digitales contra ciberataques y fallos operativos.

Las Normas de Seguridad TAPA globales se revisan y actualizan cada tres años según sea necesario.

Este documento se centra únicamente en los requisitos de FSR.

• El proceso de certificación de TAPA FSR se documenta en el documento Marco de Certificación de TAPA FSR.

• Para obtener la certificación TAPA FSR, es necesario seguir las versiones vigentes tanto del documento TAPA FSR como del Marco de Certificación de TAPA FSR.

3.2 Implementación

La correcta aplicación de las Normas de Seguridad de TAPA depende de la colaboración entre los proveedores de servicios logísticos (PSL), los solicitantes, los compradores (propietarios de la carga) y los auditores autorizados de TAPA.

TAPA Copyright © Do Not Copy

4.0 Asesoramiento legal

4.1 Alcance

La FSR es una norma global, y todas las secciones de la norma son obligatorias a menos que se conceda una excepción mediante el proceso oficial de exención (véase la Sección 6 de la norma FSR y la Sección 7 del documento del marco de certificación FSR).

4.2 Traducción

En las zonas geográficas donde el inglés no es el idioma principal, y donde la traducción es necesaria y aplicable, es responsabilidad del proveedor de servicios lingüísticos/solicitante y sus agentes garantizar que cualquier traducción de las FSR, o de cualquiera de sus partes, refleje con precisión las intenciones de TAPA en el desarrollo y la publicación de estas Normas.

4.3 La marca "TAPA"

"TAPA" es una marca registrada de la Asociación para la Protección de Activos Transportados y no puede utilizarse sin la autorización expresa y por escrito de TAPA a través de sus regiones oficialmente reconocidas. Las normas TAPA y el material asociado son publicados por y a través de TAPA, y no pueden ser revisados, editados ni modificados por terceros sin la autorización expresa y por escrito de TAPA. El uso indebido de la marca TAPA puede conllevar la revocación de la certificación o acciones legales.

4.4 Límites de responsabilidad

Mediante la publicación de estas Normas, TAPA no ofrece garantía alguna de que se prevengan todos los robos de carga, independientemente de que las Normas se implementen y apliquen correctamente. Cualquier responsabilidad derivada del robo o la pérdida de carga almacenada, conforme a las Normas FSR, correrá a cargo del Proveedor de Servicios Logísticos (PSL)/Solicitante y/o del Comprador, de acuerdo con los términos y condiciones de su contrato y las leyes o normativas aplicables en la jurisdicción correspondiente.

TAPA Copyright © Do Not Copy

5.0 Contratos y subcontratación

5.1 Contratos

El transporte, almacenamiento y manejo seguros de los activos del Comprador son responsabilidad del Proveedor de Servicios Logísticos (PSL)/Solicitante, sus agentes y subcontratistas durante la recolección, el tránsito, el almacenamiento y la entrega, según lo especificado en el acuerdo o contrato.

Cuando se haga referencia al FSR o se incluya en el contrato entre el PSL/Solicitante y el Comprador, también deberá incluirse en el programa de seguridad del PSL/Solicitante.

El PSL proporcionará al Comprador la certificación FSR y, cuando corresponda, la evidencia de que se han cumplido los requisitos del FSR. Asimismo, cualquier presunto incumplimiento por parte del PSL/Solicitante de los requisitos del FSR se resolverá de acuerdo con los términos del contrato negociado entre el Comprador y el PSL/Solicitante.

5.2 Subcontratación

Al utilizar subcontratistas, debe existir un requisito contractual que exija que estos cumplan con todos los requisitos FSR indicados. Los auditores internos autorizados de PSL deben confirmar que el subcontratista cumple con los requisitos FSR del mismo nivel.

5.3 Investigación y resolución de quejas de TAPA

Si TAPA recibe una queja formal sobre el desempeño de un proveedor de servicios lingüísticos (PSL) certificado o solicitante, TAPA (previa validación) podrá exigir que el PSL o solicitante contrate una nueva auditoría a su cargo. Si el PSL o solicitante no supera la auditoría o se niega a cumplir con este proceso, su certificado podrá ser revocado.

TAPA Copyright © Do Not Copy

6.0 Exenciones

Una exención es una autorización por escrito que permite a una instalación eximirla de un requisito específico de TAPA y aceptar una solución de cumplimiento alternativa. Se puede solicitar una exención si un proveedor de servicios logísticos (PSL) o solicitante no puede cumplir con un requisito específico del FSR y justifica la adopción de medidas alternativas. Las exenciones son válidas durante el período de certificación.

TAPA Copyright © Do Not Copy

7.0 Requisitos de seguridad de las instalaciones

S1. Requisitos generales

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
1.1.1	Todos los procedimientos o políticas exigidos por esta Norma deben estar documentados y actualizados al menos cada dos años.	Ⓐ	Ⓑ	Ⓒ
1.1.2	La gerencia debe haber designado formalmente a una persona (AA) responsable de la seguridad en las instalaciones, quien se encargará de mantener el TAPA FSR, el cierre de SCARS, la evaluación de riesgos, el informe de gestión y los requisitos de seguridad de la cadena de suministro de la empresa. Otra persona (puede ser la misma) también será responsable de supervisar el programa FSR. Esto incluye programar controles de cumplimiento, comunicarse con los AA, recertificar, gestionar cambios en el estándar FSR, etc. Estas personas pueden ser empleados o personal subcontratado para desempeñar esta función.	Ⓐ	Ⓑ	Ⓒ
1.1.3	Se deben completar y documentar las auditorías internas (realizadas por un equipo multifuncional) del sistema de gestión de seguridad, los informes de autoevaluación de la AA interna y el cierre de SCARS.	Ⓐ	Ⓑ	Ⓒ
1.1.4	Se requiere un procedimiento, registro o plan de acceso para cerraduras físicas, tarjetas de acceso y llaves que gestionen y controlen las llaves físicas y electrónicas. El procedimiento debe incluir procesos para la duplicación, el almacenamiento y la gestión de llaves extraviadas o perdidas.	Ⓐ	Ⓑ	Ⓒ
1.1.5	Se debe realizar y actualizar al menos anualmente una evaluación de riesgos documentada que reconozca la probabilidad y el impacto de las amenazas relacionadas con la seguridad. La gerencia debe revisar y confirmar que los riesgos identificados han sido evaluados y que se han implementado los controles adecuados para mitigarlos o eliminarlos a un nivel aceptable. Como mínimo, se deben evaluar los siguientes eventos internos y externos comunes: robo de carga o información, acceso no autorizado a instalaciones o carga, manipulación o destrucción de sistemas de seguridad, recogidas ficticias de carga, continuidad de la seguridad durante la escasez de personal o desastres naturales, necesidad de barreras anticolisión para ventanas o puertas de muelle accesibles a nivel del suelo, etc. Se pueden considerar amenazas adicionales en función de los riesgos locales o del país.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
1.1.6	La persona encargada de realizar las auditorías internas o anuales para el solicitante/proveedor de servicios lingüísticos (denominado Auditor Asociado del Proveedor de Servicios Lingüísticos) debe estar capacitada. Esta persona puede ser la misma que se menciona en el apartado 1.1.2 o bien un profesional externo contratado para desempeñar esta función.	Ⓐ	Ⓑ	Ⓒ
1.1.7	Para comprender el FSR y ser capaces de implementar todos sus requisitos, todos los solicitantes/auditores autorizados de PSL deben haber realizado y aprobado el examen correspondiente al estándar TAPA y la versión que deben auditar.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S2. Perímetro

2.1 Almacén, área de manipulación, envío y recepción de carga externa.

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
2.1.1	El sistema de videovigilancia (CCTV) permite visualizar todo el tráfico en la zona externa de manipulación, envío y recepción de carga (incluidos los puntos de entrada y salida), garantizando que todos los vehículos y personas sean reconocibles en todo momento, salvo obstrucciones temporales debidas a necesidades operativas (por ejemplo, carga y descarga de camiones en tiempo real).	Ⓐ	Ⓑ	
2.1.2	La iluminación adecuada en las áreas de carga y descarga debe utilizarse como un elemento básico de disuasión contra delitos y para proporcionar la capacidad de visualizar las operaciones en estas áreas durante la noche. ***Nota**: La iluminación puede ser continua, activada por alarma, movimiento, detección de sonido, etc., con iluminación inmediata garantizada.*	Ⓐ	Ⓑ	Ⓒ
2.1.3	Debe existir un procedimiento que describa cómo se deben gestionar los vehículos y las personas no autorizadas dentro del área de manipulación, envío y recepción de carga externa. Se debe impartir instrucción sobre dicho procedimiento al personal pertinente, incluidos los guardias de seguridad.	Ⓐ	Ⓑ	Ⓒ
2.1.4	La manipulación de la carga, el envío y la zona de recepción deben estar debidamente controlados para evitar el acceso no autorizado.		Ⓑ	Ⓒ
2.1.5	Para ventanas o puertas de muelle accesibles a nivel del suelo, la Evaluación de Riesgos anual debe evaluar la necesidad de barreras anticolisión. Además, debe incluir la evaluación del uso de cubiertas para ventanas para evitar la observación no autorizada de los espacios interiores (véase Evaluación de Riesgos, req. 1.1.5).	Ⓐ		

TAPA Copyright © Do Not Copy

2.2 Barreras físicas

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
2.2.1	Una barrera física delimita la zona de manipulación, envío y recepción de carga.	Ⓐ		

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
2.2.2	La barrera física que rodea la zona de manipulación, envío y recepción de carga tiene una altura mínima de 1,8 metros (6 pies). ***Not**a: La barrera física, diseñada para impedir el acceso no autorizado, debe tener una altura de 1,8 metros (6 pies) en toda su longitud, incluyendo las zonas donde el nivel del suelo varía.*	Ⓐ		
2.2.3	La barrera física que rodea la zona de manipulación, envío y recepción de carga se mantiene en buen estado.	Ⓐ		
2.2.4	Las puertas dentro del área de manipulación, envío y recepción de carga cuentan con barreras atendidas por personal o controladas electrónicamente.	Ⓐ		
2.2.5	La barrera física que rodea la zona de manipulación, envío y recepción de carga se inspecciona para comprobar su integridad y detectar posibles daños al menos semanalmente.	Ⓐ		

TAPA Copyright © Do Not Copy

2.3 Áreas de muelle exteriores

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
2.3.1	Las zonas exteriores de los muelles están cubiertas mediante cámaras de videovigilancia/VSS exteriores a color o con función "día/noche".	Ⓐ	Ⓑ	Ⓒ
2.3.2	Se han instalado cámaras de CCTV/VSS para poder visualizar todas las operaciones y movimientos alrededor del área del muelle exterior en todo momento, salvo que exista una obstrucción temporal debido a necesidades operativas (por ejemplo, carga y descarga de camiones en tiempo real).	Ⓐ	Ⓑ	Ⓒ
2.3.3	Todos los vehículos y personas que se encuentren en las inmediaciones de las zonas de los muelles exteriores deben estar cubiertos por cámaras de CCTV/VSS, que puedan mostrar claramente la información de identificación del vehículo y discernir los rasgos faciales del personal.	Ⓐ		
2.3.4	Los vehículos y las personas que se encuentren en las inmediaciones de las zonas de los muelles exteriores deberán estar cubiertos y ser visibles mediante cámaras de CCTV/VSS en al menos el 75% de los casos en un plazo de un día.		Ⓑ	Ⓒ

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
2.3.5	Todas las zonas exteriores que rodean las puertas de los muelles de carga están completamente iluminadas.	Ⓐ	Ⓑ	Ⓒ

2.4 Acceso para vehículos particulares

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
2.4.1	Los vehículos particulares solo están autorizados a acceder a las zonas de manipulación, envío y recepción de carga si cuentan con la aprobación previa, de acuerdo con una política documentada.	Ⓐ	Ⓑ	Ⓒ
2.4.2	No hay zonas de aparcamiento privadas a menos de 25 m / 82 pies de distancia a pie de las zonas de muelles exteriores.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S3. Paredes exteriores, techo y puertas

3.1 Lados exteriores de la instalación: CCTV/VSS

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
3.1.1	Se ha instalado una cámara de videovigilancia exterior (CCTV/VSS) a color o con visión diurna/nocturna que cubre todos los lados exteriores de las instalaciones.	Ⓐ		
3.1.2	Se ha instalado un sistema de cámaras de videovigilancia (CCTV/VSS) exteriores a color o de "día/noche" que cubre los lados exteriores de las instalaciones con puertas, ventanas u otras aberturas.		Ⓑ	
3.1.3	Todas las imágenes del sistema de cámaras CCTV/VSS exteriores se ven nítidas en todo momento, salvo que exista una obstrucción temporal debido a necesidades operativas (por ejemplo, carga y descarga de camiones en tiempo real).	Ⓐ		
3.1.4	Todos los vehículos y personas que se encuentren en los alrededores de las instalaciones estarán cubiertos por cámaras de CCTV/VSS, que podrán mostrar claramente la información de identificación del vehículo y ser capaces de discernir los rasgos faciales del personal..	Ⓐ		
3.1.5	Las cámaras de videovigilancia/sistemas de vigilancia exterior permiten visualizar vehículos y personas en al menos el 75% de las grabaciones diarias.		Ⓑ	

3.2 Muros exteriores y techo

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
3.2.1	Las paredes exteriores y el techo deben construirse y mantenerse de manera que resistan la penetración y proporcionen una protección física robusta. Los materiales deben ofrecer suficiente resistencia y durabilidad para resistir intentos de entrada forzada. (Ejemplos: ladrillo, bloque de hormigón, paneles de hormigón prefabricado o paneles sándwich de alta resistencia con un espesor total de al menos 50 mm y placas internas y externas de 0,7 mm). *Nota: Cuando se utilicen materiales ligeros o no estructurales, deben implementarse medidas de mitigación adicionales (como malla de acero interna o sistemas de detección de intrusiones) para lograr un nivel de seguridad equivalente.*	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
3.2.2	Todas las ventanas que se puedan abrir, las rejillas de ventilación u otras aberturas en las paredes exteriores del edificio, o cualquier ventana sellada instalada a menos de 3 metros / 9 pies 10 pulgadas del piso de trabajo en las paredes exteriores del edificio, deben tener una barrera física o estar equipadas con una alarma y conectadas al sistema de alarma principal.	Ⓐ	Ⓑ	
3.2.3	Todas las ventanas practicables, claraboyas, rejillas de ventilación, escotillas de techo y cualquier otra abertura en el techo deben estar protegidas mediante: a) una barrera física robusta (por ejemplo, rejas de seguridad, barrotes o cubiertas reforzadas), o b) un dispositivo de detección de intrusiones integrado al sistema de alarma principal del edificio. ***Nota**: Las barreras físicas deben estar diseñadas para impedir su remoción o manipulación, y las aberturas con alarma deben activar alertas inmediatas ante cualquier acceso no autorizado.*	Ⓐ		
3.2.4	El acceso exterior a la azotea (escalera o escaleras) debe estar: Cerrado físicamente y protegido por CCTV/VSS (cámaras a color o de día/noche) O Cerrado físicamente y con alarma.	Ⓐ		
3.2.5	El acceso exterior a la azotea (escalera o escaleras) está bloqueado físicamente.		Ⓑ	Ⓒ
3.2.6	Todas las puertas peatonales exteriores de almacén y de oficinas de las instalaciones cuentan con alarmas para detectar aperturas no autorizadas y están conectadas al sistema de alarma principal. ***Nota:** Las puertas de muelle no están cubiertas por este requisito. Consulte el requisito 3.2.12 para conocer los requisitos de alarma para puertas de muelle.*	Ⓐ	Ⓑ	Ⓒ
3.2.7	Cada puerta exterior del almacén, puerta de oficina u otra abertura de la instalación debe estar identificada de forma única por puerta o por zona dentro del sistema de alarma principal.	Ⓐ		

TAPA Copyright © Do Not Copy

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
3.2.8	Todas las puertas exteriores del almacén permanecen cerradas y aseguradas cuando no están en uso. En los casos que corresponda, se requiere el uso de llaves o códigos.	Ⓐ	Ⓑ	
3.2.9	Las puertas y marcos peatonales exteriores de los almacenes no deben ser fácilmente penetrables. Si las bisagras están en el exterior, deben estar fijadas con pasadores o soldadas por puntos. Las puertas de almacén, ya sean totales o parciales, no son aceptables a menos que se instalen detectores de rotura de vidrio, o que otro dispositivo de detección local proporcione cobertura (por ejemplo, infrarrojos pasivos) y active la alarma directamente en el centro de monitoreo, o bien que el vidrio esté protegido con rejas o malla. TAPA permitirá a los titulares de certificaciones existentes que no puedan cumplir con este requisito, continuar con su configuración actual hasta la próxima revisión. Los nuevos titulares de certificados o las nuevas instalaciones deben cumplir con el nuevo requisito.	Ⓐ	Ⓑ	Ⓒ
3.2.10	Las salidas de emergencia que se utilizan exclusivamente para casos de emergencia (por ejemplo, salidas de incendios) están equipadas en todo momento con una alarma sonora individual o por zonas.	Ⓐ	Ⓑ	
3.2.11	Todas las puertas de los muelles de carga deben ser lo suficientemente resistentes como para disuadir o retrasar la entrada forzada mediante el uso de pequeñas herramientas manuales eléctricas o a batería.	Ⓐ	Ⓑ	Ⓒ
3.2.12	**Puertas de muelle** Horario de inactividad: Las puertas de muelle permanecen cerradas y aseguradas (es decir, desactivadas electrónicamente o bloqueadas físicamente). Las puertas de muelle cuentan con un sistema de alarma para detectar intrusiones no autorizadas y activar una alarma conectada al sistema de alarma principal. Horario de funcionamiento: Las puertas de muelle deben permanecer cerradas cuando no estén en uso. Si se utilizan puertas de tijera, deben estar aseguradas con un pestillo mecánico y tener una altura mínima de 2,4 metros (8 pies).	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S4. Puntos de entrada y salida de oficinas y almacenes

4.1 Punto(s) de acceso para visitantes en la zona de oficinas

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
4.1.1	Los puntos de acceso para visitantes están controlados por un empleado/guardia/recepcionista que ha recibido capacitación en emisión de credenciales, controles, registro, visitantes, requisitos de acompañamiento, etc. (proceso establecido para cuando los empleados registran a sus propios invitados y cuando las visitas se realizan fuera del horario de atención).	Ⓐ	Ⓑ	Ⓒ
4.1.2	Los puntos de acceso para visitantes en las oficinas están cubiertos por cámaras de videovigilancia (cámaras a color o de día/noche) y las personas son claramente reconocibles en todo momento.	Ⓐ	Ⓑ	
4.1.3	Alarma de emergencia presente en los puntos de acceso para visitantes de la zona de oficinas, la cual se prueba semanalmente.	Ⓐ	Ⓑ	
4.1.4	Todos los visitantes a la oficina deberán identificarse mediante una identificación oficial con fotografía (por ejemplo, licencia de conducir, pasaporte o documento nacional de identidad, etc.). Si la institución acepta identificaciones digitales y la legislación local lo permite, deberá contar con un proceso de verificación riguroso (que incluya toda la infraestructura técnica necesaria).	Ⓐ	Ⓑ	Ⓒ
4.1.5	Todos los visitantes a la oficina deben registrarse y conservar un registro durante un mínimo de 30 días. Los detalles de la visita, como la persona visitada y el motivo de la misma, deben poder rastrearse a través de la información registrada en el libro de visitas.	Ⓐ	Ⓑ	Ⓒ
4.1.6	Todas las credenciales de visitante deben ser revisadas cuando el visitante abandona las instalaciones y el registro completo debe ser verificado diariamente.	Ⓐ	Ⓑ	
4.1.7	Todos los visitantes deben mostrar visiblemente sus credenciales o pases y estar acompañados por personal de la empresa.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

4.2 Punto(s) de entrada al mercado laboral

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
4.2.1	Todos los puntos de acceso para el personal están controlados las 24 horas del día, los 7 días de la semana.		Ⓑ	Ⓒ
4.2.2	Todos los puntos de acceso para el personal están controlados mediante dispositivos de control de acceso electrónico las 24 horas del día, los 7 días de la semana. Se registra el acceso.	Ⓐ		
4.2.3	Puntos de acceso para el personal cubiertos por CCTV/VSS. (Cámaras a color o de día/noche).	Ⓐ	Ⓑ	
4.2.4	Una vez finalizado el proceso de verificación de antecedentes, todos los empleados deberán recibir una credencial de identificación con fotografía de la empresa.	Ⓐ	Ⓑ	
4.2.5	Todos los demás empleados deben llevar una tarjeta de identificación de la empresa para que puedan ser reconocidos dentro de las instalaciones.	Ⓐ	Ⓑ	
4.2.6	Las credenciales de todos los empleados deben estar claramente visibles.	Ⓐ	Ⓑ	
4.2.7	Las credenciales de acceso al personal no deben compartirse bajo ninguna circunstancia, y debe existir una política de emisión de credenciales.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

4.3 Identificación del conductor y del vehículo

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
4.3.1	Todos los conductores deben ser identificados mediante una identificación oficial con fotografía (por ejemplo, licencia de conducir, pasaporte o documento nacional de identidad, etc.) y se debe mantener un registro de conducción. Si la instalación acepta identificaciones digitales y la legislación local lo permite, se debe implementar un proceso de verificación riguroso (que incluya toda la infraestructura técnica necesaria).	Ⓐ	Ⓑ	Ⓒ

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
4.3.2	Verificación de que la licencia de conducir no esté vencida y corresponda al conductor. Si la instalación acepta licencias de conducir digitales y la legislación local lo permite, debe implementarse un proceso de verificación riguroso (que incluya toda la infraestructura técnica necesaria).	Ⓐ	Ⓑ	Ⓒ
4.3.3	Los identificadores de los vehículos se registran manualmente (es decir, por escrito) o mediante cámaras. Incluya como mínimo la matrícula y el tipo de vehículo.	Ⓐ		

TAPA Copyright © Do Not Copy

S5. IDentro del almacén y la oficina

5.1 Área de almacén: Paredes para múltiples inquilinos

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.1.1	Paredes interiores de piso a techo para edificios de uso mixto y techo construidos/diseñados y mantenidos para resistir la penetración (Ejemplo: paredes de ladrillo, bloque, losa de hormigón prefabricada, paneles sándwich con un ancho mínimo de 7 mm).	Ⓐ	Ⓑ	Ⓒ
5.1.2	Si las paredes interiores de edificios de uso mixto, desde el suelo hasta el techo, están construidas con malla metálica de seguridad u otra barrera de seguridad reconocida en la industria, también deberán contar con un sistema de alarma para detectar intrusiones. Nota 1: No se aceptan redes, cercas de baja calidad ni mallas que no sean de seguridad. Nota 2: Si las paredes de edificios de uso mixto están construidas con material sólido desde el suelo hasta el techo, este requisito no aplica.	Ⓐ	Ⓑ	Ⓒ

5.2 Áreas internas del almacén

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.2.1	Se requiere la detección de intrusiones (p. ej., infrarrojos, movimiento, sonido o vibración) para monitorear las áreas internas del almacén. Las alarmas deben activarse y conectarse al sistema de alarma principal fuera del horario de operación (es decir, cuando el almacén está cerrado). Nota 1: Si el almacén opera las 24 horas del día, los 7 días de la semana, los 366 días del año, este requisito puede no aplicarse si los riesgos y las medidas de mitigación están documentados en la Evaluación de Riesgos local. (Véase el requisito 1.1.5). Nota 2: Independientemente del horario de operación, se requiere siempre la detección de intrusiones perimetrales o barreras físicas en las puertas exteriores y ventanas de la planta baja de oficinas y almacenes. (Véanse los requisitos 3.2.2 y 3.2.6).	Ⓐ		

TAPA Copyright © Do Not Copy

5.3 Puertas y áreas de muelle internas

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.3.1	Todas las puertas y áreas de los muelles de carga internos están cubiertas por CCTV/VSS (cámaras a color o de día/noche).	Ⓐ	Ⓑ	Ⓒ
5.3.2	Vistas de la carga y descarga de mercancías en todas las puertas y áreas de muelle internas, siempre despejadas a menos que exista una obstrucción temporal debido a necesidades operativas (por ejemplo, carga y descarga de camiones en tiempo real).	Ⓐ	Ⓑ	Ⓒ
5.3.3	Los activos del comprador estarán bajo vigilancia CCTV al 100% en las áreas de movimiento o preparación de la carga (es decir, áreas de desmontaje/montaje de palés, rutas hacia y desde las estanterías de almacenamiento, muelle, pasillos de tránsito).	Ⓐ	Ⓑ	
5.3.4	El análisis de puntos ciegos para lograr una cobertura del 100% del movimiento de carga mediante CCTV debe realizarse al menos anualmente, a menos que se produzcan cambios operativos o estructurales en el almacén.	Ⓐ		

TAPA Copyright © Do Not Copy

5.4 Control de acceso entre la oficina y el muelle/almacén.

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.4.1	Acceso controlado entre la oficina y el muelle/almacén.	Ⓐ	Ⓑ	
5.4.2	Las alarmas de acceso mediante tarjeta o intercomunicador, para las puertas que conectan la oficina con el muelle/almacén, son audibles localmente y generan una alarma que requiere respuesta si se mantienen abiertas durante más de 60 segundos o inmediatamente si se fuerzan para abrirlas.	Ⓐ		
5.4.3	Las alarmas de las puertas que conectan la oficina con el muelle/almacén emiten una señal sonora local o envían una alarma para que se active la alarma si se mantienen abiertas durante más de 60 segundos o si se fuerzan para abrirlas.		Ⓑ	
5.4.4	El personal autorizado del PSL/Solicitante y los visitantes acompañados tienen permitido el acceso a las áreas de muelle/almacén en función de una necesidad comercial y con acceso restringido.	Ⓐ	Ⓑ	Ⓒ
5.4.5	La lista de acceso a las áreas de muelle/almacén se revisa al menos trimestralmente para limitar/verificar que el permiso de acceso se otorgue únicamente al personal designado/autorizado.	Ⓐ	Ⓑ	

5.5 Área de carga de alto valor (HVC)

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.5.1	El tamaño y el uso del HVC pueden estar determinados por el acuerdo entre el comprador, el proveedor de servicios logísticos y el solicitante. Si no existe un acuerdo, el HVC deberá tener una capacidad mínima de 6 metros cúbicos de producto.	Ⓐ	Ⓑ	
5.5.2	HVC/ El perímetro del área está cercado con jaulas o muros rígidos en todos los lados, incluyendo la parte superior/techo.	Ⓐ	Ⓑ	
5.5.3	Dispositivo de cierre de área/calefacción en puerta/portón.	Ⓐ	Ⓑ	
5.5.4	Cobertura completa de CCTV/VSS (cámaras a color o de día/noche) en la entrada y el interior del HVC. ***Nota**: Si el HVC es demasiado pequeño para instalar una cámara en el interior, la cobertura de la entrada es suficiente.*	Ⓐ		
5.5.5	Cobertura de CCTV/VSS (cámaras a color o de día/noche) en la entrada de HVC.		Ⓑ	
5.5.6	Si se requiere el acceso al HVC para más de 10 personas, este deberá controlarse electrónicamente mediante tarjeta o llavero. Si se requiere el acceso para 10 personas o menos, se deberá utilizar un sistema de cerradura o candado de alta seguridad con un sistema de emisión de llaves controlado. Las llaves pueden prestarse a personas para cubrir un turno, pero no deben transferirse sin autorización y deben registrarse en el libro de llaves. Todas las llaves deben devolverse y registrarse cuando no se utilicen.	Ⓐ		
5.5.7	Las puertas y portones de HVC cuentan con alarmas para detectar intrusiones forzadas. Las alarmas pueden generarse mediante contactos de puerta o mediante el uso de sistemas de detección de movimiento CCTV/VSS para detectar accesos no autorizados.	Ⓐ		
5.5.8	El perímetro del HVC se mantiene en buen estado y se inspecciona mensualmente para comprobar su integridad y detectar posibles daños.	Ⓐ		

TAPA Copyright © Do Not Copy

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.5.9	El proveedor de servicios logísticos (PSL) y el solicitante deben garantizar que el acceso al HVC se otorgue únicamente al personal designado y autorizado. La lista de acceso aprobado al HVC se revisa mensualmente y se actualiza en tiempo real cuando un empleado deja la empresa o ya no necesita acceso. Existe un procedimiento establecido para el acceso al HVC.	Ⓐ	Ⓑ	

5.6 Inspección de basura del almacén

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.6.1	Los contenedores principales de recogida de basura y las zonas de compactación, tanto internas como externas, del almacén están vigilados por CCTV/VSS.	Ⓐ		
5.6.2	Las bolsas de basura que se utilizan dentro del almacén, cuando es necesario, son transparentes.		Ⓑ	Ⓒ

5.7 Precarga y preparación

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.7.1	No se permite la precarga ni el estacionamiento de camiones FTL/dedicados al Comprador fuera del almacén durante las horas no operativas, salvo acuerdo mutuo entre el Comprador y el Proveedor de Servicios Logísticos (PSL)/Solicitante. Deben implementarse medidas de seguridad alternativas (p. ej., dispositivos de seguridad adicionales en los vehículos/compartimentos de carga). ***Nota**: Se consideran "fuera del almacén" las áreas separadas de las instalaciones, pero dentro del perímetro/patio del PSL/Solicitante*.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

5.8 Registros de contenedores personales y de salida

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.8.1	Los procedimientos de seguridad por escrito definen cómo se controlan los "contenedores personales" dentro del almacén. Los contenedores personales incluyen loncheras, mochilas, neveras portátiles, bolsos, etc.	Ⓐ	Ⓑ	
5.8.2	Si la legislación local lo permite, el Proveedor de Servicios Logísticos (PSL) o el Solicitante deberá desarrollar y mantener un procedimiento documentado para las inspecciones de salida. La activación del procedimiento queda a discreción del PSL o del Solicitante, o según lo estipulado en el acuerdo entre el Comprador, el PSL y el Solicitante. Como mínimo, el procedimiento deberá contemplar los criterios del PSL o del Solicitante para realizar inspecciones en caso de que sea necesario llevarlas a cabo cuando normalmente no se requieran (por ejemplo, ante la sospecha de hurto por parte del personal). Los empleados, el personal de apoyo logístico, los subcontratistas y los visitantes deberán estar informados sobre esta política antes de su entrada al almacén.	Ⓐ		

5.9 Control de equipos de manipulación de carga

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.9.1	Procedimiento que exige la desactivación de todas las carretillas elevadoras y demás equipos motorizados de manipulación de carga durante las horas no operativas. ***Nota**: Esto no incluye transpaletas manuales ni manuales.*	Ⓐ	Ⓑ	

5.10 Integridad del contenedor o remolque: inspección de 7 puntos

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.10.1	Inspección física de 7 puntos realizada a todos los contenedores o remolques del comprador destinados a envíos: Pared frontal, lateral izquierdo, lateral derecho, piso, techo, puertas interiores y exteriores y mecanismo de cierre, y chasis exterior. ***Nota:** Esto aplica a todo tipo de remolques y contenedores con cerradura o precinto (es decir, no se limita a contenedores de carga marítima).*	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

5.11 Proceso de entrega de mercancías; precintos de seguridad

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.11.1	Salvo que el comprador lo exima expresamente, se utilizan precintos de seguridad a prueba de manipulaciones en todos los envíos directos sin escalas. Los precintos deberán estar certificados según la norma ISO 17712 (clasificación I, S o H). Nota: No se requieren precintos en envíos con múltiples escalas, debido a la complejidad y el riesgo que supone para los conductores llevar varios precintos.	Ⓐ	Ⓑ	Ⓒ
5.11.2	El proveedor de servicios logísticos/solicitante debe contar con procedimientos documentados para la gestión y el control de precintos de seguridad, cerraduras de puertas de remolques (contenedores), cerraduras de pasador y demás equipos de seguridad.	Ⓐ	Ⓑ	Ⓒ
5.11.3	Los precintos de seguridad solo pueden ser colocados o retirados por personal autorizado, es decir, personal del almacén, quienes están instruidos para identificar y reportar precintos manipulados. El conductor nunca debe colocar ni retirar los precintos, salvo que el comprador cuente con una exención.	Ⓐ	Ⓑ	Ⓒ
5.11.4	Procedimientos establecidos para reconocer y reportar sellos de seguridad comprometidos.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

5.12 Integridad de la carga; Proceso de validación de carga/descarga

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.12.1	Se han implementado procedimientos rigurosos para garantizar que todos los activos del Comprador, tanto enviados como recibidos, se validen en el momento de la entrega mediante un recuento manual o electrónico. El proceso debe asegurar que las anomalías se identifiquen, documenten e informen sistemáticamente al Proveedor de Servicios Logísticos (PSL), al Solicitante o al Comprador. Los registros manuales o electrónicos deben tener calidad probatoria. Si los conductores no están presentes para presenciar esta actividad, el Comprador, el PSL o el Solicitante deben garantizar una verificación alternativa del recuento, como escaneos o imágenes de CCTV/VSS, recopiladas y conservadas específicamente para este fin. ***Nota**: Además de las piezas faltantes, las anomalías pueden incluir daños, falta de correas o cinta adhesiva, cortes u otras aberturas evidentes, lo que indica un posible robo o hurto.*	Ⓐ	Ⓑ	Ⓒ

5.13 Recogidas fraudulentas

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
5.13.1	La identificación del conductor del camión, la documentación de recogida de la carga y los detalles de prealerta especificados por el comprador se verifican antes de la carga. Debe existir un procedimiento establecido. Si la instalación acepta identificaciones digitales y la legislación local lo permite, debe existir un proceso de verificación riguroso (que incluya toda la infraestructura técnica necesaria).	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S6. Sistemas de seguridad: diseño, monitoreo y respuesta

6.1 Puesto de vigilancia

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
6.1.1	Monitoreo de eventos de alarma las 24 horas del día, los 7 días de la semana, los 366 días del año, mediante un puesto de monitoreo interno o externo de terceros, protegido contra accesos no autorizados. Nota: Los puestos de monitoreo pueden estar ubicados dentro o fuera de las instalaciones y pueden ser propiedad de la empresa o de terceros. En todos los casos, el acceso debe controlarse mediante un sistema electrónico de control de acceso (tarjetas de identificación), cerraduras o escáneres biométricos.	Ⓐ	Ⓑ	Ⓒ
6.1.2	Puesto de vigilancia para responder a todas las alarmas del sistema de seguridad en tiempo real, las 24 horas del día, los 7 días de la semana, los 366 días del año.	Ⓐ	Ⓑ	Ⓒ
6.1.3	El puesto de vigilancia reconoce la activación de la alarma y la activa en menos de 3 minutos.	Ⓐ	Ⓑ	Ⓒ
6.1.4	Los informes de monitorización de alarmas están disponibles.	Ⓐ	Ⓑ	Ⓒ
6.1.5	Los informes de monitorización de alarmas están disponibles.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

6.2 Sistema de detección de intrusos (IDS)

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
6.2.1	Todos los sistemas de detección de intrusiones (IDS) se activan durante las horas no operativas y están conectados al sistema de alarma principal.	Ⓐ	Ⓑ	Ⓒ
6.2.2	Se conservan los registros de alarmas del sistema de detección de intrusiones (IDS) de los últimos 90 días.	Ⓐ	Ⓑ	
6.2.3	Los registros de alarmas del sistema de detección de intrusiones (IDS) se almacenan de forma segura y se realizan copias de seguridad al menos semanalmente.	Ⓐ	Ⓑ	

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
6.2.4	Procedimiento para garantizar que el acceso al IDS esté restringido a personas autorizadas o administradores del sistema. Esto incluye servidores, consolas, controladores, paneles, redes y datos. Los privilegios de acceso al IDS deben actualizarse de inmediato cuando las personas abandonan la organización o cambian de rol y ya no requieren acceso.	Ⓐ	Ⓑ	Ⓒ
6.2.5	Se activa la alarma en caso de fallo de alimentación o pérdida del sistema de detección de intrusiones (IDS). Nota: En sistemas con sistema de alimentación ininterrumpida (UPS), la alarma se activa cuando falla la batería del UPS.	Ⓐ	Ⓑ	Ⓒ
6.2.6	Verificación de activación de alarmas IDS en funcionamiento. Nota: Procedimientos para validar que las alarmas estén activadas fuera del horario operativo.	Ⓐ	Ⓑ	Ⓒ
6.2.7	Alarma del IDS transmitida por línea fija o inalámbrica y/o fallo del modo de comunicación.	Ⓐ	Ⓑ	
6.2.8	Sistema de comunicación de respaldo implementado en el dispositivo IDS y/o en caso de falla de la línea.	Ⓐ	Ⓑ	

6.3 Sistema de Control de Acceso Automático (AACS)

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
6.3.1	Disponemos de los registros de transacciones de AACS de los últimos 90 días. Los registros se almacenan de forma segura y se realizan copias de seguridad.	Ⓐ	Ⓑ	
6.3.2	Procedimiento para garantizar que el acceso a AACS esté restringido a personas autorizadas o administradores del sistema. Los privilegios de acceso deben actualizarse de inmediato cuando las personas abandonan la organización o cambian de función y ya no requieren acceso..	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
6.3.3	Los informes del sistema de acceso se revisan al menos trimestralmente para detectar irregularidades o usos indebidos (por ejemplo, múltiples intentos fallidos, lecturas erróneas (como tarjetas desactivadas), evidencia de compartición de tarjetas para permitir el acceso no autorizado, etc.). Proceso establecido.	Ⓐ	Ⓑ	

6.4 CCTV/VSS

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
6.4.1	Grabación digital de CCTV/VSS instalada.	Ⓐ	Ⓑ	Ⓒ
6.4.2	La velocidad de grabación para CCTV/VSS está configurada como mínimo a 8 fotogramas por segundo (fps) por cámara.	Ⓐ	Ⓑ	Ⓒ
6.4.3	La funcionalidad de grabación digital se verifica diariamente en días laborables mediante un procedimiento establecido. Registros disponibles.	Ⓐ	Ⓑ	Ⓒ
6.4.4	Las grabaciones de CCTV/VSS se almacenarán durante un mínimo de 30 días cuando lo permita la legislación local. El proveedor de servicios locales/solicitante deberá aportar pruebas de cualquier ley local que prohíba el uso de CCTV o que limite el almacenamiento de datos de vídeo a menos de 30 días.	Ⓐ	Ⓑ	Ⓒ
6.4.5	El acceso al sistema de videovigilancia (CCTV/VSS), incluyendo el hardware, el software y el almacenamiento de datos/vídeo, está estrictamente controlado. Esta sala debe permanecer cerrada con llave si el sistema de almacenamiento de videovigilancia (CCTV/VSS) se encuentra en las instalaciones y cuenta con controles de acceso.	Ⓐ	Ⓑ	Ⓒ
6.4.6	Las imágenes de CCTV/VSS, por motivos de seguridad, solo pueden ser visualizadas por personal autorizado.	Ⓐ	Ⓑ	Ⓒ
6.4.7	Se han establecido procedimientos que detallan la política de protección de datos de CCTV/VSS en relación con el uso de imágenes en tiempo real y de archivo, de conformidad con la legislación local.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

6.5 Iluminación exterior e interior

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
6.5.1	Los niveles de iluminación exterior e interior son suficientes para obtener imágenes de CCTV/VSS que permitan la investigación y la grabación de imágenes con calidad probatoria.	Ⓐ	Ⓑ	
6.5.2	Los niveles de iluminación exterior e interior son suficientes para reconocer claramente todos los vehículos y personas.	Ⓐ		

TAPA Copyright © Do Not Copy

S7. Capacitación y procedimientos

7.1 Procedimientos de escalamiento

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
7.1.1	Procedimientos locales establecidos para el manejo de los bienes del Comprador, incluyendo el proceso para reportar oportunamente la pérdida, extravío o robo de dichos bienes. El Proveedor de Servicios Locales (PSL) o el Solicitante deben reportar los incidentes al Comprador dentro de las 24 horas. Los robos evidentes se reportan de inmediato. El proceso se sigue de manera consistente.	Ⓐ	Ⓑ	Ⓒ
7.1.2	Listado de contactos de emergencia para compradores y proveedores de servicios legales/solicitantes en materia de gestión de instalaciones para incidentes de seguridad. El listado se actualiza cada 6 meses e incluye contactos de emergencia de las fuerzas del orden.	Ⓐ	Ⓑ	Ⓒ

7.2 Compromiso de la dirección

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
7.2.1	La dirección debe desarrollar, comunicar y mantener una política de seguridad para garantizar que todas las personas pertinentes (es decir, empleados y contratistas) conozcan claramente las expectativas de seguridad del proveedor.	Ⓐ	Ⓑ	Ⓒ

7.3 Capacitación

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
7.3.1	Se impartirá formación en seguridad y concienciación sobre amenazas a todos los miembros de la plantilla durante los primeros 60 días de empleo y, posteriormente, cada 2 años.	Ⓐ	Ⓑ	Ⓒ
7.3.2	La capacitación en concientización sobre seguridad de la información, centrada en la protección de los datos de envío electrónicos y físicos del Comprador, se imparte a los empleados que tienen acceso a la información del Comprador y, posteriormente, al menos cada 2 años, o de acuerdo con la legislación local si se define un período de actualización más corto.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

7.4 Acceso a los activos del comprador

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
7.4.1	Procedimientos establecidos para proteger los activos del Comprador (es decir, la carga) del acceso no autorizado por parte de los empleados, visitantes, etc.	Ⓐ	Ⓑ	Ⓒ

7.5 Control de la información

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
7.5.1	El acceso a los documentos de envío y a la información sobre los activos del comprador se controla según el principio de "necesidad de conocer". Debe existir un proceso establecido para garantizar la protección de la información del comprador.	Ⓐ	Ⓑ	Ⓒ
7.5.2	Se supervisa y registra el acceso a los documentos de envío y a la información sobre los activos del comprador. El proceso y los registros relacionados están establecidos.	Ⓐ	Ⓑ	Ⓒ
7.5.3	Los documentos de envío y cualquier otro documento, incluida la información sobre los activos del comprador, se custodiarán hasta su destrucción.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

7.6 Informe de incidentes de seguridad

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
7.6.1	Se ha implementado un sistema de seguimiento y notificación de incidentes de seguridad, que se utiliza para aplicar medidas proactivas.	Ⓐ	Ⓑ	

7.7 Programas de mantenimiento

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
7.7.1	Se han implementado programas de mantenimiento para todas las instalaciones/sistemas de seguridad técnica (física) para garantizar su funcionamiento en todo momento (por ejemplo, CCTV/VSS, controles de acceso, detección de intrusos e iluminación).	Ⓐ	Ⓑ	Ⓒ

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
7.7.2	El mantenimiento preventivo se realiza una vez al año o de acuerdo con las especificaciones del fabricante.	Ⓐ	Ⓑ	Ⓒ
7.7.3	Se realizan verificaciones de funcionalidad de todos los sistemas una vez por semana y se documentan, a menos que se notifique o active una alarma de falla del sistema de manera inmediata/automática.	Ⓐ	Ⓑ	
7.7.4	Se debe iniciar una orden de reparación dentro de las 48 horas posteriores al descubrimiento de la falla. Para cualquier reparación que se prevea que supere las 24 horas, se deben implementar medidas alternativas.	Ⓐ	Ⓑ	

7.8 Orientación para contratistas

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
7.8.1	El proveedor de servicios logísticos (PSL) o el solicitante deberán garantizar que todos los subcontratistas/proveedores conozcan y cumplan con los programas de seguridad pertinentes del PSL o del solicitante.	Ⓐ	Ⓑ	Ⓒ

7.9 Registros de envío y recepción

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
7.9.1	Los documentos de envío y recepción deben ser legibles, completos y precisos (es decir, hora, fecha, firmas, conductor, personal de envío y recepción, detalles y cantidad del envío, etc.). Los nombres del conductor y del remitente deben ser siempre claramente legibles.	Ⓐ	Ⓑ	Ⓒ
7.9.2	El proveedor de servicios logísticos/solicitante deberá conservar los registros de todas las recogidas y los comprobantes de entrega durante un período no inferior a dos años, y ponerlos a disposición de las investigaciones de pérdidas cuando sea necesario.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
7.9.3	Se deberá proporcionar un comprobante de entrega de acuerdo con el acuerdo escrito entre el Comprador y el PSL/Solicitante, cuando el Comprador lo requiera, el destino notificará al origen dentro del plazo acordado de recepción del envío, conciliando los detalles de la alerta previa de envío.	Ⓐ	Ⓑ	Ⓒ

7.10 Proceso de prealerta en marcha

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
7.10.1	Cuando el comprador lo requiera, se aplica un proceso de prealerta a los envíos entrantes y/o salientes. Los detalles de la prealerta deben ser acordados entre el comprador y el proveedor de servicios logísticos (PSL) o el solicitante. Los detalles sugeridos incluyen la hora de salida, la hora de llegada prevista, la empresa de transporte, el nombre del conductor, los datos de la matrícula, la información del envío (cantidad de bultos, peso, número de conocimiento de embarque, etc.) y los números de precinto del remolque.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S8. Integridad de la fuerza laboral

8.1 Selección/Verificación de antecedentes (según lo permita la legislación local)

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
8.1.1	El proveedor de servicios logísticos (PSL) o el solicitante debe someterse a un proceso de verificación de antecedentes que incluya, como mínimo, los últimos 5 años de empleo y antecedentes penales. Este proceso se aplica a todos los solicitantes, incluidos empleados y contratistas. El PSL o el solicitante también deberá haber acordado contractualmente que se aplique un proceso equivalente en las empresas contratistas que suministran trabajadores de Tasmania.	Ⓐ	Ⓑ	Ⓒ
8.1.2	El proveedor de servicios logísticos (PSL) o el solicitante deberán contar con acuerdos para que la agencia o el subcontratista que proporciona los trabajadores de TAS les proporcione la información necesaria para la verificación de antecedentes, o bien, deberán realizar dicha verificación ellos mismos. La verificación debe incluir antecedentes penales y comprobaciones laborales.	Ⓐ	Ⓑ	Ⓒ
8.1.3	Procedimiento para tratar las declaraciones falsas de los solicitantes/trabajadores antes y después de la contratación.	Ⓐ	Ⓑ	Ⓒ

8.2 Terminación o recontratación de la fuerza laboral

Nota: La terminación incluye tanto las separaciones voluntarias como las involuntarias, es decir, los miembros de la plantilla que han sido despedidos o que han renunciado..

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
8.2.1	Recuperar los bienes físicos de los empleados despedidos, incluyendo identificaciones de la empresa, tarjetas de acceso, llaves, equipos, activos informáticos e información confidencial. Se requiere un procedimiento documentado.	Ⓐ	Ⓑ	Ⓒ
8.2.2	Proteja los datos del comprador: Restrinja el acceso de los empleados que hayan rescindido su contrato a los sistemas físicos o electrónicos, incluidos aquellos que contengan datos del comprador. Se requiere un procedimiento documentado.	Ⓐ	Ⓑ	Ⓒ
8.2.3	Se ha implementado una lista de verificación para la incorporación y desvinculación de personal con fines de verificación.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
8.2.4	Recontratación: Existen procedimientos para evitar que el proveedor de servicios logísticos (PSL) o el solicitante recontraten personal si los criterios de denegación o despido siguen vigentes. ***Nota:*** *Se revisan los registros antes de la recontratación (por ejemplo, los antecedentes del personal previamente despedido o de los solicitantes rechazados; es decir, a quienes se les denegó el empleo anteriormente).*	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S9. Requisitos de la función central (solo aplicable para la certificación multisitio)

9.1 General

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
9.1.1	Existe una función central para gestionar el sistema de gestión de seguridad para todos los sitios, tal como se define en el alcance de la certificación multisitio.	Ⓐ	Ⓑ	Ⓒ
9.1.2	Todos los emplazamientos deben tener una relación legal o contractual con la función central. Este requisito no se aplica a los emplazamientos de subcontratistas incluidos en el alcance de la certificación, según la cláusula 4.2.2 del CFD.	Ⓐ	Ⓑ	Ⓒ
9.1.3	Se establece un sistema único de gestión de seguridad para garantizar que todos los sitios que forman parte del sistema cumplan con los requisitos de la norma de seguridad TAPA aplicable.	Ⓐ	Ⓑ	Ⓒ
9.1.4	La función central y su sistema de gestión estarán sujetos a auditorías internas para garantizar el cumplimiento continuo de las Normas TAPA.	Ⓐ	Ⓑ	Ⓒ
9.1.5	La función central llevará a cabo auditorías de los sitios incluidos en el ámbito de aplicación para garantizar que cada sitio cumpla con los requisitos aplicables de TAPA FSR. Las auditorías deberán realizarse utilizando las plantillas de auditoría TAPA correspondientes. Todas las auditorías anuales individuales de los sitios deberán completarse y estar disponibles para el auditor antes del proceso de certificación.	Ⓐ	Ⓑ	Ⓒ
9.1.6	La función central tendrá la autoridad y los derechos para exigir que todos los sitios cumplan con los Estándares de Seguridad de TAPA e implementar acciones correctivas y preventivas según sea necesario. Nota: Cuando corresponda, esto deberá estar estipulado en el acuerdo formal entre la función central y los sitios.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

9.2 Políticas y procedimientos

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
9.2.1	La función central deberá mantener políticas y procedimientos documentados para sus sistemas de gestión de seguridad que sean aplicables a todas sus instalaciones.	Ⓐ	Ⓑ	Ⓒ
9.2.2	La función central deberá garantizar que las políticas y los procedimientos se actualicen, comuniquen, implementen y apliquen adecuadamente en todas las sedes según sea necesario.	Ⓐ	Ⓑ	Ⓒ
9.2.3	Las políticas y los procedimientos deberán mantenerse actualizados y ser fácilmente accesibles para todos los centros según sea necesario.	Ⓐ	Ⓑ	Ⓒ

9.3 Informe de auditoría de autoevaluación realizado para todos los sitios.

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
9.3.1	La función central exigirá a todos los centros que realicen una autoevaluación, y todos los informes de autoevaluación deberán presentarse a la función central para su registro y revisión. Los registros deberán conservarse durante al menos dos (2) años.	Ⓐ	Ⓑ	Ⓒ
9.3.2	La función central garantizará que todos los SCAR derivados de la autoevaluación y las auditorías se cierren adecuadamente para mejorar sus sistemas de gestión de seguridad..	Ⓐ	Ⓑ	Ⓒ
9.3.3	Todos los centros deberán enviar actualizaciones de progreso e informes sobre todos los SCAR pendientes a la función central. La función central informará a la gerencia del PSL/Solicitante si los SCAR no se completan antes de sus fechas límite. Los registros deberán conservarse durante al menos dos (2) años.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

9.4 Registros de inspecciones, bitácoras (registros de visitantes/conductores), inspecciones de 7 puntos

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
9.4.1	La función central deberá contar con procedimientos para garantizar que todos los sitios mantengan registros de inspecciones, registros de visitantes, registros de conductores e inspección de 7 puntos, etc..	Ⓐ	Ⓑ	Ⓒ

9.5 Evaluación de riesgos de todos los sitios

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
9.5.1	La función central deberá contar con procedimientos establecidos para garantizar que se realicen evaluaciones y gestión de riesgos apropiadas en todos los sitios, y sus registros se mantendrán durante al menos dos (2) años.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

9.6 Diseño del sistema de CCTV/VSS y alarma del sitio

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
9.6.1	La función central deberá contar con procedimientos que garanticen que todas las instalaciones revisen y mantengan la documentación relativa a todos los sistemas de seguridad física, como los sistemas de videovigilancia y de alarma.	Ⓐ	Ⓑ	Ⓒ

9.7 Registros de alarmas y control de acceso

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
9.7.1	La función central deberá contar con procedimientos que garanticen el mantenimiento y las pruebas de todos los sistemas de alarma y control de acceso para asegurar su eficacia operativa.	Ⓐ	Ⓑ	Ⓒ
9.7.2	La función central deberá contar con procedimientos establecidos para que todas las instalaciones mantengan registros de todas las pruebas e incidentes relacionados con la detección de intrusiones y el control de acceso.	Ⓐ	Ⓑ	Ⓒ

9.8 Registros de capacitación

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
9.8.1	La función central deberá contar con procedimientos para garantizar que todos los centros mantengan registros adecuados de formación en gestión de la seguridad de sus empleados.	Ⓐ	Ⓑ	Ⓒ
9.8.2	La función central deberá contar con procedimientos para garantizar que todos los sitios mantengan registros de capacitación en seguridad de todo el personal. Dichos registros deberán conservarse durante al menos dos (2) años.	Ⓐ	Ⓑ	Ⓒ

9.9 Registros de selección/verificación

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
9.9.1	La función central deberá contar con procedimientos para garantizar que todos los centros realicen revisiones periódicas de la verificación y comprobación de los registros, a fin de asegurar la integridad y la eficacia de los sistemas de gestión de seguridad.	Ⓐ	Ⓑ	Ⓒ
9.9.2	La función central deberá contar con procedimientos para garantizar que se mantengan los registros de las revisiones, incluidos sus hallazgos y las acciones correctivas/preventivas 9.1.6. Los registros se conservarán durante al menos dos (2) años.	Ⓐ	Ⓑ	Ⓒ

9.10 Revisión de la dirección para evaluar las autoauditorías; informes SCAR generados; pérdidas y robos; evaluaciones de riesgos.

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
9.10.1	La función central deberá, como mínimo, realizar revisiones de gestión periódicas para garantizar el cumplimiento, la eficacia y la mejora de sus sistemas de gestión de seguridad.	Ⓐ	Ⓑ	Ⓒ
9.10.2	Las revisiones de gestión deberán abarcar, entre otros aspectos, la eficacia de las autoauditorías, el cierre de informes de incidentes graves, las evaluaciones de riesgos, los incidentes y las acciones de mejora.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

N.º de solicitud	Requisitos / Controles	Nivel aplicable		
9.10.3	La función central deberá mantener registros de todas las revisiones de gestión durante al menos dos (2) años.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

8.0 Amenazas a la seguridad informática y cibernética: opción mejorada

FSR incluye mejoras opcionales de seguridad informática y cibernética que ofrecen un nivel de protección superior y pueden utilizarse junto con los módulos. Esta mejora opcional está diseñada para que el proveedor de servicios logísticos (PSL), el solicitante o su comprador la seleccionen como requisito adicional para sus necesidades de seguridad operativa. Al seleccionar esta mejora opcional en la evaluación previa a la certificación para formar parte de la auditoría de certificación, todos los requisitos se vuelven obligatorios.

La opción mejorada de TAPA FSR proporciona un nivel básico de controles de seguridad informática y cibernética a nivel de sitio. Se recomienda encarecidamente a los miembros que adopten los Estándares de Ciberseguridad (CSS) para lograr un marco de ciberseguridad más completo y robusto.

E8. Requisitos obligatorios

N.º de solicitud	Requisitos / Controles
E8.1.1	El proveedor de servicios lingüísticos (PSL) o el solicitante debe contar con políticas de seguridad informática y cibernética. Estas políticas pueden presentarse por separado o en un documento combinado. Deben explicar: 1. Las acciones del PSL o del solicitante para identificar y responder a las amenazas. 2. Las políticas y los procedimientos establecidos para proteger, detectar, probar y responder a incidentes de seguridad. 3. Los métodos para la recuperación de sistemas informáticos y/o datos. 4. El protocolo de comunicación con los compradores/clientes para mitigar el impacto en la cadena de suministro en un plazo de 24 horas desde que se tenga conocimiento del incidente. 5. Cómo se revisan y actualizan las políticas anualmente.
E8.1.2	El proveedor de servicios lingüísticos (PSL) o el solicitante debe impartir formación sobre seguridad de la información a todos sus empleados. Esta formación debe: 1. Cubrir las funciones y responsabilidades de los usuarios de ordenadores en el mantenimiento de la seguridad y los beneficios asociados. 2. Contar con un sistema que garantice el registro de las personas que reciben la formación y su conservación durante un mínimo de dos años.

TAPA Copyright © Do Not Copy

E8.1.3	El proveedor de servicios lingüísticos (PSL) o el solicitante debe contar con una política escrita que garantice la implementación de medidas de ciberseguridad con subcontratistas y/o proveedores, asegurando lo siguiente: 1. Que los requisitos de ciberseguridad del PSL o del solicitante se comuniquen a los subcontratistas y/o proveedores y se incluyan en los acuerdos. 2. Que, en caso de que los subcontratistas y/o proveedores no reconozcan o se nieguen a adoptar los requisitos de ciberseguridad del PSL o del solicitante, se documenten e implementen medidas que mitiguen los riesgos para dichos requisitos y para sus clientes.
E8.1.4	El proveedor de servicios de TI/solicitante debe tener un plan de mitigación de interrupciones de energía (por ejemplo, fuente de alimentación alternativa o generador de respaldo) que garantice que la energía se dirija a los sistemas de TI críticos (identificados en la evaluación de riesgos local) durante un mínimo de 48 horas..
E8.1.5	Los sistemas de información del proveedor de servicios lingüísticos (PSL) o del solicitante deben tener instalado software antivirus y antimalware con licencia. Dicho software debe contener las últimas actualizaciones.
E8.1.6	El proveedor de servicios logísticos (PSL) o el solicitante deben contar con un plan de recuperación ante desastres informáticos (DRP) adecuado para recuperarse de ataques a sistemas comprometidos, que incluya, entre otros, todos los acuerdos necesarios de copia de seguridad y recuperación de datos y software.
E8.1.7	Los sistemas de información del proveedor de servicios lingüísticos (PSL) o del solicitante deben contar con copias de seguridad. Dichas copias de seguridad deben someterse a pruebas periódicas, y los datos de respaldo deben cifrarse y transferirse a una ubicación secundaria externa.

TAPA Copyright © Do Not Copy

E8.1.8	El proveedor de servicios logísticos (PSL) o el solicitante deben implementar una política para todas las cuentas de usuario que permita gestionar y controlar el acceso a los sistemas de información mediante identificadores únicos y contraseñas seguras. Los procedimientos establecidos garantizan lo siguiente: 1. Un programa de auditoría de cumplimiento de contraseñas. 2. Se debe asignar una contraseña única inicial a cada cuenta nueva al momento de su creación. 3. Las contraseñas iniciales no pueden contener el nombre del usuario, su número de identificación ni seguir ningún patrón estándar basado en la información del usuario. 4. Las contraseñas se comunicarán a los usuarios de forma segura y solo después de validar su identidad. 5. Los usuarios deben cambiar sus contraseñas al iniciar sesión por primera vez. 6. Las contraseñas deben cambiarse al menos cada 90 días.

TAPA Copyright © Do Not Copy

A título informativo: la traducción del Estándar al idioma nacional puesta a su disposición tiene como objetivo facilitar la comprensión de los requisitos de TAPA 2026. La traducción del Estándar ha sido elaborada y validada de buena fe y conforme al mejor conocimiento disponible, teniendo en cuenta los fundamentos necesarios. No obstante, a efectos de la auditoría, la versión original en inglés del Estándar correspondiente es y seguirá siendo la versión oficial y vinculante.

Información sobre publicación y derechos de autor
Este documento es publicado por la Asociación para la Protección de Activos Transportados (TAPA).

© TAPA 2026–2029
Todos los derechos reservados. Queda prohibida la reproducción, el almacenamiento en un sistema de recuperación, la transmisión de cualquier parte de esta publicación, ya sea en forma electrónica, mecánica, mediante fotocopia, grabación o cualquier otro medio, sin la autorización previa por escrito de TAPA, salvo lo permitido por la legislación vigente en materia de derechos de autor.

El aviso de derechos de autor que aparece en este documento indica el año de su última publicación.

Historial de publicación
Primera publicación: septiembre de 2026
Edición actual publicada en: septiembre de 2026
Esta Especificación de Acceso Público (PAS) entra en vigor el 15 de septiembre de 2026.

Estado de este documento
Este documento representa los Requisitos de Seguridad de Instalaciones (FSR) de TAPA – Revisión 2026 y establece los requisitos básicos de seguridad de las instalaciones dentro del marco de certificación de TAPA.

El documento permanece vigente hasta que TAPA lo reemplace, revise o retire.

TAPA podrá emitir futuras revisiones, actualizaciones o enmiendas para reflejar la evolución de las amenazas a la seguridad, las prácticas del sector y los avances tecnológicos.

Uso de este documento
El cumplimiento de esta especificación puede utilizarse como parte del proceso de certificación de TAPA para instalaciones que manejan carga de alto valor y susceptible de robo.

Las organizaciones que implementen esta especificación son responsables de garantizar el cumplimiento de todos los requisitos legales, reglamentarios y operativos aplicables, además de los descritos en este documento.

TAPA Copyright © Do Not Copy