



FACILITY SECURITY REQUIREMENTS





Requisitos de seguridad de las instalaciones FSR 2023

Estándares TAPA

TAPA Americas
5030 Champion Blvd,
G-11 #266 Boca Ratón,
Florida 33496
U.S.A.
www.tapaonline.org
Tel. (561) 617-0096

TAPA Asia Pacific
1 Paya Lebar Link, #04-01,
Paya Lebar Quarter,
Singapore 408533
www.tapa-apac.org
Tel. (65) 6514 0892

TAPA EMEA
Pastoor Ohlleen 39
3451 CB Vleuten
The Netherlands
www.tapaemea.org
Tel. +31 19573461



FSR Tabla de Contenido

1. Introducción	5
1.1 Propósito de este Documento FSR	5
Alcance	5
Usuarios	5
1.2 Recursos para implementar el FSR de TAPA	6
1.3 Protección de las políticas y procedimientos de LSP	6
2. Acerca de TAPA	7
2.1 Propósito de TAPA	7
2.2 Misión de TAPA	7
3. Normas TAPA	8
3.1 Estándares de seguridad TAPA	8
3.2 Implementación	8
4. Orientación legal	9
4.1 Ámbito de aplicación	9
4.2 Traducción	9
4.3 La marca "TAPA"	9
4.4 Límites de responsabilidad	9
5. Contratos y subcontratación	10
5.1 Contratos	10
5.2 Subcontratación	10
5.3 Investigación y resolución de quejas de TAPA	10
6. Exenciones	11
6. 1 Visión general	11
6. 2 Proceso de exención de Negocios	11
Tabla 1: Responsabilidades: Solicitud de exención / Evaluación	11
Tabla 2: Aprobación de la exención	12
6. 3 Exenciones para barreras físicas (bajo la sección 1) y para jaulas/áreas de alto valor	13
(HVC, en la sección 4.5)	13
7. Requisitos de seguridad de las instalaciones	15
7.0 Requisitos generales:	15
7.1 Manipulación de carga externa del almacén, envío y área de recepción (general)	16
7.2 Lados exteriores de la instalación: CCTV	17
7.3 Punto (s) de entrada de visitantes en el área de oficinas	19
7.4 Área de almacén: paredes para inquilinos múltiples	20
7.5 Centro de alarma y monitorización	25
7.6 Protocolos de ampliación	27
7.7 Selección / Investigación / Verificación de antecedentes (según lo permita la ley local)	29
8. Requisitos de la función central	30
8.1 General	30
8.2 Políticas y procedimientos	30
8.3 Informe de auditoría de autoevaluación realizada para todos los emplazamientos	31



8.4 Registros de inspecciones y registros en general (visitas, conductores,etc), inspecciones de 7 puntos	31
8.5 Evaluaciones de riesgos de todos los emplazamientos	31
8.6 Disposición de CCTV y alarmas de los emplazamientos	31
8.7 Registros de alarma y control de acceso	31
8.8 Registros de formación	31
8.9 Revisión/verificación de registros	32
8.10 Revisión de la dirección para evaluar las auto auditorías; acciones correctivas de seguridad (SCARs) ; pérdidas o robos; Evaluaciones de riesgos.	32
9.0. Amenazas a los sistemas informáticos y Ciberseguridad : opción mejorada	33
9. Requisitos obligatorios	33

TAPA Copyright © Do Not Copy



1. Introducción

1.1 Propósito de este Documento FSR

Este documento de Requisitos de Seguridad de Instalaciones (FSR) es el estándar oficial de TAPA para el almacenamiento y almacenamiento seguro. Es un estándar global común que se puede utilizar en acuerdos comerciales / de seguridad entre cliente s y proveedores de servicios logísticos (LSP) y / u otros solicitantes que buscan la certificación.

En el desarrollo de esta Norma, TAPA reconoce las múltiples diferencias en la forma en que se proporcionan los servicios de almacenamiento a nivel mundial, regional e incluso dentro de las empresas, y que el FSR puede aplicarse a la totalidad o parte de los servicios prestados por un Solicitante de proveedores de servicios logísticos. Dependiendo de la complejidad y el tamaño de la cadena de suministro, el cumplimiento de los estándares TAPA se puede lograr a través de un solo Solicitante de proveedor de servicios logísticos o múltiples Solicitantes de proveedores de servicios logísticos s y subcontratistas calificados.

Alcance

TAPA ha desarrollado tres opciones para apoyar la certificación:

- Certificación de un único sitio por una Entidad de Auditoría Independiente (IAB).
- Certificación Multiemplazamiento por una Entidad de Auditoría independiente. (IAB)
- Certificación de auto auditoría por auditores autorizados (AA) por el Proveedor de servicios logísticos / Solicitante o una Entidad de Auditoría independiente (IAB).

Usuarios

Los usuarios típicos de los estándares TAPA incluyen:

- Cliente s
- Proveedor de servicios logísticos / Solicitante
- Aplicación de la ley u otras organizaciones gubernamentales
- Organizaciones profesionales de la cadena de suministro
- Aseguradores



1. Introducción

1.2 Recursos para implementar el FSR de TAPA

Los recursos para cumplir con los requisitos del FSR serán responsabilidad del Proveedor de servicios logísticos / solicitante (LSP) y a expensas del Proveedor de servicios logísticos / solicitante (LSP), a menos que se negocie o acuerde lo contrario entre el cliente y el Proveedor de servicios logísticos /Solicitante. (LSP)

1.3 Protección de las políticas y procedimientos de LSP

Las copias de los documentos de políticas y procedimientos de seguridad solo se enviarán al cliente de acuerdo con los acuerdos de divulgación firmados entre el proveedor de servicios logísticos / solicitante (LSP) y Cliente y se manejarán como información confidencial.

2. Acerca de TAPA

2.1 Propósito de TAPA

El crimen de carga es uno de los mayores desafíos de la cadena de suministro para los fabricantes de productos valiosos y de alto riesgo y sus proveedores de servicios logísticos.

La amenaza ya no proviene sólo de criminales oportunistas. Hoy en día, las redes del crimen organizado operan a nivel mundial y utilizan ataques cada vez más sofisticados contra vehículos, locales y personal para lograr sus objetivos.

TAPA es un foro único que une a fabricantes globales, proveedores de logística, transportistas de carga, agencias de aplicación de la ley y otras partes interesadas con el objetivo común de reducir las pérdidas de las cadenas de suministro internacionales. El enfoque principal de TAPA es la prevención de robos mediante el uso de inteligencia en tiempo real y las últimas medidas preventivas.

2.2 Misión de TAPA

La misión de TAPA es ayudar a proteger los activos de los miembros minimizando las pérdidas de carga de la cadena de suministro. TAPA logra esto a través del desarrollo y la aplicación de estándares de seguridad globales, prácticas reconocidas de la industria, tecnología, educación, evaluación comparativa, colaboración regulatoria y la identificación proactiva de tendencias delictivas y amenazas de seguridad de la cadena de suministro.



3. Normas TAPA

3.1 Estándares de seguridad TAPA

Se han creado los siguientes estándares de seguridad globales de TAPA para garantizar el transporte y almacenamiento seguros de carga de alto valor dirigida al robo:

- Los Requisitos de Seguridad de las Instalaciones (FSR) representan estándares mínimos específicamente para el *almacenamiento seguro, o almacenamiento en tránsito*, dentro de la cadena de suministro.
- Los requisitos de seguridad de camiones (TSR) se centran exclusivamente en el transporte por camión y representan estándares mínimos específicos para el transporte *de productos por carretera* dentro de la cadena de suministro.

Los estándares de seguridad globales de TAPA se revisan según sea necesario cada tres años.

Este documento aborda únicamente los requisitos de FSR.

- El proceso de certificación para TAPA FSR está documentado en el documento Marco de certificación TAPA FSR.
- Se deben seguir las versiones actualizadas del documento TAPA FSR y TAPA FSR "Certification Framework" "DOCUMENTO DEL MARCO DE CERTIFICACION DE REQUISITOS DE SEGURIDAD DE INSTALACIONES TAPA" para lograr la certificación TAPA FSR.

3.2 Implementación

La implementación exitosa de los Estándares de Seguridad TAPA depende de que los LSP (Proveedores de Servicios Logísticos) / Solicitantes, Clientes (propietarios de la carga) y los Auditores Autorizados de TAPA trabajen juntos.



4. Orientación legal

4.1 Ámbito de aplicación

El FSR es un Estándar Global y todas las secciones del Estándar son obligatorias a menos que se otorgue una excepción a través del proceso oficial de exención. (Ver Sección 6.).

4.2 Traducción

En áreas geográficas donde el inglés no es el primer idioma, y donde la traducción es necesaria y aplicable, es responsabilidad del Proveedor de Servicios logísticos / Solicitante y su agente asegurarse de que cualquier traducción del FSR, o cualquiera de sus partes, refleje con precisión las intenciones de TAPA en el desarrollo y publicación de estas Normas.

4.3 La marca "TAPA"

"TAPA" es una marca registrada de la Asociación de Protección de Activos Transportados y no puede usarse sin el permiso escrito de TAPA en sus regiones reconocidas. Los Estándares TAPA y el material asociado se publican a través de, y por TAPA, y no pueden ser revisados, editados o cambiados por ninguna parte sin el permiso expreso por escrito de TAPA. El uso indebido de la marca TAPA puede resultar en la eliminación de la certificación o acciones legales.

4.4 Límites de responsabilidad

Mediante la publicación de estas Normas, TAPA no ofrece ninguna garantía o seguridad de que se evitarán todos los eventos de robo de carga, independientemente de que las Normas se implementen completamente y se implementen adecuadamente. Cualquier responsabilidad que pueda resultar de un robo de carga almacenada, o cualquier otra pérdida de carga almacenada bajo los Estándares FSR será por cuenta del Proveedor de servicios logísticos / solicitante y / o el Cliente de acuerdo con los términos y condiciones en su contrato entre sí y cualquier ley o estatuto que pueda aplicarse dentro de la jurisdicción sujeta.



5. Contratos y subcontratación

5.1 Contratos

El transporte, almacenamiento y manipulación seguro de los activos del cliente es responsabilidad del Proveedor de servicios logísticos / solicitante, sus agentes y subcontratistas durante la recogida, tránsito, almacenamiento y entrega, según se especifique en una liberación o contrato.

Cuando la especificación FSR se mencione o incluya en el contrato entre el proveedor de servicios/ solicitante y el cliente, también deberá hacerse referencia en el programa de seguridad del proveedor de servicios logísticos / solicitante.

El proveedor de servicios logísticos / solicitante proporcionará al cliente evidencia de la Certificación FSR y, cuando corresponda, evidencia de que se han cumplido los requisitos FSR. Además, cualquier presunta falta de implementación de los requisitos FSR por parte del proveedor de servicios logísticos / solicitante resolverá de acuerdo con los términos del contrato negociado entre el cliente y el Proveedor de servicios logísticos / solicitante.

5.2 Subcontratación

Los subcontratistas de almacenamiento incluyen un requisito contractual de que el Proveedor de servicios logísticos / Solicitante subcontratante cumpla con todos los estándares FSR establecidos.

5.3 Investigación y resolución de quejas de TAPA

Si TAPA recibe una queja formal relacionada con el desempeño de un Proveedor de Servicios Logísticos / Solicitante certificado, TAPA (sujeto a validación) puede requerir que el Proveedor de Servicios logísticos / Solicitante contrate una nueva auditoría a expensas del Proveedor de Servicios logísticos/ Solicitante. Si el Proveedor de Servicios logísticos / Solicitante no pasa la auditoría, o se niega a cumplir con este proceso, su certificado puede ser retirado.

6. Exenciones

6.1 Visión general

Una exención es una aprobación por escrito otorgada para eximir a una instalación de un requisito específico de TAPA o para aceptar una solución alternativa de cumplimiento. Se puede solicitar una exención si un Proveedor de Servicios logísticos / Solicitante no puede cumplir con un requisito específico en el FSR y puede justificar medidas alternativas. Las exenciones son válidas durante el período de la certificación.

Todas las solicitudes de exención para un requisito de seguridad específico (ya sea en parte o en su totalidad) deben enviarse a través de un formulario de solicitud de exención de TAPA a la Entidad de Auditoría Independiente (IAB) / Auditor Autorizado (AA) por el Proveedor de servicios logísticos / Solicitante (que se encuentra en el sitio web de TAPA). El Proveedor de Servicios logísticos / Solicitante asume toda la responsabilidad por la exactitud de la información proporcionada en la solicitud de exención.

Cada solicitud de exención debe enviarse a través de la Entidad de Auditoría Independiente (IAB)/ Auditor autorizado (AA) al Comité Regional de Exención de TAPA para su aprobación. Es responsabilidad de la Entidad de Auditoría Independiente (IAB) / Auditor Autorizado (AA) decidir si la solicitud está completa y justifica el procesamiento por parte de TAPA; Esto incluye la verificación de los factores atenuantes y/o controles de seguridad alternativos.

En caso de que los funcionarios de TAPA y / o el cliente impugnen que las condiciones de exención hayan cambiado, TAPA llevara a cabo una investigación formal y el Proveedor de Servicios logísticos / Solicitante entenderá que la exención puede ser revocada por TAPA.

6.2 Proceso de exención de Negocios

Si un proveedor de Servicios logísticos, (LSP) no puede cumplir con un requisito específico en el FSR, se implementa el proceso de exención que se describe a continuación.

Tabla 1: Responsabilidades: Solicitud de exención / Evaluación

Paso	Responsabilidad	Acción
1.	Proveedor de servicios logístico / Solicitante	Establece y verifica las medidas de mitigación.
2.	Proveedor de servicios logístico / Solicitante	Completa el formulario de Solicitud de Exención de TAPA y lo envía a la Entidad de Auditoría Independiente (IAB) / Auditor Autorizado (AA).

Paso	Responsabilidad	Acción
3.	IAB/ - Entidad de Auditoría independiente AA – Auditor autorizado	Revisa y verifica la integridad de la información contenida en el formulario de Solicitud de Exención de TAPA.
4.	IAB/ - Entidad de Auditoría independiente AA – Auditor autorizado	Envía el formulario de Solicitud de Exención de TAPA al Comité Regional de Exención de TAPA.
5.	Comité Regional de Exención de TAPA	Revisa la solicitud y otorga o deniega la exención.

6. Exenciones

Si se deniega la exención

En caso de que el Comité Regional de Exención de TAPA no apruebe la solicitud de exención, el Proveedor de Servicios logísticos / Solicitante está obligado a implementar todos los requisitos de seguridad del FSR.

Si se concede la exención

En caso de que el Comité Regional de Exención de TAPA apruebe la solicitud de exención, se tomarán las siguientes medidas:

Tabla 2: Aprobación de la exención

Paso	Responsabilidad	Acción
1.	Comité Regional de Exención de TAPA	Documenta y firma los detalles de la exención.
2.	Comité Regional de Exención de TAPA	Especifica la duración de la exención (hasta un máximo de tres años) y envía una copia a la AA.
3.	AA- Auditor autorizado	Informa al Proveedor de Servicios logísticos / Solicitante sobre el resultado de la Solicitud de Exención.
4.	Solicitante de proveedor logístico	Cumple con los requisitos de exención. La falta de cumplimiento anulará la aprobación de la exención.

6. 3 Exenciones para barreras físicas (bajo la sección 1) y para jaulas/áreas de alto valor (HVC, en la sección 4.5)

TAPA considerará una exención total o parcial de los requisitos de barreras perimetrales y / o para el HVC (JAULA DE ALTO VALOR) si se cumplen todas las siguientes condiciones previas:

Generales:

- La solicitud de exención se presenta utilizando el proceso oficial del formulario de solicitud de exención de TAPA y está respaldada por la Entidad de Auditoría Independiente (IAB) / Auditor Autorizado (AA).
- La solicitud de exención incluye detalles de cualquier medida mitigadora para garantizar que las mercancías vulnerables no estén innecesariamente expuestas al riesgo de robo o pérdida.
- Se debe realizar y presentar una evaluación de riesgos junto con la solicitud de exención. Cualquier vulnerabilidad significativa identificada en la evaluación de riesgos debe enumerarse por separado en la exención, junto con las medidas adoptadas para reducir el riesgo a un nivel aceptable.

6. Exenciones

Medidas de mitigación que deben estar implementadas y documentadas en la presentación de la solicitud de exención:

- **Barreras perimetrales:**
 - El equipo, los recursos y los procedimientos adicionales introducidos para detectar personas o vehículos no autorizados pueden incluir iluminación adicional, cobertura de CCTV, procedimientos mejorados de identificación de personas y vehículos, uso de chalecos de seguridad o uniformes en las áreas restringidas.
 - Se deben instalar señales perimetrales visibles en el idioma local que indiquen “Prohibido el acceso no autorizado” y “Prohibido estacionar sin autorización”
 - Se deben instalar señales visibles en las puertas externas o paredes del muelle, indicando a los conductores, visitantes, etc. que se dirijan al vestíbulo/oficina o al control de seguridad correspondiente.
 - Confirmación de que se han establecido procedimientos para garantizar que las áreas de manipulación de carga, de envío y recepción se inspeccionen y cumplan con las condiciones de exención al menos semanalmente.



- **HVC (JAULA /AEREA DE ALTO VALOR):**

- Para las exenciones de la jaula/área de alto valor (HVC), se deben considerar y documentar las acciones de mitigación adecuadas para minimizar el riesgo (cuando no esté disponible una jaula de alto valor) en la Evaluación de riesgos anual.
- La solicitud de exención incluye una declaración adjunta firmada por el Proveedor de Servicios logísticos / Solicitante que estipula que ningún cliente requiere una jaula/área de alto valor (HVC).

TAPA Copyright © Do Not Copy

7. Requisitos de seguridad de las instalaciones

Sección	Requisitos generales:	A	B	C
7.0				
7.0.1	Todos los procedimientos o políticas requeridos por esta Norma deben estar documentados.	✓	✓	✓
7.0.2	La dirección debe haber designado formalmente a una persona (AA) para la gestión de seguridad de la sede que sea responsable de mantener la normativa TAPA FSR, el cierre de las solicitudes de acciones correctivas (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 la programación de controles de cumplimiento, la comunicación con el AA, la recertificación, los cambios en normativa FSR, etc. <i>Nota: Estas personas pueden ser empleados o personas externas contratadas para desempeñar este papel.</i>	✓	✓	✓
7.0.3	Las auditorías internas (realizadas por un equipo multifuncional) sobre el sistema de gestión de seguridad, los informes de autoevaluación por parte del AA interno y el cierre de las solicitudes de acciones correctivas (SCARS) deben completarse y documentarse.	✓	✓	✓
7.0.4	Se requiere un procedimiento, registro y/o plano de llaves para las cerraduras físicas, tarjetas de acceso y/o llaves que gestionan y controlan las llaves físicas y electrónicas. El procedimiento debe incluir procesos para la duplicación, almacenamiento y respuesta ante llaves extraviadas y/o pérdidas.	✓	✓	✓
7.0.5	Se debe realizar y actualizar al menos anualmente una evaluación de riesgos que reconozca la probabilidad e impacto de los eventos relacionados con la seguridad. La dirección debe reconocer que los riesgos identificados han sido evaluados y que se han implementado controles apropiados para mitigar o eliminar los riesgos a un nivel aceptable. Como mínimo, deben evaluarse los siguientes eventos internos / externos comunes: robo de carga o información, acceso no autorizado a instalaciones o carga, manipulación / destrucción de sistemas de seguridad, recogidas ficticias de carga, continuidad de la seguridad durante escasez de mano de obra o desastres naturales, necesidad de barreras anti embestida para ventanas accesibles a nivel del suelo o puertas de muelle, etc. Eventos adicionales pueden considerarse según los riesgos locales/país.	✓	✓	✓
7.0.6	La persona que realiza auditorías internas o anuales para el proveedor de servicios logístico, llamado LSP Auditor autorizado (AA) debe estar capacitada. Esta persona puede ser la misma persona mencionada en 7.6.3 o puede ser una persona externa contratada para desempeñar este papel.	✓	✓	✓
7.0.7	Para entender el FSR y ser capaz de implementar todos sus requisitos, todos los Auditores autorizados (AA) de los solicitantes de proveedores de servicios logísticos, deben haber realizado y aprobado el examen correspondiente para la norma y versión de TAPA que se exige auditar.	✓	✓	✓

Sección	Perímetro	A	B	C
7.1	Manipulación de carga externa del almacén, envío y área de recepción (general)			
7.1.1	El sistema de circuito cerrado de televisión (CCTV) o sistema de videovigilancia (VSS) debe ser capaz de visualizar todo el tráfico en el área externa de manipulación de carga, envío y recepción (incluidos el punto de entrada y salida) para garantizar que todos los vehículos e individuos sean reconocibles en todo momento, a menos que haya obstrucciones temporales debido a necesidades operativas (por ejemplo, carga y descarga de camiones en tiempo real)	✓	✓	
7.1.2	Iluminación adecuada en zonas de carga y descarga. <i>Nota: La iluminación puede ser constante, activada por alarma, detección de movimiento, sonido, etc., con iluminación inmediata proporcionada.</i>	✓	✓	✓
7.1.3	Procedimiento establecido, que describa cómo se deben gestionar los vehículos y personas no autorizados dentro del área externa de manipulación de carga, envío y recepción. Las instrucciones sobre el procedimiento deben ser comunicadas a los miembros relevantes de trabajo, incluidos los vigilantes.	✓	✓	✓
7.1.4	El área de manipulación de carga, envío y recepción está adecuadamente controlada para prevenir el acceso no autorizado.		✓	✓
7.1.5	Para las ventanas accesibles a nivel del suelo o puertas de muelle, la evaluación anual de riesgos debe evaluar la necesidad de barreras anti embestida. Además, debe incluir la evaluación del uso de cubiertas de ventanas para evitar la visualización no autorizada de los espacios interiores (Ver Evaluación de riesgos, Sección 7.6.5.).	✓		
Barreras físicas				
7.1.6	La barrera física rodea el área de manipulación de carga, envío y recepción.	✓		
7.1.7	La barrera física alrededor del área de manipulación, envío y recepción tiene una altura mínima de 6 pies / 1.8 metros. <i>Nota: La barrera física, diseñada para evitar el acceso no autorizado, debe medir 6 pies/1.8 metros en toda su longitud, incluso en áreas donde cambia el nivel del suelo, es decir, más bajo.</i>	✓		
7.1.8	La barrera física alrededor del área de manipulación de carga, envío y recepción se mantiene en buen estado.	✓		
7.1.9	La (s) puerta(s) dentro de las barreras del área de manipulación de carga, envío y recepción están controladas por personal o de forma electrónica.	✓		
7.1.10	La barrera física alrededor del área de manipulación de carga, envío y recepción se inspecciona para verificar su integridad y daños, al menos semanalmente.	✓		
Áreas de muelle externas				
7.1.11	Las áreas exteriores de los muelles están cubiertas mediante cámaras CCTV / VSS de color o "día / noche".	✓	✓	✓

Sección	Perímetro	A	B	C
7.1.12	Cámaras CCTV/VSS instaladas para poder visualizar las operaciones y movimientos alrededor del área externa del muelle siempre, salvo que haya una obstrucción temporal por necesidades operativas (carga y descarga de camiones en tiempo real).	✓	✓	✓
7.1.13	Todos los vehículos e individuos alrededor de las áreas de muelle externas deben estar cubiertos por cámaras CCTV / VSS. que puedan mostrar claramente la información de identificación del vehículo y discernir los rasgos faciales del personal. <i>Nota: TAPA permitirá a los titulares de certificaciones existentes que no tengan la capacidad de actualizar la resolución de la cámara, continuar con su resolución actual hasta la revisión de 2026. Los nuevos titulares de certificados o las nuevas sedes deben cumplir el nuevo requisito.</i>	✓		
7.1.14	Los vehículos e individuos alrededor de las áreas externas de los muelles deben estar cubiertos y ser visibles en la mayoría de los casos por cámaras CCTV / VSS.		✓	✓
7.1.15	Todas las áreas externas alrededor de las puertas de los muelles deben estar completamente iluminadas.	✓	✓	✓
Acceso a vehículos personales				
7.1.16	Se permite el acceso de vehículos personales solo a las áreas de manipulación de carga, envío y recepción si están preaprobados y restringidos a áreas de estacionamiento señalizadas / designadas. No se permite el estacionamiento de vehículos personales dentro de una distancia de 25 m a pie de las áreas externas de los muelles. Los procedimientos para la aprobación previa y las restricciones vigentes están implementados.	✓	✓	✓

Sección	Paredes exteriores, techo y puertas	A	B	C
7.2				
Lados exteriores de la instalación: CCTV				
7.2.1	Cámara exterior de CCTV / VSS a color o "día / noche" instalada cubriendo todos los lados exteriores de la instalación.	✓		
7.2.2	Sistema de cámaras exterior CCTV / VSS a color o "día / noche" instalado cubriendo los lados exteriores de la instalación con puertas, ventanas u otras aberturas.		✓	
7.2.3	Todas las vistas del sistema de cámaras exteriores CCTV/VSS son claras siempre, salvo obstrucción temporal por necesidades operativas (carga y descarga de camiones en tiempo real).	✓		
7.2.4	Todos los vehículos e individuos alrededor de los lados exteriores de las instalaciones deben estar cubiertos por cámaras CCTV / VSS, que puedan mostrar claramente la información de identificación del vehículo y discernir las características faciales del personal.	✓		
7.2.5	Vehículos y personas son visibles en la mayoría de los casos por las cámaras exteriores CCTV / VSS.		✓	
Paredes exteriores y techo				
7.2.6	Paredes exteriores y techo diseñados y mantenidos para resistir la penetración (Ejemplo: ladrillo, bloque, losa de hormigón inclinable, paredes de panel sándwich).	✓	✓	✓

Sección	Paredes exteriores, techo y puertas	A	B	C
7.2.7	Cualquier ventana que se pueda abrir, abertura de ventilación u otra abertura en las paredes exteriores de la instalación, o cualquier ventana sellada instalada a menos de 3 metros del suelo de trabajo en las paredes exteriores de la instalación, debe tener una barrera física o estar alarmada y vinculada al sistema de alarma principal.	✓	✓	
7.2.8	Cualquier ventana, claraboya, abertura de ventilación, escotilla de acceso u otra abertura en el techo de la instalación, debe tener una barrera física o estar alarmada y conectada al sistema de alarma principal.	✓		
7.2.9	El acceso externo al techo (mediante escalera o escalones) debe estar: Físicamente cerrado y cubierto por cámaras CCTV / VSS (cámaras a color o "día / noche"). o Físicamente cerrado y alarmado.	✓		
7.2.10	El acceso externo al techo (escalera o escalones) debe estar cerrado físicamente.		✓	✓
7.2.11	Todas las puertas exteriores de la instalación y las puertas de la oficina deben estar alarmadas para detectar aperturas no autorizadas y conectadas al sistema de alarma principal. <i>Nota: Este requisito no se aplica a las puertas de los muelles; consulte la sección 7.2.17 para conocer los requisitos de alarma de puerta de muelle.</i>	✓	✓	✓
7.2.12	Cada puerta exterior de almacén, puerta de oficina u otra abertura debe identificarse de manera única, ya sea por puerta o por zona, dentro del sistema de alarma principal.	✓		
7.2.13	Todas las puertas exteriores de almacén siempre deben estar cerradas y aseguradas cuando no estén en uso activo. Cuando corresponda, las llaves/códigos deben estar controlados.	✓	✓	
7.2.14	Las puertas y marcos peatonales del almacén no deben ser fácilmente penetrables. Si las bisagras están en el exterior, deben estar fijadas con pasadores o soldaduras puntuales. Las puertas de vidrio son inaceptables si no tienen detectores de rotura de vidrio, u otro dispositivo de detección local que da cobertura (por ejemplo, PIR) y esté conectado directamente al centro de alarmas y monitorización o el vidrio esté protegido por barras/malla.	✓	✓	✓
7.2.15	Las salidas de emergencia que se utilizan únicamente con fines de emergencia (por ejemplo, salidas de incendio) deben estar siempre alarmadas con dispositivo sonoro individual o zonificado.	✓	✓	
7.2.16	Las puertas de los muelles deben tener resistencia suficiente para disuadir o retrasar la entrada forzada con pequeñas herramientas manuales portátiles.	✓	✓	✓

Sección	Paredes exteriores, techo y puertas	A	B	C
7.2.17	Puertas de muelle Horas no operativas: Las puertas del muelle deben estar cerradas, aseguradas (es decir, electrónicamente desactivadas o físicamente cerradas). las puertas de muelle deben estar alarmadas para detectar intrusiones no autorizadas y generar una alarma conectada al sistema de alarma principal. Horas operativas: Las puertas del muelle deben estar cerradas cuando no estén en uso activo. Las puertas de tijera, si se usan, deben estar aseguradas por un bloqueo mecánico de corredera o un pestillo y tener una altura mínima de 8 pies / 2,4 metros.	✓	✓	✓

Sección	Puntos de entrada y salida de oficinas y almacén	A	B	C
7.3	Punto (s) de entrada de visitantes en el área de oficinas			
7.3.1	El punto o puntos de entrada de visitantes son controlados por un empleado / guardia / recepcionista que ha sido capacitado en la emisión de credenciales, controles, registro de visitantes, requisitos de acompañamiento, etc. (Procedimiento establecido para visitas fuera del horario operativo).	✓	✓	✓
7.3.2	El punto o puntos de entrada de visitantes del área de la oficina están cubiertos por cámaras de CCTV; (cámaras a color o "día/noche"); las personas son claramente reconocibles en todo momento.	✓	✓	
7.3.3	Alarma de coacción presente en el punto o puntos de entrada de visitantes en el área de oficinas y probada semanalmente.	✓	✓	
7.3.4	Todos los visitantes al área de la oficina deben ser identificados mediante un documento de identificación con foto emitido por el gobierno (por ejemplo, carnet de conducir, pasaporte o tarjeta de identificación nacional, etc.).	✓	✓	✓
7.3.5	Todos los visitantes al área de la oficina deben registrarse y mantener un registro durante un mínimo de 30 días.	✓	✓	✓
7.3.6	Todas las credenciales de visitante deben conciliarse cuando el visitante abandona las instalaciones y el registro completo debe revisarse diariamente.	✓	✓	
7.3.7	Todos los visitantes deben llegar visiblemente los distintivos o pases y ser acompañados por personal de la empresa.	✓	✓	
Puntos de entrada para el personal de empresa				
7.3.8	Punto(s) de entrada para el personal controlado las 24 horas del día, los 7 días de la semana.		✓	✓
7.3.9	Punto(s) de entrada para el personal, controlados mediante dispositivo electrónico de control de acceso 24/7. Se registra el acceso.	✓		

Sección	Puntos de entrada y salida de oficinas y almacén	A	B	C
7.3.10	El punto o puntos de entrada para el personal están cubiertos por cámaras de CCTV (cámaras a color o día/noche)	✓	✓	
7.3.11	Después de la selección/evaluación, todos los empleados deben recibir distintivos de identificación con foto de la empresa.	✓	✓	
7.3.12	Todos los demás trabajadores deben contar con una tarjeta de identificación de la empresa para que sean reconocibles dentro de las instalaciones.	✓	✓	
7.3.13	Los distintivos de todo el personal deben mostrarse claramente.	✓	✓	
7.3.14	Los distintivos del personal no deben compartirse en ninguna circunstancia y debe existir una política de emisión de distintivos establecido.	✓	✓	
Identificación del conductor y del vehículo				
7.3.15	Todos los conductores deben ser identificados mediante un documento de identificación con foto emitida por el gobierno (por ejemplo, carnet de conducir, pasaporte o documento nacional de identidad, etc.) y se debe mantener un registro de conductores.	✓	✓	✓
7.3.16	Verificación de que el carnet de conducir es válido, la identificación con foto del conductor no haya caducado y que coincide con el conductor.	✓	✓	✓
7.3.17	Los identificadores de los vehículos se registran manualmente (es decir, por escrito) o con cámaras. Deben incluir como mínimo la matrícula y el tipo de vehículo.	✓		

Sección	Interior del almacén y la oficina	A	B	C
7.4				
Área de almacén: paredes para inquilinos múltiples				
7.4.1	Paredes, suelos o techos contruidos, para áreas compartidas por múltiples inquilinos, contruidos/diseñados y mantenidos para resistir la penetración (Ejemplo: paredes de ladrillo, bloque, losa de concreto inclinable, paredes de paneles sándwich).	✓	✓	✓
7.4.2	Si las paredes interiores de suelo a techo para múltiples inquilinos están contruidas con malla de alambre de grado de seguridad u otra barrera segura reconocida por la industria, entonces también debe alarmarse para detectar intrusiones. <i>Nota: Las redes, cercas de baja calidad o mallas no clasificadas como de seguridad no son aceptables.</i>	✓	✓	✓

Sección	Interior del almacén y la oficina	A	B	C
Áreas internas del almacén				
7.4.3	Se requiere la detección de intrusiones (por ejemplo, detección de infrarrojos, movimiento, sonido o de vibración) para para monitorear las áreas internas del almacén. Las alarmas deben activarse y vincularse al sistema de alarma principal durante las horas no operativas (es decir, cuando el almacén está cerrado). <i>Nota: Si el almacén está realmente operativo 24/7/366, este requisito puede ser N/A si los riesgos y mitigaciones están documentados en la Evaluación de riesgos local. (Ver Sección 7.0.5)</i> <i>Independientemente de las horas operativas, siempre se requiere detección de intrusión perimetral o barreras físicas en puertas externas y ventanas de la planta baja en oficinas y almacenes. (Ver sección 7.2.11).</i>	✓		
Puertas internas de los muelles y áreas del muelle internas				
7.4.4	Todas las puertas de muelle internas y áreas de muelle internas están cubiertas por cámaras CCTV. (Cámaras a color o "día/noche").	✓	✓	✓
7.4.5	La zona de la carga / descarga de mercancías, en todas las puertas de muelle internas y áreas del muelle, debe estar despejada en todo momento a menos que haya una obstrucción temporal debido a necesidades operativas (por ejemplo, carga y descarga de camiones en tiempo real).	✓	✓	✓
7.4.6	Los activos del cliente deben estar bajo vigilancia 100% CCTV en las áreas de manipulación de carga o preparación (es decir, áreas de preparación, manipulación, paletizado, movimientos hacia y desde estanterías de almacenamiento, muelles, o zonas de tránsito).	✓	✓	
Control de acceso entre la oficina y el muelle/almacén				
7.4.7	Control de acceso entre la oficina y el muelle/almacén.	✓	✓	
7.4.8	Las alarmas de acceso con tarjeta o intercomunicador, en puertas ubicadas entre la oficina y el muelle / almacén, son audibles localmente y generan una alarma para respuesta si se mantienen abiertas durante más de 60 segundos o inmediatamente si se fuerza su apertura.	✓		
7.4.9	Las alarmas de puertas entre la oficina y el muelle / almacén son localmente audibles o envían una alarma para respuesta cuando se mantienen abiertas durante más de 60 segundos o si se fuerza su apertura.		✓	
7.4.10	El personal autorizado del Proveedor de Servicios logísticos / Solicitante y los visitantes acompañados tienen permitido el acceso a las áreas de muelle / almacén según una necesidad comercial y de forma restringida.	✓	✓	✓
7.4.11	La lista de acceso a las áreas de muelle / almacén se revisa al menos trimestralmente para limitar / verificar que el permiso de acceso solo se otorgue al personal designado / autorizado.	✓	✓	
Jaula / Área de alto valor (HVC)				
7.4.12	El tamaño y el uso de la jaula/área de alto valor (HVC) pueden acordarse por el acuerdo del Cliente / Solicitante de proveedores de servicios logísticos. Si no hay un acuerdo, entonces la jaula/área de alto valor (HVC) debe poder almacenar un mínimo de 6 metros cúbicos de producto.	✓	✓	

Sección	Interior del almacén y la oficina	A	B	C
7.4.13	La jaula/área para mercancía de alto valor (HVC) / debe ser un área perimetral enjaulada o de paredes solidas en todos los lados, incluido la parte superior / techo.	✓	✓	
7.4.14	Dispositivo de bloqueo en la puerta / portón de la jaula/área de alto valor.	✓	✓	
7.4.15	Cobertura completa de CCTV / VSS (cámaras en color o "día / noche") en la entrada y área interna de la jaula/área de alto valor (HVC). <i>Nota: Si la jaula/área de alto valor (HVC) es demasiado pequeña para ubicar una cámara en el interior, la cobertura de la cámara de la entrada es suficiente.</i>	✓		
7.4.16	Cobertura de CCTV (cámaras en color o "día/noche") en la entrada de la jaula/área de alto valor. (HVC)		✓	
7.4.17	Si el acceso a la jaula/área de alto valor (HVC) es necesario para más de 10 personas, entonces el acceso debe controlarse electrónicamente mediante tarjeta de proximidad. Si el acceso es requerido por 10 personas o menos, se utilizará un sistema de cerradura de alta resistencia o candado respaldado por un sistema controlado de emisión de llaves. Las llaves pueden ser asignadas a individuos para cubrir un turno, pero no deben transferirse sin aprobación y deben registrarse en el registro de llaves. Todas las llaves deben ser devueltas y contabilizadas cuando no estén en uso.	✓		
7.4.18	Las puertas/portones de la jaula/área de alto valor (HVC) están alarmados para detectar la entrada forzada. Las alarmas se pueden generar con contactos de puerta y/o detectar movimiento CCTV/VSS para detectar accesos no autorizados.	✓		
7.4.19	El perímetro de la jaula/área de alto valor (HVC) se mantiene en buenas condiciones y se inspecciona mensualmente para verificar su integridad y detectar daños.	✓		
7.4.20	El Proveedor de Servicios logísticos / Solicitante debe garantizar que el acceso a la jaula/área de alto valor (HVC) solo se otorgue al personal designado / autorizado. La lista de acceso aprobada a la jaula/área de alto valor (HVC) se revisa mensualmente y se actualiza en tiempo real cuando el empleado deja el empleo o ya no necesita acceso. Procedimiento para el acceso a la jaula/área de alto valor (HVC), debe estar establecido.	✓	✓	
Inspección de basura del almacén				
7.4.21	Los contenedores/recintos principales de recolección/compactación de basura internos y/o externos del almacén son monitoreados por CCTV/VSS.	✓		
7.4.22	Cuando se utilizan, las bolsas de basura utilizadas dentro del almacén son transparentes.		✓	✓

Precarga y preparación				
7.4.23	No se permite la carga previa ni el estacionamiento de camiones/ FTL dedicados del cliente fuera de las instalaciones del almacén durante las horas no operativas, a menos que haya un acuerdo mutuo entre el cliente y solicitante de proveedores de servicios logísticos. Se deben implementar medidas de seguridad alternativas (por ejemplo, dispositivos de seguridad adicionales en el camión/contenedor). <i>Nota: "Fuera de la instalación del almacén se refiere a aquellas áreas separadas, alejadas de la instalación, pero aún dentro de la cerca perimetral / patio / perímetro del solicitante de proveedores de servicios logísticos.</i>	✓	✓	✓
Contenedores personales y controles de salida				
7.4.24	Hay procedimientos de seguridad establecidos que definen cómo se controlan los "contenedores personales" dentro del almacén. Los contenedores personales incluyen recipientes herméticos, mochilas, refrigeradores, carteras, bolsos, etc.	✓	✓	
7.4.25	Si lo permite la legislación local, el Proveedor de Servicios logísticos / Solicitante debe elaborar y mantener un procedimiento documentado para el control de salida. La activación del procedimiento queda a discreción del Proveedor de Servicios logísticos / Solicitante y / o según el acuerdo del Cliente / Proveedor de servicios logísticos. Como mínimo, el procedimiento debe abordar el derecho del proveedor de servicios logístico, a realizar registros en caso de que surja la necesidad de llevar a cabo controles cuando normalmente no son necesarias (por ejemplo, cuando se sospecha de robo por parte de empleados).	✓		
Control de equipos de manipulación de carga				
7.4.26	Procedimiento disponible, que requiere que todas las carretillas elevadoras y otros equipos de manipulación de carga motorizados se desactiven durante las horas no operativas. <i>Nota: Esto no incluye gatos de mano / transpaletas.</i>	✓	✓	
integridad del contenedor o remolque; Inspección de los 7 puntos				
7.4.27	Inspección física de 7 puntos realizada en todos los contenedores o remolques dedicados a la carga del cliente: pared frontal, lado izquierdo, lado derecho, suelo, techo, puertas internas/ externas y mecanismo de bloqueo, parte externa / tren de rodaje. <i>Nota: Esto se aplica a todos los tipos de remolques y contenedores bajo llave y / o precinto (es decir, No se limita a contenedores de carga marítima).</i>	✓	✓	✓
Proceso de entrega de carga; Precintos de seguridad				

7.4.28	A menos que el cliente lo exima específicamente, se utilizan precintos de seguridad a prueba de manipulaciones en todos los envíos directos y sin escalas. Los precintos deberán estar certificados según la norma ISO 17712 (clasificación I, S o H). <i>Nota: No se requieren precintos en envíos de paradas múltiples, debido a la complejidad y el riesgo asociados con los conductores que llevan múltiples precintos.</i>	✓	✓	✓
7.4.29	El Proveedor de Servicios logísticos / Solicitante debe tener procedimientos documentados para la gestión y el control de los precintos de seguridad, cerraduras de puertas de remolques (contenedores), cerraduras de pasadores y otros equipos de seguridad.	✓	✓	✓
7.4.30	Los precintos de seguridad solo pueden ser colocados o retirados por personal autorizado, es decir, personal del almacén, que tiene instrucciones de reconocer e informar sobre los precintos comprometidos/dañados. Los precintos nunca deben ser colocados o retirados por el conductor a menos que estén exentos del cliente.	✓	✓	✓
7.4.31	Se tienen procedimientos establecidos para reconocer y reportar precintos de seguridad comprometidos/dañados.	✓	✓	✓
Integridad de la carga; Proceso de validación de carga/descarga				
7.4.32	Procedimientos sólidos establecidos, que garantizan que todos los activos del cliente enviados y recibidos se validan en el punto de entrega mediante la realización de un recuento manual y / o electrónico de piezas. El proceso debe garantizar que las anomalías se reconozcan de manera consistente, se documenten y sean informadas al Proveedor de Servicios logísticos / Solicitante y / o cliente. Los registros manuales y/o electrónicos deben tener calidad probatoria. Si los conductores no están presentes para presenciar esta actividad, el cliente /Proveedor de Servicios logísticos / Solicitante debe garantizar la verificación de conteo alternativa, como escaneos y / o imágenes de CCTV / VSS, recopiladas y retenidas específicamente para este propósito. <i>Nota: Además de las piezas faltantes, las anomalías pueden incluir daños, falta de fleje o precinto, cortes u otras aberturas obvias, que puedan indicar un posible robo o hurto.</i>	✓	✓	✓
Recogidas fraudulentas				
7.4.33	La identificación del conductor del camión, la documentación de recogida de carga y los detalles de prealerta previa especificados por el cliente se validan antes de la carga. El procedimiento debe estar establecido.	✓	✓	✓

Sección	Sistemas de Seguridad; Diseño, seguimiento y respuestas.	A	B	C
7.5	Centro de alarma y monitorización			
7.5.1	Monitorización de eventos de alarma 24x7x366 a través de un centro de alarmas y monitorización interno o externo de terceros, protegido contra el acceso no autorizado. <i>Nota: Los centros de alarmas y monitorización pueden estar ubicados dentro o fuera de la sede, y pueden ser propiedad de la empresa o de terceros. En todos los casos, el acceso debe controlarse mediante el uso de un sistema electrónico de control de acceso (credenciales), cerraduras o escáneres biométricos.</i>	✓	✓	✓
7.5.2	El centro de alarmas y monitorización responde a todas las alarmas del sistema de seguridad en tiempo real 24x7x366.	✓	✓	✓
7.5.3	El centro de alarmas y monitorización reconoce la activación de la alarma y responde en menos de 3 minutos.	✓	✓	✓
7.5.4	Se dispone de informes de monitorización de alarmas.	✓	✓	✓
7.5.5	Hay procedimientos establecidos para la respuesta del centro de alarmas y monitorización.	✓	✓	✓
Sistema de detección de intrusión (IDS)				
7.5.6	Todos los sistemas de detección de intrusión se activan durante las horas no operativas y están conectados al sistema de alarma principal.	✓	✓	✓
7.5.7	Se guardan los registros de alarmas de detección de intrusión durante 60 días	✓	✓	
7.5.8	Los registros de alarma del sistema de detección de intrusión se almacenan de manera segura y se realizan copias de seguridad.	✓		
7.5.9	Los registros de alarma del sistema de detección de intrusión se almacenan de forma segura.		✓	
7.5.10	Se establece un procedimiento para garantizar que el acceso al sistema de detección de intrusión esté restringido a personas autorizadas o administradores de sistemas. Esto incluye servidores, consolas, controladores, paneles, redes y datos. Los privilegios de acceso deben actualizarse de manera rápida cuando las personas abandonan la organización o cambian de puesto de trabajo, ya no necesitan acceso.	✓	✓	✓
7.5.11	Se transmite una alarma en caso de corte de energía / pérdida del sistema de seguridad de intrusión. <i>Nota: Para sistemas con suministro de alimentación ininterrumpida (UPS), la alarma se transmite cuando falla la batería del UPS.</i>	✓	✓	✓

Sección	Sistemas de Seguridad; Diseño, seguimiento y respuestas.	A	B	C
7.5.12	Verificación que garantiza que la configuración de la alarma del sistema de detección de intrusión esta correctamente activada. <i>Nota: Procedimientos establecidos que validan que las alarmas estén activadas durante las horas no operativas.</i>	✓	✓	✓
7.5.13	Alarma del sistema de detección de intrusión, transmitida por línea fija o inalámbrica y/o también se activará si falla el modo de comunicación utilizado.	✓	✓	
7.5.14	Sistema de comunicación de respaldo implementado en caso de fallo del dispositivo de alarma del sistema de detección de intrusión y / o fallo de línea.	✓	✓	
Sistema de control de acceso automático (AACS)				
7.5.15	Registros de transacciones del sistema de control de acceso disponibles. Los registros son almacenados durante 90 días de forma segura y respaldados.	✓	✓	
7.5.16	Procedimiento establecido, para garantizar que el acceso al Sistema de control de accesos (AACS) está restringido a personas autorizadas o administradores de sistemas. Los privilegios de acceso deben actualizarse al momento, cuando las personas abandonan la empresa o cambian de puesto de trabajo, y ya no requieren acceso.	✓	✓	
7.5.17	Se revisan los informes del sistema de control de acceso, al menos trimestralmente para identificar irregularidades o mal uso (es decir, múltiples intentos fallidos, lecturas falsas (es decir, tarjeta deshabilitada), evidencia de uso compartido de tarjetas para permitir el acceso no autorizado, etc.). Procedimiento implementado.	✓	✓	
CCTV				
7.5.18	Grabación digital de CCTV/VSS implementada.	✓	✓	✓
7.5.19	La velocidad de grabación para CCTV / VSS se establece como mínimo para 8 fotogramas por segundo (fps) por cámara. <i>Nota: TAPA permitirá a los titulares actuales de certificaciones que no tengan la capacidad de actualizar a 8 fotogramas por segundo (fps) continuar con los 3 fps existentes hasta la revisión de 2026.</i> <i>Los nuevos titulares de certificados deben cumplir con el nuevo requisito.</i>	✓	✓	✓
7.5.20	La funcionalidad de grabación digital se verifica diariamente en días operativos mediante procedimiento estipulado. Registros disponibles.	✓	✓	✓
7.5.21	Las grabaciones de CCTV/VSS se almacenarán durante 30 días cuando la ley local lo permita. El Proveedor de Servicios logísticos / Solicitante deberá proporcionar evidencia de cualquier ley local que prohíba el uso de CCTV y / o limite el almacenamiento de datos de video a menos de 30 días.	✓	✓	✓
7.5.22	El acceso al sistema CCTV/VSS esta estrictamente controlado, incluido el hardware, software y el almacenamiento de datos / video. Esta sala debe estar cerrada con llave, si el sistema de almacenamiento CCTV / VSS está en las instalaciones con controles de acceso implementados.	✓	✓	✓

Sección	Sistemas de Seguridad; Diseño, seguimiento y respuestas.	A	B	C
7.5.23	Por motivos de seguridad, las imágenes de CCTV / VSS, solo serán visualizadas por personal autorizado.	✓	✓	✓
7.5.24	Procedimientos establecidos que detallan la política de protección de datos de CCTV/VSS para usar imágenes en tiempo real y de archivo según la ley local.	✓	✓	
Iluminación exterior e interior				
7.5.25	Los niveles de iluminación exteriores e interiores son suficientes para respaldar imágenes de CCTV que permiten la investigación y la grabación de imágenes de calidad probatoria.	✓	✓	
7.5.26	Los niveles de iluminación exteriores e interiores son suficientes para reconocer claramente todos los vehículos y personas.	✓		

Sección	Capacitación/ formación y procedimientos	Un	B	C
7.6				
Protocolos de ampliación				
7.6.1	Procedimientos locales establecidos para la manipulación de los activos del cliente, incluido el proceso para informar en tiempo y forma de los activos perdidos, extraviados o robados del cliente. Las incidencias deben ser reportadas por el Proveedor de Servicios logísticos / Solicitante al cliente dentro de las 24 horas. Los robos evidentes serán reportados inmediatamente. Se hará un seguimiento constante del proceso.	✓	✓	✓
7.6.2	Los contactos de emergencia de los directivos/responsables de las instalaciones del Proveedor de Servicios logísticos / Solicitante para incidentes de seguridad deben estar enumerados y disponibles. El listado se actualiza cada 6 meses e incluye los contactos de emergencia de las fuerzas del orden	✓	✓	✓
Compromiso de la Dirección				
7.6.3	Dirección debe desarrollar, comunicar y mantener una política de seguridad para garantizar que todas las personas relevantes (es decir, empleados y contratistas) conozcan claramente las expectativas de seguridad.	✓	✓	✓
Formación				
7.6.4	Se proporcionará capacitación en seguridad y concienciación sobre amenazas a todos los empleados en los primeros 60 días de empleo y, posteriormente, cada 2 años.	✓	✓	✓
7.6.5	Se proporcionará capacitación en concienciación sobre seguridad, a los empleados que tengan acceso a la información de los clientes, enfocada en proteger los datos de los envíos electrónicos y físicos del cliente.	✓	✓	✓
Acceso a los activos del cliente				
7.6.6	Procedimiento(s) establecido(s) para proteger los activos del cliente (es decir, la carga), del acceso no autorizado por parte de empleados, visitantes, etc.	✓	✓	
Control de la información				
7.6.7	El acceso a documentos de envío e información sobre los activos del cliente, están controlados en función de la "necesidad de saber".	✓	✓	✓

Sección	Capacitación/ formación y procedimientos	U n	B	C
7.6.8	El acceso a documentos de envío e información sobre los activos del cliente esta supervisado y registrado.	✓	✓	✓
7.6.9	Los documentos de envío e información sobre los activos del cliente están protegidos hasta su destrucción.	✓	✓	✓
Informes de incidentes de seguridad				
7.6.10	Sistema de notificación y seguimiento de incidentes de seguridad implementado, utilizado para implementar medidas proactivas.	✓	✓	
Programas de mantenimiento				
7.6.11	Programas de mantenimiento implementados para todas las instalaciones/sistemas de seguridad técnica (física) para garantizar su funcionalidad (como CCTV/VSS, controles de acceso, detección de intrusos e iluminación).	✓	✓	✓
7.6.12	El mantenimiento preventivo se realiza una vez al año, o de acuerdo con las especificaciones del fabricante.	✓	✓	✓
7.6.13	Las verificaciones de funcionalidad de todos los sistemas se realizan una vez por semana y se documentan, a menos que el fallo del sistema se informe o alarme de forma inmediata / automática.	✓	✓	
7.6.14	Se debe iniciar una orden de reparación en un plazo de 48 horas desde la identificación del fallo del sistema. Para cualquier reparación que se espera que exceda las 24 horas, se deben implementar mitigaciones alternativas.	✓	✓	
Orientación a contratistas				
7.6.15	El solicitante de Proveedor de Servicios logísticos (LSP) debe asegurarse de que todos los subcontratistas / colaboradores conozcan y cumplan con los programas de seguridad relevantes del LSP.	✓	✓	✓
Registros de envío y recepción				
7.6.16	Documentos de envío y recepción legibles, completos y precisos (es decir, hora, fecha, firmas, conductor, persona carga y recepción, detalles y cantidad del envío, etc.).	✓	✓	✓
7.6.17	El solicitante de Proveedor de Servicios logísticos (LSP) debe mantener registros de todas las recogidas y comprobantes de entrega, por un período no inferior a los dos años, y ponerlos a disposición de las investigaciones de pérdidas según sea necesario.	✓	✓	✓
7.6.18	El comprobante de entrega debe ser proporcionado según acuerdo escrito entre el cliente y el solicitante de proveedores de servicios logísticos. Cuando el cliente lo requiera, en destino deben notificar al punto de origen, dentro del plazo acordado de la recepción del envío, conciliando los detalles de la prealerta del envío.	✓	✓	✓
Proceso de prealerta establecido				

Sección	Capacitación/ formación y procedimientos	U n	B	C
7.6.19	Cuando el cliente lo requiera, se implementará un proceso de prealerta aplicado a los envíos entrantes y / o salientes. Los detalles de la prealerta deben ser acordados por el cliente y el solicitante de proveedores de servicios logísticos. Los detalles recomendados incluyen: hora de salida, hora prevista de llegada, empresa de transportes, nombre del conductor, detalles de la matrícula, información del envío (cantidad de bultos, peso, número de conocimiento de embarque, etc.) y números de precinto/s del camión/remolque.	✓	✓	✓
Sección	Integridad de la fuerza laboral	A	B	C
7.7	Selección / Investigación / Verificación de antecedentes (según lo permita la ley local)			
7.7.1	El Proveedor de servicios logísticos/Solicitante debe contar con un proceso de selección / investigación / antecedentes que incluya como mínimo, verificaciones de antecedentes laborales y antecedentes penales. Este proceso de evaluación/filtrado/antecedentes aplica a todos los solicitantes, incluidos empleados y Contratistas. El Proveedor de servicios logísticos/Solicitante también requerirá que se aplique un proceso equivalente a las empresas contratistas que suministran personal de trabajo temporal.	✓	✓	✓
7.7.2	Se requiere que el personal de trabajo temporal firme una declaración de que no tiene condenas penales actuales y cumplirá con los procedimientos de seguridad de Proveedor de servicios logísticos/Solicitante.	✓	✓	✓
7.7.3	La entidad proveedora de servicios logísticos o solicitante deberá tener acuerdos establecidos para obtener la información necesaria de selección, evaluación y antecedentes por parte de la agencia y/o subcontratista que proporcione personal de trabajo temporal o deberá llevar a cabo dicha selección por sí misma. La evaluación debe incluir una verificación de antecedentes penales y verificaciones de empleo.	✓	✓	✓
7.7.4	Procedimiento establecido para abordar declaraciones falsas de solicitantes/trabajadores antes y después de la contratación	✓	✓	✓
Terminación o reconstrucción de empleados				
<i>Nota: La terminación incluye separaciones voluntarias e involuntarias: miembros de la fuerza laboral despedidos y renunciados.</i>				
7.7.5	Recuperar activos físicos de empleados que son despedidos o dejan la empresa incluyendo identificaciones de empresa, tarjetas de acceso, llaves, equipos, activos de tecnología e información confidencial. Se requiere un procedimiento documentado establecido.	✓	✓	✓
7.7.6	Proteger los datos del cliente: Dar de baja el acceso del empleado a sistemas físicos o electrónicos, incluidos aquellos que contienen los datos del cliente (inventario o programaciones). Se requiere procedimiento establecido.	✓	✓	✓
7.7.7	Lista de control de incorporación y desvinculación de empleados, para su verificación.	✓	✓	✓

Sección	Capacitación/ formación y procedimientos	U n	B	C
7.7.8	Recontratación: Se han establecido procedimientos para evitar que el Proveedor de Servicios logísticos / Solicitante vuelva a contratar a persona si los criterios de denegación / terminación siguen siendo válidos. <i>Nota Se revisan los registros antes de volver a contratar (por ejemplo, antecedentes de personal previamente despedido o solicitantes rechazados anteriormente (empleo previamente denegado).</i>	✓	✓	✓

8. Requisitos de la función central (solo aplicable para la certificación de múltiples emplazamientos)

Sección	Función central	A	B	C
8.1	General			
8.1.1	Existe una función central para gestionar el sistema de gestión de seguridad para todos los emplazamientos como se define en el alcance de la certificación Multi emplazamiento.	✓	✓	✓
8.1.2	Todos los emplazamientos tendrán una relación legal o contractual con la función central.	✓	✓	✓
8.1.3	Se establece un único sistema de gestión de seguridad para garantizar que todos sus emplazamientos dentro del sistema cumplan con los requisitos de la norma de seguridad TAPA aplicable.	✓	✓	✓
8.1.4	La función central y su sistema de gestión estarán sujetos a auditorías internas para garantizar el cumplimiento continuo de estándares de TAPA.	✓	✓	✓
8.1.5	La función central llevará a cabo auditorías de los emplazamientos dentro del alcance para garantizar que cada almacén cumpla con los requisitos aplicables de TAPA FSR. Las auditorías deben realizarse con las plantillas de auditoría TAPA adecuadas. Todas las auditorías individuales anuales de los emplazamientos deben completarse y deben estar disponibles para el auditor antes del proceso de certificación.	✓	✓	✓
8.1.6	La función central tendrá la autoridad y los derechos para exigir que todos los emplazamientos cumplan con los estándares de Seguridad TAPA y para implementar acciones correctivas según sea necesario. <i>Nota: Cuando proceda, esto debe establecerse en el acuerdo formal entre la función central y los emplazamientos.</i>	✓	✓	✓
8.2	Políticas y procedimientos			
8.2.1	La función central deberá mantener políticas y procedimientos documentados para sus sistemas de gestión de la seguridad que sean aplicables a todos sus emplazamientos.	✓	✓	✓

Sección	Función central	A	B	C
8.2.2	La función central deberá garantizar que las políticas y procedimientos pertinentes se actualicen, comuniquen, implementen y desplieguen según sea necesario en todos los emplazamientos.	✓	✓	✓
8.2.3	Las políticas y procedimientos deberán mantenerse y ser fácilmente accesibles para todos los emplazamientos según sea necesario.	✓	✓	✓
8.3	Informe de auditoría de autoevaluación realizada para todos los emplazamientos			
8.3.1	La función central encomendará a todos los emplazamientos que realicen las autoevaluaciones y todos los informes de autoevaluación se presentarán a la función central para su registro y revisión. Los registros deben mantenerse durante al menos dos (2) años.	✓	✓	✓
8.3.2	La función central garantizará que todas las acciones correctivas (SCAR) de la autoevaluación y las auditorías se cierren adecuadamente para mejorar sus sistemas de gestión de la seguridad.	✓	✓	✓
8.3.3	Todos los emplazamientos presentarán actualizaciones de mejora e informes sobre todas las acciones correctivas (SCAR) pendientes a la función central. La función central deberá escalar esta información a la dirección del Proveedor de Servicios logísticos o solicitantes si los SCAR no se completan antes de sus fechas de vencimiento. Los registros deben mantenerse durante al menos dos (2) años.	✓	✓	✓
8.4	Registros de inspecciones y registros en general (visitas, conductores, etc), inspecciones de 7 puntos			
8.4.1	La función central deberá disponer de procedimientos para garantizar que todos los emplazamientos mantengan registros de inspecciones, registros de visitantes, registros de conductores e inspecciones de 7 puntos, entre otros.	✓	✓	✓
8.5	Evaluaciones de riesgos de todos los emplazamientos			
8.5.1	La función central deberá disponer de procedimientos establecidos, para garantizar que se realicen evaluaciones de riesgo y gestiones adecuadas en todos los emplazamientos y que sus registros se mantengan durante al menos dos (2) años.	✓	✓	✓
8.6	Disposición de CCTV y alarmas de los emplazamientos			
8.6.1	La función central debe disponer de procedimientos que garanticen que todos los emplazamientos revisen y mantengan los documentos sobre todos los sistemas de seguridad física, como la disposición de cámaras y alarmas.	✓	✓	✓
8.7	Registros de alarma y control de acceso			
8.7.1	La función central deberá contar con procedimientos que garanticen que todos los sistemas de alarma y control de acceso se mantengan y se testeen para garantizar su efectividad operativa.	✓	✓	✓
8.7.2	La función central dispondrá de procedimientos establecidos, para que todos los emplazamientos mantengan registros de todas las pruebas e incidentes de detección de intrusiones y control de acceso.	✓	✓	✓
8.8	Registros de formación			
8.8.1	La función central deberá disponer de procedimientos establecidos para garantizar que todos los emplazamientos mantengan registros de la formación en gestión de seguridad de sus empleados.	✓	✓	✓

Sección	Función central	A	B	C
8.8.2	La función central deberá disponer de procedimientos para garantizar que todos los emplazamientos mantengan registros de formación en materia de seguridad de todo el personal del emplazamiento. Los registros deben mantenerse durante al menos dos (2) años.	✓	✓	✓
8.9	Revisión/verificación de registros			
8.9.1	La función central dispondrá de procedimientos para garantizar que todos los emplazamientos realicen la revisión y verificación de los registros a intervalos regulares para asegurar la integridad y eficacia de los sistemas de gestión de seguridad.	✓	✓	✓
8.9.2	La función central dispondrá de procedimientos para garantizar que se mantengan registros de las revisiones, incluidos sus resultados y hallazgos y las acciones correctivas/preventivas 8.1.6. Los registros se mantendrán durante al menos dos (2) años.	✓	✓	✓
8.10	Revisión de la dirección para evaluar las auto auditorías; acciones correctivas de seguridad (SCARs) ; pérdidas o robos; Evaluaciones de riesgos.			
8.10.1	La función central deberá como mínimo llevar a cabo revisiones periódicas de la gestión para garantizar el cumplimiento, la eficacia y la mejora de sus sistemas de gestión de seguridad.	✓	✓	✓
8.10.2	Las revisiones de la dirección abarcarán, entre otras cosas, la eficacia de las auto auditorías, los cierres de las acciones correctivas (SCAR), las evaluaciones de riesgos, incidentes y acciones de mejora.	✓	✓	✓
8.10.3	La función central mantendrá registros de todas las revisiones de dirección durante al menos dos (2) años.	✓	✓	✓

9.0. Amenazas a los sistemas informáticos y Ciberseguridad : opción mejorada

FSR incluye mejoras opcionales de amenazas de ciberseguridad que se consideran un mayor nivel de protección y se pueden aplicar complementando los módulos. Esta mejora opcional está destinada a ser seleccionada por el Proveedor de servicios logísticos/ Solicitante y / o su Cliente como requisitos adicionales para sus necesidades de seguridad operativa. Cuando esta mejora opcional se selecciona en la evaluación previa a la certificación para formar parte de la auditoría de certificación, todos los requisitos se vuelven obligatorios.

Sección	Amenazas a los sistemas informáticos y Ciberseguridad: opción mejorada
9.	Requisitos obligatorios
9.1	El Proveedor de servicios logísticos/Solicitante debe disponer de políticas de seguridad para tecnologías de informática y amenazas cibernéticas. Las políticas pueden ser documentos separados o en un documento combinado y deben explicar: 1. Las acciones que llevara a cabo el Proveedor de servicios logísticos/Solicitante para identificar y responder a las amenazas. 2. Las políticas y procedimientos implementados para proteger, detectar, probar y responder a eventos de seguridad. 3. Los métodos para la recuperación de sistemas informáticos y/o datos. 4. El protocolo de comunicaciones al cliente para mitigar el impacto en la cadena de suministro en un plazo de 24 horas desde el conocimiento del incidente. 5. Cómo se revisan anualmente las políticas y se actualizan según sea necesario.
9.2	El Proveedor de servicios logísticos/Solicitante debe ofrecer capacitación de concienciación de información a todos los empleados. Esta formación debe: - 1. Cubrir las funciones y responsabilidades que tienen los usuarios de equipos informáticos en el mantenimiento de la seguridad y los beneficios asociados. 2. Contar con un sistema que garantice que se mantengan registros de las personas que reciben capacitación durante un mínimo de 2 años.
9.3	El Proveedor de servicios logísticos/Solicitante debe tener una política escrita establecida para garantizar que las medidas de Ciberseguridad estén implementadas con subcontratistas y / o proveedores garantizando lo siguiente: 1. Los requisitos de ciberseguridad del Proveedor de servicios logísticos/Solicitante se comunican a los subcontratistas y / o proveedores y se integren en los acuerdos. 2. En los casos donde los subcontratistas y/o proveedores no reconozcan o se niegan a adoptar los requisitos de ciberseguridad del Proveedor de servicios logísticos/Solicitante, deben estar documentadas y en vigor medidas que mitiguen los riesgos para los requisitos de ciberseguridad del Proveedor de servicios / Solicitante y sus clientes.
9.4	El Proveedor de servicios logísticos/Solicitante debe tener un plan de mitigación de interrupción de energía (por ejemplo, suministro de energía alternativa o generador de respaldo), que garantice que la energía se dirige a los sistemas informáticos críticos (identificados en la evaluación de riesgos local) durante un mínimo de 48 horas.
9.5	Los sistemas informáticos del Proveedor de servicios logísticos/Solicitante deben tener instalado software antivirus y antimalware con licencia. El software antivirus y antimalware debe contener las ultimas actualizaciones.



Sección	Amenazas a los sistemas informáticos y Ciberseguridad: opción mejorada
9.6	El Proveedor de Servicios logísticos / Solicitante debe tener un Plan de Recuperación de Desastres (DRP) del sistema informático adecuado para recuperarse de ataques al sistema comprometido, incluyendo, pero no limitándose a, todos los datos necesarios de respaldo y recuperación de datos y software.
9.7	Los sistemas informáticos del proveedor de servicios logísticos/Solicitante deben estar respaldados. Dichas copias de seguridad deben testearse regularmente, y los datos de copia de seguridad deben estar cifrados y transferirse a una ubicación secundaria fuera del sitio.
9.8	El Proveedor de Servicios logísticos / Solicitante debe implementar una política para todas las cuentas de usuario para gestionar y controlar el acceso a los sistemas informáticos mediante el uso de identificadores individuales únicos y contraseñas seguras. Procedimientos establecidos para garantizar: 1. Programa de auditoría de cumplimiento de contraseñas establecido. 2. Se debe asignar una contraseña única inicial a cada cuenta nueva en el momento de la creación. 3. Las contraseñas iniciales no pueden contener el nombre del usuario, el número de identificación o seguir un patrón estándar basado en la información del usuario. 4. Las contraseñas se comunicarán a los usuarios de manera segura, y solo después de validar la identidad del usuario. 5. Los usuarios deben estar obligados a cambiar las contraseñas en el inicio de sesión inicial. 6. Las contraseñas deben cambiarse al menos cada 90 días.



Para su información: la traducción de la norma al idioma local que se le ha proporcionado tiene como objetivo mejorar la comprensión de los requisitos de TAPA 2023. La traducción de la norma se inició y validó según nuestro leal saber y entender y con el conocimiento de los conceptos básicos necesarios. Sin embargo, la versión original en inglés de la norma respectiva es y sigue siendo decisiva para el examen.

Publicación e información sobre derechos de autor

El aviso de copyright de TAPA que se muestra en este documento indica cuándo se emitió por última vez el documento.

© TAPA 2023-2026

No copiar sin el permiso de TAPA, excepto según lo permitido por la ley de derechos de autor.

Historial de publicaciones

Publicado por primera vez en agosto de 2023

Primera edición (actual) publicada en agosto de 2023

Esta especificación disponible públicamente entra en vigor el 15 de septiembre de 2023