FSR 2020

REQUISITOS DE SEGURIDAD DEL ESTABLECIMIENTO

Transported Asset Protection Association

Transported Asset Protection Association

Requisitos de seguridad del establecimiento FSR 2020

Estándares de TAPA

TAPA de las Américas

5030 Champion Blvd,
G-11 N.º 266 Boca Ratón,
Florida 33496
EE. UU.
www.tapaonline.org
Tel. (561) 617-0096

TAPA de Asia-Pacífico

1 Gateway Drive, Westgate
Tower N.º 07-01,
Singapur 608531

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

TAPA de Europa, Oriente Medio y África

Rhijngeesterstraatweg 40D
2341 BV Oegstgeest
Países Bajos

www.tapaemea.org
Tel. +44 1633 251325

Índice de los FSR

Índice de los FSR (continuación)

□□□

1. Introducción

1.1 Propósito de este documento de FSR

Este documento de Requisitos de seguridad del establecimiento (Facility Security Requirements, FSR) es el estándar oficial de la Asociación para protección de activos transportados (Transported Asset Protection Association, TAPA) para el almacenamiento y depósito seguros. Es un estándar internacional común que puede utilizarse en acuerdos de negocio o seguridad entre los Compradores y los Proveedores de servicios de logística (Logistics Service Providers, LSP) u otros Solicitantes que desean obtener la certificación.

En la elaboración de este estándar, TAPA reconoce las múltiples diferencias en la forma en que se brindan 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 brindados por un LSP/Solicitante. Dependiendo de la complejidad y del tamaño de la cadena de suministro, el cumplimiento de los estándares de TAPA puede lograrse a través de uno o varios LSP/Solicitantes y subcontratistas cualificados.

Alcance

TAPA desarrolló tres opciones para avalar la certificación:

- Certificación de un sitio único por un organismo de auditoría independiente (Independent Audit Body, IAB).
- Certificación de múltiples sitios por IAB.
- Certificación de autoauditoría por auditores autorizados (AA), por LSP/Solicitante o IAB.

Audiencia

Entre los usuarios típicos de los estándares de TAPA están:

- Los Compradores.
- Los LSP/Solicitantes.
- Las fuerzas del orden público u otras organizaciones gubernamentales.
- Las organizaciones profesionales de la cadena de suministro.
- Las aseguradoras.

1. Introducción

1.2 Recursos para implementar los FSR de TAPA

Los recursos para cumplir con los requisitos FSR serán responsabilidad del LSP/Solicitante y estarán a su cargo, a menos que se negocie o se acuerde lo contrario entre Comprador y el LSP/Solicitante.

1.3 Proteger las políticas de los LSP y los procedimientos

Las copias de los documentos de políticas y procedimientos de seguridad sólo se presentarán al Comprador de conformidad con los acuerdos de divulgación firmados entre el LSP/Solicitante y el Comprador y se tratarán como información confidencial.

2. Acerca de TAPA

2.1 Propósito de TAPA

Los delitos contra la propiedad, específicamente contra la carga, son de los mayores desafíos de la cadena de suministro para los fabricantes de productos valiosos y de alto riesgo y para los proveedores de servicios de logística.

Los criminales oportunistas ya no son la única amenaza. Hoy en día, las redes de crimen organizado operan a nivel mundial y realizan ataques cada vez más sofisticados contra vehículos, instalaciones y personal para lograr sus objetivos.

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

2.2 La 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 mediante el desarrollo y la aplicación de estándares internacionales de seguridad, prácticas industriales reconocidas, tecnología, educación, evaluaciones comparativas, colaboración normativa y la identificación proactiva de las tendencias delictivas y las amenazas a la seguridad de la cadena de suministro.

3. Estándares de TAPA

3.1 Estándares de seguridad de TAPA

Se han creado los siguientes estándares internacionales de seguridad de TAPA para garantizar la seguridad en el transporte y almacenamiento de carga de alto valor con riesgo de robo:

- Los FSR representan estándares mínimos específicamente para *el almacenamiento seguro o depósito en tránsito,* dentro de una cadena de suministro.
- Los requisitos de seguridad del transporte (TSR) apuntan exclusivamente al transporte en camiones y representan los estándares mínimos específicos para el *transporte terrestre de productos* en una cadena de suministro.

Los estándares internacionales de seguridad de TAPA se revisan y modifican según sea necesario cada tres años.

En el presente documento se abordan únicamente los requisitos FSR.

- El proceso de certificación FSR de TAPA está documentado en el documento marco de certificación FSR de TAPA.
- Para obtener la certificación FSR de TAPA deben seguirse las versiones actuales del documento marco de certificación FSR de TAPA y de los FSR de TAPA.

3.2 Implementación

La implementación exitosa de los estándares de seguridad de TAPA depende de que los LSP (proveedores de servicios logísticos)/solicitantes, compradores (propietarios de la carga) y los auditores autorizados de TAPA, trabajen juntos.

4. Asesoramiento legal

4.1 Alcance

Los FSR son un estándar internacional y todas sus secciones son obligatorias, a menos que se conceda una excepción a través del proceso oficial de exoneración. (Consulte la Sección 6.).

4.2 Traducción

En zonas geográficas en las que el inglés no sea el primer idioma y en las que la traducción es necesaria y aplicable, es responsabilidad del LSP/Solicitante y de sus agentes asegurarse de que cualquier traducción de los FSR, o de cualquiera de sus partes, refleje con precisión las intenciones de TAPA en la elaboración y publicación de estos estándares.

4.3 La marca "TAPA"

"TAPA" es una marca comercial registrada de la Asociación para la protección de activos transportados (Transported Asset Protection Association) y no puede usarse sin el permiso expreso y por escrito de TAPA a través de sus regiones oficialmente reconocidas. Los estándares de TAPA y los materiales asociados son publicados a través de TAPA y por ella; y no pueden revisarse, modificarse o editarse sin el permiso expreso por escrito de TAPA. El uso indebido de la marca TAPA puede derivar en la cancelación de la certificación o en acciones legales.

4.4 Límites de responsabilidad

Mediante la publicación de estos estándares, TAPA no ofrece garantías ni avales de que se evitarán todos los eventos de robo de carga, independientemente de que los estándares se apliquen e implementen correctamente y en su totalidad. Cualquier responsabilidad que pueda resultar de un robo de la carga almacenada o de cualquier otra pérdida de carga almacenada conforme a los estándares FSR será por cuenta del LSP/Solicitante y/o del Comprador de acuerdo con los términos y condiciones del contrato entre sí y cualquier ley o estatuto que pueda aplicarse dentro de la jurisdicción en cuestión.

5. Contratos y subcontrataciones

5.1 Contratos

El transporte, almacenamiento y manejo seguros de los bienes del Comprador son responsabilidad del LSP/Solicitante, sus agentes y subcontratistas durante la recogida, tránsito, almacenamiento y entrega, según lo especificado en una divulgación o contrato.

Cuando se haga referencia a los FSR o se los incluya en el contrato entre el LSP/Solicitante y el Comprador, también se le hará referencia en el programa de seguridad del LSP/Solicitante.

El LSP deberá proporcionar al Comprador evidencia de la Certificación FSR y, si corresponde, evidencia de que se cumplieron los requisitos de FSR. Además, todo supuesto incumplimiento del LSP/Solicitante en la implementación de los requisitos FSR deberá resolverse de acuerdo con los términos del contrato negociados entre el Comprador y el LSP/Solicitante.

5.2 Subcontrataciones

Los subcontratistas de almacenamiento incluyen el requisito contractual de que la subcontratación del LSP/Solicitante cumpla con todos los estándares FSR.

5.3 Investigación y resolución de reclamos de TAPA

Si TAPA recibe un reclamo formal sobre el desempeño de un LSP/Solicitante certificado, TAPA (sujeto a validación) puede requerir que el contrato de un LSP/Solicitante realice una nueva auditoría a su cargo. Si el LSP/Solicitante no aprueba la auditoría o se niega a cumplir con este proceso, su certificado puede ser revocado.

6. Exoneraciones

6.1 Descripción general

Una exoneración es una aprobación otorgada por escrito ya sea para exonerar a un establecimiento de un requisito específico de TAPA o para aceptar una solución de cumplimiento alternativa. Se puede solicitar una exoneración si un LSP/Solicitante no puede cumplir con un requisito FSR específico y puede justificar medidas alternativas. Las exoneraciones son válidas durante el período de la certificación.

Todas las solicitudes de exoneración de un requisito de seguridad específico (ya sea en parte o en su totalidad) deben presentarse mediante un formulario de solicitud de exoneración de TAPA al IAB/AA por el LSP/Solicitante (que se encuentra en el sitio web de TAPA). El LSP/Solicitante que realiza la solicitud asume toda la responsabilidad por la exactitud de la información que se proporciona en la solicitud de exoneración.

Cada solicitud de exoneración debe presentarse por medio del IAB/AA al Comité regional de exoneraciones de TAPA para su aprobación. Es responsabilidad del IAB/AA decidir si la solicitud está completa y justifica el procesamiento por parte de TAPA; esto incluye la verificación de los factores de mitigación y/o los controles de seguridad alternativos.

Si los funcionarios de TAPA y/o los Compradores alegan que las condiciones de exoneración cambiaron, TAPA llevará a cabo una investigación formal y el LSP/Solicitante comprende que TAPA puede revocar la exoneración.

6.2 Proceso comercial de exoneraciones

Si un LSP no puede cumplir con un requisito específico de FSR, se implementa el proceso de exoneraciones siguiente.

Tabla 1: Responsabilidades: Solicitud/Evaluación de exoneración

Paso	Responsabilidad	Medida
1.	LSP/Solicitante	Establece y verifica las medidas de mitigación.
2.	LSP/Solicitante	Completa el formulario de solicitud de exoneración de TAPA y lo presenta al IAB/AA.
3.	IAB/AA	Revisa y verifica la integridad de la información contenida en el formulario de solicitud de exoneración de TAPA.
4.	IAB/AA	Presenta el formulario de solicitud de exoneración de TAPA al Comité regional de exoneraciones de TAPA.
5.	Comité regional de exoneraciones de TAPA	Revisa la solicitud y otorga o deniega la exoneración.

6. Exoneraciones

Si se deniega la exoneración

Si el Comité regional de exoneraciones de TAPA no aprueba la solicitud de exoneración, el LSP/Solicitante deberá implementar los requisitos de seguridad completos de FSR.

Si se otorga la exoneración

Si el Comité regional de exoneraciones de TAPA aprueba la solicitud de exoneración, se tomarán las siguientes medidas:

Tabla 2: Aprobación de la exoneración

Paso	Responsabilidad	Medida
1.	Comité regional de exoneraciones de TAPA	Documenta y firma los detalles de la exoneración.
2.	Comité regional de exoneraciones de TAPA	Especifica la vigencia de la exoneración (hasta un máximo de tres años) y envía una copia al AA.
3.	AA	Notifica al LSP/Solicitante el resultado de la solicitud de exoneración.
4.	LSP/Solicitante	Cumple con los requisitos de la exoneración. De lo contrario, se anula la aprobación de la exoneración.

6.3 Exoneraciones para las barreras físicas (conforme la Sección 1) y para jaulas con activos de alto valor (High Value Cages, HVC, conforme a la sección 4.5)

TAPA considerará una exoneración de todos o parte de los requisitos de barrera perimetral y/o para las HVC si se cumplen todas las siguientes condiciones previas:

General:

- La solicitud de exoneración se presenta mediante el proceso oficial del formulario de solicitud de exoneración de TAPA y es avalada por el IAB/AA.
- En la solicitud de exoneración se incluyen los detalles de las medidas de mitigación para garantizar que los bienes vulnerables no corran un riesgo innecesario de robo o pérdida.
- Se debe completar una evaluación de riesgos y presentarla con la solicitud de exoneración. Toda vulnerabilidad importante que se identifique en la evaluación de riesgos debe enumerarse por separado en la exoneración y las medidas adoptadas para reducir el riesgo a un nivel aceptable.

6. Exoneraciones

Medidas de mitigación que deben existir y documentarse en la presentación de la solicitud de exoneración:

- **Barreras perimetrales:**
  - El equipo, los recursos y los procedimientos adicionales introducidos para ayudar a la detección oportuna de personas o vehículos no autorizados pueden incluir, entre otras cosas: iluminación adicional, protección por circuito cerrado de televisión (CCTV), procedimientos mejorados de identificación de personas y vehículos, zonas restringidas con acceso con chaleco o uniforme del LSP únicamente.
  - Deben instalarse señales perimetrales visibles en el idioma local que indiquen "Prohibido el acceso no autorizado", "Prohibido el estacionamiento no autorizado".
  - Se instalarán señales visibles en las puertas o paredes externas del muelle para instruir a los conductores, visitantes, etc., a que procedan al control de seguridad del vestíbulo apropiado.
  - Confirmación de que se establecieron procedimientos que garantizan que las zonas de manipulación, envío y recepción de la carga se inspeccionan y cumplen con las condiciones de la exoneración al menos semanalmente.

- **HVC:**
  - En el caso de las exoneraciones de HVC, las medidas de mitigación apropiadas para reducir al mínimo el riesgo (cuando no se dispone de una HVC) deben considerarse y documentarse en la evaluación de riesgos anual.
  - La solicitud de exoneración incluye una declaración adjunta firmada por el LSP/Solicitante estipulando que ningún Comprador requiere una HVC.

7. Requisitos de seguridad del establecimiento

Sección	Requisitos generales:	A	B	C
7.0				
7.0.1	Deben documentarse todas las políticas o procedimientos exigidos por este estándar.	✔	✔	✔
7.0.2	Se requiere un procedimiento, registro y/o plan de llaves para las cerraduras físicas, las tarjetas de acceso y/o las llaves que gestionan y controlan las llaves físicas y electrónicas.	✔	✔	✔

Sección	Perímetro	A	B	C
7.1				
Zona externa del almacén de manejo, envío y recepción de carga (General)				
7.1.1	CCTV capaz de mostrar todo el tráfico en la zona externa de manejo, envío y recepción de carga (incluidos los puntos de entrada y salida) asegurando que todos los vehículos y personas sean reconocibles en todo momento, a menos que se produzca una obstrucción temporal debido a necesidades operativas (es decir, carga y descarga de camiones en tiempo real).	✔	✔	
7.1.2	Iluminación adecuada en zonas de carga y descarga. *Nota: la iluminación puede ser constante, activada por alarma o por movimiento, detección de sonido, etc., con iluminación proporcionada inmediatamente.*	✔	✔	✔
7.1.3	Procedimiento que describa de qué manera se deben manejar las personas y vehículos no autorizados dentro de la zona externa de manejo, envío y recepción de carga. Las instrucciones sobre el procedimiento deben entregarse al personal pertinente, incluidos los guardias.	✔	✔	✔
7.1.4	La zona de manejo, envío y recepción de carga se controla adecuadamente para prevenir el acceso no autorizado.		✔	✔
7.1.5	En el caso de ventanas accesibles a nivel del suelo o puertas del muelle, la evaluación de riesgos anual debe evaluar la necesidad de barreras anti-embestida. (Consulte la Evaluación de riesgos, sección 7.6.5.).	✔		
Barreras físicas				
7.1.6	La barrera física encierra la zona de manejo, envío y recepción de la carga.	✔		
7.1.7	La barrera física alrededor de la zona de manejo, envío y recepción de carga tiene una altura mínima de 6 pies/1,8 metros. *Nota: la barrera física, diseñada para evitar el acceso no autorizado, debe tener una altura de 6 pies/1,8 metros a lo largo de toda su longitud, incluyendo zonas en las que la nivelación del piso cambia, por ejemplo, es inferior.*	✔		
7.1.8	Barrera física alrededor de la zona de manejo, envío y recepción de carga mantenida en buenas condiciones.	✔		

Sección	Perímetro	A	B	C
7.1.9	Puerta(s) dentro de las barreras de la zona de manejo, envío y recepción de carga controlada(s) por operadores o electrónicamente.	✔		
7.1.10	Barrera física alrededor de la zona de manejo, envío y recepción de carga se inspecciona para comprobar su integridad y la existencia de daños al menos una vez por semana.	✔		
Zonas externas del muelle				
7.1.11	Las zonas externas del muelle protegidas por cámaras exteriores a color o "diurnas/nocturnas".	✔	✔	✔
7.1.12	Cámaras montadas para poder ver en todo momento todas las operaciones y movimientos alrededor de la zona externa del muelle, a menos que se produzca una obstrucción temporal debido a necesidades operativas (es decir, la carga y descarga de camiones en tiempo real).	✔	✔	✔
7.1.13	Todos los vehículos y personas alrededor de las zonas externas del muelle se reconocen con claridad.	✔		
7.1.14	Los vehículos y personas alrededor de las zonas externas del muelle son visibles en la mayoría de los casos.		✔	✔
7.1.15	Todas las zonas externas alrededor de las puertas del muelle están completamente iluminadas.	✔	✔	✔
Acceso de vehículos particulares				
7.1.16	Solo se permiten vehículos particulares en las zonas de manejo, envío y recepción de carga si son aprobados previamente y si se limitan a las zonas de estacionamiento registradas/designadas. No hay estacionamiento particular a menos de 25 metros de distancia a pie de las zonas externa de los muelles. Procesos establecidos para la aprobación previa y las restricciones.	✔	✔	✔

Sección	Paredes, techo y puertas exteriores	A	B	C
7.2				
Lados exteriores del establecimiento: CCTV				
7.2.1	Sistema de cámaras exteriores a color o "diurnas/nocturnas" en funcionamiento que proteja todos los lados exteriores del establecimiento.	✔		
7.2.2	Sistema de cámaras exteriores a color o "diurnas/nocturnas" en funcionamiento que proteja los lados exteriores del establecimiento con puertas, ventanas u otras aberturas.		✔	
7.2.3	Todas las vistas del sistema de cámaras exteriores están despejadas en todo momento a menos que se produzca una obstrucción temporal debido a las necesidades operativas (es decir, carga y descarga de camiones en tiempo real).	✔		
7.2.4	Todos los vehículos y personas se reconocen con claridad por el sistema de cámaras exteriores.	✔		

Sección	Paredes, techo y puertas exteriores	A	B	C
7.2.5	Vehículos y personas visibles, en la mayoría de los casos, por el sistema de cámaras exteriores.		✔	
Techo y paredes exteriores				
7.2.6	Techo y paredes exteriores diseñadas y mantenidas para resistir la penetración (ejemplo: ladrillo, bloque, losa de hormigón inclinada hacia arriba, paredes de paneles tipo sándwich).	✔	✔	✔
7.2.7	Toda ventana, rejilla de ventilación u otra abertura que pueda abrirse en las paredes exteriores del establecimiento o toda ventana sellada que se instale a menos de 3 metros del piso de trabajo en las paredes exteriores del establecimiento, debe tener una barrera física **o** contar con alarma y estar conectada al sistema de alarma principal.	✔	✔	
7.2.8	Toda ventana, claraboya, rejilla de ventilación, escotilla de acceso u otra abertura que se pueda abrir en el techo del establecimiento, debe tener una barrera física **o** contar con alarma y estar conectada al sistema de alarma principal.	✔		
7.2.9	El acceso externo al techo (escalera o escalones) debe ser: Cerrado físicamente y protegido por el CCTV (cámaras a color o "diurnas/nocturnas"). o Cerrado físicamente y con alarma.	✔		
7.2.10	Acceso externo al techo (escalera o escalones) cerrado físicamente.		✔	✔
7.2.11	Todas las puertas externas del almacén del establecimiento y las puertas de las oficinas que cuentan con alarma para detectar la apertura no autorizada y que están vinculadas al sistema de alarma principal. *Nota: las puertas del muelle no están protegidas por este requisito; consulte la sección 7.2.17 para conocer los requisitos de alarma de la puerta del muelle.*	✔	✔	✔
7.2.12	Cada puerta externa del almacén del establecimiento, puerta de oficina u otra abertura debe identificarse de forma única por puerta o por zona dentro del sistema de alarma principal.	✔		
7.2.13	Todas las puertas externas del almacén siempre están cerradas y aseguradas cuando no son usadas activamente. Llaves/Códigos controlados.	✔	✔	
7.2.14	Las puertas y umbrales de ingreso peatonal del almacén no pueden atravesarse fácilmente. Si tienen bisagras por fuera de ellas, deben estar articuladas con pasador o soldadas por puntos. Las puertas de vidrio son inaceptables a menos que se instalen detectores de rotura de vidrio u otro dispositivo de detección local que proporcione protección (por ejemplo, sensores infrarrojos pasivos [Passive Infrared Sensor, PIR]) y cuenten con alarma conectada directamente al centro de control o que el vidrio esté protegido por barras/mallas.	✔	✔	✔

Sección	Paredes, techo y puertas exteriores	A	B	C
7.2.15	Las salidas de emergencia que se utilizan únicamente con fines de emergencia (por ejemplo, salidas de incendios), cuentan con una alarma en todo momento con una sirena audible individual o por zonas.	✔	✔	
7.2.16	Todas las puertas del muelle tienen resistencia suficiente para disuadir y/o retrasar la entrada forzada mediante el uso de pequeñas herramientas manuales portátiles.	✔	✔	✔
7.2.17	**Puertas del muelle** **Horario no operativo:** Puertas del muelle cerradas y aseguradas (es decir, inhabilitadas electrónicamente o cerradas físicamente). Las puertas del muelle cuentan con alarma para detectar una intrusión no autorizada y activar una alarma vinculada al sistema de alarma principal. **Horario operativo:** Las puertas del muelle deben cerrarse cuando no son usadas activamente. Las puertas tipo tijera, si se utilizan, deben asegurarse mediante un sistema de deslizamiento mecánico/cerradura con pestillo y tener un mínimo de 8 pies/2,4 metros de alto.	✔	✔	✔

Sección	Puntos de ingreso y salida de oficina y almacén	A	B	C
7.3				
Punto(s) de ingreso para visitantes de la zona de oficinas				
7.3.1	El acceso a los puntos de ingreso para visitantes a la zona de oficinas es controlado por un empleado/guardia/recepcionista que fue capacitado en emisión de credenciales, controles, registro, visitantes, requisito de escolta, etc. (proceso establecido para las visitas fuera del horario operativo).	✔	✔	✔
7.3.2	Punto(s) de ingreso para visitantes de la zona de oficinas protegido(s) por CCTV (Cámaras a color o "diurnas/nocturnas"), donde las personas se reconocen con claridad en todo momento.	✔	✔	
7.3.3	Alarma silenciosa instalada en los puntos de ingreso para visitantes de la zona de oficinas y probada semanalmente.	✔	✔	
7.3.4	Todos los visitantes de la zona de oficinas deben identificarse con un documento de identidad con fotografía emitido por el gobierno (por ejemplo, licencia de conducir, pasaporte o documento nacional de identidad, etc.).	✔	✔	✔
7.3.5	Todos los visitantes a la zona de oficinas son registrados y su registro se mantiene por un período mínimo de 30 días.	✔	✔	✔
7.3.6	Todas las credenciales de los visitantes deben ser recuperadas cuando el visitante abandone el establecimiento y se debe revisar el registro completo a diario.	✔	✔	
7.3.7	Todos los visitantes deben exhibir de forma visible sus credenciales o pases y ser escoltados por personal de la compañía.	✔	✔	
Punto(s) de ingreso del personal				
7.3.8	El acceso a los puntos de ingreso del personal está controlado las 24 horas del día y los 7 días de la semana.		✔	✔
7.3.9	Los puntos de ingreso del personal son controlados por medio del dispositivo de control de acceso electrónico las 24 horas del día y los 7 días de la semana. Acceso registrado.	✔		
7.3.10	Puntos de ingreso del personal protegidos por CCTV. (Cámaras a color o "diurnas/nocturnas").	✔	✔	
7.3.11	Luego del control, todos los empleados deben recibir credenciales de identificación con fotografía de la empresa.	✔	✔	
7.3.12	El resto del personal deben recibir una credencial de identificación de la empresa para ser reconocidos dentro del establecimiento.	✔	✔	
7.3.13	Todas las credenciales del personal deben ser exhibidas de forma visible.	✔	✔	
7.3.14	Las credenciales del personal no deben compartirse bajo ninguna circunstancia y debe existir una política de emisión de credenciales.	✔	✔	
Identificación del conductor y del vehículo				

Sección	Puntos de ingreso y salida de oficina y almacén	A	B	C
7.3.15	Todos los conductores deben identificarse con un documento de identidad con fotografía emitido por el gobierno (por ejemplo, licencia de conducir, pasaporte o documento nacional de identidad, etc.) y se debe mantener un registro de los conductores.	✔	✔	✔
7.3.16	Se debe verificar que la licencia del conductor sea válida, que el documento de identidad con fotografía no haya caducado y que coincida con el conductor.	✔	✔	✔
7.3.17	Los identificación del vehículo se registra manualmente (es decir, por escrito) o con cámaras. Debe incluir como mínimo la placa de matrícula y el tipo de vehículo.	✔		

Sección	Dentro del almacén y las oficinas	A	B	C
7.4				
Zona de almacén: Paredes multiusuario				
7.4.1	Paredes internas de piso a techo multiusuario y techo construido/diseñado y mantenido para resistir la penetración (Ejemplo: ladrillo, bloque, losa de hormigón inclinada hacia arriba, paredes de paneles tipo sándwich).	✔	✔	✔
7.4.2	Si las paredes internas de piso a techo multiusuario están construidas con una malla metálica de seguridad u otra barrera segura reconocida por la industria, también deben contar con alarma para detectar una intrusión. *Nota: no se aceptan redes, vallas de baja calidad o mallas metálicas que no sean de seguridad.*	✔	✔	✔
Zonas internas del almacén				
7.4.3	La detección de intrusiones (por ejemplo, detección por infrarrojo, movimiento, sonido o vibraciones) es necesaria para controlar las zonas internas del almacén. Las alarmas deben activarse y vincularse con el sistema de alarma principal durante el horario no operativo (es decir, cuando el almacén esté cerrado). *Nota: si el almacén opera las 24 horas del día, los 7 días de la semana y los 365 días del año, es posible que este requisito no corresponda, si los riesgos y mitigaciones se documentan en la evaluación de riesgos local.* *Independientemente del horario operativo, siempre se requiere la detección de intrusiones en el perímetro o en las barreras físicas en las puertas externas y en las ventanas de la planta baja en las oficinas y el almacén. (Consulte la sección 7.2.11).*	✔		
Puertas y zonas internas del muelle				
7.4.4	Todas las puertas y zonas internas del muelle están protegidas por CCTV. (Cámaras a color o "diurnas/nocturnas").	✔	✔	✔
7.4.5	Vistas de la mercancía que se está cargando/descargando en todas las puertas y zonas internas del muelle, están despejadas en todo momento a menos que haya una obstrucción temporal debido a necesidades operativas (es decir, carga y descarga de camiones en tiempo real).	✔	✔	✔
7.4.6	Bienes del Comprador están bajo vigilancia al 100 % con CCTV en las zonas de movimiento o montaje de la carga (es decir, zonas de destrucción/construcción de palés, rutas hacia y desde los estantes de almacenamiento, muelle, corredores de tránsito).	✔	✔	
Control de acceso entre las oficinas y el muelle/almacén				
7.4.7	Acceso controlado entre las oficinas y el muelle/almacén.	✔	✔	
7.4.8	Las alarmas de acceso por tarjeta o por intercomunicador, para las puertas entre las oficinas y el muelle/almacén, son audibles localmente **y** activan una alarma de respuesta cuando se mantienen abiertas por más de 60 segundos o inmediatamente si se abren por la fuerza.	✔		

Sección	Dentro del almacén y las oficinas	A	B	C
7.4.9	Las alarmas de las puertas entre las oficinas y el muelle/almacén son audibles localmente **o** envían una alarma de respuesta cuando se mantienen abiertas por más de 60 segundos o se abren por la fuerza.		✔	
7.4.10	El personal autorizado del LSP/Solicitante y los visitantes escoltados tienen permitido el acceso a las zonas del muelle/almacén debido a una necesidad comercial y restringida.	✔	✔	✔
7.4.11	La lista de acceso a las zonas del muelle/almacén debe ser revisada al menos trimestralmente para limitar/verificar que el permiso de acceso solo se otorga al personal designado/autorizado.	✔	✔	
Zona/HVC				
7.4.12	El tamaño y el uso de la HVC pueden ser estipulado por el acuerdo del Comprador/LSP/Solicitante. Si no hubiera un acuerdo en vigor, la HVC debe tener la capacidad de almacenar un mínimo de 6 metros cúbicos de producto.	✔	✔	
7.4.13	El perímetro de la HVC/zona enjaulado o de paredes de estructura rígida en todos los lados, incluida la parte superior y el techo.	✔	✔	
7.4.14	Dispositivo de bloqueo de la HVC/zona en la puerta/compuerta.	✔	✔	
7.4.15	Protección completa con CCTV (cámaras a color o “diurnas/nocturnas”) en la entrada y zona interna de la HVC . *Nota: si la HVC es demasiado pequeña para instalar una cámara dentro, la protección con cámara de la entrada es suficiente.*	✔		
7.4.16	Protección con CCTV (cámaras a color o “diurnas/nocturnas”) en la entrada de la HVC.		✔	
7.4.17	Si más de 10 personas necesitan acceso a la HVC, el acceso se debe controlar electrónicamente por tarjeta/llavero transmisor. Si 10 o menos personas necesitan acceso, se necesita un sistema de cerradura o candado reforzado, más un sistema de emisión de llaves controlado. Las llaves pueden entregarse a personas para cubrir un turno pero no deben ser transferidas sin aprobación y registradas en el registro de llaves. Todas las llaves deben ser devueltas y contabilizadas cuando no se usen.	✔		
7.4.18	Las puertas/compuertas de la HVC cuentan con alarma para detectar una entrada forzada. Las alarmas pueden activarse mediante contactos de la puerta y/o el uso de detección de movimiento por CCTV para detectar accesos no autorizados.	✔		
7.4.19	El perímetro de la HVC se mantiene en buenas condiciones y se inspecciona mensualmente para comprobar su integridad y la existencia de daños.	✔		

Sección	Dentro del almacén y las oficinas	A	B	C
7.4.20	El LSP/Solicitante debe garantizar que el acceso a la HVC solo se conceda al personal designado/autorizado. La lista de acceso a la HVC aprobada debe ser revisada mensualmente y actualizada en tiempo real cuando el empleado deja el empleo o ya no necesita acceso. Procedimiento establecido para el acceso a la HVC.	✔	✔	
Inspección de la basura del almacén				
7.4.21	Se monitorea por CCTV los principales contenedores de basura internos y/o externos del almacén internos/las zonas de compactación.	✔		
7.4.22	Cuando se utilice bolsas de basura dentro del almacén, las mismas serán transparentes.		✔	✔

Carga previa y almacenamiento temporal				
7.4.23	No se permite la carga previa o estacionar los camiones exclusivos del Comprador/FTL fuera de las instalaciones del almacén en horarios no operativos, a menos que lo hayan acordado mutuamente el Comprador y el LSP/Solicitante. Deben implementarse medidas de seguridad alternativas (por ejemplo, dispositivos de seguridad adicionales en el contenedor). *Nota: "Fuera de las instalaciones de almacén" son aquellas zonas separadas y alejadas del establecimiento, pero que siguen dentro de la valla perimetral/predio del LSP/Solicitante.*	✔	✔	✔
Contenedores personales y búsqueda de salidas				
7.4.24	Los procedimientos de seguridad escritos definen cómo se controlan los "contenedores personales" dentro del almacén. Los contenedores personales incluyen loncheras, mochilas, hieleras, carteras, etc.	✔	✔	
7.4.25	Si la legislación local lo permite, el LSP/Solicitante debe elaborar y mantener un procedimiento documentado para la búsqueda de salidas. La activación del procedimiento queda a criterio del LSP/Solicitante y/o conforme al acuerdo del Comprador/LSP/Solicitante. Como mínimo, el procedimiento debe abordar los criterios de búsqueda del LSP/Solicitante en caso de que surja la necesidad de introducir búsquedas cuando normalmente no se requieren (por ejemplo, cuando se sospecha de hurto por parte del personal).	✔		
Control del equipo de manejo de la carga				
7.4.26	Procedimiento que requiere que todos los montacargas y otros equipos de manejo de carga motorizados se apaguen durante el horario no operativo. *Nota: esto no incluye a las carretillas manuales/transpaletas.*	✔	✔	
Integridad del contenedor o remolque: inspección de siete puntos				
7.4.27	Inspección física de siete puntos realizada en todos los contenedores o remolques de salida exclusivos del Comprador: pared frontal, lateral izquierdo, lateral derecho, piso, techo, puertas internas/externas y mecanismo de bloqueo, exterior/parte inferior del chasis. *Nota: esto se aplica a todos los tipos de remolques y contenedores bajo llave y/o precinto (es decir, no se limita a los contenedores de carga marítima).*	✔	✔	✔
Proceso de entrega de la carga: precintos de seguridad				
7.4.28	A menos que el Comprador lo exima específicamente, se utilizan precintos de seguridad contra manipulaciones en todos los envíos directos e ininterrumpidos. Los precintos deberán estar certificados según la norma ISO 17712 (clasificación I, S o H). *Nota: los precintos no son necesarios en los envíos con múltiples paradas, debido a la complejidad y el riesgo asociados a los conductores que transportan varios precintos.*	✔	✔	✔

7.4.29	El LSP/Solicitante debe contar con procedimientos documentados para la gestión y el control de precintos de seguridad, cerraduras de puertas del remolque (contenedor), cerraduras con pasador y otros equipos de seguridad.	✔	✔	✔
7.4.30	Los precintos de seguridad son colocados o retirados solo por personal autorizado, es decir, personal del almacén, que tiene instrucciones de reconocer e informar los precintos comprometidos. Los precintos nunca deben ser colocados o retirados por el conductor a menos que el Comprador lo autorice.	✔	✔	✔
7.4.31	Procedimientos establecidos para reconocer e informar los precintos de seguridad comprometidos.	✔	✔	✔
Integridad de la carga: proceso de validación de carga/descarga				
7.4.32	Procedimientos sólidos que garantizan que todos los bienes del Comprador enviados y recibidos se validen en el punto de entrega mediante la realización de un recuento de piezas manual y/o electrónico. El proceso debe asegurar que las anormalidades sean reconocidas, documentadas e informadas constantemente al LSP/Solicitante y/o Comprador. Los registros manuales y/o electrónicos deben ser de calidad probatoria. Si los conductores no están presentes para ser testigos de esta actividad, el Comprador/LSP/Solicitante debe garantizar una verificación alternativa del recuento, como escaneos o imágenes de CCTV, 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 obvias, que indiquen un posible robo o hurto.*	✔	✔	✔
Recogidas fraudulentas				
7.4.33	El documento de identificación del conductor del camión, la documentación de recogida de la carga y los detalles de alerta previa especificados por el Comprador se validan antes de la carga. Se debe establecer el procedimiento.	✔	✔	✔

Sección	Sistemas de seguridad: diseño, supervisión y respuestas.	A	B	C
7.5				
Puesto de control				
7.5.1	Control de eventos de alarma las 24 horas del día, los 7 días de la semana y los 365 días al año; a través de un puesto de control interno o externo de terceros, protegido del acceso no autorizado. *Nota: las puestos de control pueden estar ubicados dentro o fuera del sitio, y pueden ser de 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.*	✔	✔	✔

Sección	Sistemas de seguridad: diseño, supervisión y respuestas.	A	B	C
7.5.2	Puesto de control para responder a todas las alarmas del sistema de seguridad en tiempo real las 24 horas del día, los 7 días de la semana y los 365 días del año.	✔	✔	✔
7.5.3	El puesto de control reconoce la activación de la alarma y la escala en menos de 3 minutos.	✔	✔	✔
7.5.4	Informes de control de alarmas disponibles.	✔	✔	✔
7.5.5	Procedimientos establecidos de respuesta del puesto de control.	✔	✔	✔
Sistema de detección de intrusos (IDS)				
7.5.6	Todos los Sistemas de detección de intrusos (Intruder Detection System, IDS) se activan en el horario no operativo y se vinculan al sistema de alarma principal.	✔	✔	✔
7.5.7	Los registros de alarma del IDS se mantienen por 60 días.	✔	✔	
7.5.8	Los registros de alarmas del IDS son almacenados y respaldados de forma segura.	✔		
7.5.9	Los registros de alarmas del IDS son almacenados de forma segura.		✔	
7.5.10	Procedimiento para garantizar que el acceso al IDS esté restringido para personas autorizadas o administradores del sistema. Esto incluye servidores, consolas, controladores, paneles, redes y datos. Los privilegios de acceso deben actualizarse de inmediato cuando las personas se marchan de la organización o cambian sus funciones y ya no requieren el acceso.	✔	✔	✔
7.5.11	Alarma transmitida en caso de falla/pérdida del suministro eléctrico del IDS. *Nota: en el caso de sistemas de alimentación ininterrumpida (SAI), la alarma se transmite cuando falla la batería del SAI.*	✔	✔	✔
7.5.12	Debe realizarse una verificación del conjunto de alarmas del IDS. *Nota: procedimientos que validan que las alarmas están armadas durante el horario no operativo.*	✔	✔	✔
7.5.13	Alarma del IDS transmitida a través de línea fija en el dispositivo y/o falla de la línea.	✔	✔	
7.5.14	Sistema de comunicación de respaldo implementado en el dispositivo del IDS y/o falla de la línea.	✔	✔	
Sistema de control de acceso automático (AACS)				
7.5.15	Los registros de la transacción del Sistema de control de acceso automático (Automatic Access Control System, AACS) estarán disponibles por 90 días. Los registros son almacenados de forma segura y respaldados.	✔	✔	

Sección	Sistemas de seguridad: diseño, supervisión y respuestas.	A	B	C
7.5.16	Procedimiento para garantizar que el acceso al AACS esté restringido para personas autorizadas o administradores del sistema. Los privilegios de acceso deben actualizarse de inmediato cuando las personas se marchan de la organización o cambian sus funciones y ya no requieren el acceso.	✔	✔	
7.5.17	Los informes del sistema de acceso deben ser revisados por lo menos trimestralmente para identificar irregularidades o mal uso (es decir, múltiples intentos fallidos, lecturas falsas (por ejemplo, tarjeta desactivada), evidencia de que se compartió la tarjeta para permitir un acceso no autorizado, etc.). Proceso establecido.	✔	✔	
CCTV				
7.5.18	Grabación digital de CCTV instalado.	✔	✔	✔
7.5.19	La velocidad de la grabación para CCTV está fijada a como un mínimo de 8 fotogramas por segundo (frames per second, fps) por cámara. *Nota: TAPA permitirá a los titulares de certificados existentes sin la capacidad de actualizar a 8 fps continuar con los 3 fps existentes hasta la revisión de 2023. Los nuevos titulares de certificados deben cumplir con el nuevo requisito.*	✔	✔	✔
7.5.20	La funcionalidad de la grabación digital se verifica diariamente en los días operativos a través del procedimiento. Registros disponibles.	✔	✔	✔
7.5.21	Las grabaciones del CCTV serán almacenadas por un mínimo de 30 días cuando lo permita la legislación local. El LSP/Solicitante debe proporcionar evidencia de cualquier legislación local que prohíba el uso de CCTV y/o limitar el almacenamiento de datos de vídeo a menos de 30 días.	✔	✔	✔
7.5.22	El acceso al sistema de CCTV es estrictamente controlado, incluido el hardware, software y almacenamiento de datos/vídeo.	✔	✔	✔
7.5.23	Las imágenes del CCTV, con fines de seguridad, son vistas solo por el personal autorizado.	✔	✔	✔
7.5.24	Procedimientos establecidos que detallan la política de protección de datos del CCTV en relación con el uso de imágenes en tiempo real y de archivo de acuerdo con la legislación local.	✔	✔	
Iluminación interior y exterior				
7.5.25	Los niveles de iluminación del interior y exterior deben ser suficientes para permitir imágenes del CCTV que posibiliten la investigación y la grabación de imágenes de calidad probatoria.	✔	✔	
7.5.26	Los niveles de iluminación del interior y exterior deben ser suficientes para que se puedan reconocer con claridad todos los vehículos y personas.	✔		

Sección	Capacitación y procedimientos	A	B	C
7.6				
Procedimientos de escalación				
7.6.1	Procedimientos locales establecidos para manejar los bienes del Comprador, incluido el proceso para informar oportunamente los bienes del Comprador perdidos, desaparecidos o robados. Los incidentes deben ser informados por el LSP/Solicitante al Comprador en un plazo de 24 horas. Los robos evidentes se informan inmediatamente. Proceso cumplido de manera constante.	✔	✔	✔
7.6.2	Los contactos de emergencia de la administración del establecimiento del Comprador y del LSP/Solicitante están listados y disponibles en caso de incidentes de seguridad. La lista se actualiza cada 6 meses e incluye contactos de emergencia de las fuerzas del orden público.	✔	✔	✔
Compromiso de la administración				
7.6.3	La administración de los proveedores debe haber designado formalmente a una persona para la seguridad in situ que sea responsable de mantener los FSR de TAPA y los requisitos de seguridad de la cadena de suministro. El proveedor también debe tener una persona (puede ser la misma) responsable de controlar el programa FSR. Esto incluye programar las verificaciones de cumplimiento, comunicaciones con los AA, recertificación, modificaciones en el estándar FSR, etc. *Nota: estas personas pueden ser empleados o una persona tercerizada contratada para desempeñar esta función.*	✔	✔	✔
7.6.4	La administración debe elaborar, comunicar y mantener una política de seguridad para garantizar que todas las personas pertinentes (es decir, los empleados y los contratistas) sean perfectamente conscientes de las expectativas de seguridad del proveedor.	✔	✔	✔
7.6.5	Se debe actualizar/realizar al menos una vez al año una evaluación de riesgos del establecimiento que reconozca la probabilidad y el impacto de los eventos relacionados con la seguridad. El Proceso de evaluación de riesgos debe requerir que la administración tome decisiones informadas sobre las vulnerabilidades y la mitigación. Como mínimo, se deben evaluar los siguientes eventos internos/externos comunes: robo de carga o información; acceso no autorizado al establecimiento o carga; manipulación/destrucción de los sistemas de seguridad; recogidas ficticias de carga; continuidad de la seguridad durante la escasez de personal o desastres naturales, etc. Pueden considerarse eventos adicionales en función de los riesgos locales/del país.	✔	✔	✔
Capacitación				

Sección	Capacitación y procedimientos	A	B	C
7.6.6	La capacitación en concientización de seguridad/amenaza se impartirá a todo el personal durante los primeros 60 días de empleo y, a partir de entonces, cada 2 años.	✔	✔	✔
7.6.7	La capacitación en concientización de seguridad de la información se enfoca en la protección de los datos de envío electrónica y física del Comprador proporcionada al personal que tiene acceso a la información del Comprador.	✔	✔	
Acceso a los bienes del Comprador				
7.6.8	Procedimientos establecidos para proteger los bienes del Comprador (por ejemplo, la carga) del acceso no autorizado por parte del personal, los visitantes, etc.	✔	✔	
Control de la información				
7.6.9	Acceso a los documentos de embarque y a la información sobre los bienes del Comprador controlados “solo cuando sea estrictamente necesario”.	✔	✔	✔
7.6.10	Acceso a los documentos de embarque e información sobre los bienes del Comprador supervisados y registrados.	✔	✔	✔
7.6.11	Los documentos de embarque y la información sobre los bienes del Comprador se custodian hasta su destrucción.	✔	✔	✔
Informe de incidentes de seguridad				
7.6.12	Se implantó un sistema de informe y seguimiento de incidentes de seguridad, utilizado para implementar medidas proactivas.	✔	✔	
Programas de mantenimiento				
7.6.13	Programas de mantenimiento establecidos para todas las instalaciones/sistemas técnicos (físicos) de seguridad para garantizar la funcionalidad en todo momento (por ejemplo, CCTV, controles de acceso, detección de intrusos e iluminación).	✔	✔	✔
7.6.14	Mantenimiento preventivo realizado una vez al año o de acuerdo con las especificaciones del fabricante.	✔	✔	✔
7.6.15	Verificaciones de funcionalidad de todos los sistemas una vez a la semana y documentadas, a menos que la falla del sistema se informe o avise por alarma de forma inmediata/automática.	✔	✔	
7.6.16	Debe elaborarse una orden de reparación dentro de las próximas 48 horas desde que se descubre el fallo. Para cualquier reparación que se prevea que exceda las 24 horas, se deben implementar mitigaciones alternativas.	✔	✔	
Orientación del contratista				
7.6.17	El LSP/Solicitante debe asegurarse de que todos los subcontratistas/proveedores conozcan y cumplan con los programas de seguridad pertinentes del LSP/Solicitante.	✔	✔	✔
Envío y recepción de registros				

Sección	Capacitación y procedimientos	A	B	C
7.6.18	Los documentos de envío y recepción deben ser legibles, completos y precisos (es decir, deben contar con la hora, fecha, firmas, datos del conductor, personal de envío y recepción, detalles del envío y cantidad, etc.).	✔	✔	✔
7.6.19	El LSP/Solicitante debe mantener registros de todas las recogidas y los comprobantes de las entregas, por un período no inferior a dos años, y ponerlos a disposición para las investigaciones de pérdidas, según sea necesario.	✔	✔	✔
7.6.20	El comprobante de entrega debe proporcionarse de conformidad con el acuerdo escrito entre el Comprador y el LSP/Solicitante, donde el Comprador requiera, el destino para notificar el origen dentro del plazo acordado de recepción del envío, reconciliando los detalles de alerta previa del envío.	✔	✔	✔
Proceso de alerta previa establecido				
7.6.21	Cuando el Comprador lo requiera, el proceso de alerta previa aplicado a los envíos entrantes y/o salientes estará en vigor. Los detalles de alerta previa deben acordarse entre el Comprador y el LSP/Solicitante. Los detalles sugeridos incluyen: hora de salida, hora prevista de llegada, empresa de transporte, nombre del conductor, detalles de la placa de matrícula, información de envío (recuento de piezas, peso, número de conocimiento de embarque, etc.) y números de precintos del remolque.	✔	✔	✔

Sección	Integridad del personal	A	B	C
7.7				
7.1	Verificaciones de selección/investigación de historial/antecedentes (según lo permita la legislación local)			
7.7.1	El LSP/Solicitante debe tener un proceso de selección/investigación de historial /antecedentes que incluya, como mínimo, verificaciones de antecedentes penales y de empleo. La selección/investigación de historial se aplica a todos los solicitantes, incluidos empleados y contratistas. El LSP/Solicitante también requerirá que se aplique un proceso equivalente en las empresas contratantes que suministren personal temporal de la agencia (Temporary Agency Staff, TAS).	✔	✔	✔
7.7.2	El trabajador TAS debe firmar una declaración de que no tiene condenas penales actuales y que cumplirá con los procedimientos de seguridad del LSP/Solicitante.	✔	✔	✔
7.7.3	El LSP/Solicitante dispondrá de acuerdos para tener la información requerida de selección/investigación de historial/antecedentes suministrada por la agencia y/o subcontratista que proporciona los trabajadores TAS o deberá llevar a cabo dicha selección por sí mismo. La selección debe incluir la verificación de los antecedentes penales y las verificaciones de empleo.	✔	✔	✔
7.7.4	Procedimiento para lidiar con la falsa declaración del solicitante/personal antes y después de la contratación.	✔	✔	✔

Sección	Integridad del personal	A	B	C
Rescisión de contrato o recontratación de personal *Nota: la rescisión del contrato incluye el cese de la relación laboral tanto voluntaria como involuntaria: las renuncias y los despidos del personal.*				
7.7.5	Recupere los activos físicos del personal que deja de trabajar incluidos los documentos de identificación de la empresa, credenciales de acceso, llaves, equipos o información sensible. Requiere un procedimiento documentado.	✔	✔	✔
7.7.6	Proteger los datos del Comprador: Se requiere el proceso de cancelación de la autorización de acceso al personal que deja de trabajar a sistemas físicos o electrónicos que contengan información del Comprador (inventario o programas).	✔	✔	✔
7.7.7	Debe haber una lista de control del personal para verificación.	✔	✔	✔
7.7.8	Recontratación: existen procedimientos para evitar que el LSP/Solicitante recontrate personal si los criterios por los que se rescindió el contrato laboral siguen siendo válidos. *Nota: los registros se revisan antes de recontratar a alguien (por ejemplo, antecedentes de personal con contrato previamente rescindido o solicitantes rechazados [empleo previamente denegado]).*	✔	✔	✔

8. Requisitos de la función principal (solo aplicable para certificación de múltiples sitios)

Sección	Función principal	A	B	C
8.1	**General**			
8.1.1	Existe una función principal para administrar el sistema de gestión de seguridad de todos los sitios, tal y como se define en el alcance de la certificación de múltiples sitios.	✔	✔	✔
8.1.2	Todos los sitios tendrán una relación legal o contractual con la función principal.	✔	✔	✔
8.1.3	Se establece un sistema único de gestión de seguridad para asegurar que todos sus sitios dentro del sistema cumplan los requisitos del estándar de seguridad de TAPA correspondiente.	✔	✔	✔
8.1.4	La función principal y su sistema de gestión estarán sujetas a auditorías internas para garantizar el cumplimiento continuado de los estándares de TAPA.	✔	✔	✔
8.1.5	La función principal llevará a cabo auditorías de los distintos sitios para proporcionar la confianza y garantía de que el sistema de gestión de seguridad en todos los sitios del sistema cumple con los requisitos del estándar aplicable y es capaz de lograr los resultados previstos para todos los sitios implicados. Las auditorías deben realizarse con las plantillas de auditoría de TAPA adecuadas.	✔	✔	✔

Sección	Función principal	A	B	C
8.1.6	La función principal tendrá la autoridad y los derechos para exigir a todos los sitios cumplan los estándares de seguridad TAPA y para aplicar las medidas correctivas y preventivas que sean necesarias. *Nota: cuando corresponda, esto debe establecerse en el acuerdo formal entre la función principal y los sitios.*	✔	✔	✔
8.2	**Políticas y procedimientos**			
8.2.1	La función principal mantendrá políticas y procedimientos documentados para sus sistemas de gestión de seguridad que sean aplicables a todos sus sitios.	✔	✔	✔
8.2.2	La función principal se asegurará de que las políticas y procedimientos adecuados sean actualizados, comunicados, utilizados e implementados por todos los sitios según sea necesario.	✔	✔	✔
8.2.3	Las políticas y procedimientos se mantendrán y serán fácilmente accesibles por todos los sitios según sea necesario.	✔	✔	✔
8.3	**Informe de auditoría de autoevaluación realizado para todos los sitios**			
8.3.1	La función principal exigirá que todos los sitios realicen la autoevaluación y todos los informes de autoevaluación se presentarán a la función principal para registro y revisiones.	✔	✔	✔
8.3.2	La función principal deberá asegurarse de que todos los requisitos de medida correctiva de seguridad (Security Corrective Action Requirement, SCAR) de la autoevaluación y las auditorías estén debidamente cerrados para mejorar sus sistemas de gestión de seguridad.	✔	✔	✔
8.3.3	Todos los sitios deberán presentar a la función central actualizaciones e informes sobre todos los SCAR pendientes. La función principal deberá escalar a la administración del LSP/solicitante si los SCAR no se completan antes de sus fechas de vencimiento.	✔	✔	✔
8.4	**Registros de inspecciones, de visitantes y de conductores, inspecciones de siete puntos**			
8.4.1	La función principal deberá contar con procedimientos para garantizar que todos los sitios mantienen registros de inspecciones, de visitantes, de conductores e inspección de siete puntos, etc.	✔	✔	✔
8.5	**Evaluaciones de riesgos de todos los sitios**			
8.5.1	La función principal deberá contar con procedimientos para garantizar que se realizan las evaluaciones y gestión de riesgos adecuadas en todos los sitios y que se mantienen sus registros.	✔	✔	✔
8.6	**Diseño del CCTV y alarmas de los sitios**			
8.6.1	La función principal deberá contar con procedimientos para garantizar que todos los sitios revisan y mantienen documentos de todos los sistemas físicos de seguridad como el diseño del CCTV y de alarmas.	✔	✔	✔
8.7	**Registros de control de alarmas y accesos**			

Sección	Función principal	A	B	C
8.7.1	La función principal deberá contar con procedimientos que garanticen que todos los sistemas de control de alarmas y accesos se mantengan y prueben para asegurar su eficacia operativa.	✔	✔	✔
8.7.2	La función principal deberá contar con procedimientos para que todos los sitios mantengan registros de todas las pruebas e incidentes de control de acceso y detección de intrusiones.	✔	✔	✔
8.8	**Registros de la capacitación**			
8.8.1	La función principal deberá contar con procedimientos para garantizar que todos los sitios mantienen registros adecuados de la capacitación sobre la gestión de seguridad de sus empleados.	✔	✔	✔
8.8.2	La función principal deberá contar con procedimientos para garantizar que todos los sitios mantienen registros de la capacitación de seguridad de todo el personal del sitio.	✔	✔	✔
8.9	**Selección/investigación de historial de registros**			
8.9.1	La función principal deberá contar con procedimientos para garantizar que todos los sitios realizan la selección e investigación de los registros en intervalos regulares para garantizar la integridad y efectividad de los sistemas de gestión de seguridad.	✔	✔	✔
8.9.2	La función principal deberá contar con procedimientos para garantizar que se mantienen registros de revisiones, incluidos sus hallazgos y medidas correctivas/preventivas 8.1.6.	✔	✔	✔
8.10	**Revisión de la administración para evaluar las autoauditorías, los SCAR planteados, cualquier pérdida, robo y evaluaciones de riesgos.**			
8.10.1	La función principal deberá realizar una revisión regular de la administración para garantizar el cumplimiento, la efectividad y la mejora de sus sistemas de gestión de seguridad.	✔	✔	✔
8.10.2	Las revisiones de la administración deberán, entre otras, abarcar la eficacia de las autoauditorías, los cierres de los SCAR, las evaluaciones de riesgos, los incidentes y las medidas de mejora.	✔	✔	✔
8.10.3	La función principal deberá mantener registros de todas las revisiones de la administración.	✔	✔	✔

9.0. TI y amenaza de ciberseguridad: opción mejorada

Los FSR incluyen mejoras opcionales de la amenaza a la seguridad cibernética consideradas un nivel de protección más elevado y se pueden utilizar en combinación con los módulos. Esta mejora opcional está diseñada para ser seleccionada por el LSP/Solicitante y/o su Comprador como requisitos adicionales para sus necesidades de seguridad operativa. Cuando se selecciona esta mejora opcional en la evaluación de precertificación para formar parte de la auditoría de certificación, todos los requisitos son obligatorios.

Sección	TI y amenaza de ciberseguridad: opción mejorada
9.	***Requisitos obligatorios***
9.1	El LSP/Solicitante debe tener políticas de seguridad para TI y ciberamenazas. Las políticas pueden estar separadas o en un documento combinado. Las políticas deben explicar lo siguiente: Las medidas del LSP/Solicitante para identificar y responder a las amenazas. Las políticas y procedimientos implementados para proteger, detectar, probar y responder a los eventos de seguridad. Los métodos para la recuperación de sistemas y/o datos de TI. El protocolo de comunicaciones a Compradores/Clientes para mitigar el impacto en la cadena de suministro en un plazo de 24 horas desde el conocimiento del incidente. Cómo se revisan anualmente las políticas y se actualizan según proceda.
9.2	El LSP/Solicitante debe impartir una capacitación de concientización sobre información a todos los empleados. Esta capacitación debe: Abarcar las funciones y responsabilidades que tienen los usuarios de computadoras en el mantenimiento de la seguridad y los beneficios asociados. Disponer de un sistema que garantice que los registros de las personas que reciban la capacitación se mantienen y conservan durante un período mínimo de 2 años.
9.3	El LSP/Solicitante debe contar con una política escrita para garantizar que las medidas de ciberseguridad están implementadas con subcontratistas y/o proveedores que garantizan que: 1. Los requisitos de ciberseguridad del LSP/Solicitante se comunican a subcontratistas y/o proveedores y se incluyen en los acuerdos. 2. Cuando los subcontratistas y/o proveedores no reconozcan o se nieguen a adoptar los requisitos de ciberseguridad del LSP/Solicitante, se documentarán y aplicarán medidas que mitiguen los riesgos para los requisitos de ciberseguridad del LSP/Solicitante y sus clientes.
9.4	El LSP/Solicitante debe tener un plan de mitigación de interrupción de la alimentación (por ejemplo, fuente de alimentación alternativa o generador de respaldo), que garantiza que la energía se dirija a los sistemas TI críticos (identificados en la evaluación de riesgo local) durante un mínimo de 48 horas.
9.5	Los sistemas de información del LSP/Solicitante deben tener instalada una licencia de software de antivirus y antimalware. El software de antivirus y antimalware debe contener las últimas actualizaciones.
9.6	El LSP/Solicitante debe tener un Plan de recuperación de desastres (Disaster Recovery Plan, DRP) de TI apropiado para recuperarse de ataques a sistemas comprometidos, que incluya, entre otros, toda la información, copia de seguridad del software y mecanismos de recuperación necesarios.
9.7	Se deben realizar copias de seguridad de los sistemas de información del LSP/solicitante. Dichas copias de seguridad deben probarse con regularidad y los datos de la copia de seguridad deben ser encriptados y transferidos a una ubicación secundaria, fuera del sitio.

Sección	TI y amenaza de ciberseguridad: opción mejorada
9.8	El LSP/Solicitante debe aplicar una política para que todas las cuentas de usuario gestionen y controlen el acceso a los sistemas de información mediante el uso de identificadores individuales únicos y contraseñas fuertes. Procedimientos establecidos para asegurar lo siguiente: 1. Programa de auditoría de cumplimiento de contraseñas en marcha. 2. Se debe asignar una contraseña inicial única a cada nueva cuenta en el momento de su 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 serán comunicadas a los usuarios de forma segura y solo después de validar la identidad del usuario. 5. Se debe exigir a los usuarios que cambien sus contraseñas en el primer inicio de sesión. 6. Las contraseñas deben cambiarse al menos cada 90 días.

Información sobre publicaciones y derechos de autor

Historial de la publicación

Publicado por primera vez en enero de 2020

Primera edición (actual) publicada en enero de 2020

Esta Especificación disponible públicamente entra en vigor el 1 de julio de 2020