Transported Asset Protection Association

FSR 2026

TAPA Global Standard

Copyright © TAPA Not Copy

TAPA Americas

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

www.tapaonline.org

TAPA Asia Pacific

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

www.tapa-apac.org

TAPA EMEA

Kanaalpark 140
2321 JV Leiden
The Netherlands

www.tapaemea.org

© TAPA 2026

Indice

1.0 Introduzione 4

1.1 Scopo di Questo Documento FSR 4

1.2 Risorse per implementare il TAPA FSR 4

1.3 Protzione delle Politiche e delle Procedure dell'LSP 4

2.0 Informazioni su TAPA 5

2.1 Scopo di TAPA 5

2.2 Missione di TAPA 5

3.0 Standard TAPA 6

3.1 Standard di Sicurezza TAPA 6

3.2 Implementazione 6

4.0 Guida Legale 7

4.1 Ambito 7

4.2 Traduzione 7

4.3 Il marchio "TAPA" 7

4.4 Limitazione di Responsabilità 7

5.0 Contratti e Subappalto 8

5.1 Contratti 8

5.2 Subappalto 8

5.3 Indagine e Risoluzione dei Reclami TAPA 8

6.0 Deroghe 9

7.0 Requisiti di Sicurezza delle Strutture 10

S1. Requisiti Generali 10

S2. Perimetro 12

2.1 Area esterna del magazzino per la movimentazione del carico, spedizione e ricezione 12

2.2 Barriere Fisiche 12

2.3 Aree Esterne di Banchina 13

2.4 Accesso ai Veicoli Personali 14

S3. Pareti Esterne, Tetto e Porte 15

3.1 Lati esterni della struttura: CCTV/VSS 15

3.2 Pareti Esterne e Tetto 15

S4. Punti di ingresso e uscita degli uffici e del magazzino 18

4.1 Punto/i di ingresso visitatori dell'area uffici 18

4.2 Punto/i di ingresso della forza lavoro 19

4.3 Identificazione dell'Autista e del Veicolo 19

S5. All'interno del magazzino e dell'ufficio 20

5.1 Area del magazzino: Pareti multi-tenant 20

5.2 Aree interne del magazzino 20

TAPA Copyright © Do Not Copy

5.3 Porte di banchina interne e aree di banchina ... 20
5.4 Controllo degli accessi tra ufficio e banchina/magazzino ... 21
5.5 Area per Merci di Alto Valore (HVC) ... 22
5.6 Ispezione dei rifiuti dal magazzino ... 23
5.7 Precaricamento e predisposizione ... 23
5.8 Ricerca di contenitori personali e uscite ... 24
5.9 Controllo delle attrezzature per la movimentazione del carico ... 24
5.10 Integrità del container o del rimorchio: ispezione in 7 punti ... 25
5.11 Procedura di consegna della merce; sigilli di sicurezza ... 25
5.12 Integrità del carico; processo di convalida delle operazioni di carico/scarico. ... 26
5.13 Ritiri fraudolenti ... 26

S6. Sistemi di sicurezza: progettazione, monitoraggio e risposta ... 27
6.1 Posto di monitoraggio ... 27
6.2 Sistema di rilevamento delle intrusioni (IDS) ... 27
6.3 Sistema di controllo automatico degli accessi (AACS) ... 28
6.4 Videosorveglianza/VSS ... 29
6.5 Illuminazione esterna e interna ... 29

S7. Formazione e procedure ... 30
7.1 Procedure di escalation ... 30
7.2 Impegno della direzione ... 30
7.3 Formazione ... 30
7.4 Accesso ai beni degli Acquirenti/Clienti ... 31
7.5 Controllo delle informazioni ... 31
7.6 Segnalazione di incidenti di sicurezza ... 31
7.7 Programmi di manutenzione ... 31
7.8 Orientamento per gli appaltatori ... 32
7.9 Spedizione e ricezione dei documenti ... 32
7.10 Processo di pre-allerta in atto ... 33

S8. Integrità della forza lavoro ... 34
8.1 Screening/Verifica/Controllo dei precedenti (nei limiti consentiti dalla legge locale) ... 34
8.2 Cessazione o riassunzione della forza lavoro ... 34

S9. Requisiti della funzione centrale (applicabili solo alla certificazione multisito) ... 36
9.1 Generale ... 36
9.2 Politiche e procedure ... 36
9.3 Rapporto di autovalutazione redatto per tutte le sedi ... 37
9.4 Registri delle ispezioni, registri (registri visitatori/autista), ispezioni a 7 punti ... 37
9.5 Valutazione dei rischi di tutti i siti ... 38
9.6 Schema di videosorveglianza/sistema di videosorveglianza e allarme del sito ... 38
9.7 Registri di allarme e controllo accessi ... 38
9.8 Registrazione dei dati ... 38
9.9 Registri di screening/verifica ... 39
9.10 Revisione della direzione per valutare le auto-verifiche; SCAR rilevate; eventuali perdite, furti; valutazioni dei rischi ... 39

8.0 Minacce alla sicurezza informatica e IT: opzione avanzata ... 40

E8. Requisiti obbligatori ... 40

TAPA Copyright © Do Not Copy

1.0 Introduzione

1.1 Scopo di Questo Documento FSR

Questo documento sui Requisiti di Sicurezza delle Strutture (FSR) è lo Standard ufficiale TAPA per il magazzinaggio e lo stoccaggio sicuro. È uno Standard globale comune che può essere utilizzato negli accordi commerciali/di sicurezza tra Clienti e Fornitori di Servizi Logistici (LSP) e/o altri Richiedenti che cercano la Certificazione.

Nello sviluppo di questo Standard, TAPA riconosce le molteplici differenze nel modo in cui i servizi di stoccaggio sono forniti a livello globale, regionale e persino all'interno delle aziende, e che l'FSR può applicarsi a tutti o a una parte dei servizi forniti da un LSP/Richiedente. A seconda della complessità e delle dimensioni della catena di approvvigionamento, la conformità agli Standard TAPA può essere raggiunta tramite un singolo LSP/Richiedente oppure tramite più LSP/Richiedenti e subappaltatori qualificati.

Ambito

TAPA ha sviluppato tre opzioni per supportare la certificazione:

• Certificazione di singolo sito da parte di un Organismo di Audit Indipendente (IAB).

• Certificazione multisito da parte di un IAB.

• Certificazione tramite auto-audit da parte di Auditor Autorizzati (AA) dell'LSP/Richiedente o dell'IAB (che esegue un auto-audit per conto dell'LSP/Richiedente)

Destinatari

Gli utenti tipici degli Standard TAPA includono:

• Clienti

• LSP/Richiedenti

• Forze dell'ordine o altre organizzazioni governative

• Organizzazioni professionali della Supply Chain

• Assicuratori

TAPA Copyright © Do Not Copy

1.2 Risorse per implementare il TAPA FSR

Le risorse necessarie per soddisfare i requisiti dell'FSR saranno responsabilità dell'LSP/Richiedente e a spese dell'LSP/Richiedente.

1.3 Protzione delle Politiche e delle Procedure dell'LSP

Le copie dei documenti delle politiche e delle procedure di sicurezza saranno presentate all'Acquirente solo in conformità con gli accordi di divulgazione firmati tra l'LSP/Richiedente e l'Acquirente e saranno trattate come informazioni riservate.

2.0 Informazioni su TAPA

2.1 Scopo di TAPA

Il cargo crime è una delle più grandi sfide della supply chain per i produttori di prodotti di alto valore e ad alto rischio e per i loro fornitori di servizi logistici.

La minaccia non proviene più solo da criminali opportunisti. Oggi, reti di criminalità organizzata operano a livello globale e utilizzano attacchi sempre più sofisticati contro veicoli, strutture e personale per raggiungere i loro obiettivi.

TAPA è un forum unico che riunisce produttori globali, fornitori di servizi logistici, vettori di trasporto merci, forze dell'ordine e altri stakeholder con l'obiettivo comune di ridurre le perdite nelle supply chain internazionali. L'obiettivo principale di TAPA è la prevenzione dei furti attraverso l'uso di intelligence in tempo reale e delle più recenti misure preventive.

2.2 Missione di TAPA

La missione di TAPA è aiutare a proteggere i beni dei membri riducendo al minimo le perdite di carico nella supply chain. TAPA raggiunge questo obiettivo attraverso lo sviluppo e l'applicazione di Standard di Sicurezza globali, pratiche riconosciute del settore, tecnologia, formazione, benchmarking, collaborazione normativa e l'identificazione proattiva delle tendenze criminali e delle minacce alla sicurezza della supply chain.

TAPA Copyright © Do Not Copy

3.0 Standard TAPA

3.1 Standard di Sicurezza TAPA

I seguenti Standard di Sicurezza TAP**A** globali sono stati creati per garantire il trasporto e lo stoccaggio sicuri di merci di alto valore e soggette a furto:

• I **Facility Security Requirements (FSR)** rappresentano standard minimi specificamente per il magazzinaggio sicuro o lo stoccaggio in transito all'interno di una supply chain.

• I **Trucking Security Requirements (TSR)** si concentrano esclusivamente sul trasporto su camion e rappresentano standard minimi specificamente per il trasporto di prodotti su strada all'interno di una supply chain.

• I **Cyber Security Standards (CSS)** mirano a fornire uno strumento per le aziende per comprendere i requisiti minimi nella gestione IT nelle operazioni della supply chain aziendale per proteggere gli asset digitali da attacchi informatici e da interruzioni operative.

Gli Standard di Sicurezza TAPA globali vengono riesaminati e revisionati secondo necessità ogni tre anni.

Questo documento riguarda solo i requisiti FSR!

• Il processo di certificazione per il TAPA FSR è documentato nel documento TAPA FSR Certification Framework.

• Entrambe le versioni correnti del TAPA FSR e del documento TAPA FSR Certification Framework devono essere seguite per ottenere lo stato di certificazione TAPA FSR.

3.2 Implementazione

La corretta implementazione degli Standard di Sicurezza TAPA dipende dalla collaborazione tra LSP (Logistics Service Providers)/Richiedenti, Acquirenti/Clienti (proprietari del carico) e Auditor Autorizzati TAPA.

TAPA Copyright © Do Not Copy

4.0 Guida Legale

4.1 Ambito

L'FSR è uno Standard Globale e tutte le sezioni dello Standard sono obbligatorie salvo che venga concessa un'eccezione attraverso il processo ufficiale di deroga (vedere Sezione 6 dello Standard FSR e Sezione 7 del Documento FSR Certification Framework).

4.2 Traduzione

Nelle aree geografiche in cui l'inglese non è la prima lingua e dove la traduzione è necessaria e applicabile, è responsabilità dell'LSP/Richiedente e dei suoi agenti garantire che qualsiasi traduzione dell'FSR, o di qualsiasi sua parte, rifletta accuratamente le intenzioni di TAPA nello sviluppo e nella pubblicazione di questi Standard.

as

4.3 Il marchio "TAPA"

"TAPA" è un marchio registrato della Transported Asset Protection Association e non può essere utilizzato senza l'espresso permesso scritto di TAPA attraverso le sue regioni ufficialmente riconosciute. Gli Standard TAPA e il materiale associato sono pubblicati da, e tramite, TAPA e non possono essere revisionati, modificati o cambiati da alcuna parte senza l'espresso permesso scritto di TAPA. L'uso improprio del marchio TAPA può comportare la revoca della certificazione o azioni legali.

4.4 Limitazione di Responsabilità

Con la pubblicazione di questi Standard, TAPA non fornisce alcuna garanzia o assicurazione che tutti gli eventi di furto di carico saranno prevenuti, indipendentemente dal fatto che gli Standard siano pienamente applicati e correttamente implementati. Qualsiasi responsabilità che possa derivare da un furto di carico in stoccaggio, o da qualsiasi altra perdita di carico in stoccaggio secondo gli Standard FSR, sarà a carico dell'LSP/Richiedente e/o dell'Acquirente in conformità con i termini e le condizioni del loro contratto reciproco e con qualsiasi legge o statuto applicabile nella giurisdizione competente.

TAPA Copyright © Do Not Copy

5.0 Contratti e Subappalto

5.1 Contratti

Il trasporto, lo stoccaggio e la gestione sicuri dei beni dell'Acquirente sono responsabilità dell'LSP/Richiedente, dei suoi agenti e subappaltatori durante tutta la fase di ritiro, transito, stoccaggio e consegna, come specificato in una liberatoria o in un contratto.

Dove l'FSR è citato o incluso nel contratto tra l'LSP/Richiedente e l'Acquirente, esso dovrà essere anche citato nel programma di sicurezza dell'LSP/Richiedente.

L'LSP dovrà fornire all'Acquirente la prova della Certificazione FSR e, ove appropriato, la prova che i requisiti FSR siano stati soddisfatti. Inoltre, qualsiasi presunta mancata implementazione dei requisiti FSR da parte dell'LSP/Richiedente dovrà essere risolta secondo i termini del contratto negoziato tra l'Acquirente e l'LSP/Richiedente.

5.2 Subappalto

Quando si utilizzano subappaltatori, deve esserci un requisito contrattuale che stabilisca che i subappaltatori soddisfino tutti i requisiti FSR indicati. Gli **Auditor Autorizzati Interni** dell'LSP devono confermare che il subappaltatore soddisfi i requisiti FSR dello stesso livello.

5.3 Indagine e Risoluzione dei Reclami TAPA

Se TAPA riceve un reclamo formale riguardante le prestazioni di un LSP/Richiedente certificato, TAPA (previa convalida) può richiedere che l'LSP/Richiedente stipuli un contratto per un nuovo audit a spese dell'LSP/Richiedente. Se l'LSP/Richiedente non supera l'audit o rifiuta di conformarsi a questo processo, il suo certificato può essere revocato.

TAPA Copyright © Do Not Copy

6.0 Deroghe

Una Deroga è un'approvazione scritta concessa per esentare una struttura da uno specifico requisito TAPA e per accettare una soluzione alternativa di conformità. Una deroga può essere richiesta se un LSP/Richiedente non può soddisfare uno specifico requisito nell'FSR e può giustificare misure alternative. Le deroghe sono valide per il periodo della certificazione.

TAPA Copyright © Do Not Copy

7.0 Requisiti di Sicurezza delle Strutture

S1. Requisiti Generali

N. Req.	Requisiti / Controlli	Livello Applicabile		
1.1.1	Tutte le procedure o le politiche richieste da questo Standard devono essere documentate e aggiornate almeno ogni due anni.	Ⓐ	Ⓑ	Ⓒ
1.1.2	La direzione deve aver formalmente nominato una persona (AA) responsabile della sicurezza nel sito che sia incaricata di mantenere il **TAPA FSR**, la chiusura degli **SCARS**, la valutazione dei rischi, il report alla direzione e i requisiti di sicurezza della supply chain aziendale. Un'altra persona (può essere la stessa) sarà inoltre responsabile del monitoraggio del programma **FSR**. Questo include la pianificazione dei controlli di conformità, le comunicazioni con gli **AA**, la ricertificazione, le modifiche allo **Standard FSR**, ecc. Queste persone possono essere dipendenti o persone esterne in outsourcing sotto contratto per svolgere questo ruolo.	Ⓐ	Ⓑ	Ⓒ
1.1.3	Audit interni (da parte di un team interfunzionale) sul sistema di gestione della sicurezza, rapporti di autovalutazione da parte dell'AA interno e la chiusura degli SCARS devono essere completati e documentati.	Ⓐ	Ⓑ	Ⓒ
1.1.4	È richiesta una procedura, un registro e/o un piano delle chiavi per le serrature fisiche, le carte di accesso e/o le chiavi che gestiscono e controllano le chiavi fisiche ed elettroniche. La procedura dovrebbe includere processi per la duplicazione, la conservazione e la risposta a chiavi mancanti/perse.	Ⓐ	Ⓑ	Ⓒ
1.1.5	Deve essere condotta e aggiornata almeno annualmente una **valutazione del rischio documentata** che riconosca la probabilità e l'impatto delle minacce legate alla sicurezza. La direzione deve riesaminare e riconoscere che i rischi identificati sono stati valutati e che sono stati implementati controlli appropriati per mitigare o eliminare i rischi a un livello accettabile. Come minimo, devono essere valutati i seguenti eventi interni/esterni comuni: furto di carico o informazioni, accesso non autorizzato alle strutture o al carico, manomissione/distruzione dei sistemi di sicurezza, ritiri fittizi del carico, continuità della sicurezza durante carenze di personale, o disastri naturali, necessità di barriere anti-sfondamento per finestre accessibili a livello del suolo o porte di banchina, ecc. Ulteriori minacce possono essere considerate sulla base dei rischi locali/del paese.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

N. Req.	Requisiti / Controlli	Livello Applicabile		
1.1.6	La persona che esegue gli audit interni o annuali per il Richiedente / LSP (chiamata **LSP AA**) deve essere formata. Questa persona può essere la stessa persona menzionata al punto **1.1.2** oppure può essere una persona esterna in outsourcing sotto contratto per svolgere questo ruolo.	Ⓐ	Ⓑ	Ⓒ
1.1.7	Per comprendere l'FSR ed essere in grado di implementare tutti i suoi requisiti, tutti gli **AA del Richiedente/LSP** devono aver sostenuto e superato l'esame applicabile per lo **Standard TAPA** e la versione rispetto alla quale sono tenuti a effettuare l'audit.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S2. Perimetro

2.1 Area esterna del magazzino per la movimentazione del carico, spedizione e ricezione

N. Req.	Requisiti / Controlli	Livello Applicabile		
2.1.1	**CCTV (Closed-Circuit Television)/ VSS (Video Surveillance System)** in grado di monitorare tutto il traffico nell'area esterna di movimentazione del carico, spedizione e ricezione (inclusi i punti di ingresso e uscita), garantendo che tutti i veicoli e gli individui siano riconoscibili in ogni momento salvo temporanea ostruzione dovuta a esigenze operative (ad esempio carico e scarico dei camion in tempo reale).	Ⓐ	Ⓑ	
2.1.2	Illuminazione adeguata nelle aree di carico e scarico deve essere utilizzata come deterrente di base contro i reati e per consentire la visibilità delle operazioni in tali aree durante le ore notturne. ***Nota**: L'illuminazione può essere continua, attivata da allarme, movimento, rilevamento del suono, ecc., con illuminazione immediata garantita*.	Ⓐ	Ⓑ	Ⓒ
2.1.3	Deve essere in vigore una procedura che descriva come i veicoli e le persone non autorizzati devono essere gestiti all'interno dell'area esterna di movimentazione del carico, spedizione e ricezione. Le istruzioni sulla procedura devono essere fornite ai membri pertinenti della forza lavoro, incluse le guardie.	Ⓐ	Ⓑ	Ⓒ
2.1.4	L'area di movimentazione del carico, spedizione e ricezione deve essere adeguatamente controllata per prevenire accessi non autorizzati.		Ⓑ	Ⓒ
2.1.5	Per le finestre accessibili a livello del suolo o le porte di banchina, la Valutazione del Rischio annuale deve valutare la necessità di barriere anti-sfondamento. Inoltre, deve includere la valutazione dell'uso di coperture per finestre per prevenire la visualizzazione non autorizzata degli spazi interni (vedere Valutazione del Rischio, req. 1.1.5.).	Ⓐ		

TAPA Copyright © Do Not Copy

2.2 Barriere Fisiche

N. Req.	Requisiti / Controlli	Livello Applicabile		
2.2.1	Una barriera fisica racchiude l'area di movimentazione del carico, spedizione e ricezione.	Ⓐ		

N. Req.	Requisiti / Controlli	Livello Applicabile		
2.2.2	La barriera fisica intorno all'area di movimentazione del carico, spedizione e ricezione ha un'altezza minima di 6 piedi / 1,8 metri. Nota: La barriera fisica, progettata per prevenire accessi non autorizzati, deve avere un'altezza di 6 piedi / 1,8 metri lungo tutta la sua lunghezza, incluse le aree in cui il livello del suolo cambia, ad esempio è più basso.	Ⓐ		
2.2.3	La barriera fisica intorno all'area di movimentazione del carico, spedizione e ricezione è mantenuta in buone condizioni.	Ⓐ		
2.2.4	I cancelli all'interno delle barriere dell'area di movimentazione del carico, spedizione e ricezione sono presidiati o controllati elettronicamente.	Ⓐ		
2.2.5	La barriera fisica intorno all'area di movimentazione del carico, spedizione e ricezione viene ispezionata per verificarne l'integrità e l'eventuale presenza di danni almeno settimanalmente.	Ⓐ		

TAPA Copyright © Do Not Copy

2.3 Aree Esterne di Banchina

N. Req.	Requisiti / Controlli	Livello Applicabile		
2.3.1	Le aree esterne di banchina sono coperte da telecamere CCTV/VSS esterne a colori o "giorno/notte".	Ⓐ	Ⓑ	Ⓒ
2.3.2	Le telecamere CCTV/VSS sono installate in modo da poter visualizzare tutte le operazioni e i movimenti nell'area esterna di banchina in ogni momento, salvo temporanea ostruzione dovuta a esigenze operative (ad esempio carico e scarico dei camion in tempo reale).	Ⓐ	Ⓑ	Ⓒ
2.3.3	Tutti i veicoli e le persone nelle aree esterne di banchina devono essere coperti da telecamere CCTV/VSS, che possano mostrare chiaramente le informazioni di identificazione del veicolo ed essere in grado di distinguere i tratti facciali del personale.	Ⓐ		
2.3.4	I veicoli e le persone nelle aree esterne di banchina devono essere coperti e visibili dalle telecamere CCTV/VSS in non meno del 75% dei casi nell'arco di una giornata.		Ⓑ	Ⓒ
2.3.5	Tutte le aree esterne intorno alle porte di banchina sono completamente illuminate.	Ⓐ	Ⓑ	Ⓒ

2.4 Accesso ai Veicoli Personali

N. Req	Requisiti / Controlli	Livello Applicabile		
2.4.1	I veicoli personali sono consentiti nelle aree di movimentazione del carico, spedizione e ricezione solo se preventivamente approvati, secondo una politica documentata.	Ⓐ	Ⓑ	Ⓒ
2.4.2	Non sono presenti aree di parcheggio personale entro una distanza a piedi di 25 m / 82 ft dalle aree esterne di banchina.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S3. Pareti Esterne, Tetto e Porte

3.1 Lati esterni della struttura: CCTV/VSS

N. Req	Requisiti / Controlli	Livello Applicabile		
3.1.1	Telecamera CCTV/VSS esterna a colori o “giorno/notte” installata per coprire tutti i lati esterni della struttura.	Ⓐ		
3.1.2	Sistema di telecamere CCTV/VSS esterne a colori o “giorno/notte” installato per coprire i lati esterni della struttura con porte, finestre o altre aperture.		Ⓑ	
3.1.3	Tutte le visualizzazioni del sistema di telecamere CCTV/VSS esterne sono chiare in ogni momento, salvo temporanea ostruzione dovuta a esigenze operative (ad esempio carico e scarico dei camion in tempo reale).	Ⓐ		
3.1.4	Tutti i veicoli e le persone intorno ai lati esterni della struttura devono essere coperti da telecamere CCTV/VSS, che possano mostrare chiaramente le informazioni di identificazione del veicolo ed essere in grado di distinguere i tratti facciali del personale.	Ⓐ		
3.1.5	I veicoli e le persone sono visibili in non meno del 75% delle registrazioni nell’arco di una giornata da parte delle telecamere CCTV/VSS esterne.		Ⓑ	

TAPA Copyright © Do Not Copy

3.2 Pareti Esterne e Tetto

N. Req	Requisiti / Controlli	Livello Applicabile		
3.2.1	Le pareti esterne e il tetto devono essere costruiti e mantenuti in modo da resistere alla penetrazione e fornire una protezione fisica robusta. I materiali devono offrire una resistenza e una durabilità sufficienti per resistere ai tentativi di ingresso forzato. (Esempi: mattoni, blocchi di calcestruzzo, pannelli in calcestruzzo prefabbricato o pannelli sandwich ad alta resistenza con uno spessore totale di almeno 50 mm e lastre interne ed esterne di 0,7 mm). ***Nota**: Qualora vengano utilizzati materiali leggeri o non strutturali, devono essere implementate misure di mitigazione aggiuntive (come rete in acciaio interna o sistemi di rilevamento delle intrusioni) per raggiungere un livello di sicurezza equivalente.*	Ⓐ	Ⓑ	Ⓒ

N. Req	Requisiti / Controlli	Livello Applicabile		
3.2.2	Tutte le finestre apribili, le prese d'aria o altre aperture nelle pareti esterne della struttura, o qualsiasi finestra sigillata installata a meno di 3 metri / 9 piedi 10 pollici dal piano di lavoro nelle pareti esterne della struttura, devono essere dotate di una barriera fisica o essere allarmate e collegate al sistema di allarme principale.	Ⓐ	Ⓑ	
3.2.3	Tutte le finestre apribili, i lucernari, le prese d'aria, i portelli sul tetto o qualsiasi altra apertura sul tetto devono essere protetti mediante: (a) una robusta barriera fisica (ad esempio barre di sicurezza, griglie o coperture rinforzate), oppure (b) un dispositivo di rilevamento intrusioni integrato con il sistema di allarme principale della struttura. *Nota: Le barriere fisiche devono essere progettate per prevenire la rimozione o la manomissione, e le aperture allarmate devono attivare avvisi immediati in caso di accesso non autorizzato.*	Ⓐ		
3.2.4	L'accesso esterno al tetto (scala o scale) deve essere: Fisicamente bloccato e coperto da CCTV/VSS (telecamere a colori o "giorno/notte") oppure Fisicamente bloccato e allarmato.	Ⓐ		
3.2.5	Accesso esterno al tetto (scala o scale) fisicamente bloccato.		Ⓑ	Ⓒ
3.2.6	Tutte le porte esterne pedonali del magazzino e le porte degli uffici della struttura sono allarmate per rilevare aperture non autorizzate e collegate al sistema di allarme principale. Nota: Le porte di banchina non sono coperte da questo requisito, vedere req. 3.2.12 per i requisiti di allarme delle porte di banchina.	Ⓐ	Ⓑ	Ⓒ
3.2.7	Ogni porta esterna del magazzino, porta dell'ufficio o altra apertura della struttura deve essere identificata in modo univoco per porta o per zona all'interno del sistema di allarme principale	Ⓐ		
3.2.8	Tutte le porte esterne del magazzino sono sempre chiuse e protette quando non sono in uso attivo. Ove applicabile, chiavi/codici controllati.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

N. Req	Requisiti / Controlli	Livello Applicabile		
3.2.9	Le porte pedonali esterne del magazzino e i telai non devono essere facilmente penetrabili. Se le cerniere sono esterne, devono essere fissate con perni o saldate a punti. Le porte del magazzino completamente o parzialmente in vetro non sono accettabili a meno che non siano installati rilevatori di rottura vetro, o che un altro dispositivo di rilevamento locale fornisca copertura (ad esempio infrarosso passivo) e sia allarmato direttamente al centro di monitoraggio O che il vetro sia protetto da barre/rete. TAPA consentirà ai titolari di certificazioni esistenti che non sono in grado di conformarsi a questo requisito di continuare con la loro configurazione attuale fino alla prossima revisione. I nuovi titolari di certificazione o i nuovi siti devono soddisfare il nuovo requisito	Ⓐ	Ⓑ	Ⓒ
3.2.10	Le uscite di emergenza utilizzate esclusivamente per scopi di emergenza (ad es. uscite antincendio) sono sempre allarmate con un segnalatore acustico individuale o a zone.	Ⓐ	Ⓑ	
3.2.11	Tutte le porte di banchina devono avere una resistenza sufficiente tale da scoraggiare e/o ritardare l'ingresso forzato mediante l'uso di piccoli utensili manuali elettrici/a batteria.	Ⓐ	Ⓑ	Ⓒ
3.2.12	Porte di banchina Ore non operative: Le porte di banchina sono chiuse, protette (ad es. disabilitate elettronicamente o bloccate fisicamente). Le porte di banchina sono allarmate per rilevare intrusioni non autorizzate e generare un allarme collegato al sistema di allarme principale. Ore operative: Le porte di banchina devono essere chiuse quando non sono in uso attivo. I cancelli a forbice, se utilizzati, devono essere protetti da una chiusura meccanica a scorrimento/fermo ed essere alti almeno 8 piedi / 2,4 metri.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S4. Punti di ingresso e uscita degli uffici e del magazzino

4.1 Punto/i di ingresso visitatori dell'area uffici

N. Req	Requisiti / Controlli	Livello Applicabile		
4.1.1	Il/i punto/i di ingresso dei visitatori sono controllati da un dipendente/guardia/receptionist che è stato formato sull'emissione dei badge, sui controlli, sulla registrazione, sui visitatori, sul requisito di accompagnamento, ecc. (processo in atto per quando i dipendenti registrano i propri ospiti e quando le visite avvengono al di fuori degli orari operativi).	Ⓐ	Ⓑ	Ⓒ
4.1.2	Il/i punto/i di ingresso dei visitatori dell'area uffici è coperto da CCTV (telecamere a colori o "giorno/notte"); le persone sono chiaramente riconoscibili in ogni momento.	Ⓐ	Ⓑ	
4.1.3	Allarme di emergenza presente nel/i punto/i di ingresso dei visitatori dell'area uffici e testato settimanalmente.	Ⓐ	Ⓑ	
4.1.4	Tutti i visitatori dell'area uffici sono identificati utilizzando un documento di identità con foto rilasciato dal governo (ad es. patente di guida; passaporto o carta d'identità nazionale, ecc.). Se gli ID digitali sono accettati dalla struttura e consentiti dalla legislazione locale, deve essere in atto un processo di verifica robusto (inclusa tutta l'infrastruttura tecnica richiesta).	Ⓐ	Ⓑ	Ⓒ
4.1.5	Tutti i visitatori dell'area uffici sono registrati e il registro è mantenuto per un minimo di 30 giorni. I dettagli della visita, come quale individuo sarà visitato e qual è il motivo della visita, devono essere tracciabili attraverso le informazioni registrate nel registro dei visitatori.	Ⓐ	Ⓑ	Ⓒ
4.1.6	Tutti i badge dei visitatori devono essere riconciliati all'uscita del visitatore dai locali e il registro completo deve essere controllato quotidianamente.	Ⓐ	Ⓑ	
4.1.7	Tutti i visitatori espongono visibilmente badge o pass e sono accompagnati dal personale dell'azienda.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

4.2 Punto/i di ingresso della forza lavoro

N. Req	Requisiti / Controlli	Livello Applicabile		
4.2.1	Tutti i punti di ingresso della forza lavoro sono controllati per l'accesso 24/7.		Ⓑ	Ⓒ
4.2.2	Tutti i punti di ingresso della forza lavoro sono controllati tramite dispositivo elettronico di controllo accessi 24/7. Accesso registrato.	Ⓐ		
4.2.3	I punti di ingresso della forza lavoro sono coperti da CCTV/VSS (telecamere a colori o "giorno/notte").	Ⓐ	Ⓑ	
4.2.4	Tutti i dipendenti devono ricevere badge aziendali con foto dopo il completamento del processo di verifica.	Ⓐ	Ⓑ	
4.2.5	Tutto il resto della forza lavoro deve essere dotato di un badge identificativo aziendale per renderli riconoscibili all'interno della struttura	Ⓐ	Ⓑ	
4.2.6	Tutti i badge della forza lavoro sono chiaramente visibili.	Ⓐ	Ⓑ	
4.2.7	I badge della forza lavoro non devono essere condivisi in nessuna circostanza e deve essere in vigore una politica di emissione dei badge.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

4.3 Identificazione dell'Autista e del Veicolo

N. Req	Requisiti / Controlli	Livello Applicabile		
4.3.1	Tutti gli autisti sono identificati utilizzando un documento di identità con foto relocate dal governo (ad es. patente di guida; passaporto o carta d'identità nazionale, ecc.) e viene mantenuto un registro degli autisti. Se gli ID digitali sono accettati dalla struttura e consentiti dalla legislazione locale, deve essere in atto un processo di verifica robusto (inclusa tutta l'infrastruttura tecnica richiesta).	Ⓐ	Ⓑ	Ⓒ
4.3.2	Verifica che la patente di guida non sia scaduta e corrisponda all'autista. Se le patenti di guida digitali sono accettate dalla struttura e consentite dalla legislazione locale, deve essere in atto un processo di verifica robusto (inclusa tutta l'infrastruttura tecnica richiesta).	Ⓐ	Ⓑ	Ⓒ
4.3.3	Gli identificativi dei veicoli sono registrati manualmente (ad es. scritti) o tramite telecamere. Devono includere almeno la targa e il tipo di veicolo.	Ⓐ		

S5. All'interno del magazzino e dell'ufficio

5.1 Area del magazzino: Pareti multi-tenant

N. Req	Requisiti / Controlli	Livello Applicabile		
5.1.1	Le pareti interne multi-tenant dal pavimento al soffitto e il tetto devono essere costruiti/progettati e mantenuti per resistere alla penetrazione (Esempio: mattoni, blocchi, lastre di cemento prefabbricato, pareti in pannelli sandwich con uno spessore minimo di 7 mm).	Ⓐ	Ⓑ	Ⓒ
5.1.2	Se le pareti interne multi-tenant dal pavimento al soffitto sono costruite in rete metallica di grado di sicurezza o altra barriera sicura riconosciuta dal settore, devono essere anche allarmate per rilevare intrusioni. Nota 1: Reti, recinzioni di bassa qualità o reti non di grado di sicurezza non sono accettabili. Nota 2: Se le pareti multi-tenant sono costruite con materiale solido dal pavimento al soffitto, allora questo requisito diventa N/A.	Ⓐ	Ⓑ	Ⓒ

5.2 Aree interne del magazzino

N. Req	Requisiti / Controlli	Livello Applicabile		
5.2.1	Il rilevamento delle intrusioni (ad es. infrarosso, movimento, suono o rilevamento delle vibrazioni) è richiesto per monitorare le aree interne del magazzino. Gli allarmi devono essere attivati e collegati al sistema di allarme principale durante le ore non operative (ovvero quando il magazzino è chiuso). Nota 1: Se il magazzino è un'operazione reale 24/7/366, questo requisito può essere N/A se i rischi e le mitigazioni sono documentati nella Valutazione del Rischio locale. (Vedere req. 1.1.5) Nota 2: Indipendentemente dalle ore operative, il rilevamento delle intrusioni perimetrali o le barriere fisiche sono sempre richiesti su porte esterne e finestre al piano terra in ufficio e magazzino. (Vedere req. 3.2.2 e 3.2.6)	Ⓐ		

5.3 Porte di banchina interne e aree di banchina

N. Req	Requisiti / Controlli	Livello Applicabile		
5.3.1	Tutte le porte di banchina interne e le aree di banchina sono coperte da CCTV/VSS (telecamere a colori o "giorno/notte").	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

N. Req	Requisiti / Controlli	Livello Applicabile		
5.3.2	Le visualizzazioni del carico durante il carico/scarico presso tutte le porte di banchina interne e le aree di banchina sono chiare in ogni momento, salvo temporanea ostruzione dovuta a esigenze operative (ad esempio carico e scarico dei camion in tempo reale).	Ⓐ	Ⓑ	Ⓒ
5.3.3	I beni dell'Acquirente sono sotto sorveglianza CCTV al 100% nelle aree di movimentazione o di staging del carico (ad es. aree di smontaggio/montaggio pallet, percorsi da e verso le scaffalature di stoccaggio, banchina, corridoi di transito).	Ⓐ	Ⓑ	
5.3.4	I beni dell'Acquirente sono sotto sorveglianza CCTV al 100% nelle aree di movimentazione o di staging del carico (ad es. aree di smontaggio/montaggio pallet, percorsi da e verso le scaffalature di stoccaggio, banchina, corridoi di transito).	Ⓐ		

5.4 Controllo degli accessi tra ufficio e banchina/magazzino

N. Req	Requisiti / Controlli	Livello Applicabile		
5.4.1	Accesso controllato tra ufficio e banchina/magazzino.	Ⓐ	Ⓑ	
5.4.2	Gli allarmi delle porte con accesso a badge o citofono, per le porte tra ufficio e banchina/magazzino, sono udibili localmente e generano un allarme per la risposta quando rimangono aperte per più di 60 secondi o immediatamente se forzate.	Ⓐ		
5.4.3	Gli allarmi delle porte tra ufficio e banchina/magazzino sono udibili localmente o inviano un allarme per la risposta quando rimangono aperte per più di 60 secondi o vengono forzate.		Ⓑ	
5.4.4	La forza lavoro autorizzata dell'LSP/Richiedente e i visitatori accompagnati sono autorizzati ad accedere alle aree di banchina/magazzino in base a una necessità operativa e con accesso limitato.	Ⓐ	Ⓑ	Ⓒ
5.4.5	L'elenco degli accessi alle aree di banchina/magazzino è riesaminato almeno trimestralmente per limitare/verificare che le autorizzazioni di accesso siano concesse solo al personale designato/autorizzato.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

5.5 Area per Merci di Alto Valore (HVC)

N. Req	Requisiti / Controlli	Livello Applicabile		
5.5.1	Le dimensioni e l'utilizzo dell'HVC possono essere determinati dall'accordo tra Acquirente/LSP/Richiedente. Se non è presente un accordo, l'HVC deve essere in grado di stoccare un minimo di 6 metri cubi di prodotto.	Ⓐ	Ⓑ	
5.5.2	Il perimetro dell'area HVC è recintato o delimitato da pareti solide su tutti i lati, inclusa la parte superiore/tetto.	Ⓐ	Ⓑ	
5.5.3	Dispositivo di chiusura su porta/cancello dell'area HVC.	Ⓐ	Ⓑ	
5.5.4	Copertura completa CCTV/VSS (telecamere a colori o "giorno/notte") sull'ingresso dell'HVC e sull'area interna. Nota: Se l'HVC è troppo piccolo per installare una telecamera all'interno, è sufficiente la copertura della telecamera sull'ingresso.	Ⓐ		
5.5.5	Videosorveglianza/videosorveglianza (telecamere a colori o "giorno/notte") all'ingresso dell'HVC..		Ⓑ	
5.5.6	Se l'accesso all'HVC è necessario a più di 10 persone, l'accesso deve essere controllato elettronicamente tramite badge/telecomando. Se l'accesso è richiesto a 10 persone o meno, è necessario un sistema di chiusura con lucchetto o serratura di sicurezza, supportato da un sistema di emissione chiavi controllato. Le chiavi possono essere assegnate a singoli individui per coprire un turno, ma non devono essere trasferite senza autorizzazione e la chiave deve essere registrata nell'apposito registro. Tutte le chiavi devono essere restituite e registrate quando non vengono utilizzate.	Ⓐ		
5.5.7	Le porte/cancelli HVC sono dotati di allarme per rilevare i tentativi di effrazione. Gli allarmi possono essere generati da contatti porta e/o dall'utilizzo di sistemi di rilevamento del movimento CCTV/VSS per individuare accessi non autorizzati.	Ⓐ		
5.5.8	Il perimetro dell'HVC viene mantenuto in buone condizioni e ispezionato mensilmente per verificarne l'integrità e l'eventuale presenza di danni.	Ⓐ		

TAPA Copyright © Do Not Copy

N. Req	Requisiti / Controlli	Livello Applicabile		
5.5.9	LSP/Richiedente deve garantire che l'accesso all'HVC sia concesso solo al personale designato/autorizzato. L'elenco degli accessi approvati all'HVC viene rivisto mensilmente e aggiornato in tempo reale quando un dipendente lascia il lavoro o non necessita più dell'accesso. È in vigore una procedura per l'accesso all'HVC.	Ⓐ	Ⓑ	

5.6 Ispezione dei rifiuti dal magazzino

N. Req	Requisiti / Controlli	Livello Applicabile		
5.6.1	Le aree di raccolta e compattazione dei rifiuti, sia interne che esterne al magazzino, sono monitorate tramite telecamere a circuito chiuso (CCTV) e sistemi di videosorveglianza (VSS).	Ⓐ		
5.6.2	I sacchi per la spazzatura utilizzati all'interno del magazzino, laddove previsti, sono trasparenti.		Ⓑ	Ⓒ

5.7 Precaricamento e predisposizione

N. Req	Requisiti / Controlli	Livello Applicabile		
5.7.1	È vietato il pre-carico o il parcheggio di autocarri a carico completo (FTL) o di proprietà dell'Acquirente all'esterno del magazzino durante gli orari di chiusura, salvo diverso accordo tra l'Acquirente e il Fornitore di servizi logistici (LSP)/Richiedente. È necessario implementare misure di sicurezza alternative (ad esempio, dispositivi di sicurezza aggiuntivi sui veicoli/vani di carico). Nota: per "esterno del magazzino" si intendono le aree separate dalla struttura, ma comunque all'interno del piazzale/recinzione perimetrale del Fornitore di servizi logistici (LSP)/Richiedente.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

5.8 Ricerca di contenitori personali e uscite

N. Req	Requisiti / Controlli	Livello Applicabile		
5.8.1	Le procedure di sicurezza scritte definiscono le modalità di controllo dei "contenitori personali" all'interno del magazzino. I contenitori personali includono portapranzi, zainiRequisiti / Controlli, borse termiche, borsette, ecc.	Ⓐ	Ⓑ	
5.8.2	Se consentito dalla legge locale, il Fornitore di Servizi Logistici (LSP)/Richiedente deve sviluppare e mantenere una procedura documentata per le ispezioni in uscita. L'attivazione della procedura è a discrezione del Fornitore di Servizi Logistici (LSP)/Richiedente e/o in base all'accordo tra Acquirente/LSP/Richiedente. Come minimo, la procedura deve definire i criteri relativi al diritto di ispezione del Fornitore di Servizi Logistici (LSP)/Richiedente qualora si renda necessario effettuare ispezioni anche quando normalmente non sono richieste (ad esempio, in caso di sospetto furto da parte del personale). Dipendenti, Assistenti di Supporto Tecnico (TAS), Subappaltatori e Visitatori devono essere informati di questa politica prima del loro ingresso nel magazzino.	Ⓐ		

5.9 Controllo delle attrezzature per la movimentazione del carico

N. Req	Requisiti / Controlli	Livello Applicabile		
5.9.1	Procedura che prevede la disattivazione di tutti i carrelli elevatori e altre attrezzature motorizzate per la movimentazione delle merci durante le ore non operative. Nota: questa procedura non include i transpallet manuali.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

5.10 Integrità del container o del rimorchio: ispezione in 7 punti

N. Req	Requisiti / Controlli	Livello Applicabile		
5.10.1	Ispezione fisica a 7 punti eseguita su tutti i container o rimorchi dedicati all'acquirente in uscita: parete frontale, lato sinistro, lato destro, pavimento, soffitto/tetto, porte interne/esterne e meccanismo di chiusura, esterno/sottoscocca. Nota: questa procedura si applica a tutti i tipi di rimorchi e container chiusi a chiave e/o sigillati (ovvero, non limitata ai container per il trasporto marittimo).	Ⓐ	Ⓑ	Ⓒ

5.11 Procedura di consegna della merce; sigilli di sicurezza

N. Req				
5.11.1	Salvo diversa indicazione specifica da parte dell'Acquirente, su tutte le spedizioni dirette e senza scali vengono utilizzati sigilli di sicurezza antimanomissione. I sigilli devono essere certificati secondo la norma ISO 17712 (classificazione I, S o H). Nota: i sigilli non sono richiesti per le spedizioni con scali multipli, a causa della complessità e del rischio associati al trasporto di sigilli multipli da parte degli autisti.	Ⓐ	Ⓑ	Ⓒ
5.11.2	L'LSP/Richiedente deve Requisiti / Controllidisporre di procedure documentate per la gestione e il controllo di sigilli di sicurezza, serrature Livello Applicabileper porte di rimorchi (container), serrature a perno e altre attrezzature di sicurezza.	Ⓐ	Ⓑ	Ⓒ
5.11.3	I sigilli di sicurezza possono essere apposti o rimossi esclusivamente da personale autorizzato, ovvero dal personale di magazzino, che ha ricevuto istruzioni per riconoscere e segnalare i sigilli manomessi. I sigilli non devono mai essere apposti o rimossi dall'autista, salvo autorizzazione dell'Acquirente.	Ⓐ	Ⓑ	Ⓒ
5.11.4	Sono in vigore procedure per il riconoscimento e la segnalazione di sigilli di sicurezza compromessi.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

5.12 Integrità del carico; processo di convalida delle operazioni di carico/scarico.

N. Req		Livello Applicabile		
5.12.1	Sono in vigore procedure rigorose che garantiscono la validazione di tutti i beni dell'Acquirente spediti e ricevuti al momento della consegna, mediante un conteggio manuale e/o elettronico dei pezzi. Il processo deve garantire che le anomalie vengano sistematicamente individuate, documentate e segnalate al fornitore di servizi logistici/richiedente e/o all'Acquirente. Requisiti / Controlli Le registrazioni manuali e/o elettroniche devono essere di qualità probatoria. Qualora gli autisti non siano presenti per assistere a tale attività, l'Acquirente/il fornitore di servizi logistici/il richiedente deve garantire una verifica alternativa del conteggio, ad esempio tramite scansioni e/o immagini di telecamere a circuito chiuso/sistemi di videosorveglianza, raccolte e conservate specificamente per questo scopo. Nota: oltre ai pezzi mancanti, le anomalie possono includere danni, cinghie o nastro adesivo mancanti, tagli o altre aperture evidenti, che indicano un possibile furto o appropriazione indebita.	Ⓐ	Ⓑ	Ⓒ

5.13 Ritiri fraudolenti

N. Req	Requisiti / Controlli			
5.13.1	Prima del carico, vengono verificati il documento d'identità dell'autista del camion, la documentazione relativa al ritiro della merce e gli eventuali dettagli di pre-allerta specificati dall'acquirente. La procedura deve essere in vigore. Se la struttura accetta le identità digitali e la legislazione locale lo consente, è necessario implementare un solido processo di verifica (compresa tutta l'infrastruttura tecnica necessaria).	Livello Applicabile Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S6. Sistemi di sicurezza: progettazione, monitoraggio e risposta

6.1 Posto di monitoraggio

N. Req	Requisiti / Controlli	Livello Applicabile		
6.1.1	Monitoraggio degli eventi di allarme 24 ore su 24, 7 giorni su 7, 366 giorni all'anno tramite una postazione di monitoraggio interna o esterna di terze parti, protetta da accessi non autorizzati. Nota: le postazioni di monitoraggio possono essere situate all'interno o all'esterno della sede aziendale e possono essere di proprietà dell'azienda o di terzi. In ogni caso, l'accesso deve essere controllato tramite un sistema di controllo accessi elettronico (badge), serrature o scanner biometrici.	Ⓐ	Ⓑ	Ⓒ
6.1.2	Postazione di monitoraggio per rispondere in tempo reale a tutti gli allarmi del sistema di sicurezza, 24 ore su 24, 7 giorni su 7, 366 giorni all'anno.	Ⓐ	Ⓑ	Ⓒ
6.1.3	La postazione di monitoraggio rileva l'attivazione dell'allarme e inoltra la segnalazione in meno di 3 minuti.	Ⓐ	Ⓑ	Ⓒ
6.1.4	Sono disponibili i report di monitoraggio degli allarmi.	Ⓐ	Ⓑ	Ⓒ
6.1.5	Monitorare le procedure di intervento successive alla messa in atto.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

6.2 Sistema di rilevamento delle intrusioni (IDS)

N. Req	Requisiti / Controlli	Livello Applicabile		
6.2.1	Tutti i sistemi IDS sono attivati durante le ore non operative e collegati al sistema di allarme principale.	Ⓐ	Ⓑ	Ⓒ
6.2.2	Vengono conservati i registri degli allarmi IDS per 90 giorni.	Ⓐ	Ⓑ	
6.2.3	I registri degli allarmi IDS vengono archiviati in modo sicuro e sottoposti a backup almeno settimanalmente.	Ⓐ	Ⓑ	

N. Req	Requisiti / Controlli	Livello Applicabile		
6.2.4	Procedura per garantire che l'accesso al sistema IDS sia limitato a persone autorizzate o amministratori di sistema. Ciò include server, console, controller, pannelli, reti e dati. I privilegi di accesso al sistema IDS devono essere aggiornati tempestivamente quando una persona lascia l'organizzazione o cambia ruolo e non necessita più dell'accesso.	Ⓐ	Ⓑ	Ⓒ
6.2.5	Allarme trasmesso in caso di interruzione di corrente/perdita di IDS. Nota: per i sistemi con gruppo di continuità (UPS), l'allarme viene trasmesso in caso di guasto della batteria dell'UPS.	Ⓐ	Ⓑ	Ⓒ
6.2.6	Verifica dell'attivazione degli allarmi IDS in atto. Nota: Procedure per la verifica dell'attivazione degli allarmi al di fuori dell'orario di lavoro.	Ⓐ	Ⓑ	Ⓒ
6.2.7	Allarme IDS trasmesso tramite linea fissa o wireless e/o guasto della modalità di comunicazione.	Ⓐ	Ⓑ	
6.2.8	Sistema di comunicazione di backup attivo sul dispositivo IDS e/o in caso di guasto della linea.	Ⓐ	Ⓑ	

6.3 Sistema di controllo automatico degli accessi (AACS)

N. Req	Requisiti / Controlli	Livello Applicabile		
6.3.1	Sono disponibili i dati relativi alle transazioni AACS degli ultimi 90 giorni. I dati sono archiviati in modo sicuro e sottoposti a backup.	Ⓐ	Ⓑ	
6.3.2	Procedura per garantire che l'accesso ad AACS sia limitato a persone autorizzate o amministratori di sistema. I privilegi di accesso devono essere aggiornati tempestivamente quando una persona lascia l'organizzazione o cambia ruolo e non necessita più dell'accesso.	Ⓐ	Ⓑ	
6.3.3	I report del sistema di controllo degli accessi vengono esaminati almeno trimestralmente per identificare irregolarità o abusi (ad esempio, tentativi multipli non riusciti, letture errate (ad esempio, carta disattivata), prove di condivisione della carta per consentire accessi non autorizzati, ecc.). Procedura in atto.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

6.4 Videosorveglianza/VSS

N. Req	Requisiti / Controlli	Livello Applicabile		
6.4.1	Registrazione digitale delle immagini provenienti da telecamere a circuito chiuso/sistemi di videosorveglianza.	Ⓐ	Ⓑ	Ⓒ
6.4.2	La velocità di registrazione per i sistemi CCTV/VSS è impostata a un minimo di 8 fotogrammi al secondo (fps) per telecamera.	Ⓐ	Ⓑ	Ⓒ
6.4.3	La funzionalità di registrazione digitale viene verificata quotidianamente nei giorni lavorativi secondo procedura. I registri sono disponibili.	Ⓐ	Ⓑ	Ⓒ
6.4.4	Le registrazioni CCTV/VSS vengono conservate per un minimo di 30 giorni, ove consentito dalla legge locale. Il fornitore di servizi locali/richiedente deve fornire la prova di eventuali leggi locali che vietano l'uso di sistemi CCTV e/o limitano la conservazione dei dati video a meno di 30 giorni.	Ⓐ	Ⓑ	Ⓒ
6.4.5	L'accesso al sistema CCTV/VSS, compresi hardware, software e archiviazione dati/video, è strettamente controllato. Questa stanza deve essere chiusa a chiave se il sistema di archiviazione CCTV/VSS è presente in loco e dotato di controlli di accesso.	Ⓐ	Ⓑ	Ⓒ
6.4.6	Le immagini dei sistemi di videosorveglianza/televisione, per motivi di sicurezza, sono visualizzate solo dal personale autorizzato.		Ⓑ	Ⓒ
6.4.7	Sono in vigore procedure che definiscono la politica di protezione dei dati relativi ai sistemi di videosorveglianza/videosorveglianza (CCTV/VSS) in merito all'utilizzo di immagini in tempo reale e archiviate, in conformità con la legislazione locale.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

6.5 Illuminazione esterna e interna

N. Req	Requisiti / Controlli	Livello Applicabile		
6.5.1	I livelli di illuminazione esterna e interna sono sufficienti a supportare le immagini CCTV/VSS che consentono la registrazione di immagini di qualità investigativa e probatoria.	Ⓐ	Ⓑ	
6.5.2	I livelli di illuminazione esterna e interna sono sufficienti a riconoscere chiaramente tutti i veicoli e le persone.	Ⓐ		

S7. Formazione e procedure

7.1 Procedure di escalation

N. Req	Requisiti / Controlli	Livello applicabile		
7.1.1	Procedure locali in vigore per la gestione dei beni dell'Acquirente, incluso il processo per la segnalazione tempestiva di beni smarriti, mancanti o rubati. Gli incidenti devono essere segnalati dal LSP/Richiedente all'Acquirente entro 24 ore. I furti evidenti vengono segnalati immediatamente. La procedura viene seguita in modo coerente.	Ⓐ	Ⓑ	Ⓒ
7.1.2	Contatti di emergenza per Acquirenti/Clienti e fornitori di servizi di sicurezza/responsabili della gestione delle strutture per incidenti di sicurezza, elencati e disponibili. L'elenco viene aggiornato ogni 6 mesi e include i contatti di emergenza delle forze dell'ordine.	Ⓐ	Ⓑ	Ⓒ

7.2 Impegno della direzione

N. Req	Requisiti/Controlli	Livello applicabile		
7.2.1	La direzione deve sviluppare, comunicare e mantenere una politica di sicurezza per garantire che tutte le persone interessate (ovvero dipendenti e collaboratori esterni) siano chiaramente consapevoli delle aspettative di sicurezza del fornitore.	Ⓐ	Ⓑ	Ⓒ

7.3 Formazione

N. Req	Requisiti/Controlli	Livello applicabile		
7.3.1	Formazione sulla sicurezza e sulla consapevolezza delle minacce da fornire a tutti i membri della forza lavoro nei primi 60 giorni di impiego e successivamente ogni 2 anni.	Ⓐ	Ⓑ	Ⓒ
7.3.2	Formazione sulla consapevolezza della sicurezza delle informazioni incentrata sulla protezione dei dati di spedizione elettronici e fisici dell'Acquirente, fornita al personale che ha accesso alle informazioni dell'Acquirente e successivamente almeno ogni 2 anni, o secondo quanto previsto dalla legislazione locale qualora sia definito un periodo di aggiornamento più breve.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

7.4 Accesso ai beni degli Acquirenti/Clienti

N. Req	Requisiti/Controlli	Livello applicabile		
7.4.1	Procedure in atto per proteggere i beni degli Acquirenti/Clienti (ad es. il carico) da accessi non autorizzati da parte di dipendenti, visitatori, ecc.	Ⓐ	Ⓑ	Ⓒ

7.5 Controllo delle informazioni

N. Req	Requisiti/Controlli	Livello applicabile		
7.5.1	L'accesso ai documenti di spedizione e alle informazioni sui beni degli Acquirenti/Clienti è controllato in base al principio della "necessità di sapere". Deve essere predisposta una procedura per garantire la protezione delle informazioni dell'Acquirente.	Ⓐ	Ⓑ	Ⓒ
7.5.2	L'accesso ai documenti di spedizione e alle informazioni sui beni degli Acquirenti/Clienti è monitorato e registrato. Sono in essere processi e relativa documentazione.	Ⓐ	Ⓑ	Ⓒ
7.5.3	I documenti di spedizione e qualsiasi altro documento, comprese le informazioni sui beni degli Acquirenti/Clienti, saranno custoditi fino alla distruzione.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

7.6 Segnalazione di incidenti di sicurezza

N. Req	Requisiti/Controlli	Livello applicabile		
7.6.1	È attivo un sistema di segnalazione e monitoraggio degli incidenti di sicurezza, utilizzato per implementare misure proattive.	Ⓐ	Ⓑ	

7.7 Programmi di manutenzione

N. Req	Requisiti/Controlli	Livello applicabile		
7.7.1	Sono in atto programmi di manutenzione per tutti gli impianti/sistemi di sicurezza tecnici (fisici) al fine di garantirne la funzionalità in ogni momento (ad esempio, TVCC/VSS, controlli di accesso, rilevamento intrusioni e illuminazione).	Ⓐ	Ⓑ	Ⓒ

N. Req	Requisiti/Controlli	Livello applicabile		
7.7.2	La manutenzione preventiva viene effettuata una volta all'anno, o secondo le specifiche del produttore.	Ⓐ	Ⓑ	Ⓒ
7.7.3	Verifiche di funzionalità di tutti i sistemi una volta alla settimana e documentazione dei risultati, a meno che il guasto del sistema non venga segnalato o allarmizzato immediatamente/automaticamente.	Ⓐ	Ⓑ	
7.7.4	L'ordine di riparazione deve essere emesso entro 48 ore dalla scoperta del guasto. Per le riparazioni che si prevede richiedano più di 24 ore, è necessario implementare soluzioni alternative.	Ⓐ	Ⓑ	

7.8 Orientamento per gli appaltatori

N. Req	Requisiti/Controlli	Livello applicabile		
7.8.1	LSP/Richiedente deve garantire che tutti i subappaltatori/fornitori siano a conoscenza dei programmi di sicurezza pertinenti di LSP/Richiedente e li rispettino.	Ⓐ	Ⓑ	Ⓒ

7.9 Spedizione e ricezione dei documenti

N. Req	Requisiti/Controlli	Livello possibile		
7.9.1	I documenti di spedizione e ricezione devono essere leggibili, completi e accurati (ad esempio, ora, data, firme, autista, personale addetto alla spedizione e alla ricezione, dettagli e quantità della spedizione, ecc.). I nomi dell'autista e del mittente devono essere sempre chiaramente leggibili.	Ⓐ	Ⓑ	Ⓒ
7.9.2	LSP/ Il richiedente deve conservare la documentazione relativa a tutti i ritiri e le prove di consegna per un periodo non inferiore a due anni e renderla disponibile, se necessario, per le indagini sulle perdite.	Ⓐ	Ⓑ	Ⓒ
7.9.3	La prova di consegna deve essere fornita in conformità con l'accordo scritto tra il Cliente e l'LSP/Richiedente, laddove il Cliente richieda che la destinazione notifichi l'origine entro i tempi concordati di ricezione della spedizione, riconciliando i dettagli della spedizione di pre-avviso.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

7.10 Processo di pre-allerta in atto

N. Req	Requisiti/Controlli	Livello possibile		
7.10.1	Laddove richiesto dal Cliente, è in vigore una procedura di pre-avviso applicata alle spedizioni in entrata e/o in uscita. I dettagli del pre-avviso devono essere concordati tra il Cliente e il Fornitore di servizi logistici/Richiedente. I dettagli suggeriti includono l'orario di partenza, l'orario di arrivo previsto, la società di autotrasporto, il nome dell'autista, i dettagli della targa, le informazioni sulla spedizione (numero di colli, peso, numero della polizza di carico, ecc.) e i numeri dei sigilli del rimorchio.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S8. Integrità della forza lavoro

8.1 Screening/Verifica/Controllo dei precedenti (nei limiti consentiti dalla legge locale)

N. Req	Requisiti/Controlli	Livello possibile		
8.1.1	Il fornitore di servizi locali (LSP)/richiedente deve disporre di una procedura di screening/verifica/controllo dei precedenti che includa, come minimo, la verifica degli ultimi 5 anni di impiego e dei precedenti penali. Lo screening/la verifica si applica a tutti i candidati, inclusi dipendenti e collaboratori esterni. Il fornitore di servizi locali (LSP)/richiedente dovrà inoltre aver concordato contrattualmente l'applicazione di una procedura equivalente presso le aziende appaltatrici che forniscono lavoratori TAS.	Ⓐ	Ⓑ	Ⓒ
8.1.2	LSP/Il richiedente stipulerà accordi affinché l'agenzia e/o il subappaltatore che fornisce i lavoratori TAS forniscano le informazioni necessarie per lo screening/la verifica/il controllo dei precedenti, oppure effettuerà tali verifiche autonomamente. Lo screening deve includere la verifica dei precedenti penali e la verifica dell'impiego.	Ⓐ	Ⓑ	Ⓒ
8.1.3	Procedura per la gestione delle false dichiarazioni dei candidati/dipendenti prima e dopo l'assunzione.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

8.2 Cessazione o riassunzione della forza lavoro

Nota: la cessazione del rapporto di lavoro comprende sia le separazioni volontarie che quelle involontarie, ovvero i dipendenti licenziati o che si dimettono.

N. Req	Requisiti/Controlli	Livello possibile		
8.2.1	Recuperare i beni materiali dei dipendenti licenziati, inclusi badge aziendali, tessere di accesso, chiavi, attrezzature, risorse IT e informazioni sensibili. È richiesta una procedura documentata.	Ⓐ	Ⓑ	Ⓒ
8.2.2	Protezione dei dati dell'acquirente: interrompere l'accesso del personale cessato ai sistemi fisici o elettronici, compresi quelli contenenti i dati dell'acquirente. È richiesta una procedura documentata.	Ⓐ	Ⓑ	Ⓒ
8.2.3	È disponibile una checklist per la verifica dei dipendenti da utilizzare nelle fasi di onboarding e offboarding.	Ⓐ	Ⓑ	Ⓒ

N. Req	Requisiti/Controlli	Livello possibile		
8.2.4	Riassunzione: sono in vigore procedure per impedire al fornitore di servizi di lavoro/candidato di riassumere personale qualora i criteri di rifiuto/licenziamento siano ancora validi. Nota: i dati vengono esaminati prima della riassunzione (ad esempio, il background del personale precedentemente licenziato o dei candidati respinti (a cui è stato precedentemente negato un impiego)).	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S9. Requisiti della funzione centrale (applicabili solo alla certificazione multisito)

9.1 Generale

N. Req	Requisiti/Controlli	Livello possibile		
9.1.1	È prevista una funzione centrale per la gestione del sistema di gestione della sicurezza per tutti i siti, come definito nell'ambito della certificazione multisito.	Ⓐ	Ⓑ	Ⓒ
9.1.2	Tutti i siti devono avere un rapporto legale o contrattuale con la funzione centrale. Questo requisito non si estende ai siti dei subappaltatori inclusi nell'ambito di certificazione, come previsto dalla clausola 4.2.2 del CFD.	Ⓐ	Ⓑ	Ⓒ
9.1.3	Viene istituito un unico sistema di gestione della sicurezza per garantire che tutti i siti all'interno del sistema soddisfino i requisiti dello standard di sicurezza TAPA applicabile.	Ⓐ	Ⓑ	Ⓒ
9.1.4	La funzione centrale e il relativo sistema di gestione saranno soggetti a verifiche interne per garantire la continua conformità agli standard TAPA.	Ⓐ	Ⓑ	Ⓒ
9.1.5	La funzione centrale deve effettuare audit presso i siti inclusi nell'ambito di applicazione per garantire che ciascun sito soddisfi i requisiti TAPA FSR applicabili. Gli audit devono essere eseguiti utilizzando gli appositi modelli di audit TAPA. Tutti gli audit annuali individuali dei siti devono essere completati e resi disponibili all'auditor prima del processo di certificazione.	Ⓐ	Ⓑ	Ⓒ
9.1.6	La funzione centrale avrà l'autorità e il diritto di richiedere a tutte le sedi di conformarsi agli standard di sicurezza TAPA e di attuare le azioni correttive e preventive necessarie. Nota: Ove applicabile, ciò deve essere specificato nell'accordo formale tra la funzione centrale e le sedi.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

9.2 Politiche e procedure

N. Req	Requisiti/Controlli	Livello possibile		
9.2.1	La funzione centrale deve mantenere politiche e procedure documentate per i propri sistemi di gestione della sicurezza, applicabili a tutte le sue sedi.	Ⓐ	Ⓑ	Ⓒ

N. Req	Requisiti/Controlli	Livello possibile		
9.2.2	La funzione centrale deve garantire che le politiche e le procedure siano aggiornate, comunicate, implementate e attuate da tutte le sedi secondo necessità.	Ⓐ	Ⓑ	Ⓒ
9.2.3	Le politiche e le procedure devono essere mantenute e rese facilmente accessibili a tutte le sedi, secondo necessità.	Ⓐ	Ⓑ	Ⓒ

9.3 Rapporto di autovalutazione redatto per tutte le sedi

N. Req	Requisiti/Controlli	Livello possibile		
9.3.1	La funzione centrale imporrà a tutti i siti di effettuare un'autovalutazione e tutti i rapporti di autovalutazione dovranno essere inviati alla funzione centrale per la registrazione e la revisione. I registri dovranno essere conservati per almeno due (2) anni.	Ⓐ	Ⓑ	Ⓒ
9.3.2	La funzione centrale deve garantire che tutte le SCAR (Sicure Correzioni di Sicurezza) derivanti dall'autovalutazione e dagli audit vengano chiuse in modo appropriato per migliorare i propri sistemi di gestione della sicurezza.	Ⓐ	Ⓑ	Ⓒ
9.3.3	Tutti i siti devono inviare aggiornamenti sullo stato di avanzamento e rapporti su tutti gli SCAR in sospeso alla funzione centrale. La funzione centrale segnalerà alla direzione del LSP/richiedente se gli SCAR non vengono completati entro le date di scadenza. I registri devono essere conservati per almeno due (2) anni.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

9.4 Registri delle ispezioni, registri (registri visitatori/autista), ispezioni a 7 punti

N. Req	Requisiti/Controlli	Livello possibile		
9.4.1	La funzione centrale deve disporre di procedure per garantire che tutti i siti mantengano registri delle ispezioni, registri dei visitatori, registri degli autisti e ispezioni a 7 punti, ecc.	Ⓐ	Ⓑ	Ⓒ

9.5 Valutazione dei rischi di tutti i siti

N. Req	Requisiti/Controlli	Livello possibile		
9.5.1	La funzione centrale deve disporre di procedure per garantire che vengano effettuate valutazioni e gestioni del rischio appropriate su tutti i siti e che i relativi registri siano conservati per almeno due (2) anni.	Ⓐ	Ⓑ	Ⓒ

9.6 Schema di videosorveglianza/sistema di videosorveglianza e allarme del sito

N. Req	Requisiti/Controlli	Livello possibile		
9.6.1	La funzione centrale deve disporre di procedure che garantiscano che tutte le sedi esaminino e mantengano la documentazione relativa a tutti i sistemi di sicurezza fisica, come la videosorveglianza e la configurazione degli allarmi.	Ⓐ	Ⓑ	Ⓒ

9.7 Registri di allarme e controllo accessi

N. Req	Requisiti/Controlli	Livello possibile		
9.7.1	La funzione centrale deve disporre di procedure che garantiscano la manutenzione e il collaudo di tutti i sistemi di allarme e controllo accessi al fine di assicurarne l'efficacia operativa..	Ⓐ	Ⓑ	Ⓒ
9.7.2	La funzione centrale deve disporre di procedure affinché tutti i siti mantengano la documentazione relativa a tutti i test e agli incidenti di rilevamento delle intrusioni e controllo degli accessi..	Ⓐ	Ⓑ	Ⓒ

9.8 Registrazione dei dati

N. Req.	Requisiti/Controlli	Livello possibile		
9.8.1	La funzione centrale deve disporre di procedure per garantire che tutti i siti mantengano i registri della formazione in materia di sicurezza di tutto il personale del sito.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

N. Req.	Requisiti/Controlli	Livello possibile		
9.8.2	La funzione centrale deve disporre di procedure per garantire che tutti i siti mantengano i registri della formazione in materia di sicurezza di tutto il personale del sito. I registri devono essere conservati per almeno due (2) anni.	Ⓐ	Ⓑ	Ⓒ

9.9 Registri di screening/verifica

N. Req.	Requisiti/Controlli	Livello possibile		
9.9.1	La funzione centrale deve disporre di procedure che garantiscano che tutte le sedi eseguano a intervalli regolari la revisione e la verifica dei documenti al fine di assicurare l'integrità e l'efficacia dei sistemi di gestione della sicurezza.	Ⓐ	Ⓑ	Ⓒ
9.9.2	La funzione centrale deve disporre di procedure per garantire che i registri delle revisioni, compresi i relativi risultati e le azioni correttive/preventive 9.1.6, siano conservati. I registri saranno conservati per almeno due (2) anni.	Ⓐ	Ⓑ	Ⓒ

9.10 Revisione della direzione per valutare le auto-verifiche; SCAR rilevate; eventuali perdite, furti; valutazioni dei rischi

N. Req.	Requisiti/Controlli	Livello possibile		
9.10.1	La funzione centrale deve, come minimo, condurre revisioni gestionali periodiche per garantire la conformità, l'efficacia e il miglioramento dei propri sistemi di gestione della sicurezza.	Ⓐ	Ⓑ	Ⓒ
9.10.2	Le revisioni della direzione dovranno riguardare, tra l'altro, l'efficacia degli audit interni, la chiusura delle segnalazioni di eventi avversi gravi (SCAR), le valutazioni dei rischi, gli incidenti e le azioni di miglioramento.	Ⓐ	Ⓑ	Ⓒ
9.10.3	La funzione centrale deve conservare i registri di tutte le revisioni gestionali per almeno due (2) anni.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

8.0 Minacce alla sicurezza informatica e IT: opzione avanzata

Il TAPA FSR include miglioramenti opzionali per la sicurezza informatica e le minacce IT, considerati un livello di protezione superiore e utilizzabili in aggiunta ai moduli standard. Questo miglioramento opzionale è pensato per essere selezionato dal LSP/Richiedente e/o dal suo Acquirente come requisito aggiuntivo per le proprie esigenze di sicurezza operativa. Quando questo miglioramento opzionale viene selezionato nella valutazione di pre-certificazione per essere incluso nell'audit di certificazione, tutti i requisiti diventano obbligatori.
L'opzione avanzata prevista dal TAPA FSR fornisce un livello base di controlli di sicurezza informatica e IT a livello di sito. I membri sono fortemente incoraggiati ad adottare gli Standard di sicurezza informatica (CSS) per ottenere un framework di sicurezza informatica più completo e robusto.

E8. Requisiti obbligatori

N. Req	Requisiti/Controlli
E8.1.1	Il fornitore di servizi logistici (LSP)/richiedente deve disporre di politiche di sicurezza per l'IT e le minacce informatiche. Le politiche possono essere separate o contenute in un unico documento.Le politiche devono illustrare: 1. Le azioni intraprese dal fornitore di servizi logistici (LSP)/richiedente per identificare e rispondere alle minacce. 2. Le politiche e le procedure in atto per proteggere, rilevare, testare e rispondere agli eventi di sicurezza. 3. I metodi per il ripristino dei sistemi IT e/o dei dati. 4. Il protocollo di comunicazione con acquirenti/clienti per mitigare l'impatto sulla catena di fornitura entro 24 ore dalla conoscenza dell'incidente. 5. Le modalità di revisione annuale e aggiornamento delle politiche, se necessario.
E8.1.2	Il fornitore di servizi di sicurezza informatica/richiedente deve erogare una formazione sulla consapevolezza della sicurezza informatica a tutti i dipendenti. Tale formazione deve: 1. Illustrare i ruoli e le responsabilità degli utenti di computer in materia di sicurezza e i relativi vantaggi 2. Prevedere un sistema che garantisca la conservazione dei registri delle persone che hanno ricevuto la formazione per un periodo minimo di 2 anni.

TAPA Copyright © Do Not Copy

E8.1.3	Il fornitore di servizi locali (LSP)/richiedente deve disporre di una politica scritta per garantire l'implementazione di misure di sicurezza informatica con subappaltatori e/o fornitori, che assicuri: 1. Che i requisiti di sicurezza informatica del fornitore di servizi locali (LSP)/richiedente siano comunicati a subappaltatori e/o fornitori e integrati negli accordi. 2. Che, qualora subappaltatori e/o fornitori non riconoscano o si rifiutino di adottare i requisiti di sicurezza informatica del fornitore di servizi locali (LSP)/richiedente, siano documentate e implementate misure che mitighino i rischi per i requisiti di sicurezza informatica del fornitore di servizi locali (LSP)/richiedente e per i suoi clienti.
E8.1.4	Il fornitore di servizi locali/richiedente deve disporre di un piano di mitigazione delle interruzioni di corrente (ad esempio, alimentazione elettrica alternativa o generatore di riserva) che garantisca l'alimentazione dei sistemi IT critici (identificati nella valutazione locale dei rischi) per un minimo di 48 ore.
E8.1.5	I sistemi informativi del fornitore di servizi linguistici (LSP) e del richiedente devono disporre di software antivirus e antimalware con licenza installato. Il software antivirus e antimalware deve contenere gli aggiornamenti più recenti.
E8.1.6	LSP/ Il richiedente deve disporre di un adeguato piano di ripristino d'emergenza IT (DRP) per il recupero da attacchi ai sistemi compromessi, inclusi, a titolo esemplificativo ma non esaustivo, tutti i necessari accordi di backup e ripristino dei dati e dei software.
E8.1.7	I sistemi informativi del fornitore di servizi linguistici (LSP) e del richiedente devono essere sottoposti a backup. Tali backup devono essere testati regolarmente e i dati di backup devono essere crittografati e trasferiti in una posizione secondaria esterna.
E8.1.8	LSP/Il richiedente deve implementare una politica per tutti gli account utente al fine di gestire e controllare l'accesso ai sistemi informativi utilizzando identificativi individuali univoci e password complesse. Le procedure in atto devono garantire: 1. Un programma di verifica della conformità delle password. 2. A ogni nuovo account deve essere assegnata una password iniziale univoca al momento della creazione. 3. Le password iniziali non possono contenere il nome dell'utente, il numero di identificazione o seguire in altro modo uno schema standard basato sulle informazioni dell'utente. 4. Le password saranno comunicate agli utenti in modo sicuro e solo dopo averne verificato l'identità. 5. Agli utenti deve essere richiesto di cambiare la password al primo accesso. 6. Le password devono essere cambiate almeno ogni 90 giorni.

TAPA Copyright © Do Not Copy

A titolo informativo: la traduzione dello Standard nella lingua nazionale messa a vostra disposizione ha lo scopo di agevolare la comprensione dei requisiti TAPA 2026. La traduzione dello Standard è stata predisposta e convalidata secondo scienza e coscienza e sulla base delle conoscenze e dei riferimenti necessari. Tuttavia, ai fini della verifica, la versione originale inglese dello Standard applicabile è e rimane l'unica versione ufficiale e vincolante.

Informazioni su pubblicazione e copyright
Questo documento è pubblicato dalla Transported Asset Protection Association (TAPA).
© TAPA 2026–2029
Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, archiviata in un sistema di recupero dati, trasmessa in qualsiasi forma o con qualsiasi mezzo — elettronico, meccanico, fotocopia, registrazione o altro — senza la previa autorizzazione scritta di TAPA, salvo quanto consentito dalla normativa vigente in materia di copyright.
L'avviso di copyright visualizzato in questo documento indica l'anno dell'ultima pubblicazione.

Cronologia delle pubblicazioni
Prima pubblicazione: settembre 2026
Edizione attuale pubblicata a: settembre 2026
Questa specifica pubblicamente disponibile (PAS) entra in vigore il 15 settembre 2026.

Stato del documento
Questo documento rappresenta la revisione 2026 dei Requisiti di Sicurezza delle Strutture (FSR) di TAPA e stabilisce i requisiti di base per la sicurezza delle strutture nell'ambito del quadro di certificazione TAPA.

Il documento rimane valido fino a quando non viene sostituito, rivisto o ritirato da TAPA.
TAPA può pubblicare in futuro revisioni, aggiornamenti o modifiche per riflettere l'evoluzione delle minacce alla sicurezza, le pratiche del settore e gli sviluppi tecnologici.

Utilizzo del presente documento
La conformità a questa specifica può essere utilizzata come parte del processo di certificazione TAPA per le strutture che gestiscono merci di alto valore e sensibili ai furti.
Le organizzazioni che implementano questa specifica sono responsabili di garantire che vengano soddisfatti tutti i requisiti legali, normativi e operativi applicabili, oltre a quelli descritti nel presente documento.

TAPA Copyright © Do Not Copy