



Payment Card Industry (PCI) Data Security Standard

Requisiti e procedure di valutazione della sicurezza

Versione 2.0

Ottobre 2010

Modifiche del documento

Data	Versione	Descrizione	Pagine
Ottobre 2008	1.2	<i>Introdurre PCI DSS v1.2 come “Requisiti PCI DSS e procedure di valutazione della sicurezza” eliminando la ridondanza tra documenti e apportare modifiche generali e specifiche da Procedure di audit della sicurezza PCI DSS v1.1. Per informazioni complete, vedere Riepilogo delle modifiche di PCI DSS dalla versione 1.1 alla 1.2.</i>	
luglio 2009	1.2.1	<i>Aggiungere la frase erroneamente eliminata tra PCI DSS v1.1 e v1.2.</i>	5
		<i>Correggere l'errore di ortografia nelle procedure di test 6.3.7.a e 6.3.7.b.</i>	32
		<i>Rimuovere il contrassegno disattivato per le colonne “presente” e “non presente” nella procedura di verifica 6.5.b.</i>	33
		<i>Per Foglio di lavoro Controlli compensativi - Esempio, correggere la stringa all'inizio della pagina in “Utilizzare questo foglio di lavoro per definire i controlli compensativi per qualsiasi requisito contrassegnato come “presente” attraverso i controlli compensativi.”</i>	64
Ottobre 2010	2.0	<i>Aggiornare ed implementare le modifiche da v1.2.1. Per informazioni dettagliate, fare riferimento a “PCI DSS - Riepilogo delle modifiche dalla 1.2.1 alla 2.0 PCI DSS”.</i>	

Sommario

Modifiche del documento	2
Introduzione e panoramica di PCI Data Security Standard	5
Informazioni sull'applicabilità degli standard PCI DSS	7
Relazione tra PCI DSS e PA-DSS	9
Ambito della valutazione per la conformità ai requisiti PCI DSS	10
<i>Segmentazione di rete</i>	<i>10</i>
<i>Wireless</i>	<i>11</i>
<i>Terze parti/Outsourcing</i>	<i>11</i>
<i>Campionamento delle strutture aziendali e dei componenti di sistema.....</i>	<i>12</i>
<i>Controlli compensativi.....</i>	<i>13</i>
Istruzioni e contenuto per il rapporto sulla conformità.....	14
<i>Contenuto e formato del rapporto</i>	<i>14</i>
<i>Riconvalida dei problemi in attesa di soluzione.....</i>	<i>17</i>
<i>Conformità agli standard PCI DSS – Operazioni</i>	<i>18</i>
Requisiti PCI DSS e procedure di valutazione della sicurezza dettagliate.....	19
Sviluppo e gestione di una rete sicura.....	20
<i>Requisito 1: Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta</i>	<i>20</i>
<i>Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione ...</i>	<i>24</i>
Protezione dei dati di titolari di carta	28
<i>Requisito 3: Proteggere i dati di titolari di carta memorizzati</i>	<i>28</i>
<i>Requisito 4: Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche.....</i>	<i>35</i>
Utilizzare un programma per la gestione delle vulnerabilità	37
<i>Requisito 5: Utilizzare e aggiornare regolarmente il software o i programmi antivirus</i>	<i>37</i>
<i>Requisito 6: Sviluppare e gestire sistemi e applicazioni protette</i>	<i>38</i>
Implementazione di rigide misure di controllo dell'accesso	44
<i>Requisito 7: Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario.....</i>	<i>44</i>
<i>Requisito 8: Assegnare un ID univoco a chiunque abbia accesso a un computer</i>	<i>46</i>
<i>Requisito 9: Limitare l'accesso fisico ai dati dei titolari di carta</i>	<i>52</i>
Monitoraggio e test delle reti regolari	57
<i>Requisito 10: Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta</i>	<i>57</i>

<i>Requisito 11: Eseguire regolarmente test di sistemi e processi di protezione</i>	61
Gestire una politica di sicurezza delle informazioni	66
<i>Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale</i>	66
Appendice A: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso	73
Appendice B: Controlli compensativi	75
Appendice C: Foglio di lavoro - Controlli compensativi	77
Foglio di lavoro Controlli compensativi - Esempio	78
Appendice D: Segmentazione e campionamento delle strutture aziendali e dei componenti di sistema	79

Introduzione e panoramica di PCI Data Security Standard

PCI (Payment Card Industry) DSS (Data Security Standard) è stato sviluppato per favorire e migliorare la protezione dei dati di titolari di carta nonché semplificare l'implementazione di misure di sicurezza dei dati coerenti a livello globale. Gli standard PCI DSS mettono a disposizione una base di requisiti tecnici ed operativi volti a proteggere i dati dei titolari di carta. Gli standard PCI DSS si applicano a tutte le entità coinvolte nell'elaborazione di carte di pagamento, con l'inclusione di esercenti, elaboratori, acquirenti, emittenti e provider di servizi, nonché di tutte le altre entità che si occupano di memorizzare, elaborare o trasmettere dati dei titolari di carta. Gli standard PCI DSS comprendono una serie minima di requisiti per proteggere i dati dei titolari di carta e può essere migliorato attraverso pratiche e controlli aggiuntivi per ridurre ulteriormente i rischi. Di seguito, è riportata una panoramica di alto livello dei 12 requisiti PCI DSS.

PCI Data Security Standard – Panoramica di alto livello

Sviluppo e gestione di una rete sicura	<ol style="list-style-type: none">1. Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta2. Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione
Protezione dei dati di titolari di carta	<ol style="list-style-type: none">3. Proteggere i dati di titolari di carta memorizzati4. Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche
Utilizzo di un programma per la gestione delle vulnerabilità	<ol style="list-style-type: none">5. Utilizzare e aggiornare regolarmente il software o i programmi antivirus6. Sviluppare e gestire sistemi e applicazioni protette
Implementazione di rigide misure di controllo dell'accesso	<ol style="list-style-type: none">7. Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario8. Assegnare un ID univoco a chiunque abbia accesso a un computer9. Limitare l'accesso fisico ai dati dei titolari di carta
Monitoraggio e test delle reti regolari	<ol style="list-style-type: none">10. Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta11. Eseguire regolarmente test di sistemi e processi di protezione
Gestione di una politica di sicurezza delle informazioni	<ol style="list-style-type: none">12. Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale

Questo documento, *Requisiti PCI DSS e procedure di valutazione della sicurezza*, abbina i 12 requisiti PCI DSS alle relative procedure di test in uno strumento di valutazione della sicurezza. È destinato all'utilizzo durante la valutazione della conformità agli standard PCI DSS come parte di un processo di convalida di un'entità. Nelle seguenti sezioni vengono fornite delle linee guida dettagliate nonché le migliori pratiche per assistere le entità nella preparazione, realizzazione e presentazione dei risultati di una valutazione PCI DSS. Le procedure di test e i Requisiti PCI DSS iniziano a **pagina 19**.

Sul sito web di PCI Security Standards Council (PCI SSC)(www.pcisecuritystandards.org) sono disponibili ulteriori risorse, compresi:

- Attestati di conformità
- *Navigazione in PCI DSS: Comprensione dello scopo dei requisiti*
- *PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi*
- FAQ
- Supplementi informativi e linee guida

Nota: I Supplementi informativi completano gli standard PCI DSS e individuano ulteriori considerazioni e raccomandazioni per soddisfare i requisiti PCI DSS, senza però modificare, eliminare o sostituirsi agli standard PCI DSS o ad alcuno dei suoi requisiti.

Per ulteriori informazioni, fare riferimento a www.pcisecuritystandards.org.

Informazioni sull'applicabilità degli standard PCI DSS

Gli standard PCI DSS si applicano ogni qualvolta dei dati vengono memorizzati, elaborati o trasmessi. *I dati degli account* sono costituiti da *Dati di titolari di carta* più *Dati sensibili di autenticazione*, come segue.

<i>I dati dei titolari di carta comprendono:</i>	<i>I dati sensibili di autenticazione comprendono:</i>
<ul style="list-style-type: none">▪ PAN (Primary Account Number)▪ Nome titolare di carta▪ Data di scadenza▪ Codice di servizio	<ul style="list-style-type: none">▪ Dati completi della striscia magnetica o equivalenti sul chip▪ CAV2/CVC2/CVV2/CID▪ PIN/Blocchi PIN

Il PAN costituisce il fattore determinante nell'applicabilità dei requisiti PCI DSS. Gli standard PCI DSS sono applicabili se viene memorizzato, elaborato o trasmesso un PAN (Primary Account Number, numero account primario). Se il PAN non viene memorizzato, elaborato o trasmesso, i requisiti PCI DSS non sono validi.

Se il nome del titolare di carta, il codice di servizio e/o la data di scadenza sono memorizzati, elaborati o trasmessi con il PAN, oppure sono presenti in altro modo nell'ambiente di dati di titolari di carta, tali dati devono essere protetti in conformità a tutti i requisiti PCI DSS **ad eccezione dei** Requisiti 3.3 e 3.4 che si applicano solo al PAN.

Il PCI DSS costituisce una serie minima di obiettivi di controllo che possono essere migliorati da leggi e regolamenti a livello locale, regionale e di settore. Inoltre, i requisiti legislativi o regolamentari possono prevedere una protezione specifica di informazioni di identificazione personale o di altri elementi di dati (ad esempio, il nome del titolare di carta), oppure definire le pratiche di divulgazione di un'entità connesse alle informazioni sui consumatori. Esempi comprendono la legislazione correlata alla protezione dei dati dei consumatori, alla privacy, al furto di identità o alla sicurezza dei dati. Gli standard PCI DSS non sostituiscono le leggi regionali o locali, i regolamenti governativi o altri requisiti legali.

La tabella riportata di seguito illustra gli elementi dei dati dei titolari di carta e dei dati sensibili di autenticazione utilizzati più frequentemente, indica se la memorizzazione di tali dati è consentita o meno e se ogni elemento dei dati deve essere protetto. Questa tabella non è completa, ma illustra i diversi tipi di requisiti che si applicano a ciascun elemento di dati.

		Elemento di dati	Memorizzazione consentita	Rendere i dati di account memorizzati illeggibili in base al Requisito 3.4
Dati di account	Dati di titolari di carta	PAN (Primary Account Number)	Sì	Sì
		Nome titolare di carta	Sì	No
		Codice di servizio	Sì	No
		Data di scadenza	Sì	No
	Dati sensibili di autenticazione ¹	Dati completi della striscia magnetica ²	No	Impossibile memorizzare in base al Requisito 3.2
		CAV2/CVC2/CVV2/CID	No	Impossibile memorizzare in base al Requisito 3.2
		PIN/Blocco PIN	No	Impossibile memorizzare in base al Requisito 3.2

I Requisiti 3.3. e 3.4 PCI DSS si applicano solo al PAN. In caso di memorizzazione del PAN con altri elementi dei dati del titolare di carta, è solo il PAN che va reso illeggibile in conformità al Requisito 3.4 PCI DSS.

Gli standard PCI DSS **si applicano solo** in caso di memorizzazione, elaborazione e/o trasmissione dei PAN.

¹ I dati sensibili di autenticazione non devono essere memorizzati dopo l'autorizzazione (anche se cifrati).

² Dati su traccia completa dalla striscia magnetica, dati equivalenti in un chip o in altro luogo.

Relazione tra PCI DSS e PA-DSS

L'uso di un'applicazione conforme agli standard PA-DSS di per sé stessa non rende l'entità conforme agli standard PCI DSS, poiché l'applicazione in questione deve essere implementata in un ambiente conforme agli standard PCI DSS ed in conformità alla Guida per l'implementazione del programma PA-DSS messa a disposizione dal fornitore dell'applicazione di pagamento (in base al Requisito 13.1 PA-DSS).

I requisiti per gli standard PA-DSS derivano dagli *standard PCI DSS (Payment Card Industry Data Security Standard)* e dalle *Procedure di valutazione della sicurezza* (questo documento). Gli standard PA-DSS **Error! Hyperlink reference not valid.** descrivono in dettaglio gli elementi che un'applicazione di pagamento deve supportare per agevolare la conformità agli standard PCI DSS di un cliente.

Applicazioni di pagamento sicure, quando implementate in un ambiente conforme agli standard PCI DSS, riducono al minimo il rischio di violazioni della sicurezza che possono compromettere dati della striscia magnetica, valori e codici di verifica della carta (CAV2, CID, CVC2, CVV2), PIN e blocchi PIN e limitano i danni derivanti da tali violazioni.

Tra gli esempi di come le applicazioni di pagamento possono impedire di rispettare gli standard previsti:

- Memorizzazione di dati su striscia magnetica e/o dati equivalenti sul chip nella rete del cliente a seguito dell'autorizzazione;
- Applicazioni che, per un corretto funzionamento, richiedono ai clienti di disattivare altre funzioni richieste dagli standard PCI DSS, quali software antivirus o firewall;
- Uso di metodi non sicuri del fornitore per connettersi all'applicazione e fornire supporto al cliente.

Gli standard PA-DSS sono validi per i fornitori di software e altre persone che sviluppano applicazioni di pagamento che memorizzano, elaborano o trasmettono dati di titolari di carta nell'ambito del processo di autorizzazione o contabilizzazione delle transazioni, dove queste applicazioni di pagamento sono vendute, distribuite o concesse in licenza a terze parti.

Per l'applicabilità degli standard PA-DSS tener conto di quanto segue:

- Gli standard PA-DSS **si riferiscono** ad applicazioni di pagamento che solitamente sono vendute e installate come "prodotti standard" senza operazioni di personalizzazione dei fornitori software.
- Gli standard PA-DSS **NON** si riferiscono ad applicazioni di pagamento sviluppate da esercenti e provider di servizi se utilizzate solo in-house (non vendute, distribuite o concesse in licenza a terze parti), poiché le applicazioni di pagamento sviluppate in-house rientrano nel controllo della conformità agli standard PCI DSS dell'esercente o provider di servizi.

Per le linee guida dettagliate per verificare l'applicabilità degli standard PA-DSS ad una determinata applicazione di pagamento, fare riferimento a Requisiti PA-DSS e procedure di valutazione della sicurezza, disponibili all'indirizzo www.pcisecuritystandards.org.

Ambito della valutazione per la conformità ai requisiti PCI DSS

I requisiti di sicurezza PCI DSS si applicano a tutti i componenti di sistema. In ambito PCI DSS, per "componenti di sistema" si intende qualsiasi componente di rete, server o applicazione incluso o connesso all'ambiente dei dati dei titolari di carta. I "componenti di sistema" comprendono anche ogni componente di virtualizzazione come computer, switch/router, dispositivi, applicazioni/desktop virtuali e hypervisor. L'ambiente dei dati dei titolari di carta è composto da persone, processi e tecnologia che memorizzano, elaborano o trasmettono dati dei titolari di carta o dati sensibili di autenticazione. I componenti di rete includono, senza limitazioni, firewall, switch, router, punti di accesso wireless, dispositivi di rete e altri dispositivi di sicurezza. I tipi di server possono essere: Web, applicazioni, database, autenticazione, e-mail, proxy, NTP (Network Time Protocol) e DNS (Domain Name Server). Le applicazioni includono tutte le applicazioni acquistate e personalizzate, comprese applicazioni interne ed esterne (ad esempio, Internet).

Il primo passo di una valutazione PCI DSS consiste nello stabilire con precisione l'ambito della revisione. Con cadenza almeno annuale e prima della valutazione annuale, l'entità valutata dovrebbe confermare la precisione del proprio ambito PCI DSS individuando tutte le posizioni ed i flussi dei dati dei titolari di carta ed assicurando che rientrano nell'ambito PCI DSS. Per confermare la precisione e l'idoneità dell'ambito PCI DSS, eseguire quanto segue:

- L'entità valutata identifica e documenta l'esistenza di tutti i dati dei titolari di carta nel proprio ambiente, per verificare che non esista alcuna di questi dati al di fuori dell'ambiente dei dati dei titolari di carta attualmente definito.
- Una volta identificate e documentate tutte le posizioni dei dati dei titolari di carta, l'entità utilizza i risultati per verificare l'adeguatezza dell'ambito PCI DSS (ad esempio, i risultati possono essere un diagramma o un inventario delle posizioni dei dati dei titolari di carta).
- L'entità prende in considerazione ogni dato dei titolari di carta ritenuto compreso nell'ambito della valutazione PCI DSS e parte dell'ambiente dei dati dei titolari di carta a meno che tali dati non siano cancellati o migrati/consolidati nell'ambiente dei dati di carta attualmente definito.
- L'entità conserva la documentazione che mostra come l'ambito PCI DSS sia stato confermato e i risultati, per revisione del valutatore e/o riferimento durante l'attività di conferma dell'ambito PCI DSS annuale successiva.

Segmentazione di rete

Non costituisce un requisito PCI DSS la segmentazione di rete, o l'isolamento (segmentazione) dell'ambiente dei dati dei titolari di carta dal resto della rete dell'entità. Tuttavia, è un metodo fortemente consigliato che consente di ridurre:

- L'ambito della valutazione PCI DSS
- Il costo della valutazione PCI DSS
- Il costo e la difficoltà dell'implementazione e della gestione di controlli PCI DSS
- I rischi per un'organizzazione (ridotti grazie al consolidamento dei dati dei titolari di carta in un minor numero di posizioni controllate)

Senza un'adeguata segmentazione di rete (nota anche come "rete semplice"), l'intera rete è soggetta alla valutazione PCI DSS. È possibile eseguire la segmentazione di rete tramite una serie di mezzi logici o fisici, come firewall di rete interni adeguatamente configurati, router con elenchi di controllo dell'accesso avanzato o altre tecnologie che limitano l'accesso a un determinato segmento di una rete.

Per ridurre l'ambito dell'ambiente dei dati dei titolari di carta, è importante identificare preventivamente e comprendere chiaramente le esigenze e i processi aziendali correlati alla memorizzazione, elaborazione o trasmissione dei dati dei titolari di carta. La limitazione dei dati dei titolari di carta al minor numero di posizioni possibile tramite l'eliminazione dei dati non necessari e il consolidamento dei dati necessari, richiede la riprogettazione di alcune pratiche aziendali di vecchia data.

Documentando i flussi dei dati dei titolari di carta in un diagramma di flusso è possibile comprendere completamente tutti i flussi dei dati dei titolari di carta e garantire che la segmentazione di rete sia efficace in termini di isolamento dell'ambiente dei dati dei titolari di carta.

Se la segmentazione di rete è stata eseguita e viene utilizzata per ridurre l'ambito della valutazione PCI DSS, il valutatore deve verificare che la segmentazione sia adeguata per lo scopo previsto. A un elevato livello, una segmentazione di rete adeguata isola i sistemi che memorizzano, elaborano o trasmettono i dati di titolari di carta da quelli che non eseguono tali operazioni. Tuttavia, l'adeguatezza di una specifica segmentazione di rete è altamente variabile e dipende da una serie di fattori, tra cui la configurazione della rete, le tecnologie distribuite e altri controlli che possono essere implementati.

Appendice D: Segmentazione e campionamento delle strutture aziendali e dei componenti di sistema fornisce ulteriori informazioni sull'effetto della segmentazione della rete e del campionamento sull'ambito di una valutazione PCI DSS.

Wireless

Se viene utilizzata la tecnologia wireless per memorizzare, elaborare o trasmettere i dati di titolari di carta (ad esempio, le transazioni di punti di vendita e "line-busting") oppure se una LAN wireless è connessa all'ambiente dei dati di titolari di carta o a parte di esso (ad esempio, non separato chiaramente da un firewall), vengono applicati i requisiti PCI DSS e devono essere eseguite le procedure di test per gli ambienti wireless (ad esempio, i requisiti 1.2.3, 2.1.1 e 4.1.1). Prima di implementare la tecnologia wireless, un'entità deve valutare attentamente l'esigenza di tale tecnologia rispetto ai potenziali rischi. Si consiglia di utilizzare la tecnologia wireless solo per la trasmissione di dati non sensibili.

Terze parti/Outsourcing

Per i provider di servizi tenuti ad eseguire una valutazione annuale in sede, si deve effettuare la convalida della conformità su tutti i componenti di sistema nell'ambiente dei dati dei titolari di carta.

I provider di servizi o gli esercenti possono utilizzare un provider di terze parti per memorizzare, elaborare o trasmettere i dati di titolari di carta per proprio conto o gestire componenti quali router, firewall, database, sicurezza fisica e/o server. In questo caso, ciò potrebbe influire sulla sicurezza dell'ambiente dei dati dei titolari di carta.

Per le entità che si avvalgono del supporto di provider di terze parti per la memorizzazione, l'elaborazione o la trasmissione dei dati di titolari di carta, il ROC (rapporto di conformità) deve documentare il ruolo di ogni provider, identificando chiaramente i requisiti che si applicano all'entità valutata e quelli che si applicano al provider di servizi. I provider di servizi di terze parti possono convalidare la propria conformità ai requisiti PCI DSS nei due seguenti modi:

- 1) Possono eseguire la valutazione PCI DSS personalmente e fornire prova della propria conformità ai clienti; oppure
- 2) sottoponendo a revisione i propri servizi nell'ambito delle valutazioni PCI DSS di ciascuno dei loro clienti, se non possono eseguire la valutazione PCI DSS personalmente.

Per ulteriori informazioni, vedere il punto elenco che inizia con "Revisioni per i provider di servizi gestiti (MSP)" al Punto 3, "Dettagli sull'ambiente sottoposto a revisione" nella sezione "Istruzioni e contenuto per il rapporto sulla conformità" di seguito.

Inoltre, gli esercenti e i provider di servizi devono gestire e monitorare la conformità ai requisiti PCI DSS di tutti i provider di servizi di terze parti associati che dispongono dell'accesso ai dati dei titolari di carta. *Per dettagli, fare riferimento al Requisito 12.8 nel presente documento.*

Campionamento delle strutture aziendali e dei componenti di sistema

Il campionamento non costituisce un requisito PCI DSS. Tuttavia, in considerazione dell'ambito generale e della complessità dell'ambiente sottoposto a valutazione, il valutatore può scegliere, in modo indipendente, alcuni campioni rappresentativi delle strutture aziendali e dei componenti di sistema per valutare la conformità ai requisiti PCI DSS. Questi campioni devono prima essere definiti per le strutture aziendali e quindi per i componenti di sistema nell'ambito di ciascuna struttura aziendale selezionata. I campioni devono essere una selezione rappresentativa di tutti i tipi e le posizioni delle strutture aziendali nonché dei componenti di sistema nell'ambito delle strutture aziendali selezionate. I campioni devono essere sufficientemente grandi per fornire al valutatore la garanzia che i controlli vengano implementati nel modo previsto.

Il campionamento di strutture aziendali e componenti di sistema per una valutazione non riduce l'ambito dell'ambiente dei dati dei titolari di carta o l'applicabilità dei requisiti PCI DSS. Indipendentemente dall'utilizzo o meno del campionamento, i requisiti PCI DSS si applicano all'intero ambiente dei dati dei titolari di carta. In caso di utilizzo del campionamento, ogni campione deve essere valutato rispetto a tutti i requisiti PCI DSS applicabili. Il campionamento degli stessi Requisiti PCI DSS non è consentito.

Esempi di strutture aziendali includono, senza limitazioni: uffici, negozi, sedi in franchising, strutture di elaborazione, centri dati ed altri tipi di strutture con diverse sedi. Il campionamento deve includere i componenti di sistema nell'ambito di ogni struttura aziendale selezionata. Ad esempio, per ogni struttura aziendale selezionata, includere diversi sistemi operativi, funzioni e applicazioni validi per l'area sottoposta a revisione.

A titolo illustrativo, il valutatore può definire un campione presso la struttura aziendale che comprenda server Sun con Apache WWW, server Windows con Oracle, sistemi di mainframe che eseguono applicazioni per l'elaborazione dei dati delle carte precedenti, server di trasferimento dei dati con HP-UX e server Linux con MYSQL. Se tutte le applicazioni vengono eseguite da un singola versione di un sistema operativo (ad esempio, Windows 7 o Solaris 10), il campione deve includere comunque diverse applicazioni (ad esempio, server database, server Web, server di trasferimento dati).

Durante la scelta dei campioni di strutture aziendali e componenti di sistema, i valutatori devono considerare i seguenti fattori:

- In presenza di processi di sicurezza e operativi PCI DSS standard e centralizzati che assicurano congruenza e a cui deve attenersi ogni struttura aziendale/componente di sistema, il campione può essere più piccolo rispetto a quando non sono presenti processi/controlli standard. Il campione deve essere sufficientemente grande per fornire al valutatore una ragionevole garanzia che tutte le strutture aziendali/componenti di sistema siano configurati in base ai processi standard.

- In presenza di più tipi di processi di sicurezza e/o operativi standard e centralizzati (ad esempio, per diversi tipi di strutture aziendali/componenti di sistema), il campione deve essere sufficientemente grande per includere strutture aziendali/componenti di sistema protetti con ogni tipo di processo.
- Se non sono presenti processi/controlli PCI DSS standard e ogni componente di sistema/struttura aziendale è gestito non utilizzando processi standard, il campione deve essere sufficientemente grande per garantire al valutatore che ogni struttura aziendale/componente di sistema ha implementato in modo adeguato i requisiti PCI DSS.

In ogni caso in cui si utilizza il campionamento, il valutatore è tenuto a:

- Documentare il motivo alla base della tecnica di campionamento e della dimensione del campione,
- Documentare e convalidare i processi e controlli PCI DSS standardizzati e i controlli utilizzati per stabilire la dimensione del campione, e
- Illustrare come il campione sia adeguato e rappresentativo dell'intera popolazione.

Fare riferimento anche a:
Appendice D:
Segmentazione e
campionamento delle
strutture aziendali e dei
componenti di sistema.

I valutatori devono riconvalidare il motivo del campionamento per ogni valutazione. Se si utilizza il campionamento, per ogni valutazione è necessario selezionare diversi campioni di strutture aziendali e componenti di sistema.

Controlli compensativi

Su base annuale, i controlli compensativi devono essere documentati, revisionati e convalidati dal valutatore e inoltrati con il rapporto sulla conformità, come definito nell'*Appendice B: Controlli compensativi* e nell'*Appendice C: Foglio di lavoro - Controlli compensativi*.

Per ogni controllo compensativo, **deve** essere completato il Foglio di lavoro - Controlli compensativi (*Appendice C*). Inoltre, i risultati dei controlli compensativi devono essere documentati nel rapporto sulla conformità (ROC) nella sezione dei requisiti PCI DSS corrispondente.

Vedere le *Appendici B e C* sopra menzionate per ulteriori informazioni sui "controlli compensativi".

Istruzioni e contenuto per il rapporto sulla conformità

Questo documento deve essere utilizzato come modello per la creazione del *Rapporto sulla conformità*. L'entità valutata, per garantire che il proprio stato di conformità venga riconosciuto da ogni marchio di pagamento, deve attenersi ai requisiti di reporting specifici di ogni marchio di pagamento. Per informazioni sui requisiti di reporting e per istruzioni specifiche, contattare ciascun marchio di pagamento.

Contenuto e formato del rapporto

Per il completamento del rapporto sulla conformità, attenersi alle seguenti istruzioni per il contenuto e il formato del rapporto:

1. Riepilogo esecutivo

Includere quanto segue:

- Descrivere le attività relative alla carta di pagamento svolte dall'entità, includendo:
 - Il loro ruolo nella gestione delle carte di pagamento, ossia come e perché memorizzano, elaborano e/o trasmettono dati dei titolari di carta.
Nota: non effettuare un semplice "copia e incolla" dal sito Web dell'entità, ma fornire una descrizione personalizzata che dimostri di aver compreso il pagamento e il ruolo dell'entità.
 - La modalità di elaborazione del pagamento (diretto, indiretto e così via)
 - I tipi di canali di pagamento offerti, transazioni con carta non presente (ad esempio, ordine via e-mail, ordine telefonico (MOTO), e-Commerce) oppure con carta presente
 - Altre aziende con cui l'entità collabora per la trasmissione o l'elaborazione del pagamento, incluse relazioni con elaboratori
- Un diagramma della rete di alto livello (ottenuto dall'entità o creato dal valutatore) della topografia di rete dell'entità che include:
 - Connessioni interne ed esterne alla rete
 - Componenti critici all'interno dell'ambiente dei dati di titolari di carta, inclusi dispositivi POS, sistemi, database e server Web, come applicabile
 - Altri componenti di pagamento necessari, come applicabile

2. Descrizione delle attività da eseguire e dell'approccio adottato

Descrivere l'ambito, in base al contenuto della sezione Ambito di valutazione del presente documento, includendo quanto riportato di seguito:

- Documentare le modalità adottate dal valutatore per la convalidare la precisione dell'ambito della valutazione PCI DDS, compresi:
 - I metodi o i processi utilizzati per individuare e documentare tutte le esistenze di dati dei titolari di carta
 - Come sono stati valutati e documentati i risultati
 - Come sono state verificate l'efficacia e la precisione dei metodi di valutazione
 - La convalida da parte del valutatore che l'ambito della valutazione è preciso ed adeguato.
- Ambiente sottoposto a valutazione (ad esempio, punti di accesso Internet del client, rete aziendale interna, connessioni per elaborazione)
- Se la segmentazione di rete è in atto ed è stata utilizzata per ridurre l'ambito della revisione PCI DSS, illustrare brevemente la segmentazione e il modo in cui il valutatore ha convalidato l'efficacia della segmentazione
- Se durante la valutazione si fa ricorso al campionamento, per ogni set di campione selezionato (di strutture aziendali /componenti di sistema) documentare quanto segue:
 - Popolazione totale
 - Numero campionato
 - Motivo del campione selezionato
 - Descrizione dei processi e dei controlli operativi e di sicurezza PCI DSS standardizzati per determinare la dimensione del campione e le modalità di convalida di processi/controlli
 - In che modo il campione è adeguato e rappresentativo dell'intera popolazione.
 - Descrivere posizioni o ambienti che memorizzano, elaborano o trasmettono i dati di titolari di carta ESCLUSI dall'ambito della revisione e il motivo per cui tali posizioni/ambienti sono stati esclusi
- Elencare tutte le entità di completa proprietà che richiedono la conformità agli standard PCI DSS e indicare se sono state revisionate separatamente o nell'ambito di questa valutazione
- Elencare tutte le entità internazionali che richiedono la conformità agli standard PCI DSS e indicare se sono state revisionate separatamente o nell'ambito di questa valutazione
- Elencare le LAN wireless e/o le applicazioni di pagamento wireless (ad esempio, terminali POS) connesse o che potrebbero influire sulla sicurezza dell'ambiente dei dati di titolari di carta e descrivere le misure di sicurezza in atto per questi ambienti wireless
- La versione del documento Requisiti PCI DSS e procedure di valutazione della sicurezza utilizzata per eseguire la valutazione

3. Dettagli sull'ambiente sottoposto a revisione

In questa sezione, includere i seguenti dettagli:

- Diagramma di ciascuna parte del link di comunicazione, incluse LAN, WAN o Internet
- Descrizione dell'ambiente dei dati dei titolari di carta, ad esempio:
 - Documentare la trasmissione e l'elaborazione dei dati dei titolari di carta, inclusi i flussi di autorizzazione, acquisizione, contabilizzazione, rettifica e di altro tipo, come applicabile
 - Elenco di file e tabelle contenenti dati di titolari di carta, supportato da un inventario creato (oppure ottenuto dal client) e conservato dal valutatore nei documenti. Questo inventario deve includere, per ciascuna memorizzazione dei dati di titolari di carta (file, tabella, eccetera):
 - Elenco di tutti gli elementi di dati di titolari di carta memorizzati
 - Modalità di protezione dei dati
 - Modalità di registrazione dell'accesso ai dati memorizzati
- Elenco di hardware e software critico in uso nell'ambiente dei dati di titolari di carta, insieme alla descrizione di funzione/uso di ciascuno di essi
- Elenco dei provider di servizi e di altre terze parti con i quali l'entità condivide dati dei titolari di carta
Nota: queste entità sono soggette al Requisito 12.8 PCI DSS).
- Elenco di prodotti e numeri di versione di applicazioni di pagamento di terze parti in uso, inclusa l'eventuale convalida della conformità di ciascuna applicazione di pagamento agli standard PA-DSS. Anche se un'applicazione di pagamento è stata convalidata in base agli standard PA-DSS, il valutatore è ancora tenuto a verificare che l'applicazione sia stata implementata in un modo e in un ambiente conformi agli standard PCI DSS e in base alla *Guida per l'implementazione del programma PA-DSS* del fornitore dell'applicazione di pagamento.
Nota: l'uso di applicazioni convalidate in base agli standard PA-DSS non è un requisito PCI DSS. Consultare ogni marchio di pagamento singolarmente per verificare i relativi requisiti di conformità agli standard PA-DSS).
- Elenco delle persone intervistate, organizzazioni di appartenenza, ruolo ed argomenti affrontati
- Elenco della documentazione sottoposta a revisione
- Per le revisioni di provider di servizi gestiti (MSP, Managed Service Provider), il valutatore deve identificare in modo chiaro quali requisiti nel presente documento applicare al provider di servizi (e includere nella revisione) e quali sono esclusi dalla revisione e devono essere inclusi dai clienti del provider di servizi nelle relative revisioni. Indicare gli indirizzi IP del provider di servizi gestito (MSP) che vengono inclusi nelle scansioni delle vulnerabilità trimestrali del provider e gli indirizzi IP che devono essere inclusi nelle scansioni trimestrali dei clienti del provider.

4. Informazioni di contatto e data del rapporto

Includere:

- Informazioni di contatto per l'esercente o il provider di servizi e il valutatore
- Tempi di valutazione—specificare la durata ed il periodo di tempo nel corso del quale è avvenuta la valutazione
- Data del rapporto

5. Risultati delle scansioni trimestrali

- Riepilogare i risultati delle quattro scansioni trimestrali più recenti nel Riepilogo esecutivo nonché nei commenti del Requisito 11.2.2

Nota: non è necessario completare con successo quattro scansioni trimestrali per la conformità iniziale agli standard PCI DSS se il valutatore verifica che:

- 1) il risultato della scansione più recente era positivo,
- 2) l'entità dispone di politiche e procedure documentate che richiedono l'esecuzione di scansioni trimestrali, e
- 3) ogni vulnerabilità rilevata nella scansione iniziale è stata corretta come dimostrato da una nuova scansione.

Per gli anni successivi alla revisione PCI DSS iniziale, è necessario eseguire quattro scansioni trimestrali con esito positivo.

- La scansione deve coprire tutti gli indirizzi IP (Internet) accessibili esternamente dell'entità, in base alla *Guida del programma per i fornitori di scansioni approvati PCI*.

6. Risultati e osservazioni

Riepilogare nel Riepilogo esecutivo i risultati che potrebbero non rientrare nel formato del modello del Rapporto sulla conformità standard.

Tutti i valutatori *devono*:

- Utilizzare il modello Requisiti PCI DSS dettagliati e procedure di valutazione della sicurezza per fornire descrizioni e risultati dettagliati su ogni requisito e sottorequisito.
- Assicurare che tutte le risposte N/A siano spiegate in modo chiaro.
- Esaminare e documentare tutti i controlli compensativi presi in considerazione per verificare che vi sia un controllo in atto.

Per ulteriori dettagli sui controlli compensativi fare riferimento alla precedente sezione "Controlli compensativi" e alle *Appendici B e C*.

Riconvalida dei problemi in attesa di soluzione

Per verificare la conformità, è richiesto un rapporto sui "controlli in atto". Il rapporto viene considerato non conforme se contiene "problemi in attesa di soluzione" o che verranno risolti in un secondo momento. L'esercente/provider di servizi deve risolvere tali problemi prima del termine del periodo di convalida. Dopo che l'esercente/provider di servizi ha risolto questi problemi, il valutatore esegue nuovamente la valutazione per confermare che la correzione sia stata apportata e che tutti i requisiti siano stati soddisfatti. Dopo la riconvalida, il valutatore prepara un nuovo Rapporto sulla conformità, in cui dichiara che l'ambiente dei dati di titolari di carta è completamente conforme e invia tale rapporto come da istruzioni (vedere di seguito).

Conformità agli standard PCI DSS – Operazioni

1. Completare il Rapporto sulla conformità in base alla sezione sopra riportata "Istruzioni e contenuto per il rapporto sulla conformità".
2. Garantire che le scansioni delle vulnerabilità con esito positivo siano state completate da un fornitore di scansioni approvato (ASV, Approved Scanning Vendor) PCI SSC e richiedere all'ASV prova delle scansioni completate con successo.
3. Completare per intero l'Attestato di conformità per i provider di servizi o per gli esercenti, come applicabile. Gli Attestati di conformità sono disponibili sul sito Web PCI SSC (www.pcisecuritystandards.org).
4. Inviare il Rapporto sulla conformità, la prova di una scansione completata con esito positivo e l'attestato di conformità, insieme ad eventuale altra documentazione richiesta, al proprio acquirente (per gli esercenti) o al marchio di pagamento o ad altra entità richiedente (per i provider di servizi).

Requisiti PCI DSS e procedure di valutazione della sicurezza dettagliate

Per la sezione *Requisiti PCI DSS e procedure di valutazione della sicurezza*, i seguenti sono gli elementi che costituiscono le intestazioni delle colonne dalla tabella:

- **Requisiti PCI DSS:** questa colonna definisce lo standard DSS (Data Security Standard) ed elenca i requisiti per la conformità agli standard PCI DSS; la conformità verrà convalidata in base a tali requisiti.
- **Procedure di test :** questa colonna indica i processi che il valutatore deve seguire per confermare che i requisiti PCI DSS sono "presenti".
- **Presente :** questa colonna deve essere utilizzata dal valutatore per fornire una breve descrizione dei controlli convalidati come "presenti" per ogni requisito, includendo le descrizioni dei controlli rilevati come in atto identificati dai controlli compensativi oppure a seguito di un requisito "non applicabile".
- **Non presente:** questa colonna deve essere utilizzata dal valutatore per fornire una breve descrizione dei controlli non presenti. Tenere presente che un rapporto non conforme non deve essere inviato a un marchio di pagamento o a un acquirente se non specificamente richiesto. Per ulteriori istruzioni sui rapporti di non conformità, fare riferimento agli Attestati di conformità, disponibili sul sito Web PCI SSC (www.pcisecuritystandards.org).
- **Data di scadenza/Commenti:** per i controlli "non presenti", il valutatore può includere una data di scadenza entro la quale è previsto che l'esercente o il provider di servizi implementi tali controlli. È possibile includere qui anche eventuali note o commenti aggiuntivi.

Nota: questa colonna non deve essere utilizzata per controlli che non sono ancora in atto o per problemi in attesa di soluzione che verranno risolti successivamente.

Sviluppo e gestione di una rete sicura

Requisito 1: Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta

I firewall sono dispositivi di computer che controllano il traffico consentito tra le reti di un'entità (interne) e reti non attendibili (esterne) nonché il traffico all'interno e all'esterno delle aree più sensibili delle reti attendibili interne di un'entità. L'ambiente dei dati dei titolari di carta rappresenta un esempio di un'area più sensibile all'interno di una rete attendibile di un'entità.

Un firewall esamina tutto il traffico di rete e blocca le trasmissioni che non soddisfano i criteri di sicurezza specificati.

Tutti i sistemi devono essere protetti da accesso non autorizzato da reti non attendibili, ad esempio accesso al sistema tramite Internet come e-commerce, accesso dei dipendenti a Internet tramite browser desktop, accesso alla posta elettronica dei dipendenti, connessioni dedicate quali connessioni tra le aziende, accesso tramite reti wireless o di altro tipo. Spesso, percorsi apparentemente insignificanti per e da reti non attendibili possono consentire di accedere a sistemi chiave. I firewall sono un meccanismo di protezione chiave per qualsiasi rete di computer.

Altri componenti di sistema possono fornire funzionalità firewall, a condizione che soddisfino i requisiti minimi per i firewall come specificato al Requisito 1. Nei casi in cui si utilizzano altri componenti di sistema all'interno dell'ambiente dei dati dei titolari di carta per fornire funzionalità di firewall, questi dispositivi devono essere compresi nell'ambito e nella valutazione del Requisito 1.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
1.1 Stabilire standard di configurazione del firewall e del router che includano:	1.1 Richiedere ed esaminare gli standard di configurazione del firewall e del router e altra documentazione specificata di seguito per verificare che tali standard siano completi. Completare quanto segue:			
1.1.1 Un processo formale per l'approvazione e il test di tutte le connessioni di rete e le modifiche apportate alla configurazione del firewall e del router	1.1.1 Verificare la presenza di un processo formale per il test e l'approvazione di tutte le connessioni di rete e le modifiche apportate alla configurazione del firewall e del router.			
1.1.2 Un diagramma aggiornato della rete con tutte le connessioni ai dati di titolari di carta, comprese eventuali reti wireless	1.1.2.a Verificare la presenza di un diagramma di rete aggiornato (ad esempio, un diagramma che illustra il flusso dei dati di titolari di carta attraverso la rete) che documenti tutte le connessioni ai dati di titolari di carta, compresa qualsiasi rete wireless.			
	1.1.2.b Verificare che il diagramma sia aggiornato.			
1.1.3 Requisiti per un firewall per ogni connessione Internet e tra tutte le zone demilitarizzate (DMZ) e la zona della rete interna	1.1.3.a Verificare che gli standard di configurazione del firewall includano i requisiti per un firewall per ogni connessione Internet e tra la zona DMZ e la zona della rete interna.			
	1.1.3.b Verificare che il diagramma di rete aggiornato sia coerente			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
	con gli standard di configurazione del firewall.			
1.1.4 Descrizione di gruppi, ruoli e responsabilità per la gestione logica dei componenti della rete	1.1.4 Verificare che gli standard di configurazione del firewall e del router includano una descrizione dei gruppi, dei ruoli e delle responsabilità per la gestione logica dei componenti della rete.			
1.1.5 La documentazione e la giustificazione aziendale per l'uso di tutti i servizi, i protocolli e le porte consentite, inclusa la documentazione delle funzioni di sicurezza implementate per i protocolli considerati non sicuri. Esempi di servizi, protocolli o porte non sicuri includono, senza limitazioni, FTP, Telnet, POP3, IMAP e SNMP.	1.1.5.a Verificare che gli standard di configurazione del firewall e del router includano un elenco documentato di servizi, protocolli e porte necessari per l'azienda, ad esempio i protocolli HTTP (Hypertext Transfer Protocol) e SSL (Secure Sockets Layer), SSH (Secure Shell) e VPN (Virtual Private Network).			
	1.1.5.b Identificare i servizi, i protocolli e le porte consentite non sicuri, verificare la loro necessità e che le funzioni di sicurezza siano documentate e implementate esaminando gli standard di configurazione del firewall e del router e le impostazioni per ogni servizio.			
1.1.6 Una revisione dei set di regole del firewall e del router almeno ogni sei mesi	1.1.6.a Verificare che gli standard di configurazione del firewall e del router richiedano una revisione dei set di regole del firewall e del router almeno ogni sei mesi.			
	1.1.6.b Richiedere ed esaminare la documentazione per verificare che i set di regole vengano revisionati almeno ogni sei mesi.			
1.2 Creare la configurazione del firewall e del router che limiti le connessioni tra le reti non attendibili e qualsiasi componente di sistema nell'ambiente dei dati dei titolari di carta. <i>Nota: una "rete non attendibile" è una qualsiasi rete esterna alle reti che appartengono all'entità sottoposta a revisione e/o che l'entità non è in grado di controllare o gestire.</i>	1.2 Esaminare la configurazione del firewall e del router per verificare che le connessioni tra le reti non attendibili e i componenti di sistema nell'ambiente dei dati di titolari di carta siano limitate, nel modo illustrato di seguito:			
1.2.1 Limitazione del traffico in entrata e in uscita a quello indispensabile per l'ambiente dati dei titolari di carta.	1.2.1.a Verificare che il traffico in entrata e in uscita sia limitato a quello necessario per l'ambiente dei dati di titolari di carta e che le restrizioni siano documentate.			
	1.2.1.b Verificare che il resto del traffico in entrata e in uscita venga negato in modo specifico, ad esempio utilizzando un comando esplicito "deny all" o un comando implicito di negazione dopo un'istruzione "allow".			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
1.2.2 Protezione e sincronizzazione dei file di configurazione del router.	1.2.2 Verificare che i file di configurazione del router, ad esempio, i file di configurazione di esecuzione (utilizzati per la normale esecuzione dei router) e i file di configurazione all'avvio (utilizzati al riavvio dei computer) siano sicuri e sincronizzati e che dispongano delle stesse configurazioni sicure.			
1.2.3 Installare firewall perimetrali tra le reti wireless e l'ambiente dei dati dei titolari di carta e configurare tali firewall per negare o controllare il traffico (se necessario per gli scopi aziendali) dall'ambiente wireless all'ambiente dei dati dei titolari di carta.	1.2.3 Verificare che siano stati installati firewall perimetrali tra le reti wireless e i sistemi che memorizzano i dati dei titolari di carta e che tali firewall neghino o controllino il traffico (se necessario per gli scopi aziendali) dall'ambiente wireless all'ambiente dei dati di titolari di carta.			
1.3 Vietare l'accesso pubblico diretto tra Internet e i componenti di sistema nell'ambiente dei dati di titolari di carta.	1.3 Esaminare le configurazioni di firewall e router, inclusi, senza limitazioni, il router interno ad Internet, il router e il firewall DMZ, il segmento di titolari di carta DMZ, il router perimetrale ed il segmento di rete di titolari di carta interno, per determinare che non vi sia accesso diretto tra Internet e i componenti di sistema nel segmento di rete dei titolari di carta interno, nel modo descritto di seguito.			
1.3.1 Implementare una zona DMZ per limitare il traffico in entrata ai soli componenti di sistema che forniscono servizi, protocolli e porte autorizzati accessibili pubblicamente.	1.3.1 Verificare l'implementazione di una zona DMZ per limitare il traffico in entrata ai soli componenti di sistema che forniscono servizi, protocolli e porte autorizzati accessibili pubblicamente.			
1.3.2 Limitare il traffico Internet in entrata agli indirizzi IP all'interno della zona DMZ.	1.3.2 Verificare che il traffico Internet in entrata sia limitato agli indirizzi IP all'interno della zona DMZ.			
1.3.3 Non consentire alcun percorso diretto per il traffico in entrata o in uscita tra Internet e l'ambiente dei dati di titolari di carta.	1.3.3 Verificare che non siano consentiti percorsi diretti per il traffico in entrata o in uscita tra Internet e l'ambiente dei dati di titolari di carta.			
1.3.4 Non consentire agli indirizzi interni di passare da Internet alla zona DMZ.	1.3.4 Verificare che gli indirizzi interni non possano passare da Internet alla zona DMZ.			
1.3.5 Non consentire il traffico in uscita non autorizzato dall'ambiente dei dati dei titolari di carta ad Internet.	1.3.5 Verificare che sia espressamente autorizzato il traffico in uscita dall'ambiente dei dati dei titolari di carta ad Internet			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>1.3.6 Implementare un controllo efficiente, anche noto come "dynamic packet filtering" (ossia che consente solo alle connessioni già "stabilite" di accedere alla rete).</p>	<p>1.3.6 Verificare che il firewall esegua un controllo efficiente (dynamic packet filtering). (Si dovrebbero consentire solo le connessioni già "stabilite" e solo se sono associate ad una sessione stabilita in precedenza).</p>			
<p>1.3.7 Posizionare i componenti di sistema che memorizzano dati dei titolari di carta (come un database) in una zona di rete interna, separata dalla zona DMZ e da altre reti non attendibili.</p>	<p>1.3.7 Verificare che i componenti di sistema che memorizzano dati dei titolari di carta siano in una zona di rete interna, separata dalla zona DMZ e da altre reti non attendibili.</p>			
<p>1.3.8 Non divulgare indirizzi IP privati ed informazioni di routing a parti non autorizzate.</p> <p>Nota: i metodi per oscurare l'indirizzamento IP possono includere, senza limitazioni:</p> <ul style="list-style-type: none"> ▪ NAT (Network Address Translation) ▪ Posizionamento di server contenenti dati dei titolari di carta dietro server/firewall proxy o cache contenuti, ▪ Rimozione o filtraggio di annunci di instradamento per reti private che utilizzano indirizzamento registrato, ▪ uso interno di spazio indirizzi RFC1918 invece degli indirizzi registrati. 	<p>1.3.8.a Verificare che siano in atto metodi per impedire la divulgazione di indirizzi IP privati ed informazioni di routing da reti interne ad Internet.</p>			
	<p>1.3.8.b Verificare che siano autorizzate eventuali divulgazioni di indirizzi IP privati ed informazioni di routing ad entità esterne.</p>			
<p>1.4 Installare firewall personali (software) su tutti i computer portatili e i computer di proprietà dei dipendenti con connettività diretta a Internet (ad esempio, laptop utilizzati dai dipendenti), che vengono utilizzati per accedere alla rete aziendale.</p>	<p>1.4.a Verificare l'installazione e l'attivazione di firewall personali (software) su tutti i computer portatili e i computer di proprietà dei dipendenti con connettività diretta a Internet (ad esempio, laptop utilizzati dai dipendenti), che vengono utilizzati per accedere alla rete aziendale.</p>			
	<p>1.4.b Verificare la configurazione da parte dell'organizzazione di firewall personali (software) in base a standard specifici e che gli utenti di computer portatili e/o computer di proprietà dei dipendenti non possano modificarli.</p>			

Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione

Utenti non autorizzati (all'interno o all'esterno dell'entità) utilizzano spesso password e altre impostazioni predefinite dei fornitori per accedere in modo improprio ai sistemi. Queste password e impostazioni sono ben note alle comunità di hacker e vengono determinate facilmente tramite informazioni pubbliche.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
2.1 Modificare sempre le impostazioni predefinite dei fornitori prima di procedere all'installazione di un sistema sulla rete, incluso, senza limitazione, password, stringhe di comunità SNMP (simple network management protocol) ed eliminazione di account non necessari.	2.1 Scegliere un campione di componenti di sistema, quindi tentare l'accesso (con l'aiuto dell'amministratore di sistema) ai dispositivi utilizzando account e password predefiniti del fornitore per verificare che siano stati modificati. Per trovare account/password del fornitore, consultare i manuali e le fonti su Internet.			
2.1.1 Per gli ambienti wireless connessi all'ambiente dei dati di titolari di carta o che trasmettono tali dati, modificare le impostazioni predefinite del fornitore wireless, incluse, senza limitazione, chiavi di cifratura wireless predefinite, password e stringhe di comunità SNMP.	2.1.1 Verificare quanto segue per quanto riguarda le impostazioni predefinite del fornitore per ambienti wireless:			
	2.1.1.a Le chiavi di cifratura predefinite sono state modificate al momento dell'installazione e vengono modificate ogni volta che un utente a conoscenza delle chiavi lascia l'azienda o cambia sede.			
	2.1.1.b Le stringhe di comunità SNMP predefinite sui dispositivi wireless sono state modificate.			
	2.1.1.c Le password/passphrase predefinite ai punti di accesso sono state modificate.			
	2.1.1.d Il firmware sui dispositivi wireless è aggiornato per supportare la cifratura avanzata per l'autenticazione e la trasmissione su reti wireless			
	2.1.1.e Sono state modificate altre impostazioni predefinite del fornitore wireless relative alla sicurezza, se applicabili.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>2.2. Sviluppare standard di configurazione per tutti i componenti di sistema. Accertarsi che questi standard risolvano tutte le vulnerabilità della sicurezza note e siano coerenti con gli standard di hardening accettati dal settore.</p> <p>Le fonti di standard di hardening accettati dal settore possono includere, senza limitazione:</p> <ul style="list-style-type: none"> ▪ CIS (Center for Internet Security) ▪ ISO (International Organization for Standardization) ▪ Istituto SANS (SysAdmin Audit Network Security) ▪ NIST (National Institute of Standards Technology) 	<p>2.2.a Esaminare che gli standard di configurazione del sistema dell'organizzazione per tutti i tipi di componenti di sistema e verificare che tali standard siano coerenti con gli standard di hardening accettati dal settore.</p>			
	<p>2.2.b Verificare che gli standard di configurazione del sistema siano aggiornati quando vengono identificati nuovi problemi di vulnerabilità, secondo quanto definito al Requisito 6.2.</p>			
	<p>2.2.c Verificare che gli standard di configurazione del sistema vengano applicati quando si configurano nuovi sistemi.</p>			
	<p>2.2.d Verificare che gli standard di configurazione del sistema includano ogni elemento riportato di seguito (nelle sezioni 2.2.1 – 2.2.4).</p>			
<p>2.2.1 Implementare solo una funzione principale per server per impedire la coesistenza sullo stesso server di funzioni che richiedono livelli di sicurezza diversi. Ad esempio, server Web, database server e DNS devono essere implementati su server separati.</p> <p><i>Nota: Dove si utilizzano tecnologie di virtualizzazione, implementare solo una funzione principale per componente di sistema virtuale.</i></p>	<p>2.2.1.a Per un campione di componenti di sistema, verificare che sia stata implementata una sola funzione principale per server.</p>			
	<p>2.2.1.b Se si utilizzano tecnologie di virtualizzazione, verificare che sia stata implementata una sola funzione principale per dispositivo o componente di sistema virtuale.</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>2.2.2 Abilitare solo servizi, protocolli, daemon ecc. necessari e sicuri, come richiesto per la funzione del sistema.</p> <p>Implementare funzioni di sicurezza per ogni servizio, protocollo o daemon necessario considerato non sicuro, ad esempio, utilizzare tecnologie sicure come SSH, S-FTP, SSL o IPSec VPN per proteggere servizi non sicuri come NetBIOS, file-sharing, Telnet, FTP, ecc.</p>	<p>2.2.2.a Per campione di componenti di sistema, ispezionare servizi di sistema, daemon e protocolli attivati. Verificare che siano attivati soli i servizi o i protocolli necessari.</p>			
	<p>2.2.2.b Identificare ogni servizio, daemon o protocollo non sicuro attivato. Verificare che siano giustificati e che le funzionalità di protezione siano documentate ed implementate.</p>			
<p>2.2.3 Configurare i parametri di sicurezza del sistema per evitare un uso improprio.</p>	<p>2.2.3.a Consultare gli amministratori del sistema e/o i responsabili della sicurezza per verificare che conoscano le impostazioni dei parametri della sicurezza comuni per i componenti di sistema.</p>			
	<p>2.2.3.b Verificare che le impostazioni dei parametri di sicurezza comuni siano incluse negli standard di configurazione del sistema.</p>			
	<p>2.2.3.c Per un campione di componenti di sistema, verificare che i parametri di sicurezza comuni siano impostati correttamente.</p>			
<p>2.2.4 Rimuovere tutta la funzionalità non necessaria, ad esempio script, driver, funzioni, sottosistemi, file system e server Web non utilizzati.</p>	<p>2.2.4.a Per un campione di componenti del sistema, verificare che tutta la funzionalità non necessaria (ad esempio, script, driver, funzioni, sottosistemi, file system, eccetera) sia rimossa.</p>			
	<p>2.2.4.b. Verificare che le funzioni attivate siano documentate e supportino la configurazione sicura.</p>			
	<p>2.2.4.c. Verificare che solo la funzionalità documentata sia presente sui componenti di sistema inseriti nel campione.</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
2.3 Eseguire la cifratura di tutto l'accesso amministrativo non da console, tramite crittografia avanzata. Utilizzare tecnologie quali SSH, VPN o SSL/TLS per la gestione basata su Web e altre attività amministrative non da console.	2.3 Per un campione di componenti di sistema, verificare che l'accesso amministrativo non da console sia cifrato nei seguenti modi:			
	2.3.a Osservare un amministratore al momento dell'accesso a ciascun sistema per verificare che venga richiamato un metodo di crittografia avanzata prima della richiesta della password.			
	2.3.b Esaminare servizi e file di parametri sui sistemi per accertarsi che non siano disponibili per uso interno comandi Telnet e altri comandi di accesso remoto.			
	2.3.c Verificare che l'accesso amministratore alle interfacce di gestione basate su Web sia cifrato con un metodo di crittografia avanzata.			
2.4 I provider di hosting condiviso devono proteggere l'ambiente ospitato e i dati di titolari di carta di ciascuna entità. Questi provider devono soddisfare specifici requisiti come descritto nell' <i>Appendice A: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso</i> .	2.4 Eseguire le procedure di test da A.1.1 a A.1.4 descritte nell' <i>Appendice A: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso</i> per valutazioni PCI DSS di provider di hosting condiviso, per verificare che i provider di hosting condiviso garantiscano la protezione dell'ambiente ospitato (esercenti e provider di servizi) e dei dati delle relative entità.			

Protezione dei dati di titolari di carta

Requisito 3: *Proteggere i dati di titolari di carta memorizzati*

I metodi di protezione quali cifratura, troncatura, mascheratura e hashing sono componenti critici della protezione dei dati di titolari di carta. Se un utente non autorizzato elude altri controlli di sicurezza e ottiene l'accesso ai dati cifrati, senza le chiavi di crittografia corrette, tale utente non potrà leggere o utilizzare i dati. È consigliabile prendere in considerazione altri metodi efficaci per la protezione dei dati memorizzati per limitare i possibili rischi. Ad esempio, è possibile evitare di memorizzare i dati di titolari di carta a meno che non sia assolutamente necessario, eseguire la troncatura dei dati di titolari di carta se non è richiesto il PAN completo, non inviare i PAN non protetti usando tecnologie di messaggistica degli utenti finali, come messaggi e-mail e messaggistica istantanea.

Fare riferimento al documento *PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi* per la definizione di "crittografia avanzata" e di altri termini PCI DSS.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
3.1 Mantenere al minimo la memorizzazione dei dati dei titolari di carta implementando politiche, procedure e processi per la conservazione e l'eliminazione dei dati, come segue.	3.1 Richiedere ed esaminare le politiche, le procedure e i processi per la conservazione e l'eliminazione dei dati ed effettuare quanto segue:			
3.1.1 Implementare una politica per la conservazione e l'eliminazione dei dati che comprenda: <ul style="list-style-type: none"> ▪ Limitazione della quantità dei dati memorizzati e il tempo di conservazione in base alle esigenze aziendali, legali e legislative ▪ Processi per la rimozione sicura dei dati quando non sono più necessari ▪ Requisiti specifici di conservazione dei dati dei titolari di carta ▪ Processo manuale o automatico trimestrale per identificare ed 	3.1.1.a Verificare che le politiche e le procedure siano implementate e includano requisiti legali, legislativi e aziendali per la conservazione dei dati, inclusi requisiti specifici per la conservazione dei dati di titolari di carta (ad esempio, è necessario conservare i dati di titolari di carta per un periodo X per scopi aziendali Y).			
	3.1.1.b Verificare che le politiche e le procedure includano disposizioni per l'eliminazione dei dati non più necessari per scopi legali, legislativi o aziendali, inclusa l'eliminazione dei dati di titolari di carta.			
	3.1.1.c Verificare che le politiche e le procedure includano disposizioni per ogni tipo di memorizzazione dei dati di titolari di carta.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>eliminare in modo sicuro i dati dei titolari di carta memorizzati che superano i requisiti di conservazione definiti</p>	<p>3.1.1.d Verificare che le politiche e le procedure includano almeno uno dei seguenti: Un processo programmatico (automatico o manuale) per rimuovere, almeno su base trimestrale, i dati di titolari di carta memorizzati che superano i requisiti definiti nella politica per la conservazione dei dati Requisiti per una revisione, realizzata almeno su base trimestrale, per verificare che i dati dei titolari di carta memorizzati non superano i requisiti definiti nella politica per la conservazione dei dati.</p> <p>3.1.1.e Per un campione di componenti di sistema che memorizzano dati di titolari di carta, verificare che i dati memorizzati non superino i requisiti definiti nella politica per la conservazione dei dati.</p>			
<p>3.2 Non memorizzare dati sensibili di autenticazione dopo l'autorizzazione (anche se crittografati). I dati sensibili di autenticazione includono i dati citati nei seguenti Requisiti da 3.2.1 a 3.2.3: <i>Nota: ad emittenti e società che supportano servizi di emissione è consentita la memorizzazione di dati sensibili di autenticazione in presenza di una giustificazione aziendale ed i dati vengono memorizzati in modo sicuro.</i></p>	<p>3.2.a Per emittenti e/o società che supportano servizi di emissione e memorizzano dati sensibili di autenticazione, verificare la presenza di una giustificazione aziendale per la memorizzazione di dati sensibili di autenticazione e che i dati siano protetti.</p> <p>3.2.b Per tutte le altre entità, se sono stati ricevuti ed eliminati dati sensibili di autenticazione, richiedere ed esaminare i processi per l'eliminazione sicura dei dati per verificare che i dati non siano recuperabili.</p> <p>3.2.c Per ogni elemento di dati sensibili di autenticazione di seguito, effettuare la seguente procedura:</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>3.2.1 Non memorizzare l'intero contenuto delle tracce (dalla striscia magnetica presente sul retro della carta, dati equivalenti contenuti in un chip o in altro luogo). Questi dati sono denominati anche traccia completa, traccia, traccia 1, traccia 2 e dati di striscia magnetica.</p> <p>Nota: <i>nel normale svolgimento delle attività, è possibile che sia necessario conservare i seguenti elementi di dati della striscia magnetica:</i></p> <ul style="list-style-type: none"> ▪ Nome del titolare della carta ▪ PAN (Primary Account Number) ▪ Data di scadenza ▪ Codice di servizio <p><i>Per ridurre al minimo il rischio, memorizzare solo gli elementi di dati necessari per l'azienda.</i></p>	<p>3.2.1 Per un campione di componenti di sistema, esaminare i file di dati, incluso, senza limitazione, quanto segue, e verificare che l'intero contenuto delle tracce della striscia magnetica sul retro della carta o dati equivalenti in un chip non sia memorizzato in nessun caso:</p> <ul style="list-style-type: none"> ▪ Dati di transazioni in entrata ▪ Tutti i registri (ad esempio, transazioni, cronologia, debug o errori) ▪ File di cronologia ▪ File di traccia ▪ Diversi schemi di database ▪ Contenuto di database 			
<p>3.2.2 Non memorizzare il codice o il valore di verifica della carta (numero a tre o quattro cifre impresso sulla parte anteriore o posteriore della carta di pagamento) utilizzato per verificare le transazioni con carta non presente.</p>	<p>3.2.2 Per un campione di componenti di sistema, esaminare i file di dati, incluso, senza limitazione, quanto segue, e verificare che il codice o il valore di verifica della carta a tre o quattro cifre impresso sulla parte anteriore della carta o nel riquadro della firma (dati CVV2, CVC2, CID, CAV2) non venga memorizzato in nessun caso:</p> <ul style="list-style-type: none"> ▪ Dati di transazioni in entrata ▪ Tutti i registri (ad esempio, transazioni, cronologia, debug o errori) ▪ File di cronologia ▪ File di traccia ▪ Diversi schemi di database ▪ Contenuto di database 			
<p>3.2.3 Non memorizzare il numero di identificazione personale (PIN) o il blocco PIN cifrato.</p>	<p>3.2.3 Per un campione di componenti di sistema, esaminare i file di dati, incluso, senza limitazioni, quando segue e verificare che i PIN e blocchi PIN cifrati non siano memorizzati in nessun caso:</p> <ul style="list-style-type: none"> ▪ Dati di transazioni in entrata 			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
	<ul style="list-style-type: none"> ▪ Tutti i registri (ad esempio, transazioni, cronologia, debug o errori) ▪ File di cronologia ▪ File di traccia ▪ Diversi schemi di database ▪ Contenuto di database 			
<p>3.3 Mascherare il PAN quando visualizzato (non devono essere visibili più di sei cifre all'inizio e quattro cifre alla fine).</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ <i>questo requisito non si applica ai dipendenti e ad altre parti che hanno l'esigenza aziendale legittima di visualizzare l'intero PAN.</i> ▪ <i>Questo requisito non sostituisce i requisiti più rigorosi per la visualizzazione dei dati di titolari di carta, ad esempio per ricevute di punti di vendita (POS).</i> 	<p>3.3 Richiedere ed esaminare le politiche scritte e le visualizzazioni del PAN (ad esempio, su schermo e in ricevute cartacee) per verificare che i PAN (Primary Account Number) siano mascherati durante la visualizzazione dai dati di titolari di carta, ad eccezione dei casi in cui occorre visualizzare il PAN completo per un'esigenza aziendale legittima.</p>			
<p>2.3 Rendere illeggibile il PAN ovunque sia memorizzato (inclusi i dati su supporti digitali portatili, supporti di backup, registri) utilizzando uno dei seguenti approcci:</p> <ul style="list-style-type: none"> ▪ Hash one-way basati su crittografia avanzata (l'hash deve essere dell'intero PAN) ▪ Troncatura (non si può usare l'hashing per sostituire la parte troncata del PAN) ▪ Token e pad indicizzati (i pad devono essere custoditi in un luogo sicuro) ▪ Crittografia avanzata con relativi processi e procedure di gestione 	<p>3.4.a Richiedere ed esaminare la documentazione relativa al sistema utilizzato per proteggere il PAN, incluso il fornitore, il tipo di sistema/processo e gli algoritmi di cifratura (se applicabili). Verificare che il PAN sia stato reso illeggibile tramite uno dei seguenti metodi:</p> <ul style="list-style-type: none"> ▪ Hash one-way basati su crittografia avanzata ▪ Troncatura ▪ Token e pad indicizzati, con pad custoditi in un luogo sicuro ▪ Crittografia avanzata, con relativi processi e procedure di gestione delle chiavi <p>3.4.b Esaminare diverse tabelle o file del campione di repository dei dati per verificare che il PAN sia illeggibile (cioè, non memorizzato come testo semplice).</p> <p>3.4.c Esaminare un campione dei supporti rimovibili (ad esempio, nastri di backup) per confermare che il PAN sia illeggibile.</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>delle chiavi</p> <p>Nota: per un utente non autorizzato è relativamente facile ricostruire i dati PAN originali se ha accesso alla versione troncata e hash del PAN. Nel caso in cui versioni troncata e hash dello stesso PAN siano presenti nell'ambiente di un'entità, andrebbero predisposti ulteriori controlli per verificare che non sia possibile correlare le versioni troncata e hash per ricostruire il PAN originale.</p>	<p>2.3.d Esaminare un campione di log di audit per confermare che il PAN è reso illeggibile oppure è stato eliminato dai log.</p>			
<p>2.4 Se si utilizza la cifratura del disco (anziché la cifratura del database a livello di file o colonna), l'accesso logico deve essere gestito in modo indipendente dai meccanismi di controllo dell'accesso al sistema operativo nativo (ad esempio, non utilizzando database di account utente locali). Le chiavi di decifratura non devono essere associate agli account utente.</p>	<p>3.4.1.a Se viene utilizzata la cifratura del disco, verificare che l'accesso logico a file system cifrati venga implementato tramite un meccanismo separato dal meccanismo dei sistemi operativi nativi (ad esempio, non utilizzando i database di account utente locali).</p>			
	<p>3.4.1.b Verificare che le chiavi crittografiche siano memorizzate in modo sicuro (ad esempio, su un supporto rimovibile adeguatamente protetto con controlli di accesso rigorosi).</p>			
	<p>3.4.1.c Verificare che i dati di titolari di carta su supporti rimovibili siano cifrati in ogni posizione di memorizzazione.</p> <p>Nota: se la cifratura su disco non è utilizzata per cifrare supporti rimovibili, sarà necessario rendere illeggibili i dati memorizzati sul supporto in questione utilizzando altri metodi.</p>			
<p>3.5 Proteggere le chiavi usate per rendere sicuri i dati dei titolari di carta da divulgazione e uso improprio:</p> <p>Nota: questo requisito riguarda anche le KEK (key-encrypting keys) usate per proteggere le chiavi di crittografia dei dati—tali KEK devono essere almeno avanzate almeno quanto la chiave di crittografia dei dati.</p>	<p>3.5 Verificare i processi per proteggere le chiavi utilizzati per la cifratura dei dati di titolari di carta da divulgazione e uso improprio effettuando quanto segue:</p>			
<p>3.5.1 Limitare l'accesso alle chiavi di crittografia al minor numero possibile di persone necessarie.</p>	<p>3.5.1 Esaminare gli elenchi di accesso utente per verificare che l'accesso alle chiavi sia consentito ad un numero limitato di persone.</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
3.5.2 Memorizzare le chiavi di crittografia in modo sicuro nel minor numero possibile di posizioni e moduli.	3.5.2.a Esaminare i file di configurazione dei sistemi per verificare che le chiavi siano memorizzate in un formato cifrato e che le KEK siano memorizzate separatamente dalle chiavi di crittografia dei dati.			
	3.5.2.b Individuare i luoghi di conservazione delle chiavi per verificare che le chiavi siano conservate nel minor numero possibile di posizioni e moduli.			
3.6 Documentare e implementare completamente tutti i processi e le procedure di gestione delle chiavi di crittografia utilizzate per la cifratura dei dati di titolari di carta, incluso quanto segue: <i>Nota: sono disponibili numerosi standard di settore per la gestione delle chiavi, tra cui il sito del NIST all'indirizzo http://csrc.nist.gov.</i>	3.6.a Verificare l'esistenza delle procedure di gestione delle chiavi per le chiavi utilizzate per la cifratura dei dati di titolari di carta.			
	3.6.b Solo per i provider di servizi: Se il provider di servizi condivide le chiavi con i propri clienti per la trasmissione o la memorizzazione dei dati dei titolari di carta, verificare che il provider di servizi fornisca ai clienti istruzioni dettagliate per l'aggiornamento, la memorizzazione e la trasmissione sicura delle chiavi dei clienti, in conformità ai successivi Requisiti da 3.6.1 a 3.6.8.			
	3.6.c Esaminare le procedure di gestione delle chiavi ed effettuare quanto segue:			
3.6.1 Generazione di chiavi di crittografia avanzata	3.6.1 Verificare che siano implementate procedure di gestione delle chiavi per richiedere la generazione di chiavi avanzate.			
3.6.2 Distribuzione di chiavi di crittografia sicure	3.6.2 Verificare che siano implementate procedure di gestione delle chiavi per richiedere la distribuzione di chiavi sicure.			
3.6.3 Memorizzazione di chiavi di crittografia sicure	3.6.3 Verificare che siano implementate procedure di gestione delle chiavi per richiedere la distribuzione di chiavi sicure.			
3.6.4 Modifiche delle chiavi di crittografia per le chiavi giunte al termine del loro periodo di validità (ad esempio, una volta trascorso un periodo di tempo definito e/o dopo la produzione da parte di una determinata chiave di una quantità definita di testo di cifratura), come specificato dal fornitore dell'applicazione associato o dal proprietario delle chiavi, ed in base alle linee guida ed alle migliori pratiche del settore (ad esempio, NIST Special Publication 800-57).	3.6.4 Verificare l'implementazione delle procedure di gestione delle chiavi per richiedere modifiche delle chiavi periodiche al termine di ciascun periodo di crittografia definito.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>3.6.5 Ritiro o sostituzione (ad esempio: archiviazione, distruzione e/o revoca) delle chiavi come ritenuto necessario in caso di indebolimento dell'integrità della chiave (ad esempio, partenza di un dipendente a conoscenza di chiavi con testo in chiaro), oppure in presenza del sospetto che le chiavi siano state compromesse.</p> <p><i>Nota: In caso di ritiro o sostituzione, le chiavi crittografiche devono essere conservate e vanno archiviate in modo sicuro (ad esempio usando una KEK). Le chiavi crittografiche archiviate dovrebbero essere usate solo per scopi di decifratura/verifica.</i></p>	<p>3.6.5.a Verificare l'implementazione delle procedure di gestione delle chiavi per ritirarle quando è stata indebolita la loro integrità.</p>			
	<p>3.6.5.b Verificare l'implementazione di procedure di gestione delle chiavi per richiedere la sostituzione delle chiavi potenzialmente o effettivamente compromesse.</p>			
	<p>3.6.5.c In caso di ritiro o sostituzione, le chiavi crittografiche vengono conservate, verificare che l'applicazione non utilizzi queste chiavi per operazioni di cifratura.</p>			
<p>3.6.6 Se si utilizzano operazioni manuali di gestione delle chiavi di crittografia con testo in chiaro, tali operazioni devono essere gestite usando "split knowledge" e controllo duale (ad esempio, rendendo necessarie due o tre persone, ciascuna a conoscenza di una sola parte della chiave, per ricostruire l'intera chiave).</p> <p><i>Nota: Esempi di operazioni manuali di gestione delle chiavi includono, senza limitazioni: la generazione, la trasmissione, il caricamento, la memorizzazione e la distruzione delle chiavi.</i></p>	<p>3.6.6 Verificare che le procedure manuali di gestione di chiavi con testo in chiaro richiedano split knowledge e controllo duale delle chiavi.</p>			
<p>3.6.7 Prevenzione di tentativi di sostituzione non autorizzata delle chiavi di crittografia</p>	<p>3.6.7 Verificare che siano implementate procedure di gestione delle chiavi per richiedere la prevenzione dai tentativi di sostituzione non autorizzata delle chiavi.</p>			
<p>3.6.8 Obbligo per custodi delle chiavi di crittografia di riconoscere in modo formale che accettano e confermano di conoscere le proprie responsabilità.</p>	<p>3.6.8 Verificare che siano implementate procedure di gestione delle chiavi per richiedere ai custodi delle chiavi di riconoscere (per iscritto o elettronicamente) che accettano e confermano di conoscere le proprie responsabilità.</p>			

Requisito 4: *Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche*

Le informazioni sensibili devono essere cifrate durante la trasmissione su reti a cui utenti non autorizzati possono accedere facilmente. Reti wireless configurate in modo errato e vulnerabilità in protocolli di cifratura e autenticazione precedenti continuano ad essere gli obiettivi di utenti non autorizzati che sfruttano tali vulnerabilità per ottenere privilegi di accesso per ambienti di dati di titolari di carta.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>4.1 Usare protocolli di crittografia e sicurezza avanzati (ad esempio, SSL/TLS, IPSEC, SSH, ecc.) per proteggere i dati dei titolari di carta sensibili quando sono trasmessi su reti pubbliche aperte.</p> <p><i>Esempi di reti pubbliche e aperte nell'ambito della valutazione PCI DSS includono, senza limitazioni:</i></p> <ul style="list-style-type: none"> ▪ Internet ▪ Tecnologie wireless ▪ Comunicazioni GSM (Global System for Mobile) ▪ GPRS (General Packet Radio Service) 	<p>4.1 Verificare l'uso di protocolli di sicurezza ogni volta che i dati dei titolari di carta sono trasmessi o ricevuti su reti pubbliche e aperte. Verificare l'utilizzo di crittografia avanzata durante la trasmissione dati, come segue:</p>			
	<p>4.1.a Selezionare un campione di transazioni al momento della ricezione e osservare l'esecuzione delle transazioni per accertarsi che i dati di titolari di carta siano cifrati durante la transazione.</p>			
	<p>4.1.b Verificare che siano accettati solo certificati e/o chiavi affidabili.</p>			
	<p>4.1.c Verificare che il protocollo sia implementato per utilizzare solo configurazioni sicure e non supporti versioni o configurazioni non sicure.</p>			
	<p>4.1.d Verificare che sia implementato il livello di cifratura corretto per la metodologia di cifratura in uso. Controllare suggerimenti/pratiche consigliate del fornitore.</p>			
	<p>4.1.e Per le implementazioni SSL/TLS:</p> <ul style="list-style-type: none"> ▪ Verificare che HTTPS venga visualizzato come parte dell'URL del browser. ▪ Verificare che nessuno dei dati di titolari di carta sia richiesto quando HTTPS non viene visualizzato nell'URL. 			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>4.1.1 Garantire che le reti wireless che trasmettono i dati di titolari di carta o connesse all'ambiente dei dati di titolari di carta utilizzano le pratiche di settore consigliate (ad esempio, IEEE 802.11i) per implementare la crittografia avanzata per l'autenticazione e la trasmissione.</p> <p><i>Nota: l'utilizzo della tecnologia WEP per controllare la sicurezza è stato vietato a partire dal 30 giugno 2010.</i></p>	<p>4.1.1 Per le reti wireless che trasmettono i dati di titolari di carta o connesse all'ambiente dei dati di titolari di carta verificare che utilizzano le pratiche di settore consigliate (ad esempio, IEEE 802.11i) per implementare la crittografia avanzata per l'autenticazione e la trasmissione.</p>			
<p>4.2 Non inviare mai PAN non cifrati mediante tecnologie di messaggistica degli utenti finali (ad esempio, e-mail, messaggistica istantanea, chat, ecc.).</p>	<p>4.2.a Verificare che il PAN sia stato reso illeggibile o sicuro con crittografia avanzata ogni volta che viene inviato mediante tecnologie di messaggistica degli utenti finali.</p>			
	<p>4.2.b Verificare l'esistenza di una politica in cui viene stabilito che i PAN non cifrati non devono essere inviati tramite tecnologie di messaggistica degli utenti finali.</p>			

Utilizzare un programma per la gestione delle vulnerabilità

Requisito 5: Utilizzare e aggiornare regolarmente il software o i programmi antivirus

I software dannosi, comunemente noti come "malware", inclusi virus, worm e cavalli di Troia, accedono alla rete durante molte attività aziendali approvate, quali la posta elettronica dei dipendenti e l'uso di Internet, computer portatili e dispositivi di memorizzazione, sfruttando così le vulnerabilità del sistema. È necessario utilizzare software antivirus su tutti i sistemi comunemente colpiti da malware per proteggerli da minacce di software dannosi presenti e future.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
5.1 Distribuire il software antivirus su tutti i sistemi comunemente colpiti da malware (in particolare PC e server).	5.1 Per un campione di componenti di sistema che include tutti i tipi di sistemi operativi comunemente colpiti da malware, verificare che il software antivirus sia stato distribuito, se applicabile.			
5.1.1 Garantire che tutti i programmi antivirus siano in grado di rilevare e rimuovere tutti i tipi di malware nonché garantire una protezione sicura.	5.1.1 Per un campione di componenti di sistema, verificare che tutti i programmi antivirus siano in grado di rilevare e rimuovere tutti i tipi di malware noti (ad esempio, virus, cavalli di Troia, worm, spyware, adware e rootkit) nonché garantire una protezione sicura.			
5.2 Garantire che tutti i meccanismi antivirus siano aggiornati, in esecuzione e in grado di generare log di audit.	5.2 Verificare che tutti i software antivirus siano aggiornati, in esecuzione e in grado di generare registri, effettuando quanto segue:			
	5.2.a Richiedere ed esaminare la politica e verificare che richieda l'aggiornamento del software antivirus e delle definizioni.			
	5.2.b Verificare che l'installazione principale del software sia impostata in modo che vengano eseguiti aggiornamenti automatici e scansioni periodiche.			
	5.2.c Per un campione di componenti di sistema che include tutti i tipi di sistema operativo comunemente colpiti da malware, verificare che siano attivati aggiornamenti automatici e scansioni periodiche.			
	5.2.d Per un campione di componenti di sistema, verificare che vengano generati registri del software antivirus e che tali registri siano conservati in base al Requisito 10.7 PCI DSS.			

Requisito 6: **Sviluppare e gestire sistemi e applicazioni protette**

Gli utenti non autorizzati sfruttano le vulnerabilità per ottenere l'accesso privilegiato ai sistemi. Molte di queste vulnerabilità sono risolte dalle patch di sicurezza dei fornitori, che devono essere installate dalle entità che gestiscono i sistemi. Tutti i sistemi critici devono disporre delle patch di software corrette più recenti per proteggere i dati dei titolari di carta da uso non autorizzato e malware.

Nota: le patch software corrette sono le patch valutate e testate in modo soddisfacente per garantire che non siano in conflitto con le configurazioni di sicurezza esistenti. Per le applicazioni sviluppate in-house, è possibile evitare numerose vulnerabilità utilizzando processi di sviluppo del sistema standard e tecniche di codifica sicure.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
6.1 Assicurare che tutti i componenti di sistema ed il software siano protetti dalle vulnerabilità note mediante l'installazione delle più recenti patch di sicurezza dei fornitori. Installare patch di sicurezza critiche entro un mese dal rilascio. Nota: è possibile adottare un approccio basato su rischio per dare priorità alle installazioni delle patch. Ad esempio, dare la massima priorità all'infrastruttura critica (dispositivi e sistemi rivolti al pubblico e database), rispetto ai dispositivi interni meno importanti, per garantire che le patch necessarie vengano installate sui sistemi e sui dispositivi ad alta priorità entro un mese e su altri dispositivi e sistemi meno importanti entro tre mesi.	6.1.a Per un campione di componenti di sistema e il software correlato, confrontare l'elenco delle patch di sicurezza installate su ogni sistema con l'elenco delle patch di sicurezza del fornitore più recenti, per verificare che siano installate le patch del fornitore correnti.			
	6.1.b Esaminare la politica per l'installazione della patch di sicurezza per verificare che venga richiesta l'installazione di tutte le nuove patch di sicurezza critiche entro un mese.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>6.2 Stabilire un processo per identificare ed assegnare una classificazione di rischio alle vulnerabilità della sicurezza recentemente rilevate.</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ <i>le classificazioni di rischio si dovrebbero basare sulle migliori pratiche del settore. Ad esempio, i criteri per la classificazione di vulnerabilità di rischio elevato possono comprendere un punteggio base CVSS di 4.0 o superiore, e/o una patch del fornitore da questi classificata come "critica", e/o una vulnerabilità che interessa un componente critico del sistema.</i> ▪ <i>La classificazione delle vulnerabilità come riportata al punto 6.2.a è considerata una delle migliori pratiche fino al 30 giugno 2012; dopo tale data, diventerà un requisito.</i> 	<p>6.2.a Consultare il personale responsabile per verificare che i processi per identificare le nuove vulnerabilità della sicurezza siano stati implementati e che a tali vulnerabilità sia assegnata una classificazione di rischio. (Le vulnerabilità di rischio più elevato, più critiche dovrebbero essere classificate almeno come "Elevate".)</p> <p>6.2.b Verificare che i processi per identificare le nuove vulnerabilità della sicurezza includano l'uso di risorse esterne per le informazioni sulla vulnerabilità della sicurezza.</p>			
<p>6.3 Sviluppare applicazioni software (interne ed esterne, ed includendo l'accesso amministrativo tramite Web alle applicazioni) in conformità agli standard PCI DSS (ad esempio, autenticazione sicura e registrazione) ed in base alle pratiche di settore consigliate. Incorporare la protezione delle informazioni per l'intera durata del ciclo di sviluppo del software. Questi processi devono includere quanto segue:</p>	<p>6.3.a Ottenere ed esaminare i processi di sviluppo del software scritti per verificare che si basino sugli standard e/o sulle migliori pratiche di settore.</p> <p>6.3.b Esaminare i processi di sviluppo del software scritti per verificare che la sicurezza delle informazioni sia inserita per l'intera durata del ciclo di sviluppo del software.</p> <p>6.3.c Esaminare i processi di sviluppo del software scritti per verificare che le applicazioni del software siano sviluppate in conformità agli standard PCI DSS.</p> <p>6.3.d Sulla base dell'analisi dei processi di sviluppo del software scritti e della consultazione di sviluppatori del software, verificare che:</p>			
<p>6.3.1 Account, ID utente e password di applicazioni personalizzate vengono rimossi prima dell'attivazione o della distribuzione di tali applicazioni ai clienti</p>	<p>6.3.1 Account, ID utente e/o password di applicazioni personalizzate vengono rimossi prima della produzione o della distribuzione di tali applicazioni ai clienti.</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>6.3.2 Il codice personalizzato viene analizzato prima del rilascio in produzione o della distribuzione ai clienti per identificare eventuali vulnerabilità.</p> <p><i>Nota: questo requisito per le analisi del codice si applica a tutti i codici personalizzati (interni ed esterni), come parte della durata del ciclo di sviluppo del sistema.</i></p> <p><i>Le analisi del codice possono essere condotte da personale interno preparato o da terze parti. Le applicazioni Web sono anche soggette a controlli aggiuntivi, se sono pubbliche, per risolvere le minacce costanti e le vulnerabilità dopo l'implementazione, secondo quanto definito nel Requisito 6.6 PCI DSS.</i></p>	<p>6.3.2.a Richiedere ed esaminare le politiche per confermare che tutte le modifiche del codice di applicazioni personalizzate devono essere analizzate (tramite processi manuali o automatici), come segue:</p> <ul style="list-style-type: none"> ▪ Le modifiche del codice vengono analizzate da utenti singoli diversi dall'autore del codice originario e da utenti esperti di tecniche di analisi del codice e pratiche di codifica sicure. ▪ L'analisi del codice garantisce che il codice venga sviluppato in base a linee guida di codifica sicure (fare riferimento al Requisito 6.5 PCI DSS). ▪ Le correzioni appropriate vengono implementate prima del rilascio. ▪ I risultati dell'analisi del codice vengono esaminati e approvati dal management prima del rilascio. 			
	<p>6.3.2.b Selezionare un campione di modifiche di applicazioni personalizzate recenti e verificare che il codice dell'applicazione venga analizzato in base al precedente punto 6.3.2.a.</p>			
<p>6.4 Seguire i processi e le procedure di controllo delle modifiche per tutte le modifiche apportate ai componenti di sistema. I processi devono includere quanto segue:</p>	<p>6.4 Sulla base dell'analisi dei processi di controllo delle modifiche, dei colloqui con gli amministratori di rete e di sistema e dell'esame dei relativi dati (documentazione della configurazione di rete, dati di produzione e test, ecc.), verificare quanto segue:</p>			
<p>6.4.1 Separare ambienti di sviluppo/test e ambienti di produzione</p>	<p>6.4.1 Gli ambienti di sviluppo/test sono separati dagli ambienti di produzione; i metodi di controllo dell'accesso adottati consentono di mantenere separati tali ambienti.</p>			
<p>6.4.2 Separare le responsabilità tra ambienti di sviluppo/test e ambienti di produzione</p>	<p>6.4.2 Esiste una separazione di responsabilità tra il personale assegnato agli ambienti di sviluppo/test e il personale assegnato all'ambiente di produzione.</p>			
<p>6.4.3 I dati di produzione (PAN attivi) sono esclusi dalle attività di test o sviluppo</p>	<p>6.4.3 I dati di produzione (PAN attivi) sono esclusi dalle attività di test o sviluppo.</p>			
<p>6.4.4 Rimuovere i dati e gli account di test prima dell'attivazione dei sistemi di produzione</p>	<p>6.4.4 Rimuovere i dati e gli account di test prima dell'attivazione dei sistemi di produzione.</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
6.4.5 Modificare le procedure di controllo per l'implementazione di patch di sicurezza e modifiche del software. Le procedure devono includere quanto segue:	6.4.5.a Verificare che le procedure di controllo delle modifiche correlate all'implementazione di patch di sicurezza e modifiche del software siano documentate e richiedano quanto previsto ai successivi punti da 6.4.5.1 a 6.4.5.4.			
	6.4.5.b Per un campione di componenti di sistema e recenti modifiche/patch di sicurezza, tenere traccia delle modifiche in base alla documentazione correlata. Per ogni modifica esaminata, effettuare quanto segue:			
6.4.5.1 Documentazione dell'impatto	6.4.5.1 Verificare che la documentazione dell'impatto sia inclusa nella documentazione di controllo delle modifiche per ciascuna modifica inserita nel campione.			
6.4.5.2 Approvazione documentata per ogni modifica effettuata da parti autorizzate.	6.4.5.2 Verificare la presenza dell'approvazione documentata delle parti autorizzate per ogni modifica inserita nel campione.			
6.4.5.3 Esecuzione del test della funzionalità per verificare che la modifica non influisca negativamente sulla sicurezza del sistema.	6.4.5.3.a Per ogni modifica inserita nel campione, verificare che sia eseguito il test della funzionalità per controllare che la modifica non influisca negativamente sulla sicurezza del sistema.			
	6.4.5.3.b Per modifiche del codice personalizzate, verificare che tutti gli aggiornamenti siano sottoposti a test per la conformità al Requisito 6.5 PCI DSS prima del rilascio in produzione.			
6.4.5.4 Procedure di back-out.	6.4.5.4 Verificare che siano pronte procedure di back-out per ogni modifica inserita nel campione.			
6.5 Sviluppare applicazioni in base a linee guida di codifica sicura. Prevenire possibili vulnerabilità del codice comuni nei processi di sviluppo del software, incluso quanto segue: Nota: le vulnerabilità elencate dal punto	6.5.a Ottenere ed esaminare i processi di sviluppo del software. Verificare che i processi richiedano la formazione su tecniche di codifica sicura per gli sviluppatori, basata sulle istruzioni e sulle migliori pratiche del settore.			
	6.5.b Consultare alcuni sviluppatori e verificarne la preparazione relativamente alle tecniche di codifica sicura.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
6.5.1 al punto 6.5.9 erano presenti nelle migliori pratiche del settore al momento della pubblicazione di questa versione degli standard PCI DSS. Tuttavia, poiché le migliori pratiche del settore per la gestione delle vulnerabilità sono state aggiornate (ad esempio, la Guida OWASP, la Top 25 SANS CWE, la Codifica Sicura CERT, ecc.), per questi requisiti è necessario utilizzare le migliori pratiche più recenti.	6.5.c. Verificare che siano in atto processi per garantire che le applicazioni non siano vulnerabili, almeno, alle seguenti minacce:			
6.5.1 Injection flaw, in particolare SQL injection. Considerare, inoltre, OS Command Injection, LDAP e XPath injection flaw, nonché altri tipi di injection flaw.	6.5.1 Injection flaw, in particolare SQL injection. (Convalidare l'input per verificare che i dati dell'utente non possono modificare il significato di comandi e query, utilizzare query parametrizzate, ecc.)			
6.5.2 Overflow del buffer	6.5.2 Overflow del buffer (Convalidare limiti di buffer e troncatura stringhe di input).			
6.5.3 Memorizzazione di dati crittografici non sicura	6.5.3 Memorizzazione di dati crittografici non sicura (impedire errori di crittografia)			
6.5.4 Comunicazioni non sicure	6.5.4 Comunicazioni non sicure (cifrare in modo appropriato tutte le comunicazioni autenticate e riservate)			
6.5.5 Gestione degli errori non corretta	6.5.5 Gestione degli errori non corretta (non perdere informazioni mediante messaggi di errore)			
6.5.6 Tutte le vulnerabilità "Elevate" identificate nel processo di identificazione delle vulnerabilità (come definito nel Requisito 6.2 PCI DSS). Nota: questo requisito è considerato una delle pratiche migliori fino al 30 giugno 2012; dopo tale data, diventerà un requisito	6.5.6 Tutte le vulnerabilità di livello elevato come individuate nel Requisito 6.2 PCI DSS.			
Nota: i requisiti da 6.5.7 a 6.5.9, riportati di seguito, si riferiscono ad applicazioni Web ed interfacce di applicazioni (interne o esterne):				

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
6.5.7 XSS (Cross-Site Scripting)	6.5.7 Cross-site scripting (XSS) (Convalidare tutti i parametri prima dell'inclusione, utilizzando sblocco contestuale, ecc.)			
6.5.8 Controllo di accesso non corretto (come riferimenti a oggetti diretti non sicuri, errore di limitazione dell'accesso URL e scansione trasversale directory)	6.5.8 Controllo di accesso non corretto, come riferimenti a oggetti diretti non sicuri, errore di limitazione di accesso URL e scansione trasversale directory (Autenticare in modo corretto utenti e modificare input. Non esporre riferimenti a oggetti interni agli utenti.)			
5.2.9 Cross-site request forgery (CSRF)	5.2.5 Cross-site request forgery (CSRF). (Non considerare sicure credenziali di autorizzazione e token inviati automaticamente dai browser).			
<p>6.6 Per le applicazioni Web esterne, assicurare una protezione costante da nuove minacce e vulnerabilità e garantire che queste applicazioni siano protette da attacchi noti mediante <i>uno</i> dei seguenti metodi:</p> <ul style="list-style-type: none"> ▪ Analisi delle applicazioni Web rivolte al pubblico tramite strumenti o metodi di valutazione della sicurezza delle applicazioni manuali o automatici, almeno una volta all'anno e dopo ogni modifica ▪ Installazione di un firewall di applicazioni Web davanti alle applicazioni Web rivolte al pubblico 	<p>6.6 Per le applicazioni Web rivolte al pubblico, garantire che <i>una</i> delle seguenti misure di protezione sia in atto:</p> <ul style="list-style-type: none"> ▪ Verificare che le applicazioni Web rivolte al pubblico vengano analizzate (tramite strumenti o metodi di valutazione della sicurezza manuali o automatici), come descritto di seguito: <ul style="list-style-type: none"> - Almeno una volta all'anno - Dopo ogni modifica - Da un'organizzazione specializzata in sicurezza delle applicazioni - Che tutte le vulnerabilità vengano corrette - Che l'applicazione venga nuovamente valutata dopo le correzioni ▪ Verificare che un firewall per applicazioni Web sia presente davanti alle applicazioni Web rivolte al pubblico per rilevare ed evitare attacchi basati su Web. <p>Nota: per "organizzazione specializzata nella sicurezza delle applicazioni" si intende una società esterna oppure un'organizzazione interna specializzata nella sicurezza delle applicazioni e in grado di dimostrare indipendenza dal team di sviluppo.</p>			

Implementazione di rigide misure di controllo dell'accesso

Requisito 7: Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario

Per garantire che solo il personale autorizzato possa accedere a dati critici, occorre mettere in atto sistemi e processi per limitare l'accesso in base alle esigenze e alle responsabilità del ruolo.

Per "solo se effettivamente necessario" si intendono situazioni in cui vengono concessi diritti di accesso solo alla quantità minima di dati e privilegi necessari per svolgere una mansione.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
7.1 Limitare l'accesso ai componenti di sistema e ai dati di titolari di carta solo alle persone che svolgono mansioni per le quali tale accesso risulta realmente necessario. Le limitazioni di accesso devono includere quanto segue:	7.1 Richiedere ed esaminare la politica scritta per il controllo dei dati e verificare che tale politica comprenda quanto segue:			
7.1.1 Limitazione dei diritti di accesso a ID utente privilegiati alla quantità minima necessaria per le responsabilità di ruolo	7.1.1 Confermare che i diritti di accesso per gli ID utente privilegiati siano limitati alla quantità minima necessaria per svolgere le responsabilità del ruolo.			
7.1.2 Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale	7.1.2 Confermare che i privilegi vengono assegnati a utenti singoli in base alla classificazione e alla funzione del relativo ruolo (anche noto come controllo dell'accesso basato su ruolo).			
7.1.3 Requisito per un'approvazione documentata delle parti autorizzate specificando i privilegi necessari.	7.1.3 Confermare che l'approvazione documentata delle parti autorizzate sia necessaria (in forma scritta o elettronica) per tutti gli accessi, e che deve specificare i privilegi necessari.			
7.1.4 Implementazione di un sistema di controllo dell'accesso automatico	7.1.4 Confermare che siano stati implementati controlli dell'accesso tramite un sistema di controllo dell'accesso automatico.			
7.2 Stabilire un sistema di controllo dell'accesso per i componenti di sistema con utenti multipli che limiti l'accesso in base all'effettiva esigenza di un utente e che sia impostato su "deny all" a meno che non sia specificatamente consentito. Il sistema di controllo dell'accesso deve includere quanto segue:	7.2 Esaminare le impostazioni del sistema e la documentazione del fornitore per verificare che un sistema di controllo dell'accesso sia implementato come segue:			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
7.2.1 Copertura di tutti i componenti di sistema	7.2.1 Confermare che siano in atto sistemi di controllo dell'accesso su tutti i componenti di sistema.			
7.2.2 Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale	7.2.2 Confermare che i sistemi di controllo dell'accesso siano configurati in modo che i privilegi vengano assegnati agli utenti in base alla classificazione e alla funzione del ruolo.			
7.2.3 Impostazione predefinita "deny-all" <i>Nota: alcuni sistemi di controllo dell'accesso sono impostati in modo predefinito su "allow-all" consentendo, pertanto, l'accesso a meno che/finché non viene scritta una regola per negare l'accesso in modo specifico.</i>	7.2.3 Confermare che i sistemi di controllo dell'accesso abbiano un'impostazione predefinita "deny-all".			

Requisito 8: Assegnare un ID univoco a chiunque abbia accesso a un computer

Assegnare un ID univoco a tutti gli utenti che dispongono dell'accesso, per garantire che ogni utente sia responsabile in modo univoco per le proprie azioni. In questo modo, le azioni effettuate su dati e sistemi critici vengono eseguite da utenti noti e autorizzati e possono essere registrate come tali.

Nota: questi requisiti sono applicabili a tutti gli account, compresi gli account dei punti vendita, con funzionalità amministrative e a tutti gli account utilizzati per visualizzare o accedere a dati dei titolari di carta o per accedere a sistemi con dati dei titolari di carta. Tuttavia, i Requisiti 8.1, 8.2 e da 8.5.8 a 8.5.15 non sono validi per account utenti all'interno di un'applicazione di pagamento dei punti vendita che ha accesso ad un solo numero di carta alla volta per facilitare una singola transazione (come gli account cassiere).

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
8.1 Assegnare a tutti gli utenti un ID univoco prima di consentire l'accesso ai componenti di sistema o ai dati di titolari di carta.	8.1 Verificare che tutti gli utenti dispongano di un ID univoco per l'accesso ai componenti di sistema o ai dati di titolari di carta.			
8.2 Oltre ad assegnare un ID univoco utilizzare almeno uno dei seguenti metodi per l'autenticazione di tutti gli utenti: <ul style="list-style-type: none"> ▪ Qualcosa che l'utente conosce, come una password o una passphrase ▪ Qualcosa in possesso dell'utente, come un dispositivo token o una smart card ▪ Qualcosa che l'utente è, come biometrico 	8.2 Per verificare che gli utenti vengano autenticati tramite un ID univoco e un altro elemento di autenticazione (ad esempio, una password) per l'accesso all'ambiente dei dati di titolari di carta, effettuare quanto segue: <ul style="list-style-type: none"> ▪ Richiedere ed esaminare la documentazione che descrive i metodi di autenticazione utilizzati. ▪ Per ogni tipo di metodo di autenticazione utilizzato e per ogni tipo di componente di sistema, osservare un'autenticazione per verificare venga eseguita nel modo documentato. 			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>8.3 Incorporare l'autenticazione a due fattori per l'accesso remoto alla rete (accesso a livello di rete dall'esterno) da parte di dipendenti, amministratori e terze parti. (Ad esempio, RADIUS (Remote Authentication and Dial-in Service) con token; TACACS (Terminal Access Controller Access Control System) con token; oppure altre tecnologie che facilitano l'autenticazione a due fattori.)</p> <p><i>Nota: L'autenticazione a due fattori richiede per l'autenticazione l'utilizzo di due dei tre metodi di autenticazione (fare riferimento al Requisito 8.2 per le descrizioni dei metodi di autenticazione). Usare due volte un fattore (ad esempio, l'uso di due password separate) non viene considerato come un'autenticazione a due fattori.</i></p>	<p>8.3 Per verificare che l'autenticazione a due fattori sia implementata per tutti gli accessi remoti alla rete, osservare la connessione remota di un dipendente (ad esempio, un amministratore) alla rete e verificare che siano utilizzati due dei tre metodi di autenticazione.</p>			
<p>8.4 Rendere illeggibili tutte le password durante la trasmissione e la memorizzazione su tutti i componenti di sistema utilizzando crittografia avanzata.</p>	<p>8.4.a Per un campione di componenti di sistema, esaminare i file di password per verificare che le password siano illeggibili durante la trasmissione e la memorizzazione.</p> <p>8.4.b Solo per i provider di servizi, osservare i file di password per verificare che le password dei clienti siano cifrate.</p>			
<p>8.5 Garantire una corretta identificazione utente e gestione delle autenticazioni per amministratori e utenti non consumatori su tutti i componenti di sistema nel seguente modo:</p>	<p>8.5 Rivedere le procedure e consultare il personale per verificare che siano implementate procedure per l'identificazione utente e la gestione delle autenticazioni, effettuando quanto segue:</p>			
<p>8.5.1 Controllare le operazioni di aggiunta, eliminazione e modifica di ID utente, credenziali e altri oggetti identificativi.</p>	<p>8.5.1 Selezionare un campione di ID utente, che includa amministratori e utenti generici. Verificare che ogni utente sia autorizzato a utilizzare il sistema in base alla politica, effettuando quanto segue:</p> <ul style="list-style-type: none"> ▪ Richiedere ed esaminare un modulo di autorizzazione per ogni ID. ▪ Verificare che gli ID utente inseriti nel campione siano 			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
	implementati secondo il modulo di autorizzazione (inclusi i privilegi specificati e tutte le firme ottenute) tenendo traccia delle informazioni per l'intero percorso dal modulo al sistema.			
8.5.2 Verificare l'identità dell'utente prima di eseguire il ripristino delle password.	8.5.2 Esaminare le procedure di password ed autenticazioni e osservare il personale responsabile della sicurezza per verificare che, se l'utente richiede il ripristino di una password per telefono, e-mail, Web o in altra forma non diretta, l'identità di tale utente venga controllata prima di ripristinare la password.			
8.5.3 Impostare la password per il primo accesso ed il ripristino su un valore univoco per ogni utente e modificarlo immediatamente dopo il primo uso.	8.5.3 Esaminare le procedure delle password e osservare il personale responsabile della sicurezza per verificare che le password per il primo accesso per i nuovi utenti, e le password di ripristino per gli utenti esistenti, siano impostate su un valore univoco per ogni utente e modificate dopo il primo uso.			
8.5.4 Revocare immediatamente l'accesso per gli utenti non attivi.	8.5.4 Selezionare un campione di utenti non attivi negli ultimi sei mesi e analizzare gli elenchi di accesso utente attuali per verificare che gli ID relativi a tali utenti siano stati disattivati o rimossi.			
8.5.5 Rimuovere/disabilitare gli account utente non attivi almeno ogni 90 giorni.	8.5.5 Verificare che gli account non attivi da oltre 90 giorni siano stati rimossi o disabilitati.			
8.5.6 Abilitare gli account utilizzati dai fornitori per la gestione in remoto solo durante il periodo di tempo necessario. Monitorare gli account per l'accesso remoto dei fornitori durante l'uso.	8.5.6.a Verificare che gli account utilizzati dai fornitori per accedere, supportare e gestire i componenti di sistema siano disabilitati e vengano abilitati solo quando necessario durante l'uso.			
	8.5.6.b Verificare che gli account per l'accesso remoto dei fornitori siano monitorati durante l'uso.			
8.5.7 Comunicare le procedure e le politiche di autenticazione a tutti gli utenti che hanno accesso ai dati dei titolari di carta.	8.5.7 Consultare gli utenti appartenenti a un campione di ID utente per verificare che siano a conoscenza delle procedure e delle politiche relative all'autenticazione.			
8.5.8 Non utilizzare account e password di gruppo, condivisi o generici, o altri metodi di autenticazione.	8.5.8.a Per un campione di componenti di sistema, esaminare gli elenchi di ID utente per verificare quanto segue: <ul style="list-style-type: none"> ▪ Gli ID e gli account utente generici sono disabilitati o rimossi. ▪ Non esistono ID utente condivisi per le attività di amministrazione del sistema e altre funzioni critiche. ▪ Gli ID utente condivisi e generici non vengono utilizzati per gestire i componenti di sistema. 			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
	8.5.8.b Esaminare le politiche/procedure di autenticazione per verificare che siano espressamente vietati le password di gruppo o condivise o altri metodi di autenticazione.			
	8.5.8.c Consultare gli amministratori di sistema per verificare che non vengano distribuite, anche se richiesto, password di gruppo o condivise o altri metodi di autenticazione.			
8.5.9 Modificare le password utente almeno ogni 90 giorni.	8.5.9.a Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password utente siano impostati in modo che ne venga richiesta la modifica almeno ogni 90 giorni.			
	8.5.9.b Solo per i provider di servizi, esaminare i processi interni e la documentazione per clienti/utenti per verificare che venga richiesta la modifica periodica delle password utenti non consumatori e che a tali utenti vengano fornite tutte le informazioni necessarie relativamente a quando e in quali circostanze occorre modificare la password.			
8.5.10 Richiedere una lunghezza minima della password di 7 caratteri.	8.5.10a Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password utente siano impostati in modo che la lunghezza minima sia di 7 caratteri.			
	8.5.10.b Solo per i provider di servizi, esaminare i processi interni e la documentazione per clienti/utenti per verificare che sia richiesto per le password di utenti non consumatori di soddisfare i requisiti di lunghezza minima.			
8.5.11 Utilizzare password contenenti valori numerici e alfabetici.	8.5.11.a Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password siano impostati in modo che vengano richieste password composte da valori numerici e alfabetici.			
	8.5.10.b Solo per i provider di servizi, esaminare i processi interni e la documentazione per clienti/utenti per verificare che sia richiesto che le password di utenti non consumatori siano composte da valori numerici e alfabetici.			
8.5.12 Non consentire l'invio di una nuova password uguale a una delle ultime quattro password utilizzate.	8.5.12.a Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password siano impostati in modo			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
	che vengano richieste nuove password diverse dalle ultime quattro password utilizzate.			
	8.5.12.b Solo per i provider di servizi, esaminare i processi interni e la documentazione per clienti/utenti per verificare che le nuove password di utenti non consumatori siano diverse dalle ultime quattro password utilizzate.			
8.5.13 Limitare i tentativi di accesso ripetuti bloccando l'ID utente dopo un massimo di sei tentativi.	8.5.13.a Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che i parametri di autenticazione siano impostati in modo che venga richiesto il blocco dell'account utente dopo un massimo di sei tentativi di accesso.			
	8.5.13.b Solo per i provider di servizi, esaminare i processi interni e la documentazione per clienti/utenti per verificare che gli account utenti non consumatori siano temporaneamente bloccati dopo un massimo di sei tentativi di accesso.			
8.5.14 Impostare la durata del blocco a un minimo di 30 minuti o finché l'amministratore non abilita l'ID utente.	8.5.14 Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password siano impostati in modo che venga richiesto il blocco dell'account utente per almeno 30 minuti o finché l'amministratore non ripristina l'account.			
8.5.15 Se una sessione è inattiva per più di 15 minuti, è necessario che l'utente autentichi di nuovo il terminale o la sessione.	8.5.15 Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che la funzione del periodo di inattività del sistema/sessione sia stata impostata al massimo su 15 minuti.			
8.5.16 Autenticare tutti gli accessi al database contenente i dati di titolari di carta. Sono compresi gli accessi da applicazioni, amministratori e tutti gli altri utenti. Consentire l'accesso diretto utente o le query ai database solo agli amministratori del database.	8.5.16.a Esaminare le impostazioni di configurazione del database e dell'applicazione e verificare che venga eseguita l'autenticazione utente prima dell'accesso.			
	8.5.16.b Verificare che le impostazioni di configurazione del database e dell'applicazione assicurino che tutti gli accessi, le query e le azioni dell'utente (ad esempio, spostamento, copia, eliminazione) sul database si verificano solo tramite metodi programmatici (ad esempio, procedure memorizzate).			
	8.5.16.c Verificare che le impostazioni di configurazione del database e dell'applicazione consentano l'accesso diretto utente e le query ai database solo agli amministratori del database.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
	8.5.16.d Esaminare le applicazioni del database e gli ID di applicazione correlati per verificare che tali ID possano essere utilizzati solo dalle applicazioni e non da utenti singoli o altri processi.			

Requisito 9: Limitare l'accesso fisico ai dati dei titolari di carta

Gli accessi fisici ai dati o ai sistemi che ospitano i dati di titolari di carta offrono la possibilità di accedere ai dispositivi o ai dati e di rimuovere i sistemi o le copie cartacee; pertanto dovrebbero essere limitati in modo appropriato. Ai fini del Requisito 9, per "personale in sede" si intendono le persone assunte a tempo pieno o part-time, le persone con contratto a tempo determinato, i collaboratori o i consulenti che sono fisicamente presenti presso i locali dell'entità. Per "visitatore" si intende un fornitore, un ospite del personale in sede, un tecnico dell'assistenza o chiunque abbia necessità di accedere alla struttura per un breve periodo di tempo, solitamente non più di un giorno. Per "supporti" si intendono tutti i supporti cartacei ed elettronici contenenti i dati dei titolari di carta.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
9.1 Utilizzare i controlli dell'accesso alle strutture appropriati per limitare e monitorare gli accessi fisici ai sistemi nell'ambiente dei dati di titolari di carta.	<p>9.1 Verificare la presenza di controlli di sicurezza fisica per ogni area computer, centro dati e altre aree fisiche con sistemi nell'ambiente dei dati di titolari di carta.</p> <ul style="list-style-type: none"> ▪ Verificare che l'accesso sia controllato da lettori di tessere magnetiche o altri dispositivi, incluse tessere magnetiche autorizzate e lucchetti con chiavi. ▪ Osservare un tentativo di accesso dell'amministratore del sistema a console per sistemi selezionati casualmente nell'ambiente dei dati di titolari di carta e verificare che siano "sotto chiave" per impedire l'uso non autorizzato. 			
<p>9.1.1 Utilizzare videocamere o altri meccanismi di controllo dell'accesso per monitorare gli accessi fisici ad aree sensibili. Esaminare i dati raccolti e correlarli con altri. Conservare i dati per almeno tre mesi, se non diversamente richiesto dalle leggi in vigore.</p> <p><i>Nota: per "aree sensibili" si intende centri dati, aree server e aree che ospitano sistemi di memorizzazione, elaborazione o trasmissione dei dati di titolari di carta. Ciò esclude le aree in cui vi sono i terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio.</i></p>	9.1.1.a Verificare che siano presenti videocamere e/o altri meccanismi di controllo dell'accesso per monitorare i punti di ingresso/uscita ad aree sensibili.			
	9.1.1.b Verificare che videocamere e/o altri meccanismi di controllo dell'accesso siano protetti da manomissione o disattivazione.			
	9.1.1.c Verificare che videocamere e/o altri meccanismi di controllo dell'accesso siano monitorati e che i dati delle videocamere o di altri meccanismi vengano conservati per almeno tre mesi.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>9.1.2 Limitare l'accesso fisico a connettori di rete accessibili pubblicamente.</p> <p>Ad esempio, nelle aree accessibili ai visitatori non dovrebbero essere attivate porte di rete a meno che l'accesso alla rete non sia espressamente autorizzato.</p>	<p>9.1.2 Verificare, tramite consultazione con gli amministratori di rete e osservazione che i connettori di rete vengano attivati solo se necessario da parte di personale in sede autorizzato. In alternativa, verificare che i visitatori siano scortati costantemente nelle aree con connettori di rete attivi.</p>			
<p>9.1.3 Limitare l'accesso fisico a punti di accesso wireless, gateway, dispositivi portatili, hardware di rete e comunicazione e linee di telecomunicazione.</p>	<p>9.1.3 Verificare che sia opportunamente limitato l'accesso fisico a punti di accesso wireless, gateway, dispositivi portatili, hardware di rete e comunicazione e linee di telecomunicazione.</p>			
<p>9.2 Sviluppare procedure che consentono di distinguere facilmente tra personale in sede e visitatori, in particolare in aree che permettono l'accesso ai dati di titolari di carta.</p>	<p>9.2.a Esaminare i processi e le procedure per l'assegnazione delle tessere magnetiche a personale in sede e visitatori e verificare che tali processi includano quanto segue:</p> <ul style="list-style-type: none"> ▪ Concessione di nuove tessere magnetiche, ▪ Modifica dei requisiti di accesso, e ▪ Revoca per il personale in sede che ha lasciato l'azienda e tessere magnetiche per visitatori scadute 			
	<p>9.2.b Verificare che l'accesso al sistema delle tessere magnetiche sia limitato al personale autorizzato.</p>			
	<p>9.2.c Esaminare le tessere magnetiche in uso per verificare che identificano in modo chiaro i visitatori e che sia facile distinguere il personale in sede dai visitatori.</p>			
<p>9.3 Accertarsi che tutti i visitatori vengano gestiti nel modo seguente:</p>	<p>9.3 Verificare che siano in atto controlli sui visitatori come segue:</p>			
<p>9.3.1 Siano autorizzati prima di accedere alle aree in cui i dati di titolari di carta sono elaborati o custoditi.</p>	<p>9.3.1 Osservare l'uso di tessere magnetiche di identificazione per i visitatori per verificare che tali tessere non consentano l'accesso senza scorta ad aree fisiche in cui sono conservati i dati dei titolari di carta.</p>			
<p>9.3.2 Ricevano un token fisico (ad esempio, una tessera magnetica o un dispositivo di accesso) con scadenza, che identifica i visitatori come non</p>	<p>9.3.2.a Osservare le persone all'interno della struttura per verificare l'uso di tessere magnetiche di identificazione per i visitatori e che sia possibile distinguere facilmente i visitatori dal personale in sede.</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
personale in sede.	9.3.2.b Verificare che le tessere magnetiche per i visitatori abbiano una scadenza.			
9.3.3 Restituiscano il token fisico prima di lasciare la struttura o in corrispondenza della data di scadenza.	9.3.3 Osservare i visitatori che lasciano la struttura per verificare che venga loro richiesta la restituzione della tessera magnetica di identificazione all'uscita o al momento della scadenza.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
9.4 Utilizzare un registro visitatori per conservare un audit trail fisico dell'attività dei visitatori. Documentare il nome del visitatore, l'azienda rappresentata e il personale in sede che autorizza l'accesso fisico sul registro. Conservare questo registro per almeno tre mesi, se non diversamente richiesto dalla legge.	9.4.a Verificare che l'uso di un registro dei visitatori sia in atto per registrare gli accessi fisici alla struttura nonché alle aree computer e ai centri dati in cui vengono memorizzati o trasmessi i dati di titolari di carta.			
	9.4.b Verificare che il registro contenga il nome del visitatore, l'azienda rappresentata e il personale in sede che autorizza l'accesso fisico e che tale registro venga conservato per almeno tre mesi.			
9.5 Conservare i backup dei supporti in un luogo sicuro, preferibilmente in una struttura esterna, come un luogo alternativo di backup oppure un magazzino. Controllare la sicurezza del luogo almeno una volta all'anno.	9.5.a Osservare la sicurezza fisica del luogo di conservazione per confermare che la conservazione dei supporti di backup sia sicura.			
	9.5.b Verificare che la sicurezza del luogo di conservazione sia rivista almeno una volta all'anno.			
9.6 Proteggere fisicamente tutti i supporti.	9.6 Verificare che nelle procedure per la protezione dei dati dei titolari di carta siano compresi controlli per proteggere fisicamente tutti i supporti (inclusi, senza limitazioni, computer, supporti elettronici rimovibili, ricevute cartacee, resoconti cartacei e fax).			
9.7 Mantenere un rigido controllo sulla distribuzione interna o esterna di qualsiasi tipo di supporto, incluso quanto segue:	9.7 Verificare che esista una politica di controllo della distribuzione dei supporti e che tale politica copra tutti i supporti distribuiti inclusi quelli distribuiti a singoli utenti.			
9.7.1 Classificare i supporti in modo che si possa determinare la sensibilità dei dati.	9.7.1 Verificare che tutti i supporti siano classificati in modo da poter determinare la sensibilità dei dati.			
9.7.2 Inviare il supporto tramite un corriere affidabile o un altro metodo di consegna che possa essere monitorato in modo appropriato.	9.7.2 Verificare tutti i supporti inviati all'esterno della struttura siano registrati e autorizzati dal management e che vengano inviati tramite corriere affidabile o un altro metodo di consegna monitorato in modo appropriato.			
9.8 Accertarsi che il management approvi tutti i supporti che vengono spostati da un'area protetta (in particolare quando i supporti vengono distribuiti a singoli utenti).	9.8 Selezionare un campione recente di alcuni giorni dei registri di controllo fuori sede per tutti i supporti e verificare la presenza dei dettagli di controllo e dell'autorizzazione appropriata del management.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
9.9 Mantenere un rigido controllo sulla conservazione e sull'accessibilità dei supporti.	9.9 Richiedere ed esaminare la politica per il controllo della memorizzazione e della gestione di tutti i supporti e verificare che tale politica richieda l'esecuzione di inventari dei supporti periodici.			
9.9.1 Conservare in modo appropriato i registri di inventario per tutti i supporti ed eseguire tali inventari almeno una volta all'anno.	9.9.1 Richiedere ed esaminare il registro di inventario dei supporti per verificare che vengano eseguiti periodicamente inventari dei supporti almeno una volta all'anno.			
9.10 Distruggere i supporti quando non sono più necessari per scopi aziendali o legali, come segue:	9.10 Richiedere ed esaminare la politica di distruzione dei supporti periodica e verificare che tale politica copra tutti i supporti e confermare quanto riportato di seguito:			
9.10.1 Stracciare, bruciare o mandare al macero i materiali cartacei in modo che i dati di titolari di carta non possano essere ricostruiti.	9.10.1.a Verificare che i materiali cartacei vengano stracciati tramite trinciatrice, bruciati o macerati in modo da garantire ragionevolmente che tali materiali non potranno essere ricostruiti.			
	9.10.1.b Esaminare i contenitori utilizzati per le informazioni da distruggere per verificare che siano sicuri. Ad esempio, verificare che un contenitore per "informazioni da distruggere" disponga di un dispositivo di blocco che impedisce l'accesso al contenuto.			
9.10.2 Rendere i dati di titolari di carta su supporti elettronici non recuperabili, in modo che non sia possibile ricostruirli.	9.10.2 Verificare che i dati di titolari di carta su supporti elettronici vengano resi irrecuperabili tramite un programma di pulizia basato su standard di settore accettati per l'eliminazione sicura oppure distruggere fisicamente i supporti (ad esempio, smagnetizzandoli).			

Monitoraggio e test delle reti regolari

Requisito 10: Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta

I meccanismi di accesso e la possibilità di tenere traccia delle attività degli utenti sono di fondamentale importanza per impedire, rilevare o ridurre al minimo l'impatto di una compromissione di dati. La presenza dei registri in tutti gli ambienti consente di tenere traccia, dare l'allarme ed eseguire un'analisi quando si verifica un problema. Senza registri di attività del sistema, è molto difficile determinare la causa di una compromissione di dati.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
10.1 Stabilire un processo per collegare tutti gli accessi ai componenti di sistema (in particolare l'accesso eseguito con privilegi di amministratore, ad esempio come utente root) a ciascun utente.	10.1 Verificare tramite osservazione e consultazione dell'amministratore di sistema che gli audit trail siano attivi e funzionanti per i componenti di sistema.			
10.2 Implementare audit trail automatici per tutti i componenti di sistema per ricostruire i seguenti eventi:	10.2 Tramite consultazioni ed esami dei registri di audit e delle relative impostazioni, effettuare quanto segue:			
10.2.1 Tutti gli accessi utente ai dati di titolari di carta	10.2.1 Verificare che tutti gli accessi utente ai dati di titolari di carta siano registrati.			
10.2.2 Tutte le azioni intraprese da un utente con privilegi di utente root o amministratore	10.2.2 Verificare che siano registrate tutte le azioni intraprese da un utente con privilegi di utente root o amministratore.			
10.2.3 Accesso a tutti gli audit trail	10.2.3 Verificare che l'accesso a tutti gli audit trail sia registrato.			
10.2.4 Tentativi di accesso logico non validi	10.2.4 Verificare che siano registrati i tentativi di accesso logico non validi.			
10.2.5 Uso dei meccanismi di identificazione e autenticazione	10.2.5 Verificare che l'uso dei meccanismi di identificazione e autenticazione sia registrato.			
10.2.6 Inizializzazione dei registri di audit	10.2.6 Verificare che sia registrata l'inizializzazione dei registri di audit.			
10.2.7 Creazione ed eliminazione di oggetti a livello di sistema	10.2.7 Verificare che la creazione e l'eliminazione di oggetti a livello di sistema siano registrate.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
10.3 Registrare almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento:	10.3 Eseguire quanto indicato di seguito, tramite consultazioni e osservazione, per ogni evento inseribile nell'audit (da 10.2):			
10.3.1 Identificazione utente	10.3.1 Verificare che l'identificazione utente sia inclusa nelle voci di registro.			
10.3.2 Tipo di evento	10.3.2 Verificare che il tipo di evento sia incluso nelle voci di registro.			
10.3.3 Data e ora	10.3.3 Verificare che data e ora siano incluse nelle voci di registro.			
10.3.4 Indicazione di successo o fallimento	10.3.4 Verificare che l'indicazione di successo o fallimento sia inclusa nelle voci di registro.			
10.3.5 Origine dell'evento	10.3.5 Verificare che l'origine dell'evento sia inclusa nelle voci di registro.			
10.3.6 Identità o nome dell'elemento interessato (dati, componente di sistema o risorsa)	10.3.6 Verificare che l'identità o il nome dell'elemento interessato (dati, componente di sistema o risorsa) sia inclusa nelle voci di registro.			
10.4 Utilizzando la tecnologia per la sincronizzazione dell'ora, sincronizzare tutti gli orologi e gli orari critici del sistema ed assicurare che sia implementato quanto segue per l'acquisizione, la distribuzione e la memorizzazione dell'ora. Nota: NTP (Network Time Protocol) è un esempio di tecnologia per la sincronizzazione dell'ora.	10.4.a Verificare che la tecnologia per la sincronizzazione dell'ora sia implementata e tenuta aggiornata in base ai 6.1 e 6.2 Requisiti PCI DSS.			
	10.4.b Richiedere ed esaminare il processo di acquisizione, distribuzione e memorizzazione dell'ora esatta all'interno dell'organizzazione e, per un campione di componenti di sistema, esaminare le impostazioni di parametri del sistema correlate all'orario. Verificare che quanto indicato di seguito sia incluso nel processo e implementato:			
10.4.1 I sistemi critici hanno l'ora esatta e coerente.	10.4.1.a Verificare che solo i server di rilevamento dell'orario centrali designati ricevono i segnali orari da sorgenti esterne e che tali segnali si basino su International Atomic Time o UTC.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
	10.4.1.b Verificare che i server per il rilevamento dell'orario centrali designati comunicano tra loro per mantenere un orario esatto e che altri server interni ricevono l'orario solo dai server centrali.			
10.4.2 I dati dell'ora sono protetti.	10.4.2.a Esaminare le configurazioni di sistema e le impostazioni per la sincronizzazione dell'ora per verificare che l'accesso ai dati dell'ora sia limitato solo al personale per il quale l'accesso a tali dati sia effettivamente necessario.			
	10.4.2.b Esaminare le configurazioni di sistema e le impostazioni ed i processi per la sincronizzazione dell'ora per verificare che ogni modifica alle impostazioni dell'ora su sistemi critici sia registrata, monitorata ed esaminata.			
10.4.3 Le impostazioni dell'ora sono ricevute da sorgenti per l'orario accettate dal settore.	10.4.3 Verificare che i server di rilevamento dell'orario accettino gli aggiornamenti di ora da specifiche sorgenti esterne accettate dal settore (per evitare che utenti non autorizzati modifichino l'ora). Facoltativamente, tali aggiornamenti possono essere cifrati con una chiave simmetrica ed è possibile creare elenchi di controllo dell'accesso che specifichino gli indirizzi IP dei computer client ai quali verranno forniti gli aggiornamenti di ora (per evitare un uso non autorizzato dei server di rilevamento dell'ora interni).			
10.5 Proteggere gli audit trail in modo che non possano essere modificati.	10.5 Consultare l'amministratore di sistema ed esaminare le autorizzazioni per verificare che gli audit trail siano protetti e non possano essere modificati, come segue:			
10.5.1 Limitare la visualizzazione degli audit trail a coloro che realmente necessitano di tali informazioni per scopi aziendali.	10.5.1 Verificare che solo coloro che necessitano di tali informazioni per scopi aziendali possano visualizzare i file di audit trail.			
10.5.2 Proteggere i file di audit trail da modifiche non autorizzate.	10.5.2 Verificare che i file di audit trail correnti siano protetti da modifiche non autorizzate tramite meccanismi di controllo dell'accesso, separazione fisica e/o di rete.			
10.5.3 Eseguire immediatamente il backup dei file di audit trail su un server di registro centralizzato o un supporto difficile da modificare.	10.5.3 Verificare che venga eseguito immediatamente il backup dei file di audit trail su un server di registro centralizzato o un supporto difficile da modificare.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
10.5.4 Scrivere registri per tecnologie rivolte al pubblico su un server di registro sulla LAN interna.	10.5.4 Verificare che i registri per le tecnologie rivolte al pubblico (ad esempio, wireless, firewall, DNS, e-mail) vengano scaricati o copiati su un server di registro interno centralizzato o un supporto sicuro.			
10.5.5 Utilizzare un meccanismo di monitoraggio dell'integrità dei file o un software di rilevamento delle modifiche sui registri per accertarsi che i dati di registro esistenti non possano essere modificati senza generare avvisi (sebbene l'aggiunta di nuovi dati non dovrebbe generare avvisi).	10.5.5 Verificare l'uso di un software di monitoraggio dell'integrità dei file o di rilevamento delle modifiche per i registri esaminando le impostazioni di sistema, i file monitorati e i risultati delle attività di monitoraggio.			
10.6 Esaminare i registri per tutti i componenti di sistema almeno una volta al giorno. Le revisioni dei registri devono includere i server che eseguono funzioni di sicurezza, quali i servizi antintrusione IDS (Intrusion Detection System), i server AAA (Autenticazione, Autorizzazione e Accounting), ad esempio RADIUS. <i>Nota: gli strumenti di raccolta, analisi e generazione di avvisi per i log possono essere utilizzati ai fini della conformità al requisito 10.6.</i>	10.6.a Richiedere ed esaminare le politiche e le procedure di sicurezza per verificare che includano l'analisi dei registri di sicurezza su base giornaliera e che venga richiesto un intervento per le eccezioni.			
	10.6.b Verificare che vengano eseguite revisioni dei registri regolari per tutti i componenti di sistema, tramite osservazione e consultazioni.			
10.7 Conservare la cronologia dell'audit trail per almeno un anno, con un minimo di tre mesi di disponibilità immediata per l'analisi (ad esempio, online, archiviazione o recuperabile da backup).	10.7.a Richiedere ed esaminare le politiche e le procedure di sicurezza e verificare che includano politiche per la conservazione del registro di audit per almeno un anno.			
	10.7.b Verificare che i registri di audit siano disponibili per almeno un anno e che siano in atto processi di recupero dei registri degli ultimi tre mesi per eseguire un'analisi.			

Requisito 11: Eseguire regolarmente test di sistemi e processi di protezione.

Nuove vulnerabilità vengono scoperte continuamente da utenti non autorizzati e ricercatori e introdotte da nuovo software. I componenti di sistema, i processi e il software personalizzato devono essere sottoposti frequentemente a test per garantire un allineamento dei controlli di sicurezza a un ambiente in continua evoluzione.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>11.1 Verificare la presenza di punti di accesso wireless e rilevare punti di accesso wireless non autorizzati almeno su base trimestrale.</p> <p><i>Nota: I metodi che si possono utilizzare nel processo comprendono, senza limitazioni, scansioni della rete wireless, controlli di tipo fisico e logico di infrastrutture e componenti di sistema, NAC (Network Access Control) o IDS/IPS wireless.</i></p> <p><i>Qualunque sia il metodo adottato, questo deve essere in grado di rilevare ed identificare qualsiasi dispositivo non autorizzato.</i></p>	<p>11.1.a Verificare che l'entità disponga di un processo documentato per rilevare ed identificare punti di accesso wireless su base trimestrale.</p>			
	<p>11.1.b Verificare l'adeguatezza della metodologia per rilevare ed identificare punti di accesso wireless non autorizzati, compreso almeno quanto segue:</p> <ul style="list-style-type: none"> ▪ Schede WLAN inserite nei componenti di sistema ▪ Dispositivi portatili wireless collegati a componenti di sistema (ad esempio, via USB, ecc.) ▪ Dispositivi wireless collegati ad una porta o a un dispositivo di rete 			
	<p>11.1.c Verificare che il processo documentato per identificare punti di accesso wireless non autorizzati venga eseguito almeno ogni tre mesi per tutte le strutture e i componenti di sistema.</p>			
	<p>11.1.d In caso di utilizzo di monitoraggio automatico (ad esempio, IDS/IPS wireless, NAC, ecc.), verificare che la configurazione generi avvisi per il personale.</p>			
	<p>11.1.e Verificare che il piano di risposta agli incidenti aziendale (Requisito 12.9) includa una risposta in caso di rilevamento di dispositivi wireless non autorizzati.</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>11.2 Eseguire scansioni di vulnerabilità della rete interne ed esterne almeno una volta ogni tre mesi e dopo ogni cambiamento significativo apportato alla rete (ad esempio, installazione di nuovi componenti di sistema, modifica della topologia della rete, modifica delle regole del firewall o aggiornamento di un prodotto).</p> <p><i>Nota: non è necessario completare quattro scansioni trimestrali per la conformità iniziale a PCI DSS, se il valutatore verifica che 1) il risultato della scansione più recente era positivo, 2) l'entità dispone di politiche e procedure documentate che richiedono l'esecuzione di scansioni trimestrali e 3) ogni vulnerabilità rilevata dalla scansione è stata corretta nel modo dimostrato da una nuova scansione. Per gli anni successivi alla scansione PCI DSS iniziale, è necessario eseguire quattro scansioni trimestrali con esito positivo.</i></p>	<p>11.2 Verificare che le scansioni di vulnerabilità interne ed esterne vengano eseguite come segue:</p>			
<p>11.2.1 Eseguire scansioni di vulnerabilità interne ogni tre mesi.</p>	<p>11.2.1.a Esaminare i rapporti delle scansioni e verificare che siano state eseguite quattro scansioni interne trimestrali negli ultimi 12 mesi.</p>			
	<p>11.2.1.b Esaminare i rapporti delle scansioni e verificare che il processo di scansione prevede l'esecuzione di ulteriori scansioni finché non vengono ottenuti risultati positivi, o siano state risolte tutte le vulnerabilità "Elevate" in base alla definizione contenuta nel Requisito 6.2 PCI DSS.</p>			
	<p>11.2.1.c Convalidare che la scansione sia stata eseguita da una risorsa interna o da una terza parte qualificata e che chi esegue la scansione sia indipendente dall'organizzazione, ove possibile (non necessariamente un QSA o un ASV).</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>11.2.2 Far eseguire le scansioni esterne della vulnerabilità trimestrali ad un fornitore di scansioni approvato (ASV) autorizzato da PCI SSC.</p> <p><i>Nota: le scansioni esterne delle vulnerabilità trimestrali devono essere eseguite da un fornitore di scansioni approvato (ASV) e autorizzato da PCI SSC. Le scansioni dopo le modifiche della rete possono essere eseguite da personale interno.</i></p>	<p>11.2.2.a Esaminare l'output degli ultimi quattro trimestri di scansioni esterne delle vulnerabilità e verificare che sono state realizzate quattro scansioni trimestrali negli ultimi 12 mesi.</p>			
	<p>11.2.2.b Esaminare i risultati di ogni scansione trimestrale per verificare che soddisfino i requisiti della Guida del programma per i fornitori di scansioni approvati (ad esempio, nessuna vulnerabilità classificata superiore a 4.0 dal CVSS e nessun errore automatico).</p>			
	<p>11.2.2.c Esaminare i rapporti delle scansioni per verificare che le scansioni siano state eseguite da un ASV autorizzato da PCI SSC.</p>			
<p>11.2.3 Eseguire scansioni interne ed esterne dopo ogni modifica significativa.</p> <p><i>Nota: Le scansioni dopo le modifiche possono essere eseguite da personale interno.</i></p>	<p>11.2.3.a Esaminare la documentazione di controllo delle modifiche e i rapporti delle scansioni per verificare l'esecuzione della scansione per i componenti di sistema che hanno subito modifiche significative.</p>			
	<p>11.2.3.b Esaminare i rapporti delle scansioni per verificare che il processo di scansione preveda l'esecuzione di ulteriori scansioni fino a quando:</p> <ul style="list-style-type: none"> ▪ Per le scansioni esterne, non esistano vulnerabilità a cui sia assegnato un punteggio superiore a 4.0 da parte del CVSS, ▪ Per le scansioni interne, sia stato conseguito un risultato positivo oppure siano state risolte tutte le vulnerabilità "Elevate" in base alle definizioni contenute nel Requisito 6.2 PCI DSS. 			
	<p>11.2.3.c Convalidare che la scansione sia stata eseguita da una risorsa interna o da una terza parte qualificata e che chi esegue la scansione sia indipendente dall'organizzazione, ove possibile (non necessariamente un QSA o un ASV).</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
11.3 Eseguire test di penetrazione esterna ed interna almeno una volta all'anno e dopo ogni aggiornamento o modifica significativa dell'infrastruttura o dell'applicazione (quale un aggiornamento del sistema operativo, l'aggiunta all'ambiente di una subnet o di un server Web). Questi test di penetrazione devono includere quanto segue:	11.3.a Richiedere ed esaminare i risultati dell'ultimo test di penetrazione per verificare che tali test vengano eseguiti almeno una volta all'anno e dopo ogni modifica significativa dell'ambiente.			
	11.3.b Verificare che le vulnerabilità rilevate sfruttabili siano state corrette e il test ripetuto.			
	11.3.b Verificare che il test sia stato eseguito da una risorsa interna o da una terza parte qualificata e che chi esegue il test sia indipendente dall'organizzazione, ove possibile (non necessariamente un QSA o un ASV).			
11.3.1 Test di penetrazione a livello di rete	11.3.1 Verificare che il test di penetrazione includa anche i test di penetrazione a livello di rete. Tali test devono includere i componenti che supportano le funzioni di rete nonché i sistemi operativi.			
11.3.2 Test di penetrazione a livello di applicazione	11.3.1 Verificare che il test di penetrazione includa anche i test di penetrazione a livello di applicazione. I test devono includere almeno le vulnerabilità elencate nel Requisito 6.5.			
11.4 Utilizzare sistemi di rilevamento e/o di prevenzione delle intrusioni per monitorare tutto il traffico in corrispondenza del perimetro dell'ambiente dei dati di titolari di carta nonché ai punti critici all'interno dell'ambiente stesso e segnalare possibili rischi al personale addetto. Mantenere aggiornati tutti i sistemi, basi e firme di rilevamento e prevenzione delle intrusioni.	11.4.a Verificare l'uso di sistemi di rilevamento e/o di prevenzione delle intrusioni ed il monitoraggio di tutto il traffico in corrispondenza del perimetro dell'ambiente dei dati di titolari di carta nonché ai punti critici all'interno dell'ambiente stesso.			
	11.4.b Confermare che i dispositivi IDS e/o IPS siano configurati per segnalare possibili compromissioni al personale.			
	11.4.c Esaminare le configurazioni IDS/IPS e confermare che i dispositivi IDS/IPS vengano configurati, conservati e aggiornati secondo le istruzioni del fornitore per garantire una protezione ottimale.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>11.5 Distribuire gli strumenti di monitoraggio dell'integrità dei file per segnalare al personale modifiche non autorizzate di file system, file di configurazione o file di contenuto critici; inoltre, configurare il software in modo che esegua confronti di file critici almeno una volta alla settimana.</p> <p><i>Nota: ai fini del monitoraggio dell'integrità dei file, i file critici sono solitamente file che non cambiano frequentemente, ma la cui modifica può indicare la compromissione, effettiva o potenziale, del sistema. In genere, i prodotti per il monitoraggio dell'integrità dei file sono preconfigurati con file critici per il sistema operativo in uso. Altri file critici, ad esempio quelli per applicazioni personalizzate, devono essere valutati e definiti dall'entità (ossia dall'esercente o dal provider di servizi).</i></p>	<p>11.5.a Verificare l'uso degli strumenti di monitoraggio dell'integrità dei file all'interno dell'ambiente dei dati di titolari di carta osservando le impostazioni del sistema e i file monitorati ed esaminando i risultati delle attività di monitoraggio.</p> <p>Esempi di file che devono essere monitorati:</p> <ul style="list-style-type: none"> ▪ Eseguibili di sistema ▪ Eseguibili di applicazioni ▪ File di configurazione e parametri ▪ File memorizzati centralmente, di cronologia o archiviazione, di registro e audit 			
	<p>11.5.b Verificare che gli strumenti siano configurati per segnalare al personale modifiche non autorizzate a file critici ed eseguire confronti di file critici almeno una volta alla settimana.</p>			

Gestire una politica di sicurezza delle informazioni

Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale.

Una politica di sicurezza rigida definisce il livello di sicurezza per l'intera entità e spiega al personale quali sono le aspettative nei loro confronti in termini di sicurezza. Tutto il personale deve essere a conoscenza della sensibilità dei dati e delle proprie responsabilità in termini di protezione. Ai fini del Requisito 12, per "personale" si intende un dipendente a tempo pieno o part-time, un dipendente con contratto a tempo determinato, un collaboratore o consulente che svolge le sue prestazioni in sede o che abbia in altro modo accesso all'ambiente dei dati dei titolari di carta.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
12.1 Stabilire, pubblicare, conservare e rendere disponibile una politica di sicurezza conforme a quanto indicato di seguito:	12.1 Esaminare la politica di sicurezza delle informazioni e verificare che venga pubblicata e resa disponibile a tutto il personale interessato (inclusi fornitori e partner aziendali).			
12.1.1 Risponde a tutti i requisiti PCI DSS.	12.1.1 Verificare che la politica risponda a tutti i requisiti PCI DSS.			
12.1.2 Include un processo annuale che identifica minacce e vulnerabilità e che consente di ottenere una valutazione dei rischi formale. (Esempi di metodologie per la valutazione dei rischi includono, senza limitazioni, OCTAVE, ISO 27005 e NIST SP 800-30.)	12.1.2.a Verificare che sia documentato un processo per la valutazione dei rischi annuale che identifichi minacce, vulnerabilità e che consenta di ottenere una valutazione dei rischi formale.			
	12.1.2.b Esaminare la documentazione per la valutazione dei rischi per verificare che il processo per la valutazione dei rischi venga eseguito con cadenza almeno annuale.			
12.1.3 Includa una revisione almeno annuale ed esegua gli aggiornamenti quando si apportano modifiche all'ambiente.	12.1.3 Verificare che la politica di sicurezza delle informazioni venga analizzata almeno una volta all'anno e venga aggiornata per riflettere i cambiamenti negli obiettivi aziendali o nell'ambiente a rischio.			
12.2 Sviluppare procedure di sicurezza operativa giornaliere coerenti con i requisiti di questa specifica (ad esempio, procedure per la manutenzione degli account utente e procedure di revisione dei registri).	12.2 Esaminare le procedure di sicurezza operative giornaliere. Verificare che siano coerenti con la presente specifica e che includano procedure tecniche e amministrative per ogni requisito.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
12.3 Sviluppare politiche che regolano l'uso per le tecnologie critiche (ad esempio, tecnologie di accesso remoto, wireless, supporti elettronici rimovibili, laptop, tablet, PDA, uso della posta elettronica e di Internet) e definire l'uso corretto di queste tecnologie. Accertarsi che tali politiche richiedano quanto segue:	12.3 Richiedere ed esaminare le politiche che regolano l'uso per le tecnologie critiche ed eseguire quanto segue:			
12.3.1 Approvazione esplicita delle parti autorizzate	12.3.1 Verificare che le politiche che regolano l'uso richiedano l'approvazione esplicita delle parti autorizzate per usare le tecnologie.			
12.3.2 Autenticazione per l'uso della tecnologia	12.3.2 Verificare che le politiche che regolano l'uso richiedano che tutte le tecnologie utilizzate vengano autenticate da ID utente e password o un altro elemento di autenticazione (ad esempio, un token).			
12.3.3 Un elenco di tutti i dispositivi di questo tipo e del personale autorizzato all'accesso	12.3.3 Verificare che le politiche che regolano l'uso richiedano un elenco di tutti i dispositivi e del personale autorizzato a utilizzarli.			
12.3.4 Etichettatura dei dispositivi con indicazione di proprietario, informazioni di contatto e scopo	12.3.4 Verificare che le politiche che regolano l'uso richiedano l'etichettatura dei dispositivi con informazioni che possono essere correlate a proprietario, informazioni di contatto e scopo.			
12.3.5 Usi accettabili della tecnologia	12.3.5 Verificare che le politiche che regolano l'uso richiedano usi accettabili della tecnologia.			
12.3.6 Posizioni di rete accettabili per le tecnologie	12.3.6 Verificare che le politiche che regolano l'uso richiedano posizioni di rete accettabili per la tecnologia.			
12.3.7 Elenco di prodotti approvati dalla società	12.3.7 Verificare che le politiche che regolano l'uso richiedano un elenco dei prodotti approvati dalla società.			
12.3.8 Disconnessione automatica delle sessioni per tecnologie di accesso remoto dopo un periodo di tempo specifico di inattività	12.3.8 Verificare che le politiche che regolano l'uso richiedano la disconnessione automatica delle sessioni per tecnologie di accesso remoto dopo un periodo di tempo specifico di inattività.			
12.3.9 Attivazione di tecnologie di accesso remoto per fornitori e partner aziendali solo quando necessario, con disattivazione immediata dopo l'uso	12.3.9 Verificare che le politiche che regolano l'uso richiedano l'attivazione di tecnologie di accesso remoto usate da fornitori e partner aziendali solo quando necessario, con disattivazione immediata dopo l'uso.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>12.3.10 Per il personale che accede ai dati dei titolari di carta utilizzando tecnologie di accesso remoto, proibire la copia, lo spostamento o la memorizzazione dei dati dei titolari di carta su dischi rigidi locali e supporti elettronici rimovibili, a meno che ciò non sia stato espressamente autorizzato per un'esigenza aziendale specifica.</p>	<p>12.3.10.a Verificare che le politiche che regolano l'uso proibiscano la copia, lo spostamento o la memorizzazione dei dati di titolari di carta su dischi rigidi locali e supporti elettronici rimovibili quando si accede ai dati tramite tecnologie di accesso remoto.</p> <p>12.3.10.b Per il personale in possesso di opportuna autorizzazione, verificare che le politiche che regolano l'uso richiedano la protezione dei dati dei titolari di carta in conformità ai Requisiti PCI DSS.</p>			
<p>12.4 Assicurare che nelle procedure e nella politica per la sicurezza siano definite in modo chiaro le responsabilità in termini di protezione delle informazioni per tutto il personale.</p>	<p>12.4 Verificare che le politiche di protezione delle informazioni definiscano chiaramente le responsabilità in termini di protezione delle informazioni per tutto il personale.</p>			
<p>12.5 Assegnare a un utente singolo o a un team le seguenti responsabilità di gestione della sicurezza delle informazioni:</p>	<p>12.5 Verificare l'assegnazione formale della responsabilità di protezione delle informazioni a un CSO (Chief Security Officer) o a un altro membro del management esperto in sicurezza. Richiedere ed esaminare le politiche e le procedure di protezione delle informazioni per verificare che le responsabilità di protezione delle informazioni vengano assegnate in modo specifico e formale:</p>			
<p>12.5.1 Stabilire, documentare e distribuire le politiche e le procedure di sicurezza.</p>	<p>12.5.1 Verificare che venga formalmente assegnata la responsabilità per la creazione e la distribuzione delle politiche e delle procedure di sicurezza.</p>			
<p>12.5.2 Monitorare ed esaminare avvisi e informazioni sulla sicurezza e distribuirli al personale appropriato.</p>	<p>12.5.2 Verificare che venga formalmente assegnata la responsabilità del monitoraggio e dell'analisi degli avvisi di sicurezza e della distribuzione delle informazioni al personale addetto alla protezione delle informazioni appropriato e al management della business unit.</p>			
<p>12.5.3 Stabilire, documentare e distribuire le procedure di risposta ed escalation in caso di problemi di sicurezza per garantire una gestione tempestiva ed efficiente di tutte le situazioni.</p>	<p>12.5.3 Verificare che venga formalmente assegnata la responsabilità di creazione e distribuzione delle politiche di risposta in caso di problemi e le procedure di escalation.</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
12.5.4 Amministrare gli account utente, incluse aggiunte, eliminazioni e modifiche	12.5.4 Verificare che venga formalmente assegnata la responsabilità per l'amministrazione degli account utente e la gestione delle autenticazioni.			
12.5.5 Monitorare e controllare tutti gli accessi ai dati.	12.5.5 Verificare che venga formalmente assegnata la responsabilità per il monitoraggio e il controllo di tutti gli accessi ai dati.			
12.6 Implementare un programma formale di consapevolezza della sicurezza per rendere tutto il personale consapevole dell'importanza della sicurezza dei dati di titolari di carta.	12.6.a Verificare l'esistenza di un programma formale di consapevolezza della sicurezza per tutto il personale.			
	12.6.b Richiedere ed esaminare le procedure e la documentazione del programma di consapevolezza della sicurezza ed effettuare quanto segue:			
12.6.1 Formare il personale al momento dell'assunzione e almeno una volta all'anno. <i>Nota: i metodi possono essere diversi in funzione del ruolo svolto dal personale e del loro livello di accesso ai dati dei titolari di carta.</i>	12.6.1.a Verificare che il programma di consapevolezza della sicurezza utilizzi diversi strumenti di comunicazione e formazione del personale (ad esempio, poster, lettere, promemoria, formazione basata su Web, riunioni e promozioni).			
	12.6.1.b Verificare che il personale partecipi alla formazione sulla consapevolezza al momento dell'assunzione e almeno una volta all'anno.			
12.6.2 Richiedere al personale di certificare almeno una volta all'anno di aver letto e compreso la politica e le procedure di sicurezza.	12.6.2 Verificare che il programma di consapevolezza della sicurezza richieda al personale di certificare, per iscritto o elettronicamente, almeno una volta all'anno di aver letto e compreso la politica di sicurezza delle informazioni.			
12.7 Sottoporre il personale potenziale a screening prima dell'assunzione per ridurre al minimo il rischio di attacchi da fonti interne. Esempi di indagini sulla storia personale sono informazioni su impieghi precedenti, precedenti penali, storico del credito e controlli delle referenze. <i>Nota: Per quel personale potenziale da assumere per determinate posizioni come cassieri di un negozi, che hanno accesso a un solo numero di carta alla volta durante una transazione, questo requisito è solo consigliato.</i>	12.7 Consultare il management responsabile del reparto delle Risorse Umane e verificare che vengano condotte indagini sulla storia personale (nei limiti previsti dalle leggi in vigore) sul personale potenziale prima di assumere coloro i quali avranno accesso ai dati di titolari di carta o al relativo ambiente.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>12.8 Se i dati di titolari di carta sono condivisi con provider di servizi, gestire e implementare politiche e procedure per i provider di servizi per includere quanto segue:</p>	<p>12.8 Se l'entità condivide i dati di titolari di carta con provider di servizi (ad esempio, strutture di conservazione dei nastri di backup, provider di servizi gestiti come le società di hosting Web, provider di servizi di sicurezza oppure soggetti che ricevono i dati a scopo di "fraud modeling", cioè per analizzare modelli di possibili truffe), effettuare quanto indicato di seguito, tramite osservazione, revisione delle politiche e delle procedure e analisi della documentazione di supporto:</p>			
<p>12.8.1 Conservare un elenco dei provider di servizi.</p>	<p>12.8.1 Verificare che venga conservato un elenco di provider di servizi.</p>			
<p>12.8.2 Conservare un accordo scritto in base al quale il provider di servizi si assume la responsabilità della protezione dei dati di titolari di carta di cui entra in possesso.</p>	<p>12.8.2 Verificare che nell'accordo scritto il provider di servizi si assuma la responsabilità della protezione di dati di titolari di carta.</p>			
<p>12.8.3 Accertarsi che esista un processo definito per incaricare i provider di servizi, che includa tutte le attività di dovuta diligenza appropriate prima dell'incarico.</p>	<p>12.8.3 Verificare che le politiche e le procedure siano documentate e rispettate, inclusa la dovuta diligenza appropriata prima di assegnare l'incarico al provider di servizi.</p>			
<p>12.8.4 Conservare un programma per monitorare lo stato di conformità agli standard PCI DSS dei provider di servizi con cadenza almeno annuale.</p>	<p>12.8.4 Verificare che l'entità conservi un programma per monitorare lo stato di conformità agli standard PCI DSS dei provider di servizi con cadenza almeno annuale.</p>			
<p>12.9 Implementare un piano di risposta agli incidenti. Prepararsi a rispondere immediatamente a una violazione del sistema.</p>	<p>12.9 Richiedere ed esaminare il piano di risposta agli incidenti e le procedure correlate ed effettuare quanto segue:</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>12.9.1 Creare il piano di risposta agli incidenti da attuare in caso di violazione del sistema. Accertarsi che il piano includa almeno i seguenti elementi:</p> <ul style="list-style-type: none"> ▪ Ruoli, responsabilità e strategie di comunicazione e contatto in caso di violazione, nonché notifiche ai marchi di pagamento ▪ Procedure specifiche di risposta agli incidenti ▪ Procedure di ripristino e continuità delle attività aziendali ▪ Processi di backup dei dati ▪ Analisi dei requisiti legali per la segnalazione delle violazioni ▪ Copertura e risposte per tutti i componenti di sistema critici ▪ Riferimenti e descrizioni delle procedure di risposta agli incidenti adottate dai marchi di pagamento 	<p>12.9.1.a Verificare che il piano di risposta agli incidenti includa i seguenti elementi:</p> <ul style="list-style-type: none"> ▪ Ruoli, responsabilità e strategie di comunicazione in caso di violazione, nonché notifiche ai marchi di pagamento ▪ Procedure specifiche di risposta agli incidenti ▪ Procedure di ripristino e continuità delle attività aziendali ▪ Processi di backup dei dati ▪ Analisi dei requisiti legali per la segnalazione di violazioni (ad esempio, il disegno di legge 1386 della California che richiede l'obbligo di inviare una notifica ai consumatori interessati in caso di avvenuta o sospetta violazione per tutte le imprese i cui database contengano i dati di cittadini residenti in California) ▪ Copertura e risposte per tutti i componenti di sistema critici ▪ Riferimenti e descrizioni delle procedure di risposta agli incidenti adottate dai marchi di pagamento <p>12.9.1.b Esaminare la documentazione relativa ad un incidente o un allarme segnalato in precedenza per verificare che siano stati seguiti le procedure ed il piano di risposta agli incidenti documentato.</p>			
<p>12.9.2 Eseguire un test del piano almeno una volta all'anno.</p>	<p>12.9.2 Verificare che il piano venga testato almeno una volta all'anno.</p>			
<p>12.9.3 Nominare personale specifico disponibile 24 ore al giorno, 7 giorni su 7 in caso di emergenza.</p>	<p>12.9.3 Attraverso l'osservazione e l'analisi delle politiche, verificare che il personale specifico sia disponibile per il monitoraggio e la capacità di risposta 24 ore su 24, 7 giorni su 7, in caso di sospetta attività non autorizzata, rilevamento di punti di accesso wireless non autorizzati, avvisi IDS critici e/o segnalazione di modifiche non autorizzate a un sistema o un file critico.</p>			
<p>12.9.4 Formare in modo appropriato il personale addetto al controllo delle violazioni della sicurezza.</p>	<p>12.9.4 Attraverso l'osservazione e l'analisi delle politiche, verificare che il personale addetto al controllo delle violazioni della sicurezza partecipi regolarmente a corsi di formazione.</p>			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>12.9.5 Includere allarmi dai sistemi di rilevamento e prevenzione delle intrusioni e dai sistemi di monitoraggio dell'integrità dei file.</p>	<p>12.9.5 Attraverso l'osservazione e l'analisi dei processi, verificare che il piano di risposta agli incidenti preveda processi di monitoraggio e risposta agli avvisi dai sistemi critici, incluso il rilevamento di punti di accesso wireless non autorizzati.</p>			
<p>12.9.6 Sviluppare un processo che consenta di correggere e migliorare il piano di risposta agli incidenti tenendo conto delle lezioni apprese e degli ultimi sviluppi nel settore.</p>	<p>12.9.6 Attraverso l'osservazione e l'analisi delle politiche, verificare che esista un processo per la correzione e il miglioramento del piano di risposta agli incidenti in base alle lezioni apprese e agli ultimi sviluppi nel settore.</p>			

Appendice A: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso

Requisito A.1: I provider di hosting condiviso devono proteggere l'ambiente dei dati di titolari di carta

Come citato nel requisito 12.8, tutti i provider di servizi con accesso ai dati di titolari di carta (compresi i provider di hosting condiviso) devono aderire agli standard PCI DSS. Inoltre il Requisito 2.4 prevede che i provider di servizi di hosting condiviso proteggano l'ambiente e i dati dell'entità ospitata. Di conseguenza, i provider di hosting condiviso devono rispondere anche ai requisiti descritti in questa appendice.

Requisiti	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
<p>A.1 Proteggere l'ambiente e i dati di ogni entità ospitata (esercente, provider di servizi o altra entità), nei modi previsti dal punto A.1.1 al punto A.1.4: Il provider di hosting è tenuto a soddisfare questi requisiti, oltre a tutte le altre sezioni rilevanti degli standard PCI DSS.</p> <p>Nota: anche se un provider di hosting soddisfa tutti questi requisiti, la conformità dell'entità che utilizza tale provider di hosting non è automaticamente garantita. Ogni entità deve soddisfare i requisiti e ottenere la convalida della conformità agli standard PCI DSS, come applicabile.</p>	<p>A.1 Per quanto riguarda specificamente la valutazione PCI DSS di un provider di hosting condiviso, per verificare che i provider di hosting condiviso proteggano gli ambienti e i dati ospitati (esercenti e provider di servizi), selezionare un campione di server (Microsoft Windows e Unix/Linux) all'interno di un campione rappresentativo di esercenti e provider di servizi ospitati ed eseguire le operazioni descritte nei punti da A.1.1 a A.1.4 riportati di seguito.</p>			
<p>A.1.1 Garantire che ogni entità esegua processi con accesso esclusivo al proprio ambiente dei dati di titolari di carta.</p>	<p>A.1.1 Se un provider di hosting condiviso consente alle entità (ad esempio, esercenti o provider di servizi) di eseguire proprie applicazioni, verificare che i processi di tali applicazioni vengano eseguiti utilizzando l'ID univoco assegnato all'entità. Ad esempio: Nessuna entità nel sistema può utilizzare un ID utente di un server Web condiviso. Tutti gli script CGI utilizzati dall'entità devono essere creati ed eseguiti con l'ID utente univoco dell'entità.</p>			

Requisiti	Procedure di test	Presente	Non presente	Data di scadenza/Commenti
A.1.2 Limitare l'accesso e i privilegi di ciascuna entità esclusivamente al relativo ambiente di dati di titolari di carta.	A.1.2.a Verificare che l'ID utente di tutti i processi dell'applicazione non sia un utente privilegiato (root/amministratore).			
	A.1.2.b Verificare che ogni entità (esercente, provider di servizi) disponga dei diritti di lettura, scrittura o esecuzione solo per i propri file e directory o per i system file necessari (tramite autorizzazione su file system, elenchi di controllo degli accessi, funzioni chroot o jailshell, eccetera). Importante: i file di un'entità non possono essere condivisi per gruppi.			
	A.1.2.c Verificare che gli utenti di un'entità non abbiano accesso in scrittura a file di sistema binari condivisi.			
	A.1.2.d Verificare che la visualizzazione delle voci del registro sia consentita solo all'entità proprietaria.			
	A.1.2.e Per impedire che un'entità monopolizzi le risorse del server per sfruttarne le vulnerabilità (condizioni di errore, "race" e riavvio che generano, ad esempio, buffer overflow), verificare che siano applicate limitazioni all'uso di queste risorse del sistema: <ul style="list-style-type: none"> ▪ Spazio sul disco ▪ Larghezza di banda ▪ Memoria ▪ CPU 			
A.1.3 Accertarsi che le funzioni di audit trail e di generazione dei registri siano abilitate e siano univoche per l'ambiente dei dati di titolari di carta di ciascuna entità e che siano coerenti con il Requisito 10 PCI DSS.	A.1.3 Verificare che il provider di hosting condiviso abbia abilitato la generazione dei registri per l'ambiente di esercenti e provider di servizi nel modo descritto di seguito: I registri sono abilitati per applicazioni di terze parti comuni. I registri sono attivi per impostazione predefinita. I registri sono disponibili per la revisione da parte dell'entità proprietaria. Le posizioni dei registri sono comunicate in modo chiaro all'entità proprietaria.			
A.1.4 Abilitare processi in grado di fornire tutte le informazioni necessarie per un'indagine legale tempestiva in caso di violazione di dati di un esercente o un provider di servizi ospitato.	A.1.4 Verificare che il provider di hosting condiviso disponga di politiche scritte che forniscono tutte le informazioni necessarie per un'indagine legale tempestiva dei server correlati in caso di violazione.			

Appendice B: Controlli compensativi

È possibile adottare i controlli compensativi per la maggior parte dei requisiti PCI DSS, quando un'entità non è in grado di soddisfare un requisito nel modo esplicitamente richiesto, a causa di limitazioni aziendali tecniche o documentate legittime, ma ha posto in essere altri controlli (anche compensativi) sufficienti a mitigare il rischio associato a tale requisito.

I controlli compensativi devono soddisfare i seguenti criteri:

1. Rispondere allo scopo e alla severità del requisito PCI DSS originale.
2. Offrire un livello di protezione simile al requisito PCI DSS originale, ad esempio, il controllo compensativo mitiga sufficientemente il rischio per cui il requisito PCI DSS originale era stato progettato. Vedere *Navigazione in PCI DSS* per una spiegazione dello scopo di ciascun requisito PCI DSS.
3. Superare e integrare altri requisiti PCI DSS (garantire la conformità ad altri requisiti PCI DSS non è un controllo compensativo).

Per valutare un criterio di superamento dei controlli compensativi, tenere presente quanto riportato di seguito:

Nota: *gli elementi descritti da a) a c) sono da intendersi semplicemente come esempi. Tutti i controlli compensativi devono essere analizzati e convalidati dal valutatore che conduce la revisione PCI DSS. L'efficacia di un controllo compensativo dipende dalle specifiche dell'ambiente in cui il controllo viene implementato, dai controlli di sicurezza circostanti e dalla configurazione del controllo. Le società devono considerare che un determinato controllo compensativo potrebbe non essere efficace in tutti gli ambienti.*

- a) I requisiti PCI DSS esistenti **NON POSSONO** essere considerati controlli compensativi se sono già richiesti per l'elemento sottoposto a revisione. Ad esempio, le password per l'accesso amministrativo non da console devono essere inviate già cifrate per ridurre il rischio di intercettazione delle password amministrative con testo in chiaro. Un'entità non può utilizzare altri requisiti di password PCI DSS (blocco intrusioni, password complesse, ecc.) per compensare la mancanza di password cifrate, poiché tali altri requisiti di password non riducono il rischio di intercettazione delle password con testo in chiaro. Inoltre, gli altri controlli delle password rappresentano già requisiti PCI DSS per l'elemento sottoposto a revisione (password).
 - b) I requisiti PCI DSS esistenti **POSSONO** essere considerati controlli compensativi se sono richiesti per un'altra area, ma non sono richiesti per l'elemento sottoposto a revisione. Ad esempio, l'autenticazione a due fattori è un requisito PCI DSS per l'accesso remoto. L'autenticazione a due fattori *dalla rete interna* può anche essere considerata un controllo compensativo per l'accesso amministrativo non da console se la trasmissione di password cifrate non è supportata. L'autenticazione a due fattori può rappresentare un controllo compensativo accettabile se: (1) risponde allo scopo del requisito originale riducendo il rischio di intercettazione delle password amministrative con testo in chiaro e (2) è configurata correttamente e in un ambiente protetto.
 - c) I requisiti PCI DSS esistenti possono essere combinati con nuovi controlli per diventare un controllo compensativo. Ad esempio, se una società non è in grado di rendere illeggibili i dati di titolari di carta secondo il Requisito 3.4 (ad esempio, tramite cifratura), un controllo compensativo potrebbe essere composto da un dispositivo o da una combinazione di dispositivi, applicazioni e controlli che rispondano a tutte le seguenti condizioni: (1) segmentazione di rete interna; (2) filtro degli indirizzi IP o MAC; (3) autenticazione a due fattori dalla rete interna.
4. Essere adeguato al rischio ulteriore provocato dalla mancata adesione al requisito PCI DSS

Il valutatore deve analizzare in modo approfondito i controlli compensativi durante ogni valutazione PCI DSS annuale per confermare che ogni controllo compensativo riduca adeguatamente il rischio previsto dal requisito PCI DSS originale, come definito ai punti 1-4 descritti sopra. Per mantenere la conformità,

devono essere in atto processi e controlli per garantire che i controlli compensativi rimangano attivi una volta terminata la valutazione.

Appendice C: Foglio di lavoro - Controlli compensativi

Utilizzare questo foglio di lavoro per definire i controlli compensativi per qualsiasi requisito nel caso in cui questi vengano utilizzati per rispondere a un requisito PCI DSS. Tenere presente che i controlli compensativi dovrebbero essere documentati nel Rapporto sulla conformità nella sezione del requisito corrispondente PCI DSS.

Nota: solo le società che hanno eseguito un'analisi dei rischi e presentano limitazioni aziendali tecniche o documentate legittime possono considerare l'uso dei controlli compensativi per garantire la conformità agli standard PCI DSS.

Numero e definizione del requisito:

	Informazioni richieste	Spiegazione
1. Vincoli	Elencare i vincoli che impediscono di soddisfare il requisito originale.	
2. Obiettivo	Definire l'obiettivo del controllo originale; identificare l'obiettivo soddisfatto mediante il controllo compensativo.	
3. Rischio identificato	Identificare eventuali rischi aggiuntivi dovuti alla non applicazione del controllo originale.	
4. Definizione di controlli compensativi	Definire i controlli compensativi e spiegare come soddisfano gli obiettivi del controllo originale e il rischio maggiore, se presente.	
5. Convalida dei controlli compensativi	Definire la modalità di convalida e test dei controlli compensativi.	
6. Manutenzione	Definire il processo e i controlli in atto per i controlli compensativi.	

Foglio di lavoro Controlli compensativi - Esempio

Utilizzare questo foglio di lavoro per definire i controlli compensativi per qualsiasi requisito contrassegnato come "presente" attraverso i controlli compensativi.

Numero requisito: 8.1–Tutti gli utenti sono identificati con un nome utente univoco prima di consentire loro l'accesso a componenti del sistema o dati di titolari di carta?

	Informazioni richieste	Spiegazione
1. Vincoli	Elencare i vincoli che impediscono di soddisfare il requisito originale.	<i>La società XYZ utilizza server Unix standalone senza LDAP. Pertanto, ciascun server richiede un login "root". Non è possibile per la società XYZ gestire il login "root" né è possibile registrare tutte le attività "root" di ciascun utente.</i>
2. Obiettivo	Definire l'obiettivo del controllo originale; identificare l'obiettivo soddisfatto mediante il controllo compensativo.	<i>L'obiettivo di richiedere login univoci è raddoppiato. In primo luogo, non è considerato accettabile da un punto di vista della sicurezza condividere credenziali di login. In secondo luogo, login condivisi rendono impossibile determinare in modo sicuro che una persona è responsabile di una determinata azione.</i>
3. Rischio identificato	Identificare eventuali rischi aggiuntivi dovuti alla non applicazione del controllo originale.	<i>La non assegnazione di ID univoci a tutti gli utenti e, di conseguenza, l'impossibilità di tenere traccia delle loro attività rappresenta un ulteriore rischio per il sistema di controllo dell'accesso.</i>
4. Definizione di controlli compensativi	Definire i controlli compensativi e spiegare come soddisfano gli obiettivi del controllo originale e il rischio maggiore, se presente.	<i>La società XYZ richiederà a tutti gli utenti di accedere ai server dai propri desktop utilizzando il comando SU. Tale comando consente a un utente di accedere all'account "root" ed eseguire le azioni come utente "root", ma essere registrato nella directory di log SU. In questo modo, le azioni di ciascun utente possono essere registrate mediante l'account SU.</i>
5. Convalida dei controlli compensativi	Definire la modalità di convalida e test dei controlli compensativi.	<i>La società XYZ dimostra al valutatore che il comando SU è in esecuzione e che gli utenti che utilizzano tale comando sono registrati per identificare l'utente che esegue le azioni con i privilegi root.</i>
6. Manutenzione	Definire il processo e i controlli in atto per i controlli compensativi.	<i>La società XYZ documenta i processi e le procedure per garantire che le configurazioni SU non vengano modificate, alterate o rimosse per consentire ai singoli utenti di eseguire comandi root senza essere identificati e registrati singolarmente.</i>

Appendice D: Segmentazione e campionamento delle strutture aziendali e dei componenti di sistema.

