



Settore delle carte di pagamento (PCI) Standard di protezione dei dati

Requisiti e procedure di valutazione della sicurezza

**Versione 3.2
Aprile 2016**

Modifiche del documento

Data	Versione	Descrizione	Pagine
Ottobre 2008	1.2	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 Standard di protezione dei dati Riepilogo delle modifiche di PCI DSS dalla versione 1.1 alla 1.2.	
Luglio 2009	1.2.1	Aggiungere la frase erroneamente eliminata tra PCI DSS v1.1 e v1.2.	5
		Correggere l'errore di ortografia nelle procedure di test 6.3.7.a e 6.3.7.b.	32
		Rimuovere il contrassegno disattivato per le colonne “presente” e “non presente” nella procedura di test 6.5.b.	33
		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.”	64
Ottobre 2010	2.0	Aggiornare ed implementare le modifiche da v1.2.1. Vedere Riepilogo delle modifiche di <i>PCI DSS dalla versione 1.2.1 alla 2.0</i> .	
Novembre 2013	3.0	Aggiornamento da v2.0. Vedere <i>PCI DSS - Riepilogo delle modifiche dalla versione 2.0 alla 3.0</i> .	
Aprile 2015	3.1	Aggiornamento da PCI DSS v3.0. Per informazioni dettagliate sulle modifiche, fare riferimento a <i>PCI DSS - Riepilogo delle modifiche di PCI DSS dalla versione 3.0 alla 3.1</i> .	
Aprile 2016	3.2	Aggiornamento da PCI DSS v3.1. Per informazioni dettagliate sulle modifiche, fare riferimento a <i>PCI DSS - Riepilogo delle modifiche di PCI DSS dalla versione 3.1 alla 3.2</i> .	

Sommario

Aprile 2016	2
Modifiche del documento	2
Introduzione e panoramica di PCI DSS	5
<i>Risorse PCI DSS</i>	6
Informazioni sull'applicabilità dello standard PCI DSS	7
Relazione tra PCI DSS e PA-DSS	9
<i>Applicabilità dello standard PCI DSS alle applicazioni PA-DSS</i>	9
<i>Applicabilità dello standard PCI DSS ai fornitori di applicazioni di pagamento</i>	9
Ambito dei requisiti PCI DSS	10
<i>Segmentazione di rete</i>	11
<i>Wireless</i>	11
<i>Uso di provider di servizi di terzi/esternalizzazione</i>	12
Migliori pratiche per implementare lo standard PCI DSS nei processi business-as-usual	13
Per valutatori: campionamento delle strutture aziendali e dei componenti di sistema	15
Controlli compensativi	16
Istruzioni e contenuti per il rapporto sulla conformità	17
Processo di valutazione PCI DSS	17
Versioni PCI DSS	18
Requisiti PCI DSS e procedure di valutazione della sicurezza dettagliate	19
Sviluppo e gestione di sistemi e reti sicure	20
<i>Requisito 1 - Installare e gestire una configurazione firewall per proteggere i dati dei titolari di carta</i>	20
<i>Requisito 2 - Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione</i>	29
Protezione dei dati dei titolari di carta	37
<i>Requisito 3 - Proteggere i dati dei titolari di carta memorizzati</i>	37
<i>Requisito 4 - Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche</i>	51
Utilizzare un programma per la gestione delle vulnerabilità	54
<i>Requisito 5 - Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus</i>	54
<i>Requisito 6 - Sviluppare e gestire sistemi e applicazioni protette</i>	58
Implementazione di rigide misure di controllo dell'accesso	75

<i>Requisito 7</i>	<i>Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario</i>	<i>75</i>
<i>Requisito 8 -</i>	<i>Individuare e autenticare l'accesso ai componenti di sistema</i>	<i>78</i>
<i>Requisito 9 -</i>	<i>Limitare l'accesso fisico ai dati dei titolari di carta.....</i>	<i>88</i>
Monitoraggio e test delle reti regolari		99
<i>Requisito 10 -</i>	<i>Registrare e monitorare tutti gli accessi a risorse di rete e dati dei titolari di carta</i>	<i>99</i>
<i>Requisito 11 -</i>	<i>Eseguire regolarmente test dei sistemi e processi di protezione.....</i>	<i>109</i>
Gestione di una politica di sicurezza delle informazioni.....		119
<i>Requisito 12 -</i>	<i>Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale.</i>	<i>119</i>
Appendice A - Requisiti PCI DSS aggiuntivi		132
<i>Appendice A1: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso.....</i>		<i>133</i>
<i>Appendice A2: Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale.....</i>		<i>135</i>
<i>Appendice A3: Convalida aggiuntiva delle entità designate (DESV).....</i>		<i>138</i>
Appendice B - Controlli compensativi.....		154
Appendice C - Foglio di lavoro - Controlli compensativi.....		156
Appendice D - Segmentazione e campionamento delle strutture aziendali e dei componenti di sistema.....		159

Introduzione e panoramica di PCI DSS

Lo standard di protezione dei dati per il settore delle carte di pagamento (PCI DSS) è stato sviluppato per favorire e migliorare la protezione dei dati dei titolari di carta nonché per semplificare l'implementazione di misure di sicurezza dei dati coerenti a livello globale. Lo standard PCI DSS mette a disposizione una base di requisiti tecnici e operativi volti a proteggere i dati di account. Lo standard PCI DSS si applica a **tutte** le entità coinvolte nell'elaborazione di carte di pagamento, con l'inclusione di esercenti, elaboratori, acquirenti, emittenti e provider di servizi. Si applica anche a **tutte** le altre entità che si occupano di memorizzare, elaborare o trasmettere dati dei titolari di carta (CHD) e/o dati sensibili di autenticazione (SAD). Di seguito, è riportata una panoramica di alto livello dei 12 requisiti PCI DSS.

PCI DSS - Panoramica di alto livello

Sviluppo e gestione di sistemi e reti sicure	<ol style="list-style-type: none"> 1. Installare e gestire una configurazione firewall per proteggere i dati dei titolari di carta 2. Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione
Protezione dei dati dei titolari di carta	<ol style="list-style-type: none"> 3. Proteggere i dati dei titolari di carta memorizzati 4. Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche
Utilizzare un programma per la gestione delle vulnerabilità	<ol style="list-style-type: none"> 5. Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus 6. 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 dei titolari di carta solo se effettivamente necessario 8. Individuare e autenticare l'accesso ai componenti di sistema 9. 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 dei titolari di carta 11. Eseguire regolarmente test dei 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 le valutazioni della conformità allo standard PCI DSS nell'ambito 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 15.

Lo standard PCI DSS comprende una serie minima di requisiti per proteggere i dati di account e può essere migliorato attraverso pratiche e controlli aggiuntivi per ridurre ulteriormente i rischi, nonché attraverso leggi e normative locali, statali e di settore. Inoltre, i requisiti legislativi o regolatori possono prevedere una protezione specifica delle informazioni personali o di altri elementi di dati (ad esempio, il nome del titolare di carta). Lo standard PCI DSS non sostituisce le leggi statali o locali, le normative governative o altri requisiti legali.

Risorse PCI DSS

Sul sito Web dell'Ente responsabile degli standard di protezione PCI (PCI SSC) (www.pcisecuritystandards.org) sono disponibili ulteriori risorse che facilitano l'esecuzione di valutazioni e convalide da parte delle organizzazioni, compresi:

- Raccolta documenti, inclusi:
 - *PCI DSS - Riepilogo delle modifiche dalla versione PCI DSS 2.0 alla 3.0*
 - *Guida di riferimento rapido PCI DSS*
 - *Glossario, abbreviazioni e acronimi PCI DSS e PA-DSS*
 - *Supplementi informativi e linee guida*
 - *Approccio prioritario per PCI DSS*
 - *Rapporto sulla conformità (ROC), modello di reporting e istruzioni per il reporting*
 - *Questionari di autovalutazione (SAQ) e Istruzioni e linee guida per i questionari di autovalutazione*
 - *Attestati di conformità (AOC)*
- FAQ
- PCI per siti Web di piccoli esercenti
- Corsi di formazione e webinar informativi su PCI
- Elenco di aziende qualificate per la valutazione (QSA) e di fornitori di prodotti di scansione approvati (ASV)
- Elenco di dispositivi approvati PTS e di applicazioni di pagamento convalidate PA-DSS

Nota: i supplementi informativi completano lo standard PCI DSS e individuano ulteriori considerazioni e raccomandazioni per soddisfare i requisiti PCI DSS, senza però modificare, eliminare o sostituirsi allo standard PCI DSS o ai relativi requisiti.

Per informazioni su queste e altre risorse, fare riferimento al sito Web www.pcisecuritystandards.org.

Informazioni sull'applicabilità dello standard PCI DSS

Lo standard PCI DSS si applica a **tutte** le entità coinvolte nell'elaborazione di carte di pagamento, con l'inclusione di esercenti, elaboratori, acquirenti, emittenti e provider di servizi. Si applica anche a **tutte** le altre entità che si occupano di memorizzare, elaborare o trasmettere dati dei titolari di carta e/o dati sensibili di autenticazione.

Di seguito sono elencati i dati dei titolari di carta e i dati sensibili di autenticazione:

Dati di account	
I dati dei titolari di carta comprendono:	I dati sensibili di autenticazione comprendono:
<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 della traccia completa (dati della striscia magnetica o dati equivalenti in un chip)▪ CAV2/CVC2/CVV2/CID▪ PIN/Blocchi PIN

Il numero PAN è il fattore determinante per i dati dei titolari di carta. 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 dei titolari di carta (CDE), tali dati devono essere protetti in conformità ai requisiti PCI DSS applicabili.

I requisiti PCI DSS si applicano alle organizzazioni in cui vengono memorizzati, elaborati o trasmessi i dati di account (dati dei titolari di carta e/o dati sensibili di autenticazione). È possibile che alcuni requisiti PCI DSS siano validi anche per le organizzazioni che si avvalgono di provider esterni per l'esecuzione di operazioni di pagamento o di gestione dell'ambiente dei dati dei titolari di carta¹. Inoltre, le organizzazioni che si avvalgono di terzi per l'esecuzione delle operazioni relative all'ambiente dei dati dei titolari di carta o al pagamento sono tenute a garantire che tali terzi proteggano i dati degli account in base ai requisiti PCI DSS applicabili.

La tabella riportata nella pagina successiva 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.

¹ Conforme ai programmi di conformità dei singoli marchi di pagamento

		Elemento di dati	Memorizzazione consentita	Rendere i dati memorizzati illeggibili in base al Requisito 3.4
Dati di account	Dati dei 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 ²	Dati della traccia completa ³	No	Impossibile memorizzare in base al Requisito 3.2
		CAV2/CVC2/CVV2/CID ⁴	No	Impossibile memorizzare in base al Requisito 3.2
		PIN/Blocco PIN ⁵	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 dei titolari di carta, è solo il PAN che va reso illeggibile in conformità al Requisito 3.4 PCI DSS.

I dati sensibili di autenticazione non devono essere memorizzati dopo l'autorizzazione, anche se cifrati. Questo vale anche se l'ambiente non prevede PAN. Le organizzazioni sono tenute a contattare direttamente i propri acquirenti o i singoli marchi di pagamento per verificare se e per quanto tempo è possibile memorizzare i dati sensibili di autenticazione prima dell'autorizzazione e per conoscere gli eventuali requisiti d'uso e protezione correlati.

² I dati sensibili di autenticazione non devono essere memorizzati dopo l'autorizzazione (anche se cifrati).

³ Dati della traccia completa dalla striscia magnetica, dati equivalenti in un chip o in altro luogo.

⁴ Il valore di tre o quattro cifre stampato nella parte anteriore o posteriore di una carta di pagamento.

⁵ Numero di identificazione personale inserito dal titolare della carta durante una transazione con carta presente e/o blocco PIN cifrato presente all'interno del messaggio di transazione.

Relazione tra PCI DSS e PA-DSS

Applicabilità dello standard PCI DSS alle applicazioni PA-DSS

L'uso di un'applicazione conforme allo standard di protezione dei dati per le applicazioni di pagamento (PA-DSS) di per sé non rende l'entità conforme allo standard PCI DSS, poiché l'applicazione in questione deve essere implementata in un ambiente conforme allo standard PCI DSS e in conformità alla Guida per l'implementazione del programma PA-DSS messa a disposizione dal fornitore di applicazioni di pagamento.

Tutte le applicazioni che memorizzano, elaborano o trasmettono i dati dei titolari di carta rientrano nella valutazione PCI DSS di un'entità, comprese le applicazioni convalidate in base allo standard PA-DSS. La valutazione PCI DSS deve verificare che l'applicazione di pagamento convalidata in base allo standard PA-DSS sia configurata correttamente e implementata in modo sicuro nel rispetto dei requisiti PCI DSS. Se l'applicazione di pagamento è stata sottoposta a una qualsiasi personalizzazione, sarà necessario un esame più approfondito durante la valutazione PCI DSS, perché l'applicazione potrebbe non rappresentare più la versione convalidata in base allo standard PA-DSS.

I requisiti PA-DSS derivano dai *Requisiti PCI DSS e dalle procedure di valutazione della sicurezza* (definiti in questo documento). Lo standard PA-DSS descrive in dettaglio i requisiti che un'applicazione di pagamento deve soddisfare per agevolare la conformità allo standard PCI DSS di un cliente. Poiché le minacce sono in costante evoluzione, le applicazioni non più supportate dal fornitore (ad es., identificate dal fornitore come "fine della vita utile") potrebbero non offrire lo stesso livello di sicurezza delle versioni supportate.

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

Per determinare se lo standard PA-DSS si applica ad una determinata applicazione di pagamento, consultare la Guida del programma PA-DSS disponibile all'indirizzo www.pcisecuritystandards.org.

Applicabilità dello standard PCI DSS ai fornitori di applicazioni di pagamento

Lo standard PCI DSS potrebbe applicarsi ai fornitori di applicazioni di pagamento se il fornitore memorizza, elabora o trasmette i dati dei titolari di carta o ha accesso ai dati dei titolari di carta dei clienti (ad esempio, in qualità di provider di servizi).

Ambito dei requisiti PCI DSS

I requisiti di sicurezza PCI DSS sono applicabili a tutti i componenti di sistema inclusi nell'ambiente dei dati dei titolari di carta o collegati ad esso. L'ambiente dei dati dei titolari di carta è composto da persone, processi e tecnologie che memorizzano, elaborano o trasmettono i dati dei titolari di carta o i dati sensibili di autenticazione. I "componenti di sistema" includono dispositivi di rete, server, dispositivi informatici e applicazioni. Esempi di componenti di sistema possono essere:

- sistemi che offrono servizi di sicurezza (ad esempio, server di autenticazione), facilitano la segmentazione (ad esempio, firewall interni) o che influiscono sulla sicurezza dell'ambiente dei dati dei titolari di carta (ad esempio, server di risoluzione dei nomi o di reindirizzamento Web);
- componenti di virtualizzazione, quali macchine virtuali, switch/router virtuali, dispositivi virtuali, applicazioni/desktop virtuali e hypervisor;
- componenti di rete tra cui, senza limitazioni, firewall, switch, router, punti di accesso wireless, dispositivi di rete e altri dispositivi di sicurezza;
- tipi di server tra cui, senza limitazioni, server Web, di applicazioni, database, autenticazione, e-mail, proxy, NTP (Network Time Protocol) e DNS (Domain Name System);
- applicazioni tra cui tutte le applicazioni acquistate e personalizzate, comprese le applicazioni interne ed esterne (ad esempio, Internet);
- qualsiasi altro componente o dispositivo all'interno del CDE o a esso connesso.

Il primo passo di una valutazione PCI DSS consiste nello stabilire con precisione l'ambito della revisione. Almeno una volta all'anno e prima della valutazione annuale, l'entità valutata dovrebbe confermare la precisione del proprio ambito PCI DSS individuando tutte le posizioni e i flussi dei dati dei titolari di carta e identificare tutti i sistemi che sono connessi a o, se compromessi, potrebbero influire sul CDE (ad esempio, i server di autenticazione) per accertarsi che rientrino nell'ambito PCI DSS. Tutti i tipi di sistemi e posizioni devono essere considerati come parte del processo di determinazione dell'ambito, inclusi i siti di backup/ripristino e i sistemi di failover.

Per confermare la precisione del CDE definito, effettuare quanto segue:

- l'entità valutata identifica e documenta l'esistenza di tutti i dati dei titolari di carta nel proprio ambiente, per verificare che nessuno di questi dati dei titolari di carta sia 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 tutti i dati dei titolari di carta che rientrano nell'ambito della valutazione PCI DSS e che fanno parte dell'ambiente dei dati dei titolari di carta. Se l'entità individua dati non attualmente inclusi nell'ambiente dei dati dei titolari di carta, tali dati verranno eliminati in modo sicuro, spostati nell'ambiente dei dati dei titolari di carta attualmente definito o nell'ambiente dei dati dei titolari di carta ridefinito in modo da includere tali dati;

l'entità conserva la documentazione che mostra in che modo è stato determinato l'ambito della valutazione PCI DSS. La documentazione viene conservata per la revisione da parte del valutatore e/o per scopo informativo durante la successiva attività annuale di conferma dell'ambito della valutazione PCI DSS.

Per ogni valutazione PCI DSS, il valutatore è tenuto a confermare che l'ambito della valutazione sia definito e documentato con accuratezza.

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 non rientrare nell'ambito della valutazione PCI DSS, è necessario che il componente di sistema sia adeguatamente isolato (segmentato) dall'ambiente dei dati dei titolari di carta, in modo tale che anche qualora il componente di sistema che non rientra nell'ambito sia stato danneggiato, la sicurezza dell'ambiente dei dati dei titolari di carta non risulta compromessa.

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 dei 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 nell'ambito di una valutazione PCI DSS.

Wireless

Se viene utilizzata la tecnologia wireless per memorizzare, elaborare o trasmettere i dati dei titolari di carta (ad esempio, le transazioni di punti di vendita e "line-busting") oppure se una WLAN è connessa all'ambiente dei dati dei titolari di carta o fa parte di esso, 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.

Uso di provider di servizi di terzi/esternalizzazione

I provider di servizi o gli esercenti possono utilizzare un provider di terzi per memorizzare, elaborare o trasmettere i dati dei 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.

Le parti sono tenute a identificare chiaramente i servizi e i componenti di sistema inclusi nell'ambito della valutazione PCI DSS del provider di servizi, i requisiti PCI DSS specifici soddisfatti dal provider di servizi ed eventuali requisiti che i clienti del provider di servizi sono tenuti a includere nelle proprie revisioni PCI DSS. Ad esempio, un provider di hosting gestito è tenuto a definire chiaramente gli indirizzi IP che vengono inclusi nelle scansioni nell'ambito del processo di scansione delle vulnerabilità trimestrale e gli indirizzi IP che devono essere inclusi nelle scansioni trimestrali del cliente.

I provider di servizi sono responsabili di fornire prova della propria conformità allo standard PCI DSS e questo potrebbe essere richiesto dai marchi di pagamento. I provider di servizi sono tenuti a contattare direttamente il proprio acquirente e/o marchio di pagamento per determinare la convalida della conformità appropriata.

I provider di servizi di terzi possono convalidare la propria conformità ai requisiti PCI DSS nei due seguenti modi:

- 1) **Valutazione annuale:** i provider di servizi possono eseguire una valutazione PCI DSS annuale personalmente e fornire prova della propria conformità ai clienti; oppure
- 2) **Più valutazioni on-demand:** se non eseguono le valutazioni PCI DSS annuali, i provider di servizi devono eseguire valutazioni su richiesta dei loro clienti e/o partecipare a ciascuna delle revisioni PCI DSS del cliente, con i risultati di ciascuna revisione fornita al rispettivo cliente.

Se la valutazione PCI DSS viene eseguita personalmente da terzi, queste sono tenute a dimostrare ai clienti che l'ambito della valutazione PCI DSS del provider di servizi si riferisce ai servizi applicabili al cliente e che i relativi requisiti PCI DSS sono stati esaminati e sono presenti. Il tipo di dimostrazione specifico che il provider di servizi deve fornire ai clienti dipende dagli accordi/contratti stipulati tra le parti. Ad esempio, l'attestato di conformità e/o le sezioni rilevanti del rapporto sulla conformità del provider di servizi (redatto per proteggere le informazioni riservate) consentono di fornire tutte o alcune delle informazioni necessarie.

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 terzi associati che dispongono dell'accesso ai dati dei titolari di carta. *Per dettagli, fare riferimento al Requisito 12.8 nel presente documento.*

Migliori pratiche per implementare lo standard PCI DSS nei processi business-as-usual

Per garantire che i controlli di sicurezza continuino ad essere correttamente implementati, è opportuno implementare lo standard PCI DSS nelle attività BAU (business-as-usual) nell'ambito della strategia di sicurezza complessiva dell'entità. In questo modo, l'entità ha la possibilità di monitorare l'efficacia costante dei propri controlli di sicurezza e di garantire la conformità del proprio ambiente allo standard PCI DSS tra una valutazione PCI DSS e l'altra. Esempi di come incorporare lo standard PCI DSS nelle attività BAU possono essere, senza limitazioni:

1. Monitoraggio dei controlli di sicurezza, quali firewall, sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS), monitoraggio dell'integrità dei file (FIM), antivirus, controlli degli accessi, ecc., per dimostrare di operare in modo efficiente e come pianificato.
2. Garanzia di rilevamento e risoluzione tempestiva di tutti gli errori presenti nei controlli di sicurezza. I processi di risoluzione degli errori presenti nei controlli di sicurezza includono:
 - ripristino del controllo di sicurezza;
 - identificazione della causa dell'errore;
 - identificazione e risoluzione di eventuali problemi di sicurezza che insorgono durante l'errore del controllo di sicurezza;
 - implementazione della riduzione dei rischi (ad esempio, controlli tecnici o di processo) per impedire che la causa dell'errore si ripresenti;
 - prosecuzione del monitoraggio del controllo di sicurezza, magari con un monitoraggio avanzato per un determinato periodo, per verificare che il controllo funzioni in modo efficiente.
3. Revisione delle modifiche all'ambiente (ad esempio, aggiunta di nuovi sistemi, modifiche delle configurazioni di rete o di sistema) prima del completamento della modifica e realizzazione delle seguenti operazioni:
 - determinazione del potenziale impatto sull'ambito della valutazione PCI DSS (ad esempio, una nuova regola del firewall che consente di collegare un sistema nell'ambiente dei dati dei titolari di carta a un altro sistema potrebbe inserire ulteriori sistemi o reti nell'ambito della valutazione PCI DSS);
 - identificazione dei requisiti PCI DSS applicabili ai sistemi e alle reti interessati dalle modifiche (ad esempio, se un nuovo sistema viene inserito nell'ambito della valutazione PCI DSS, è necessario configurarlo in base agli standard di configurazione dei sistemi, inclusi FIM, AV, patch, log di audit, ecc., e aggiungerlo nel piano trimestrale delle scansioni delle vulnerabilità);
 - aggiornamento dell'ambito della valutazione PCI DSS e implementazione dei controlli di sicurezza secondo le esigenze.
4. Modifiche alla struttura organizzativa (ad esempio, fusione o acquisizione aziendale) che comportano un'analisi formale dell'impatto sui requisiti e sull'ambito PCI DSS.
5. Esecuzione di revisioni e comunicazioni periodiche per confermare che i requisiti PCI DSS continuano a essere presenti e che il personale sta seguendo processi sicuri. Queste recensioni periodiche devono fornire tutte le informazioni su strutture e sedi, inclusi punti vendita, centri dati ecc., e devono includere la revisione dei componenti di sistema (o campioni dei componenti di sistema) per verificare che i requisiti PCI DSS continuano a essere presenti (ad esempio, gli standard di configurazione sono stati applicati, le patch e l'antivirus sono

aggiornati, i log di audit sono stati sottoposti a revisione, ecc.). L'entità è tenuta a stabilire la frequenza delle revisioni periodiche a seconda delle dimensioni e della complessità del proprio ambiente.

È possibile utilizzare queste revisioni per verificare che sia stata conservata la prova corretta (ad esempio, log di audit, rapporti delle scansioni delle vulnerabilità, revisioni dei firewall, ecc.) e facilitare la preparazione dell'entità alla prossima valutazione della conformità.

6. Revisione delle tecnologie hardware e software almeno una volta all'anno, per confermare che continuano a essere supportate dal fornitore e che sono in grado di soddisfare i requisiti di sicurezza dell'entità, inclusi i requisiti PCI DSS. Se emerge che le tecnologie non sono più supportate da fornitore o che non riescono più a soddisfare le esigenze di sicurezza dell'entità, l'entità è tenuta ad adottare un piano di azioni correttive ed eventualmente a sostituire le tecnologie secondo necessità.

Oltre alle prassi menzionate sopra, è possibile che le organizzazioni intendano prendere in considerazione l'implementazione della separazione delle responsabilità per le proprie funzioni di sicurezza, in modo da separare le funzioni di sicurezza e/o audit da quelle operative. Negli ambienti in cui un singolo individuo svolge più mansioni (ad esempio, operazioni di amministrazione e sicurezza), è possibile assegnare le responsabilità in modo da evitare che un singolo individuo abbia l'intero controllo di un processo senza la presenza di un punto di controllo indipendente. Ad esempio, è possibile assegnare a soggetti diversi la responsabilità della configurazione e la responsabilità dell'approvazione delle modifiche.

Nota: per alcune entità, queste migliori pratiche sono anche requisiti per garantire la costante conformità agli standard PCI DSS. Ad esempio, PCI DSS include questi principi in alcuni requisiti e la convalida aggiuntiva delle entità designate (Appendice A3 PCI DSS) richiede entità designate da convalidare in base a questi principi.

Tutte le organizzazioni dovrebbero valutare la possibilità di implementare queste migliori pratiche nel loro ambiente, anche quando l'organizzazione non è tenuta a convalidarle.

Per valutatori: campionamento delle strutture aziendali e dei componenti di sistema

Il campionamento è facoltativo per i valutatori e consente di facilitare il processo di valutazione in cui è presente un elevato numero di strutture aziendali e/o componenti di sistema.

Se da un lato un assessore può effettuare il campionamento delle strutture aziendali e dei componenti di sistema nell'ambito della revisione della conformità allo standard PCI DSS dell'entità, dall'altro un'entità non può applicare i requisiti PCI DSS solo per effettuare il campionamento del proprio ambiente (ad esempio, i requisiti per le scansioni trimestrali della vulnerabilità valgono per tutti i componenti di sistema). In modo simile, non è accettabile che un valutatore esamini soltanto un campione di requisiti PCI DSS per la conformità.

Dopo aver preso in considerazione l'ambito generale e la 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 dell'entità 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 sedi 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.

Esempi di strutture aziendali includono, senza limitazioni: uffici, negozi, sedi in franchising, strutture di elaborazione, centri dati e 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, 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 una 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 controlli e processi di sicurezza e operativi PCI DSS standard e centralizzati che assicurano uniformità 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. Il valutatore è tenuto a verificare che i controlli standard, centralizzati vengano implementati e funzionino in modo efficace;
- 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;

- i campioni dei componenti di sistema devono includere tutti i tipi e le combinazioni in uso. Ad esempio, quando le applicazioni vengono campionate, il campione deve includere tutte le versioni e le piattaforme per ciascun tipo di applicazione.

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 standard e i controlli utilizzati per stabilire la dimensione del campione;
- 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 contenuti per il rapporto sulla conformità

Le istruzioni e i contenuti per il rapporto sulla conformità (ROC) ora vengono forniti nel *modello di reporting ROC PCI DSS*.

Il *modello di reporting ROC PCI DSS* deve essere utilizzato come modello per creare il *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 o l'acquirente.

Processo di valutazione PCI DSS

Il processo di valutazione PCI DSS include il completamento delle seguenti operazioni:

1. Confermare l'ambito della valutazione PCI DSS.
2. Eseguire la valutazione PCI per l'ambiente, seguendo le procedure di test per ogni requisito.
3. Compilare il rapporto applicabile per la valutazione (ad esempio, il *Questionario di autovalutazione*, SAQ, o il Rapporto sulla conformità, ROC) compresa la documentazione di tutti i controlli compensativi, in base alle istruzioni PCI applicabili.
4. 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.
5. Inviare il questionario di autovalutazione o il rapporto sulla conformità e l'Attestato di conformità, insieme ad eventuale altra documentazione richiesta (ad esempio, i rapporti delle scansioni dei fornitori di prodotti di scansione approvati) al proprio acquirente (per gli esercenti) o al marchio di pagamento o ad altra entità richiedente (per i provider di servizi).
6. Se richiesto, eseguire attività di correzione per soddisfare i requisiti non applicati e fornire un rapporto aggiornato.

Versioni PCI DSS

Alla data di pubblicazione di questo documento, PCI DSS v3.1 è valida fino al 31 ottobre 2016, dopodichè sarà ritirata. Tutte le convalide PCI DSS dopo questa data devono fare riferimento a PCI DSS versione 3.2 o successiva.

La tabella riportata di seguito fornisce un riepilogo delle versioni PCI DSS e delle relative date di validità⁶.

Versione	Data di pubblicazione:	Data di ritiro:
PCI DSS v3.2 (questo documento)	Aprile 2016	Da determinare
PCI DSS v3.1	Aprile 2015	31 ottobre 2016

⁶ Dati soggetti a modifiche in caso di rilascio di una nuova versione di PCI DSS.

Requisiti PCI DSS e procedure di valutazione della sicurezza dettagliate

Di seguito, vengono riportati gli elementi che costituiscono le intestazioni delle colonne per i requisiti PCI DSS e le procedure di valutazione della sicurezza.

- **Requisiti PCI DSS:** questa colonna definisce i requisiti dello Standard di protezione dei dati; la conformità allo standard PCI DSS viene 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 rispettati e “presenti”.
- **Istruzioni:** questa colonna descrive lo scopo o l’obiettivo di sicurezza di ogni requisito PCI DSS. Questa colonna contiene soltanto istruzioni e mira a facilitare la comprensione dello scopo di ciascun requisito. Le istruzioni di questa colonna non sostituiscono né estendono i requisiti PCI DSS e le procedure di test.

Nota: i requisiti PCI DSS non vengono considerati presenti se i controlli non sono stati ancora implementati o se sono programmati per una data futura. Dopo che eventuali elementi aperti o non a norma sono stati corretti dall’entità, il valutatore esegue nuovamente la valutazione per confermare che la correzione sia stata apportata e che tutti i requisiti siano stati soddisfatti.

Consultare le seguenti risorse (disponibili su sito Web PCI SSC) per documentare la valutazione PCI DSS:

- per le istruzioni sul completamento dei rapporti di conformità (ROC), consultare il modello di reporting ROC PCI DSS;
- per le istruzioni sul completamento del questionario di autovalutazione (SAQ), consultare le Istruzioni e linee guida SAQ PCI DSS;
- per istruzioni sull’inoltro dei rapporti di convalida della conformità PCI DSS, consultare gli Attestati di conformità PCI DSS.

Sviluppo e gestione di sistemi e reti sicure

Requisito 1 - Installare e gestire una configurazione firewall per proteggere i dati dei 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 della 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	Istruzioni
1.1 Stabilire e implementare standard di configurazione del firewall e del router che includano:	1.1 Esaminare lo standard di configurazione del firewall e del router e altra documentazione specificata di seguito e verificare che tali standard siano completi e implementati come segue:	Firewall e router sono i componenti principali dell'architettura che controlla l'accesso e l'uscita dalla rete. Questi dispositivi di tipo software o hardware bloccano l'accesso indesiderato e gestiscono l'accesso autorizzato alla rete e l'uscita dalla stessa. Gli standard e le procedure di configurazione aiuteranno a garantire che la prima linea di difesa dell'organizzazione per la protezione dei suoi dati sia sempre solida.
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.a Esaminare le procedure documentate per verificare se è presente un processo formale per il test e l'approvazione di: <ul style="list-style-type: none"> connessioni di rete e modifiche a configurazioni di firewall e router 	Un processo documentato e implementato per approvare e testare tutte le connessioni e le modifiche ai firewall e ai router aiuterà a prevenire i problemi di protezione causati dall'errata configurazione della rete, del router o del firewall. Senza approvazione formale e test delle modifiche, i record dei cambiamenti potrebbero non essere aggiornati, il che porterebbe a incongruenze tra la documentazione di rete e la configurazione effettiva.
	1.1.1.b Per ottenere un campione di connessioni di rete, consultare il personale responsabile ed esaminare i record per verificare che le connessioni di rete siano approvate e testate.	

Requisiti PCI DSS	Procedure di test	Istruzioni
	1.1.1.c Identificare un campione di modifiche effettive apportate alle configurazioni di firewall e router, confrontarle con i record delle modifiche e consultare il personale responsabile per verificare che le modifiche siano approvate e testate.	
1.1.2 Diagramma di rete aggiornato che identifica tutte le connessioni tra ambiente dei dati dei titolari di carta e altre reti, comprese eventuali reti wireless	1.1.2.a Esaminare i diagrammi e osservare le configurazioni di rete per verificare che sia presente un diagramma di rete aggiornato e che documenti tutte le connessioni ai dati dei titolari di carta, comprese eventuali reti wireless.	<p>I diagrammi di rete descrivono come le reti vengono configurate e identificano la posizione di tutti i dispositivi di rete.</p> <p>In assenza dei diagrammi di rete aggiornati e del flusso di dati, i dispositivi possono essere trascurati e privati inconsapevolmente dei controlli di protezione implementati per PCI DSS, rimanendo così vulnerabili in caso di compromissione.</p>
	1.1.2.b Consultare il personale responsabile per verificare che il diagramma sia sempre aggiornato.	
1.1.3 Diagramma aggiornato che mostra tutti i flussi dei dati dei titolari di carta sui sistemi e sulle reti	1.1.3 Esaminare il diagramma del flusso di dati e consultare il personale per verificare il diagramma: <ul style="list-style-type: none"> mostra tutti i flussi dei dati dei titolari di carta sui sistemi e sulle reti; viene sempre aggiornato non appena si verifica una modifica all'ambiente. 	<p>I diagrammi del flusso di dati dei titolari di carta identificano la posizione di tutti i dati dei titolari di carta memorizzati, elaborati o trasmessi all'interno della rete.</p> <p>I diagrammi del flusso di dati dei titolari di carta aiutano un'organizzazione a comprendere e a registrare la portata del loro ambiente, mostrando come i dati dei titolari di carta vengono trasmessi sulle reti e tra sistemi e dispositivi singoli.</p>
1.1.4 Requisiti per un firewall per ogni connessione Internet e tra tutte le zone demilitarizzate (DMZ) e la zona della rete interna	1.1.4.a Esaminare gli standard di configurazione del firewall e verificare che includano i requisiti per un firewall a ogni connessione Internet e tra la zona DMZ e la zona della rete interna.	<p>L'uso di un firewall su ogni connessione Internet in ingresso (e in uscita) nella rete, e tra la zona DMZ e la rete interna, consente all'organizzazione di monitorare e controllare l'accesso, nonché di ridurre al minimo le possibilità che un utente non autorizzato ottenga l'accesso alla rete interna attraverso una connessione non protetta.</p>
	1.1.4.b Verificare che il diagramma di rete aggiornato sia coerente con gli standard di configurazione del firewall.	
	1.1.4.c Osservare le configurazioni di rete per verificare che un firewall sia attivo a ogni connessione Internet e tra una zona DMZ e la rete interna, come previsto dagli standard di configurazione documentati e dai diagrammi di rete.	

Requisiti PCI DSS	Procedure di test	Istruzioni
1.1.5 Descrizione di gruppi, ruoli e responsabilità per la gestione dei componenti di rete	1.1.5.a Verificare che gli standard di configurazione del firewall e del router includano una descrizione dei gruppi, dei ruoli e delle responsabilità per la gestione dei componenti di rete.	<p>Questa descrizione dei ruoli e dell'assegnazione di responsabilità fa in modo che il personale conosca chi è responsabile della sicurezza di tutti i componenti di rete e che le persone assegnate alla gestione dei componenti conoscano bene le proprie responsabilità. Se i ruoli e le responsabilità non vengono assegnati in modo formale, si rischia di avere dispositivi non gestiti.</p>
	1.1.5.b Consultare il personale responsabile della gestione dei componenti di rete per confermare che i ruoli e le responsabilità siano assegnati e documentati.	
1.1.6 Documentazione della giustificazione e dell'approvazione aziendali per l'uso di tutti i servizi, i protocolli e le porte consentiti, inclusa la documentazione delle funzioni di sicurezza implementate per i protocolli considerati non sicuri.	1.1.6.a Verificare che gli standard di configurazione del firewall e del router includano un elenco documentato di tutti i servizi, i protocolli e le porte, comprese la giustificazione e l'approvazione aziendali per ciascuno.	<p>Le compromissioni spesso avvengono a causa di servizi e porte inutilizzati o non protetti, in quanto spesso essi presentano delle vulnerabilità note. Molte organizzazioni non applicano le patch per la correzione delle vulnerabilità di servizi, protocolli e porte non in uso (anche se le vulnerabilità sono tuttora presenti). Se definiscono e documentano in modo chiaro i servizi, i protocolli e le porte che sono necessari a livello aziendale, le organizzazioni possono garantire che tutti gli altri servizi, protocolli e porte vengano disabilitati o rimossi.</p> <p>Le approvazioni dovrebbero essere concesse dal personale indipendente dal personale di gestione della configurazione.</p> <p>Se servizi, protocolli o porte non sicuri sono indispensabili per l'azienda, è necessario comprendere pienamente il rischio posto dall'uso di questi protocolli e accettarlo; occorre inoltre giustificare l'uso del protocollo e documentare e implementare le funzionalità di protezione che consentono l'uso sicuro di tali protocolli. Se questi servizi, protocolli o porte non sicuri non sono indispensabili per l'azienda, è opportuno disabilitarli o rimuoverli.</p> <p>Per istruzioni su servizi, protocolli o porte considerati non sicuri, fare riferimento alle linee guida e agli standard di settore (ad es., NIST, ENISA, OWASP, ecc.).</p>
	1.1.6.b Identificare i servizi, i protocolli e le porte non sicuri consentiti e verificare che le funzioni di sicurezza siano documentate per ogni servizio.	
	1.1.6.c Esaminare le configurazioni di firewall e router per verificare che le funzioni di sicurezza documentate siano implementate per ogni servizio, protocollo e porta.	

Requisiti PCI DSS	Procedure di test	Istruzioni
1.1.7 Una revisione dei set di regole del firewall e del router almeno ogni sei mesi	1.1.7.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.	<p>Questa revisione consente all'organizzazione di cancellare ogni sei mesi eventuali regole inutili, obsolete o errate, garantendo che tutti i set di regole consentano solamente le porte e i servizi autorizzati corrispondenti alle giustificazioni aziendali documentate.</p> <p>Le organizzazioni che apportano un elevato volume di modifiche ai set di regole di firewall e router possono prendere in considerazione la possibilità di eseguire le revisioni con maggiore frequenza, per garantire che i set di regole siano sempre conformi alle esigenze dell'azienda.</p>
	1.1.7.b Esaminare la documentazione relativa al set di regole e consultare il personale responsabile per verificare che il set di regole sia rivisto almeno una volta ogni sei mesi.	
1.2 Creazione di configurazioni di firewall e router che limitino le connessioni tra le reti non attendibili e qualsiasi componente di sistema nell'ambiente dei dati dei titolari di carta. <p>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.</p>	1.2 Esaminare le configurazioni di firewall e router ed eseguire le seguenti operazioni per verificare che le connessioni tra le reti non attendibili e i componenti di sistema nell'ambiente dei dati dei titolari di carta siano limitate:	<p>È fondamentale installare una protezione di rete tra la rete attendibile interna e qualsiasi rete non attendibile esterna e/o che l'entità non è in grado di controllare o gestire. La mancata implementazione di questa misura comporta la vulnerabilità dell'entità all'accesso non autorizzato da parte di utenti o software dannosi.</p> <p>Affinché la funzionalità firewall sia efficace, è necessario configurarla correttamente per controllare e/o limitare il traffico all'interno e all'esterno della rete dell'entità.</p>
1.2.1 Limitazione del traffico in entrata e in uscita a quello indispensabile per l'ambiente dati dei titolari di carta e, specificatamente, rifiutare tutto l'altro traffico.	1.2.1.a Esaminare gli standard di configurazione di firewall e router per verificare che siano in grado di identificare il traffico in entrata e in uscita necessario per l'ambiente dei dati dei titolari di carta.	<p>L'esame di tutte le connessioni in entrata e in uscita consente di controllare e limitare il traffico in base a indirizzo di origine e/o destinazione, in modo da evitare l'accesso non filtrato tra ambienti attendibili e non attendibili. Questo requisito intende impedire agli utenti non autorizzati di accedere alla rete dell'entità tramite indirizzi IP non autorizzati o mediante l'uso di servizi, protocolli o porte in maniera non autorizzata (ad esempio per inviare i dati ottenuti all'interno della rete dell'entità verso un server non attendibile).</p> <p>L'implementazione di una regola che impedisca tutto il traffico in entrata e in uscita che non sia specificatamente necessario aiuta a prevenire l'apertura involontaria di falle che potrebbe</p>
	1.2.1.b Esaminare le configurazioni di firewall e router per verificare che il traffico in entrata e in uscita sia limitato a quello necessario per l'ambiente dei dati dei titolari di carta.	
	1.2.1.c Esaminare le configurazioni di firewall e router per 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	Istruzioni
		consentire del traffico in entrata o in uscita non intenzionale e potenzialmente dannoso.
1.2.2 Protezione e sincronizzazione dei file di configurazione del router.	1.2.2.a Esaminare i file di configurazione del router per verificare che siano protetti contro l'accesso non autorizzato.	<p>Mentre i file di configurazione del router in esecuzione (o attivo) comprendono le impostazioni attuali sicure, i file di avvio (utilizzati in caso di riavvio dei router) devono essere aggiornati con le stesse impostazioni sicure per garantire che queste impostazioni vengano applicate quando si esegue la configurazione all'avvio.</p> <p>Poiché eseguiti solo occasionalmente, i file di configurazione all'avvio vengono spesso ignorati e non aggiornati. Quando un router esegue il riavvio e carica una configurazione al riavvio che non è stata aggiornata con le stesse impostazioni sicure della configurazione in esecuzione, le regole potrebbero indebolirsi e consentire la presenza sulla rete di individui non autorizzati.</p>
	1.2.2.b Esaminare le configurazioni del router per verificare che siano sincronizzate, ad esempio che la configurazione in esecuzione (o attiva) corrisponda alla configurazione all'avvio (utilizzata in caso di riavvio delle macchine).	
1.2.3 Installazione di firewall perimetrali tra le reti wireless e l'ambiente dei dati dei titolari di carta e configurazione di tali firewall per negare o controllare (se necessario per gli scopi aziendali) solo il traffico autorizzato tra l'ambiente wireless e l'ambiente dei dati dei titolari di carta.	1.2.3.a Esaminare le configurazioni di firewall e router per verificare che siano stati installati firewall perimetrali tra tutte le reti wireless e l'ambiente dati dei titolari di carta.	<p>L'implementazione e lo sfruttamento noti (o sconosciuti) della tecnologia wireless all'interno di una rete rappresentano un percorso noto agli utenti non autorizzati per ottenere l'accesso alla rete e ai dati dei titolari di carta. Se viene installato un dispositivo o una rete wireless senza che l'entità ne sia a conoscenza, un utente non autorizzato potrebbe accedere alla rete con facilità e in modo "invisibile". Se i firewall non limitano l'accesso dalle reti wireless all'ambiente dei dati dei titolari di carta, gli utenti che ottengono accesso non autorizzato alla rete wireless possono facilmente connettersi a tale ambiente e compromettere le informazioni dei conti.</p> <p>Si devono installare i firewall tra tutte le reti wireless ed l'ambiente dei dati dei titolari di carta (CDE), indipendentemente dallo scopo dell'ambiente al quale la rete wireless network è collegata. Ciò può comprendere, senza limitazioni, reti aziendali, negozi di vendita al</p>
	1.2.3.b Verificare che il firewall blocchi il traffico o, se necessario per gli scopi aziendali, controlli solo il traffico autorizzato tra l'ambiente wireless e l'ambiente dati dei titolari di carta.	

Requisiti PCI DSS	Procedure di test	Istruzioni
		dettaglio, reti guest, ambienti magazzino, ecc.
1.3 Vietare l'accesso pubblico diretto tra Internet e i componenti di sistema nell'ambiente dei dati dei 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 e il segmento di rete di titolari di carta interno, ed eseguire le operazioni riportate di seguito per determinare che non vi sia accesso diretto tra Internet e i componenti di sistema nel segmento di rete dei titolari di carta interno:	Sebbene possano sussistere motivi legittimi per consentire connessioni non attendibili a sistemi DMZ (ad es., per consentire l'accesso pubblico a un server Web), non si deve mai concedere tali connessioni a sistemi presenti nella rete interna. Lo scopo di un firewall è gestire e controllare tutte le connessioni tra sistemi pubblici e sistemi interni, in particolare quelli che memorizzano, elaborano o trasmettono i dati dei titolari di carta. Se è consentito l'accesso diretto tra sistemi pubblici e l'ambiente dei dati dei titolari di carta, la protezione offerta dal firewall viene superata e i componenti di sistema che memorizzano i dati dei titolari di carta sono esposti alla compromissione.
1.3.1 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.	1.3.1 Esaminare le configurazioni di firewall e router per 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.	La zona DMZ è la parte della rete che gestisce le connessioni tra Internet (o altre reti non attendibili) e i servizi interni che un'organizzazione deve mettere a disposizione del pubblico (ad esempio un server Web).
1.3.2 Limitazione del traffico Internet in entrata agli indirizzi IP all'interno della zona DMZ.	1.3.2 Esaminare le configurazioni di firewall e router per verificare che il traffico Internet in entrata sia limitato agli indirizzi IP all'interno della zona DMZ.	Questa funzionalità intende impedire agli utenti non autorizzati di accedere alla rete interna dell'organizzazione tramite Internet o mediante l'uso di servizi, protocolli o porte in maniera non autorizzata.

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>1.3.3 Implementare misure anti-spoofing per rilevare gli indirizzi IP di origine contraffatti e per impedire loro di accedere alla rete.</p> <p>(Ad esempio, bloccare il traffico proveniente da Internet con un indirizzo di origine interno.)</p>	<p>1.3.3 Esaminare le configurazioni di firewall e router per verificare che siano state implementate le misure anti-spoofing; gli indirizzi interni non possono, ad esempio, passare da Internet alla zona DMZ.</p>	<p>In genere un pacchetto contiene l'indirizzo IP del computer che lo ha inviato originariamente così gli altri computer della rete conoscono la provenienza del pacchetto. Spesso gli utenti non autorizzati cercano di falsificare (o imitare) l'indirizzo IP di invio in modo da fare credere al sistema di destinazione che la provenienza del pacchetto sia attendibile.</p> <p>I pacchetti di filtri in ingresso nella rete consentono, tra le altre cose, di garantire che i pacchetti non siano stati "falsificati" per far sì che sembrino provenire dalla rete interna di un'organizzazione.</p>
<p>1.3.4 Non consentire il traffico in uscita non autorizzato dall'ambiente dei dati dei titolari di carta a Internet.</p>	<p>1.3.4 Esaminare le configurazioni di firewall e router per verificare che il traffico in uscita dall'ambiente dei dati dei titolari di carta a Internet sia esplicitamente autorizzato.</p>	<p>Tutto il traffico in uscita dall'ambiente dei dati dei titolari di carta dovrebbe essere valutato per assicurare che segua norme autorizzate e definite. Si dovrebbero controllare le connessioni per limitare il traffico solo alle comunicazioni autorizzate (ad esempio limitando indirizzi/porte fonte/destinazione e/o bloccando i contenuti).</p>
<p>1.3.5 Consentire nella rete solo le connessioni già "stabilite".</p>	<p>1.3.5 Esaminare le configurazioni di firewall e router per verificare che il firewall consenta nella rete interna solo le connessioni già stabilite e neghi eventuali connessioni in entrata non associate a una sessione stabilita in precedenza.</p>	<p>Mantenendo lo "stato" per ciascuna connessione, il firewall sa se quella che sembra essere la risposta a una connessione precedente è realmente una risposta valida, autorizzata (in quanto memorizza lo stato di tutte le connessioni) o se si tratta di traffico dannoso che cerca di indurre il firewall a consentire la connessione.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>1.3.6 Posizionare i componenti di sistema che memorizzano i 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>1.3.6 Esaminare le configurazioni di firewall e router per verificare che i componenti di sistema che memorizzano i dati dei titolari di carta siano in una zona di rete interna, separata dalla zona DMZ e da altre reti non attendibili.</p>	<p>Se i dati dei titolari di carta sono all'interno della zona DMZ, un aggressore esterno può accedere più facilmente a queste informazioni, in quanto esistono meno strati da penetrare. La protezione dei componenti di sistema che memorizzano i dati dei titolari di carta in una zona di rete interna, separata dalla zona DMZ e da altre reti non attendibili mediante firewall, consente di impedire al traffico di rete non autorizzato di raggiungere il componente di sistema.</p> <p>Nota: questo requisito non è valido per l'archiviazione temporanea dei dati dei titolari di carta nella memoria volatile.</p>
<p>1.3.7 Non divulgare indirizzi IP privati e 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; • 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>1.3.7.a Esaminare le configurazioni di firewall e router per verificare che siano in atto metodi per impedire la divulgazione di indirizzi IP privati e di informazioni di routing da reti interne a Internet.</p> <p>1.3.7.b Consultare il personale ed esaminare la documentazione per verificare che siano autorizzate eventuali divulgazioni di indirizzi IP privati e di informazioni di routing a entità esterne.</p>	<p>La limitazione della divulgazione degli indirizzi IP interni o privati è fondamentale per evitare che un hacker si "impossessi" degli indirizzi IP della rete interna e utilizzi tali informazioni per accedere alla rete.</p> <p>I metodi utilizzati per soddisfare lo scopo di questo requisito possono variare in funzione della tecnologia di rete specifica in uso nell'ambiente. Ad esempio, i controlli adottati per soddisfare questo requisito possono essere diversi per reti IPv4 rispetto a quelli in uso per le reti IPv6.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>1.4 Installare il firewall personale o funzionalità equivalente su tutti i dispositivi mobili (inclusi quelli di proprietà dell'azienda e/o dei dipendenti) con connettività a Internet se all'esterno della rete (ad esempio, laptop utilizzati dai dipendenti) e che vengono utilizzati anche per accedere al CDE. Le configurazioni del firewall (o funzionalità equivalente) includono quanto segue:</p> <ul style="list-style-type: none"> vengono definite impostazioni di configurazione specifiche; il firewall personale (o funzionalità equivalente) è attivamente in esecuzione; il firewall personale (o funzionalità equivalente) non è modificabile dagli utenti di dispositivi mobili. 	<p>1.4.a Esaminare le politiche e gli standard di configurazione per verificare che:</p> <ul style="list-style-type: none"> il firewall personale o funzionalità equivalente sia richiesto per tutti i dispositivi mobili (inclusi quelli di proprietà dell'azienda e/o dei dipendenti) con connettività a Internet se all'esterno della rete (ad esempio, laptop utilizzati dai dipendenti) e che vengono utilizzati anche per accedere al CDE; per il firewall personale (o funzionalità equivalente) vengano definite specifiche impostazioni di configurazione; il firewall personale (o funzionalità equivalente) sia configurato per essere attivamente eseguito; il firewall personale (o funzionalità equivalente) sia configurato per non essere modificabile dagli utenti di dispositivi mobili. 	<p>I dispositivi portatili autorizzati a connettersi a Internet dall'esterno del firewall aziendale sono più vulnerabili alle minacce basate su Internet. L'uso di un firewall (ad es. hardware o firewall personale) aiuta a proteggere i dispositivi dagli attacchi basati su Internet, che potrebbero utilizzare il dispositivo per accedere ai sistemi e ai dati dell'organizzazione quando il dispositivo si riconnette alla rete.</p> <p>Le impostazioni specifiche di configurazione del firewall vengono stabilite dall'organizzazione.</p> <p>Nota: questo requisito si applica ai dispositivi mobili di proprietà dei dipendenti e dell'azienda. I sistemi che non possono essere gestiti dalla politica aziendale introducono dei punti deboli e offrono opportunità di cui gli utenti non autorizzati possono approfittare. Consentendo ai sistemi non attendibili di connettersi al CDE dell'organizzazione, è possibile che si fornisca l'accesso ad aggressori e altri utenti non autorizzati.</p>
	<p>1.4.b Controllare un campione di dispositivi di proprietà dell'azienda e/o dei dipendenti per verificare che:</p> <ul style="list-style-type: none"> il firewall personale (o funzionalità equivalente) sia installato e configurato in base alle specifiche impostazioni di configurazione dell'organizzazione; il firewall personale (o funzionalità equivalente) sia attivamente in esecuzione; il firewall personale (o funzionalità equivalente) non sia modificabile dagli utenti di dispositivi mobili. 	
<p>1.5 Verificare che le politiche di sicurezza e le procedure operative per la gestione dei firewall siano documentate, in uso e note a tutte le parti coinvolte.</p>	<p>1.5 Esaminare la documentazione e consultare il personale per verificare che le politiche di sicurezza e le procedure operative per la gestione dei firewall siano:</p> <ul style="list-style-type: none"> documentate; in uso note a tutte le parti coinvolte. 	<p>È necessario che il personale sia a conoscenza delle seguenti politiche di sicurezza e procedure operative per garantire che i firewall e i router siano costantemente gestiti in modo da impedire l'accesso non autorizzato alla rete.</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	Istruzioni
<p>2.1 Modificare sempre i valori predefiniti del fornitore e rimuovere o disabilitare account predefiniti non necessari prima di installare un sistema sulla rete.</p> <p>Questo vale per TUTTE le password predefinite, incluse, senza limitazioni, quelle utilizzate da sistemi operativi, software che fornisce servizi di sicurezza, account di applicazioni e sistemi, <i>terminali</i> POS (Point-Of-Sale), stringhe di comunità SNMP (Simple Network Management Protocol), ecc.</p>	<p>2.1.a Scegliere un campione di componenti di sistema e tentare l'accesso (con l'aiuto dell'amministratore di sistema) ai dispositivi e alle applicazioni che utilizzano account e password predefinite dal fornitore, per verificare che TUTTE le password predefinite (incluse quelle di sistemi operativi, software che offrono servizi di sicurezza, account di applicazioni e sistemi, terminali POS e stringhe di comunità SNMP (Simple Network Management Protocol)) siano state modificate. (Per trovare account/password del fornitore, consultare i manuali e le fonti su Internet).</p>	<p>Gli utenti non autorizzati (all'interno o all'esterno di un'organizzazione) utilizzano spesso le impostazioni predefinite, i nomi degli account e le password dei fornitori per compromettere i sistemi operativi, le applicazioni e i sistemi su cui sono installati. Dal momento che queste impostazioni predefinite vengono spesso pubblicate e sono conosciute nelle comunità degli hacker, la modifica di tali impostazioni rende i sistemi meno vulnerabili agli attacchi.</p> <p>Anche se l'account predefinito non viene utilizzato, modificando la password predefinita con una password univoca complessa e disattivando l'account si impedisce agli utenti non autorizzati di riattivare l'account e accedere con la password predefinita.</p>
	<p>2.1.b Per il campione dei componenti di sistema, verificare che tutti gli account predefiniti non necessari (inclusi gli account utilizzati da sistemi operativi, software di sicurezza, applicazioni, sistemi, terminali POS, SNMP, ecc.) siano stati rimossi o disattivati.</p>	
	<p>2.1.c Consultare il personale ed esaminare la documentazione di supporto per verificare che:</p> <ul style="list-style-type: none"> tutti i valori predefiniti dei fornitori (inclusi password predefinite nei sistemi operativi, software che offrono servizi di sicurezza, account di applicazioni e sistemi, terminali POS, stringhe di comunità SNMP (Simple Network Management Protocol), ecc.) sono stati modificati prima dell'installazione di un sistema sulla rete; gli account predefiniti non necessari (inclusi gli account utilizzati da sistemi operativi, software di sicurezza, applicazioni, sistemi, terminali POS, SNMP, ecc.) sono stati rimossi o disattivati prima dell'installazione di un sistema sulla rete. 	

Requisiti PCI DSS	Procedure di test	Istruzioni
2.1.1 Per gli ambienti wireless connessi all'ambiente dei dati dei titolari di carta o che trasmettono tali dati, modificare TUTTE le impostazioni predefinite del fornitore wireless, incluse, senza limitazioni, chiavi di cifratura wireless predefinite, password e stringhe di comunità SNMP.	2.1.1.a Consultare il personale responsabile ed esaminare la documentazione di supporto per verificare che: <ul style="list-style-type: none"> le chiavi di cifratura sono state modificate al momento dell'installazione per impostazione predefinita; le chiavi di cifratura vengono modificate ogni volta che un utente a conoscenza delle chiavi lascia l'azienda o cambia sede. 	<p>Se le reti wireless non vengono implementate con configurazioni di sicurezza sufficienti (che comprendono la modifica delle impostazioni predefinite), gli sniffer wireless possono ascoltare di nascosto il traffico, acquisire facilmente i dati e le password e accedere alla rete per l'attacco.</p> <p>Inoltre, il protocollo di scambio delle chiavi per le precedenti versioni della cifratura 802.11x (WEP, Wired Equivalent Privacy) è stato violato e può rendere inutile la cifratura. È necessario che il firmware dei dispositivi venga aggiornato per supportare protocolli più sicuri.</p>
	2.1.1.b Consultare il personale ed esaminare politiche e procedure da verificare: <ul style="list-style-type: none"> in seguito all'installazione, è necessario modificare le stringhe di comunità SNMP predefinite; in seguito all'installazione, è necessario modificare le password/passphrase predefinite sui punti di accesso. 	
	2.1.1.c Esaminare la documentazione del fornitore e accedere ai dispositivi wireless, con l'aiuto dell'amministratore di sistema, per verificare che: <ul style="list-style-type: none"> le stringhe di comunità SNMP predefinite non sono utilizzate; le password/passphrase predefinite sui punti di accesso non sono utilizzate. 	
	2.1.1.d Esaminare la documentazione del fornitore e osservare le impostazioni di configurazione wireless per verificare che il firmware dei dispositivi wireless sia aggiornato per supportare la cifratura avanzata per: <ul style="list-style-type: none"> l'autenticazione su reti wireless; la trasmissione su reti wireless. 	
	2.1.1.e Esaminare la documentazione del fornitore e osservare le impostazioni di configurazione wireless per verificare che gli altri valori predefiniti del fornitore connessi alla sicurezza siano stati modificati, se applicabile.	

Requisiti PCI DSS	Procedure di test	Istruzioni
<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 limitazioni:</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>Esistono punti deboli noti in molti sistemi operativi, database e applicazioni aziendali, ma esistono anche metodi noti per configurare questi sistemi e risolvere le vulnerabilità di protezione. Per aiutare i meno esperti nel campo della sicurezza, molte organizzazioni che si occupano di sicurezza hanno stabilito alcune linee guida e raccomandazioni per il rafforzamento dei sistemi che spiegano come gestire questi punti deboli.</p> <p>Esempi di fonti di istruzioni sugli standard di configurazione includono, senza limitazioni: www.nist.gov, www.sans.org e www.cisecurity.org, www.iso.org e i fornitori di prodotti.</p> <p>È necessario tenere aggiornati gli standard di configurazione del sistema per assicurare che i punti deboli rilevati di recente vengano corretti prima dell'installazione del sistema sulla rete.</p>
	<p>2.2.b Esaminare le politiche e consultare il personale per verificare che gli standard di configurazione del sistema siano aggiornati quando vengono identificati nuovi problemi di vulnerabilità, secondo quanto definito al Requisito 6.1.</p>	
	<p>2.2.c Esaminare le politiche e consultare il personale per verificare che gli standard di configurazione del sistema vengano applicati quando si configurano e si verificano nuovi sistemi prima dell'installazione di un sistema sulla rete.</p>	
	<p>2.2.d Verificare che gli standard di configurazione del sistema includano le seguenti procedure per tutti i tipi di componenti di sistema:</p> <ul style="list-style-type: none"> • modifica di tutti i valori predefiniti del fornitore ed eliminazione di account predefiniti non necessari; • implementazione di una sola funzione principale per server per impedire la coesistenza sullo stesso server di funzioni che richiedono livelli di sicurezza diversi; • abilitazione di servizi, protocolli, daemon, ecc. necessari, come richiesto per la funzione del sistema; • implementazione di funzioni di sicurezza aggiuntive per servizi, protocolli o daemon necessari considerati non sicuro; • configurazione di parametri di sicurezza del sistema per evitare un uso improprio; • rimozione di tutta la funzionalità non necessaria, ad esempio script, driver, funzioni, sottosistemi, file system e server Web non utilizzati. 	

Requisiti PCI DSS	Procedure di test	Istruzioni
<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>Nota: dove si utilizzano tecnologie di virtualizzazione, implementare solo una funzione principale per componente di sistema virtuale.</p>	<p>2.2.1.a Selezionare un campione di componenti di sistema e controllare le configurazioni di sistema per verificare che sia stata implementata una sola funzione principale per server.</p>	<p>Se le funzioni server che necessitano di livelli di sicurezza diversi si trovano sullo stesso server, si verifica una riduzione del livello di sicurezza delle funzioni che richiedono livelli di sicurezza più elevati a causa della presenza di funzioni che richiedono minore protezione. Inoltre, è possibile che le funzioni server con un livello di sicurezza inferiore introducano punti deboli a livello di sicurezza nelle altre funzioni dello stesso server. Prendendo in considerazione i livelli di sicurezza richiesti dalle varie funzioni server nell'ambito degli standard di configurazione del sistema e dei relativi processi, le organizzazioni sono in grado di garantire che le funzioni che richiedono livelli di sicurezza diversi non coesistano sullo stesso server.</p>
	<p>2.2.1.a Se vengono utilizzate le tecnologie di virtualizzazione, controllare le configurazioni di sistema per verificare che sia stata implementata una sola funzione principale per componente di sistema virtuale o dispositivo.</p>	
<p>2.2.2 Abilitazione di servizi, protocolli, daemon, ecc. necessari, come richiesto per la funzione del sistema.</p>	<p>2.2.2.a Selezionare un campione di componenti di sistema e controllare i servizi di sistema, i daemon e i protocolli attivi per verificare che siano attivi solo i servizi o i protocolli necessari.</p>	<p>Come affermato nel Requisito 1.1.6, esistono molti protocolli di cui un'azienda potrebbe avere bisogno (o che sono attivati per impostazione predefinita) e che sono comunemente utilizzati da utenti non autorizzati per compromettere una rete. L'inserimento di questo requisito nell'ambito degli standard di configurazione dell'organizzazione e dei processi correlati consente di attivare solo i servizi e i protocolli necessari.</p>
	<p>2.2.2.b Identificare eventuali servizi, daemon o protocolli attivi non sicuri e consultare il personale per verificare che siano giustificati in base agli standard di configurazione documentati.</p>	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>2.2.3 Implementare funzioni di sicurezza aggiuntive per eventuali servizi, protocolli o daemon richiesti considerati non sicuri.</p> <p>Nota: laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.</p>	<p>2.2.3.a Controllare le impostazioni di configurazione per verificare che le funzioni di sicurezza siano documentate e implementate per tutti i servizi, daemon o protocolli non sicuri.</p>	<p>L'attivazione delle funzioni di sicurezza prima dell'implementazione dei nuovi server impedisce l'installazione dei server nell'ambiente con configurazioni non sicure.</p>
	<p>2.2.3.b Se si utilizza SSL/TLS iniziale, eseguire le procedure di test riportate nell'Appendice A2: <i>Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale</i>.</p>	<p>L'adeguata protezione di tutti i servizi, protocolli e daemon mediante adeguate funzioni di sicurezza ostacola gli utenti non autorizzati a trarre vantaggio dai punti di compromissione comunemente utilizzati all'interno di una rete.</p> <p>Per informazioni su crittografia avanzata e protocolli sicuri (ad es. NIST SP 800-52 e SP 800-57, OWASP, ecc.), fare riferimento alle migliori pratiche e agli standard di settore.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
2.2.4 Configurazione dei parametri di sicurezza del sistema per evitare un uso improprio.	2.2.4.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>Gli standard di configurazione dei sistemi e i processi correlati dovrebbero gestire nello specifico le impostazioni e i parametri di protezione che presentano implicazioni note per la sicurezza in tutti i tipi di sistemi in uso.</p> <p>Affinché i sistemi vengano configurati correttamente, il personale responsabile della configurazione e/o dell'amministrazione dei sistemi deve conoscere i parametri e le impostazioni di sicurezza specifici che si applicano al sistema.</p>
	2.2.4.b Esaminare gli standard di configurazione del sistema per verificare che le impostazioni dei parametri di sicurezza comuni siano incluse.	
	2.2.4.c Selezionare un campione di componenti di sistema e verificare che i parametri di sicurezza comuni siano impostati correttamente e siano conformi agli standard di configurazione.	
2.2.5 Rimozione di tutta la funzionalità non necessaria, ad esempio script, driver, funzioni, sottosistemi, file system e server Web non utilizzati.	2.2.5.a Selezionare un campione di componenti di sistema e controllare le configurazioni per verificare che tutta la funzionalità non necessaria (ad esempio, script, driver, funzioni, sottosistemi, file system, ecc.) sia rimossa.	<p>Le funzioni non necessarie possono offrire opportunità aggiuntive di accesso al sistema agli utenti non autorizzati. Rimuovendo la funzionalità non necessaria, le organizzazioni possono concentrarsi sulla protezione delle funzioni necessarie e ridurre il rischio di sfruttamento delle funzioni sconosciute.</p> <p>Includendo questa funzione negli standard di protezione dei server e nelle procedure, è possibile gestire le implicazioni specifiche per la sicurezza associate alle funzioni non necessarie (ad esempio la rimozione/disabilitazione di FTP o del server Web se il server non eseguirà queste funzioni).</p>
	2.2.5.b. Esaminare la documentazione e i parametri di sicurezza per verificare che le funzioni attive siano documentate e supportino la configurazione protetta.	
	2.2.5.c. Esaminare la documentazione e i parametri di sicurezza per verificare che solo la funzionalità documentata sia presente sui componenti di sistema inseriti nel campione.	
2.3 Eseguire la cifratura di tutto l'accesso amministrativo non da console, tramite crittografia avanzata. Nota: laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.	2.3 Selezionare un campione di componenti di sistema e verificare che l'accesso amministrativo non da console sia cifrato nei seguenti modi:	<p>Se l'amministrazione non da console (inclusa quella da remoto) non utilizza l'autenticazione sicura e comunicazioni cifrate, un utente non autorizzato può rilevare informazioni sensibili a livello amministrativo o operativo (ad esempio ID e password degli amministratori). Un utente non autorizzato può utilizzare queste informazioni per accedere alla rete, divenire un amministratore e sottrarre i dati.</p> <p>I protocolli con testo in chiaro (quali HTTP, telnet, ecc.) non cifrano i dettagli su traffico o accesso, rendendo più semplice l'intercettazione di queste informazioni da parte di un utente non autorizzato.</p> <p><i>(continua alla pagina successiva)</i></p>
	2.3.a Osservare un amministratore al momento dell'accesso a ciascun sistema ed esaminare le configurazioni di sistema per verificare che venga richiamato un metodo di cifratura avanzata prima della richiesta della password.	
	2.3.b Esaminare servizi e file di parametri sui sistemi per accertarsi che non siano disponibili per accesso non da console comandi Telnet e altri comandi di accesso remoto non sicuri.	

Requisiti PCI DSS	Procedure di test	Istruzioni
	2.3.c Osservare un amministratore al momento dell'accesso a ciascun sistema per verificare che l'accesso dell'amministratore alle interfacce di gestione basate su Web sia cifrato con crittografia avanzata.	Perché si possa parlare di “crittografia avanzata”, è necessaria la presenza di protocolli riconosciuti nel settore con livelli di attendibilità e gestione delle chiavi adeguati come applicabile in base al tipo di tecnologia utilizzata. Fare riferimento alla “crittografia avanzata” nel documento <i>Glossario, abbreviazioni e acronimi PCI DSS e PA-DSS</i> e le migliori pratiche e gli standard di settore come NIST SP 800-52 e SP 800-57, OWASP, ecc.
	2.3.d Esaminare la documentazione del fornitore e consultare il personale per verificare che la crittografia avanzata per la tecnologia in uso venga implementata in conformità alle migliori pratiche di settore e/o alle raccomandazioni del fornitore.	
	2.3.e Se si utilizza SSL/TLS iniziale, eseguire le procedure di test riportate nell' <i>Appendice A2: Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale</i> .	
2.4 Realizzazione di un inventario dei componenti di sistema nell'ambito dello standard PCI DSS.	2.4.a Esaminare l'inventario del sistema e verificare che venga conservato un elenco di componenti hardware e software comprensivo di descrizione della funzione/uso.	La memorizzazione di un elenco aggiornato di tutti i componenti di sistema consente alle organizzazioni di definire con precisione ed efficienza l'ambito del proprio ambiente per l'implementazione dei controlli PCI DSS. Senza un inventario, è possibile che alcuni componenti di sistema vengano dimenticati e siano inavvertitamente esclusi dagli standard di configurazione dell'organizzazione.
	2.4.b Consultare il personale per verificare che l'inventario documentato sia aggiornato.	
2.5 Verificare che le politiche di sicurezza e le procedure operative per la gestione delle impostazioni predefinite del fornitore e di altri parametri di sicurezza siano documentate, in uso e note a tutte le parti coinvolte.	2.5 Esaminare la documentazione e consultare il personale per verificare che le politiche di sicurezza e le procedure operative per la gestione delle impostazioni predefinite del fornitore e dei parametri di sicurezza siano: <ul style="list-style-type: none"> • documentate • in uso • note a tutte le parti coinvolte 	È necessario che il personale sia a conoscenza delle seguenti politiche di sicurezza e delle procedure operative giornaliere per garantire che le impostazioni predefinite del fornitore e gli altri parametri di sicurezza siano costantemente gestiti in modo da impedire configurazioni non sicure.

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>2.6 I provider di hosting condiviso devono proteggere l'ambiente ospitato e i dati dei titolari di carta di ciascuna entità. Questi provider devono soddisfare specifici requisiti come descritto nell'<i>Appendice A1 - Requisiti PCI DSS aggiuntivi per provider di hosting condiviso</i>.</p>	<p>2.6 Eseguire le procedure di test da A.1.1 a A.1.4 descritte nell'<i>Appendice A1 - 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 e dei dati delle relative entità (esercenti e provider di servizi).</p>	<p>Questo requisito è destinato ai provider di hosting che forniscono ambienti di hosting condiviso per più client sullo stesso server. Quando tutti i dati si trovano sullo stesso server e sono sotto il controllo di un singolo ambiente, spesso le impostazioni di questi server condivisi non sono gestite dai singoli client, pertanto i client possono aggiungere funzioni e script non sicuri che influiscono sulla sicurezza di tutti gli altri ambienti client; di conseguenza, diventa più facile che un utente non autorizzato comprometta i dati di un client e ottenga così l'accesso ai dati di tutti gli altri client. Vedere l'<i>Appendice A1</i> per i dettagli dei requisiti.</p>

Protezione dei dati dei titolari di carta

Requisito 3 - *Proteggere i dati dei titolari di carta memorizzati*

I metodi di protezione quali cifratura, troncatura, mascheratura e hashing sono componenti critici della protezione dei dati dei 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 anche altri metodi efficaci per la protezione dei dati memorizzati per limitare i possibili rischi. Ad esempio, è possibile evitare di memorizzare i dati dei titolari di carta a meno che non sia assolutamente necessario, eseguire la troncatura dei dati dei titolari di carta se non è richiesto il numero PAN completo, non inviare i numeri 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	Istruzioni
<p>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 che includano per tutta la memorizzazione dei dati dei titolari di carta almeno quanto riportato di seguito:</p> <ul style="list-style-type: none"> • limitazione della quantità dei dati memorizzati e del tempo di conservazione in base alle esigenze aziendali, legali e/o legislative; • requisiti specifici di conservazione dei dati dei titolari di carta; • processi per la rimozione sicura dei dati quando non sono più necessari; • processo trimestrale per identificare ed 	<p>3.1.a Esaminare le politiche, le procedure e i processi per la conservazione e l'eliminazione dei dati e verificare che includano per tutta la memorizzazione dei dati dei titolari di carta (CHD) quanto riportato di seguito:</p> <ul style="list-style-type: none"> • limitazione della quantità dei dati memorizzati e del tempo di conservazione in base alle esigenze aziendali, legali e/o legislative; • requisiti specifici per la conservazione dei dati di titolari di carta (ad esempio, è necessario conservare i dati dei titolari di carta per un periodo X per scopi aziendali Y); • processi per l'eliminazione sicura dei dati dei titolari di carta non più necessari per scopi legali, legislativi o aziendali; • processo trimestrale per identificare ed eliminare in modo sicuro i dati dei titolari di carta memorizzati che superano i requisiti di conservazione definiti. 	<p>Una politica formale per la conservazione dei dati identifica quali dati devono essere conservati e dove sono collocati in modo da poter essere distrutti o cancellati in modo sicuro non appena non servono più.</p> <p>I soli dati dei titolari di carta che possono essere conservati dopo l'autorizzazione sono il PAN (primary account number) (reso illeggibile), la data di scadenza, il nome e il codice di servizio.</p> <p>Conoscere dove sono collocati i dati dei titolari di carta è necessario per conservarli o eliminarli in maniera corretta quando non servono più. Al fine di definire dei requisiti di conservazione adeguati, un'entità deve prima comprendere quali siano le sue esigenze aziendali nonché ogni obbligo di natura legale o legislativa che sia valido per il loro</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
eliminare in modo sicuro i dati dei titolari di carta memorizzati che superano i requisiti di conservazione definiti.	3.1.b Consultare il personale per verificare che: <ul style="list-style-type: none"> tutte le posizioni in cui sono memorizzati i dati dei titolari di carta sono incluse nei processi di conservazione ed eliminazione dei dati; sia presente un processo trimestrale automatico o manuale per identificare ed eliminare in sicurezza i dati dei titolari di carta memorizzati; il processo trimestrale automatico o manuale venga eseguito per tutte le posizioni dei dati dei titolari di carta. 	settore e/o che riguarda il tipo di dati che viene conservato.
	3.1.c Per un campione di componenti di sistema che memorizza i dati dei titolari di carta: <ul style="list-style-type: none"> esaminare i file e i record del sistema per verificare che i dati memorizzati non superino i requisiti definiti nella politica di conservazione dei dati; osservare il meccanismo di eliminazione per verificare che i dati vengano eliminati in sicurezza. 	<p>L'identificazione e l'eliminazione dei dati memorizzati che hanno superato il periodo di conservazione specificato impediscono di conservare inutilmente dati non più necessari. Questo processo può essere automatico o manuale o un mix dei due. Ad esempio, è possibile eseguire una procedura programmatica (automatica o manuale) per individuare e rimuovere i dati e/o una revisione manuale delle aree di archiviazione dei dati.</p> <p>L'implementazione di metodi di eliminazione sicura garantisce che i dati non possano essere recuperati quando non servono più.</p> <p>Se non sono necessari, non conservarli!</p>
3.2 Non memorizzare dati sensibili di autenticazione dopo l'autorizzazione (anche se cifrati). Se si ricevono dati sensibili di autenticazione, dopo il completamento del processo di autorizzazione rendere tutti i dati non recuperabili.	3.2.a Per emittenti e/o società che supportano servizi di emissione e memorizzano dati sensibili di autenticazione, esaminare le politiche e consultare il personale per verificare la presenza di una giustificazione aziendale per la memorizzazione dei dati sensibili di autenticazione.	I dati sensibili di autenticazione sono costituiti da dati della traccia completa, valore o codice di convalida della carta e dati PIN. La memorizzazione dei dati sensibili di autenticazione dopo l'autorizzazione è vietata. Questi dati sono particolarmente preziosi per gli utenti non autorizzati, in quanto consentono loro di generare carte di pagamento contraffatte e conseguenti transazioni fraudolente.
<p><i>Gli emittenti e le società che supportano servizi di emissione sono autorizzati a memorizzare i dati sensibili di autenticazione in presenza di:</i></p> <ul style="list-style-type: none"> una giustificazione aziendale memorizzazione sicura dei dati 	3.2.b Per emittenti e/o società che supportano servizi di emissione e memorizzano dati sensibili di autenticazione, esaminare i dati memorizzati e le configurazioni di sistema verificare che i dati sensibili di autenticazione siano protetti.	Le entità che emettono carte di pagamento o che eseguono o supportano servizi di emissione spesso creano e controllano dati sensibili di autenticazione durante il processo di emissione.

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>I dati sensibili di autenticazione includono i dati citati nei seguenti Requisiti da 3.2.1 a 3.2.3:</p>	<p>3.2.c Per tutte le altre entità, se sono stati ricevuti dati sensibili di autenticazione, esaminare le politiche, le procedure e le configurazioni di sistema per verificare che i dati non vengano conservati in seguito all'autorizzazione.</p>	<p>Alle società che eseguono, facilitano o supportano servizi di emissione è consentito memorizzare dati sensibili di autenticazione SOLO SE hanno un'esigenza aziendale legittima per farlo.</p> <p>Tenere presente che tutti i requisiti PCI DSS si riferiscono agli emittenti e l'unica eccezione per emittenti ed elaboratori di emittenti è che i dati sensibili di autenticazione possono essere conservati in presenza di un motivo legittimo per farlo. Un motivo legittimo è quello necessario per l'esecuzione della funzione che viene fornita dall'emittente e non un motivo di convenienza. Ciascuno di questi dati deve essere memorizzato in sicurezza e in conformità ai requisiti PCI DSS e a quelli specifici del marchio di pagamento.</p>
	<p>3.2.d Per tutte le altre entità, se sono stati ricevuti dati sensibili di autenticazione, esaminare le procedure e i processi per l'eliminazione sicura dei dati per verificare che i dati non siano recuperabili.</p>	<p>Per le entità che non emettono direttamente, la conservazione di dati sensibili di autenticazione dopo l'autorizzazione non è consentita.</p>
<p>3.2.1 Non memorizzare l'intero contenuto di qualsiasi traccia (dalla striscia magnetica presente sul retro della carta, dati equivalenti contenuti in un chip o in altro luogo) dopo l'autorizzazione. Questi dati sono denominati anche traccia completa, traccia, traccia 1, traccia 2 e dati della striscia magnetica.</p> <p>Nota: nel normale svolgimento delle attività, è possibile che sia necessario conservare i seguenti elementi di dati della striscia magnetica:</p> <ul style="list-style-type: none"> • nome del titolare della carta • PAN (Primary Account Number) • data di scadenza • codice di servizio <p>Per ridurre al minimo il rischio, memorizzare solo gli elementi di dati necessari per l'azienda.</p>	<p>3.2.1 Per un campione di componenti di sistema, esaminare le origini dei dati incluse quelle riportate di seguito, senza limitazioni, e verificare che non venga memorizzato, dopo l'autorizzazione, l'intero contenuto di ogni traccia dalla striscia magnetica sulla carta o i dati equivalenti in un chip.</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>Se vengono memorizzati dati della traccia completa, gli utenti non autorizzati che otterranno tali dati potranno riprodurre carte di pagamento e completare transazioni fraudolente.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>3.2.2 Non memorizzare il Card Validation Code or Value (numero a tre o quattro cifre impresso sulla parte anteriore o posteriore di una carta di pagamento utilizzato per verificare le transazioni con carta non presente) dopo l'autorizzazione.</p>	<p>3.2.2 Per un campione di componenti di sistema, esaminare le origini dei dati, incluse quelle riportate di seguito, senza limitazioni, e verificare che il codice di validazione della carta a tre o quattro cifre stampato sulla parte anteriore della carta o nel riquadro della firma (dati CVV2, CVC2, CID, CAV2) non sia memorizzato dopo l'autorizzazione.</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>Lo scopo del codice di validazione della carta è proteggere le transazioni in cui il consumatore e la carta non sono presenti, ad esempio ordini via Internet oppure ordini via posta/telefono (MO/TO).</p> <p>Se questi dati vengono sottratti, gli individui non autorizzati possono eseguire transazioni Internet e MO/TO fraudolente.</p>
<p>3.2.3 Dopo l'autorizzazione, 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 le origini dei dati, incluse quelle riportate di seguito, senza limitazioni, e verificare che non vengano memorizzati, dopo l'autorizzazione, i PIN e i blocchi PIN cifrati.</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>Questi valori dovrebbero essere noti soltanto al proprietario della carta o alla banca che ha emesso la carta. Se questi dati vengono sottratti, gli individui non autorizzati possono eseguire transazioni fraudolente di addebito basate su PIN (ad esempio, prelievi Bancomat).</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>3.3 Mascherare il PAN completo quando visualizzato (non devono essere visibili più di sei cifre all'inizio e quattro cifre alla fine) per renderlo visibile solo al personale con un'esigenza aziendale legittima.</p> <p><i>Nota: questo requisito non sostituisce i requisiti più rigorosi per la visualizzazione dei dati dei titolari di carta, ad esempio requisiti legali o del marchio di carta di pagamento per ricevute di punti di vendita (POS).</i></p>	<p>3.3.a Esaminare le politiche e le procedure scritte per mascherare la visualizzazione di PAN e verificare che:</p> <ul style="list-style-type: none"> sia documentato l'elenco di ruoli che devono accedere alle visualizzazioni di più di sei cifre all'inizio/quattro cifre alla fine (include il PAN completo), insieme a un'esigenza aziendale legittima per ciascun ruolo di disporre di tale accesso; il PAN sia mascherato quando viene visualizzato in modo che il PAN completo sia visibile solo al personale con un'esigenza aziendale legittima; tutti gli altri ruoli non specificatamente autorizzati a visualizzare il PAN completo sono tenuti a visualizzare solo i PAN mascherati. 	<p>La visualizzazione dell'intero PAN su elementi quali monitor di computer, ricevute di carte di pagamento, fax o rendicontazioni cartacee può comportare il recupero di tali dati da parte di utenti non autorizzati e il loro utilizzo fraudolento. La visualizzazione del PAN completo solo da chi ha un'esigenza aziendale legittima consente di ridurre il rischio di accesso ai dati PAN da parte di utenti non autorizzati.</p> <p>L'approccio di mascheratura deve sempre garantire che venga visualizzato solo il numero minimo di cifre secondo necessità per eseguire una funzione aziendale specifica. Ad esempio, se per eseguire una funzione aziendale sono necessarie solo le ultime quattro cifre, mascherare il PAN in modo che singoli utenti che eseguono tale funzione possano visualizzare solo le ultime quattro cifre. Come altro esempio, se una funzione deve accedere al numero di identificazione bancaria (BIN) per finalità di routing, disabilitare la mascheratura solo delle cifre BIN (in genere le prime sei cifre) durante tale funzione.</p> <p>Questo requisito si riferisce anche alla protezione del PAN <u>visualizzato</u> su schermi, ricevute cartacee, stampe ecc. e non deve essere confuso con il Requisito 3.4 per la protezione del PAN quando <u>viene memorizzato</u> in file, database, ecc.</p>
	<p>3.3.b Esaminare le configurazioni di sistema per verificare che il PAN completo venga visualizzato solo per gli utenti/ruoli con un'esigenza aziendale documentata e che il PAN sia mascherato per tutte le altre richieste.</p>	
	<p>3.3.c Esaminare le visualizzazioni del PAN (ad esempio, su schermo e in ricevute cartacee) per verificare che i PAN siano mascherati durante la visualizzazione dei dati dei titolari di carta e che il PAN completo sia visibile solo al personale con un'esigenza aziendale legittima.</p>	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>3.4 Rendere illeggibile il numero PAN ovunque sia memorizzato (inclusi i supporti digitali portatili, i supporti di backup e i 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 delle chiavi. <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 la versione troncata e hash dello stesso PAN siano presenti nell'ambiente di un'entità, devono essere predisposti ulteriori controlli</p>	<p>3.4.a Esaminare la documentazione relativa al sistema utilizzato per proteggere il numero PAN, incluso il fornitore, il tipo di sistema/processo e gli algoritmi di cifratura (se applicabili) per verificare che il PAN sia stato reso illeggibile mediante 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> <p>3.4.d Esaminare un campione di log di audit, inclusi i log delle applicazioni di pagamento, per confermare che il PAN è reso illeggibile o non è presente nei log.</p>	<p>I PAN conservati nella memoria principale (database o file flat, ad esempio fogli elettronici su file di testo) e nella memoria non principale (backup, log di audit, log di eccezioni o risoluzione dei problemi) devono essere protetti.</p> <p>Le funzioni di hash one-way basate sulla crittografia avanzata possono essere utilizzate per rendere illeggibili i dati dei titolari di carta. Le funzioni di hash sono adatte all'uso quando non è necessario recuperare il numero originale (l'hash one-way è irreversibile). Si consiglia, ma non si tratta di un requisito, di aggiungere un ulteriore valore di ingresso casuale ai dati dei titolari di carta prima dell'hashing per ridurre la possibilità che un aggressore riesca a confrontare i dati (da cui ricavare il PAN) con tabelle di valori hash precalcolati.</p> <p>Lo scopo della troncatura è rimuovere definitivamente un segmento dei dati PAN in modo da memorizzare solo una parte (in genere non oltre le prime sei e le ultime quattro cifre) del PAN.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<i>per verificare che non sia possibile correlare la versione troncata e hash per ricostruire il PAN originale.</i>	3.4.e Nel caso in cui versioni troncata e hash dello stesso PAN siano presenti nell'ambiente, esaminare i controlli implementati per verificare che non sia possibile correlare le versioni troncata e hash per ricostruire il PAN originale.	<p>Un token indicizzato è un token crittografico che sostituisce il PAN in base a un determinato indice per un valore imprevedibile. Un pad one-time è un sistema in cui una chiave privata, generata in modo casuale, viene utilizzata una sola volta per cifrare un messaggio, che successivamente sarà decifrato utilizzando una chiave e un pad one-time corrispondente.</p> <p>Lo scopo della crittografia avanzata (come chiarito in <i>PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi</i>) è basare la cifratura su un algoritmo accettato e collaudato nel settore (non un algoritmo proprietario o personale) con chiavi di crittografia avanzata.</p> <p>Correlando le versioni troncata e hash di un determinato PAN, un utente non autorizzato può facilmente ricavare il valore del PAN originale. I controlli volti a impedire la correlazione di questi dati aiuteranno a garantire che il PAN originale rimanga illeggibile.</p>
3.4.1 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 distinto e indipendente dai meccanismi di controllo dell'accesso e di autenticazione del sistema operativo nativo (ad esempio, non utilizzando database di account utente locali o credenziali di accesso alla rete generiche). Le chiavi di decifratura non devono essere associate agli account	3.4.1.a Se viene utilizzata la cifratura del disco, controllare la configurazione e osservare il processo di autenticazione per verificare che l'accesso logico ai file system cifrati venga implementato tramite un meccanismo separato dal meccanismo di autenticazione dei sistemi operativi nativi (ad esempio, non utilizzando i database di account utente locali o le credenziali di accesso alla rete generiche).	<p>Lo scopo di questo requisito è gestire l'accettazione della cifratura a livello di disco per rendere illeggibili i dati dei titolari di carta. La cifratura a livello di disco permette di cifrare l'intero disco/partizione su un computer e di decifrare automaticamente le informazioni quando sono richieste da un utente autorizzato. Le soluzioni di cifratura del disco intercettano le operazioni di lettura/scrittura del sistema operativo ed eseguono le opportune trasformazioni crittografiche senza richiedere particolari azioni all'utente, se non la specifica di una password o di</p>
	3.4.1.b Osservare i processi e consultare il personale per verificare che le chiavi di crittografia siano memorizzate in modo sicuro (ad esempio, su un supporto rimovibile adeguatamente protetto con controlli di accesso rigorosi).	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>utente.</p> <p>Nota: questo requisito si applica in aggiunta a tutti gli altri requisiti di gestione delle chiavi e di cifratura PCI DSS.</p>	<p>3.4.1.c Esaminare le configurazioni e osservare i processi per verificare che i dati dei titolari di carta su supporti rimovibili siano cifrati in ogni posizione di memorizzazione.</p> <p>Nota: se la cifratura del disco non è utilizzata per cifrare supporti rimovibili, è necessario rendere illeggibili i dati memorizzati sul supporto in questione utilizzando altri metodi.</p>	<p>una passphrase all'avvio del sistema o all'inizio di una sessione. Sulla base di queste caratteristiche della cifratura a livello di disco, per la conformità a questo requisito il metodo non può:</p> <ol style="list-style-type: none"> 1) utilizzare la stessa autenticazione dell'account utente utilizzata per il sistema operativo; 2) Utilizzare una chiave di decifratura associata o derivante dal database degli account utente locali del sistema o credenziali di accesso alla rete generiche. <p>La cifratura dell'intero disco consente di proteggere i dati in caso di perdita del disco e pertanto è opportuna per i dispositivi portatili su cui sono memorizzati i dati dei titolari di carta.</p>
<p>3.5 Documentazione e implementazione di procedure per proteggere le chiavi usate per tutelare i dati dei titolari di carta contro divulgazione e uso improprio.</p> <p>Nota: questo requisito si applica alle chiavi utilizzate per cifrare i dati dei titolari di carta memorizzati e alle chiavi di cifratura delle chiavi (KEK) utilizzate per proteggere le chiavi di cifratura dei dati. Tali KEK devono essere avanzate almeno quanto la chiave di cifratura dei dati.</p>	<p>3.5 Esaminare le politiche e le procedure di gestione delle chiavi per verificare che siano stati specificati i processi per proteggere le chiavi utilizzate per la cifratura dei dati dei titolari di carta da divulgazione e uso improprio e che includano almeno quanto segue:</p> <ul style="list-style-type: none"> • l'accesso alle chiavi è limitato al minor numero possibile di persone necessarie; • le KEK sono avanzate almeno quanto le chiavi di cifratura dei dati che devono proteggere; • le KEK sono memorizzate separatamente dalle chiavi di cifratura dei dati; • le chiavi sono memorizzate in modo sicuro nel minor numero possibile di posizioni e moduli. 	<p>Le chiavi di crittografia devono essere protette in modo avanzato, perché chiunque le ottenga sarà in grado di decifrare i dati. Se utilizzate, le KEK devono essere avanzate almeno quanto la chiave di cifratura dei dati per assicurare un'adeguata protezione della chiave che cifra i dati nonché dei dati cifrati con tale chiave.</p> <p>Il requisito per proteggere le chiavi da divulgazione e uso improprio si riferisce sia alle chiavi di cifratura dei dati che alle KEK. Dal momento che una KEK può consentire l'accesso a molte chiavi di cifratura dei dati, per questo tipo di chiavi sono necessarie delle misure di protezione rigide.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>3.5.1 Requisito aggiuntivo solo per provider di servizi: conservare una descrizione documentata dell'architettura crittografica che includa:</p> <ul style="list-style-type: none"> • dettagli di tutti gli algoritmi, i protocolli e le chiavi utilizzati per la protezione dei dati dei titolari di carta, incluse la data di scadenza e l'attendibilità della chiave; • descrizione dell'utilizzo per ciascuna chiave; • inventario di eventuali HSM e altri SCD utilizzati per la gestione delle chiavi. <p><i>Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.</i></p>	<p>3.5.1 Consultare il personale responsabile e analizzare la documentazione per verificare che esista un documento per descrivere l'architettura crittografica, inclusi:</p> <ul style="list-style-type: none"> • dettagli di tutti gli algoritmi, i protocolli e le chiavi utilizzati per la protezione dei dati dei titolari di carta, incluse la data di scadenza e l'attendibilità della chiave; • descrizione dell'utilizzo per ciascuna chiave; • inventario di eventuali HSM e altri SCD utilizzati per la gestione delle chiavi. 	<p><i>Nota: questo requisito si applica solo quando l'entità in corso di valutazione è un provider di servizi.</i></p> <p>Conservare la documentazione corrente dell'architettura crittografica consente a un'entità di comprendere gli algoritmi, i protocolli e le chiavi di crittografia utilizzati per proteggere i dati dei titolari di carta, nonché i dispositivi che generano, utilizzano e proteggono le chiavi. Ciò consente a un'entità di affrontare le minacce future all'architettura, in modo da poter pianificare aggiornamenti poiché i livelli di attendibilità forniti da algoritmi/forza delle chiavi differenti cambiano. Conservare tale documentazione consente anche a un'entità di rilevare eventuali chiavi o dispositivi di gestione delle chiavi persi o mancanti e identificare aggiunte non autorizzate all'architettura crittografica.</p>
<p>3.5.2 Limitare l'accesso alle chiavi di crittografia al minor numero possibile di custodi necessari.</p>	<p>3.5.2 Esaminare gli elenchi di accessi utente per verificare che l'accesso alle chiavi sia consentito al minor numero possibile di custodi necessari.</p>	<p>Dovrebbe essere molto limitato il numero di persone che ha accesso alle chiavi di crittografia (riducendo la possibilità di rendere visibili i dati dei titolari di carta a utenti non autorizzati), di solito solo coloro che hanno responsabilità di custodia delle chiavi.</p>
<p>3.5.3 Memorizzare sempre le chiavi segrete e private utilizzate per cifrare/decifrare costantemente i dati dei titolari di carta in una (o più) delle seguenti forme:</p> <ul style="list-style-type: none"> • Cifrate con chiave KEK avanzata almeno quanto la chiave di cifratura dei dati che viene memorizzata separatamente dalle chiavi di cifratura dei dati • interne a un dispositivo crittografico protetto (come un modulo di 	<p>3.5.2.a Esaminare sempre le procedure documentate per verificare che le chiavi di crittografia utilizzate per cifrare/decifrare i dati dei titolari di carta siano presenti esclusivamente in una (o più) delle seguenti forme:</p> <ul style="list-style-type: none"> • Cifrate con chiave KEK avanzata almeno quanto la chiave di cifratura dei dati che viene memorizzata separatamente dalle chiavi di cifratura dei dati • interne a un dispositivo crittografico protetto (come un modulo di sicurezza (host) hardware (HSM) o un dispositivo di punto di interazione approvato PTS); • come componenti principali o condivisioni principali, in conformità a un metodo accettato nel settore. 	<p>È necessario memorizzare le chiavi di crittografia in modo sicuro per impedire l'accesso non autorizzato o non necessario che potrebbe comportare l'esposizione dei dati dei titolari di carta.</p> <p>Non si prevede la cifratura delle KEK, ad ogni modo queste chiavi devono essere protette da divulgazione e uso improprio come indicato al Requisito 3.5. Se vengono utilizzate le KEK, la loro memorizzazione in posizioni logicamente e/o fisicamente separate rispetto alle chiavi di cifratura dei dati riduce il rischio di accesso non</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>sicurezza (host) hardware (HSM) o un dispositivo di punto di interazione approvato PTS);</p> <ul style="list-style-type: none"> come almeno due componenti o condivisioni di chiavi a lunghezza integrale, in conformità a un metodo accettato nel settore. <p>Nota: non è necessario memorizzare le chiavi pubbliche in uno di questi moduli.</p>	<p>3.5.3.b Esaminare sempre le configurazioni di sistema e i luoghi di memorizzazione delle chiavi per verificare che le chiavi di crittografia utilizzate per cifrare/decifrare i dati dei titolari di carta siano presenti esclusivamente in una (o più) delle seguenti forme:</p> <ul style="list-style-type: none"> cifrate con KEK; interne a un dispositivo crittografico protetto (come un modulo di sicurezza (host) hardware (HSM) o un dispositivo di punto di interazione approvato PTS); come componenti principali o condivisioni principali, in conformità a un metodo accettato nel settore. <p>3.5.3.c Ogni volta che vengono utilizzare le KEK, esaminare le configurazioni di sistema e i luoghi di memorizzazione delle chiavi e verificare quanto segue:</p> <ul style="list-style-type: none"> le KEK sono avanzate almeno quanto le chiavi di cifratura dei dati che devono proteggere; le KEK sono memorizzate separatamente dalle chiavi di cifratura dei dati; 	<p>autorizzato a entrambe le chiavi.</p>
<p>3.5.4 Memorizzare le chiavi di crittografia nel minor numero possibile di posizioni.</p>	<p>3.5.4 Esaminare i luoghi di memorizzazione delle chiavi e osservare i processi per verificare che le chiavi siano memorizzate nel minor numero possibile di posizioni.</p>	<p>Memorizzare le chiavi di crittografia nel minor numero di posizioni consente alle organizzazioni di tenere traccia e monitorare tutte le posizioni delle chiavi e di ridurre il rischio di esposizione delle chiavi a utenti non autorizzati.</p>
<p>3.6 Documentare e implementare completamente tutti i processi e le procedure di gestione delle chiavi di crittografia utilizzate per la cifratura dei dati dei titolari di carta, incluso quanto segue:</p> <p>Nota: sono disponibili numerosi standard di settore per la gestione delle chiavi, tra cui il</p>	<p>3.6.a Ulteriore procedura di test solo per le valutazioni dei 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, esaminare che la documentazione che il provider di servizi fornisce ai clienti e verificare che includa istruzioni su come trasmettere, memorizzare e aggiornare in modo sicuro le chiavi dei clienti, in conformità ai Requisiti da 3.6.1 a 3.6.8 di seguito.</p>	<p>La gestione delle chiavi di crittografia è una parte fondamentale della sicurezza continua della soluzione di cifratura. Un valido processo di gestione delle chiavi, sia esso manuale o automatico, come parte del prodotto di cifratura, è basato sugli standard di settore e gestisce tutti gli elementi chiave da 3.6.1 a 3.6.8.</p> <p>Fornire ai clienti istruzioni su come trasmettere,</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
sito del NIST all'indirizzo http://csrc.nist.gov .	3.6.b Esaminare le procedure e i processi di gestione delle chiavi utilizzate per la cifratura dei dati dei titolari di carta ed eseguire le operazioni seguenti:	memorizzare e aggiornare le chiavi di crittografia in modo sicuro contribuisce a prevenire l'errata gestione delle chiavi o la loro divulgazione a entità non autorizzate. Lo scopo di questo requisito riguarda le chiavi utilizzate per cifrare i dati dei titolari di carta memorizzati e ogni rispettiva KEK. <i>Nota: la procedura di test 3.6.a è una procedura aggiuntiva applicabile solo se l'entità in corso di valutazione è un provider di servizi.</i>
3.6.1 Generazione di chiavi di crittografia avanzata	3.6.1.a Verificare che le procedure di gestione delle chiavi specifichino come generare chiavi avanzate.	La soluzione di cifratura deve generare chiavi avanzate, come descritto nel documento <i>Glossario, abbreviazioni e acronimi PCI DSS e PA-DSS</i> sotto "Generazione di chiavi di crittografia". L'uso di chiavi di crittografia avanzate aumenta notevolmente il livello di sicurezza dei dati dei titolari di carta cifrati.
	3.6.1.b Osservare le procedure per la generazione di chiavi per verificare che vengano generate chiavi avanzate.	
3.6.2 Distribuzione di chiavi di crittografia sicure	3.6.2.a Verificare che le procedure di gestione delle chiavi specifichino come distribuire in sicurezza le chiavi.	La soluzione di cifratura deve distribuire le chiavi in modo sicuro, vale a dire che le chiavi vengono distribuite solo alle persone definite in 3.5.1 e non vengono mai distribuite in chiaro.
	3.6.2.b Osservare il metodo per la distribuzione delle chiavi per verificare che vengano distribuite in modo sicuro.	
3.6.3 Memorizzazione di chiavi di crittografia sicure	3.6.3.a Verificare che le procedure di gestione delle chiavi specifichino come memorizzare in sicurezza le chiavi.	La soluzione di cifratura deve memorizzare le chiavi in modo sicuro, ad esempio applicando una cifratura con una KEK. La memorizzazione di chiavi senza un'adeguata protezione potrebbe fornire l'accesso agli aggressori, con conseguente decifratura ed esposizione dei dati dei titolari di carta.
	3.6.3.b Osservare il metodo per la memorizzazione delle chiavi per verificare che vengano memorizzate in modo sicuro.	
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	3.6.4.a Verificare che le procedure di gestione delle chiavi includano un periodo di validità definito per ciascun tipo di chiave in uso e illustrino un processo per la modifica delle chiavi al termine dei periodi di validità definiti.	Il periodo di validità è il periodo durante il quale una determinata chiave di crittografia può essere usata per uno scopo preciso. Le considerazioni per la definizione del periodo di validità includono,

Requisiti PCI DSS	Procedure di test	Istruzioni
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 di settore (ad esempio, NIST Special Publication 800-57).	3.6.4.b Consultare il personale e verificare che le chiavi vengano modificate al termine dei periodi di validità definiti.	senza limitazioni, la solidità dell'algoritmo sottostante, le dimensioni o la lunghezza della chiave, il rischio che la chiave possa essere compromessa e la sensibilità dei dati che vengono cifrati. La modifica periodica delle chiavi di cifratura che sono giunte al termine del loro periodo di validità è fondamentale per ridurre al minimo il rischio che qualcuno ottenga le chiavi e le utilizzi per decifrare i dati.
3.6.5 Ritiro o sostituzione delle chiavi (ad esempio, archiviazione, distruzione e/o revoca) 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) o chiavi per le quali esista il sospetto che siano state compromesse. Nota: se ritirate o sostituite le chiavi di crittografia devono essere conservate, queste chiavi devono essere archiviate in modo sicuro (ad esempio usando una KEK). Le chiavi di crittografia archiviate dovrebbero essere usate solo per scopi di decifratura/verifica.	3.6.5.a Verificare che le procedure di gestione delle chiavi specificano i processi per eseguire le seguenti operazioni: <ul style="list-style-type: none"> • ritiro o sostituzione delle chiavi in caso di indebolimento dell'integrità della chiave; • sostituzione di chiavi potenzialmente o effettivamente compromesse; • chiavi conservate in seguito a ritiro o sostituzione e non utilizzate per le operazioni di cifratura. 	Le chiavi che non sono più necessarie o in uso o le chiavi di cui si conosce o si sospetta la compromissione, vanno ritirate e/o distrutte per garantire che non possano essere più utilizzate. Se è necessario conservare tali chiavi (ad esempio, per supportare i dati cifrati in archivio), si deve applicare loro una protezione avanzata. La soluzione di cifratura dovrebbe fornire o favorire un processo di sostituzione delle chiavi che devono essere sostituite o di cui si conosce o si sospetta la compromissione.
	3.6.5.b Consultare il personale e verificare che i processi seguenti siano implementati: <ul style="list-style-type: none"> • le chiavi vengono ritirate o sostituite secondo necessità in caso di indebolimento dell'integrità della chiave e ogni volta che un utente a conoscenza delle chiavi lascia l'azienda; • le chiavi vengono sostituite se se ne conosce o se ne sospetta la compromissione; • chiavi conservate in seguito a ritiro o sostituzione e non utilizzate per le operazioni di cifratura. 	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>3.6.6 Se vengono utilizzate le operazioni manuali di gestione delle chiavi di crittografia con testo in chiaro, tali operazioni vanno gestite utilizzando i principi di “split knowledge” e controllo duale.</p> <p>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.</p>	<p>3.6.6.a Verificare che le procedure di gestione delle chiavi con testo in chiaro specificano i processi per l'utilizzo di quanto segue:</p> <ul style="list-style-type: none"> • principi di split knowledge delle chiavi, in modo che i componenti principali siano controllati da almeno due utenti che conoscono soltanto i relativi componenti principali; • controllo duale delle chiavi, in modo che almeno due utenti effettuino operazioni di gestione delle chiavi e nessuno abbia accesso ai materiali di autenticazione (ad esempio, password o chiavi) dell'altro. 	<p>I principi “split knowledge” il controllo duale delle chiavi sono utilizzati per eliminare la possibilità che una singola persona abbia accesso all'intera chiave. Questo controllo è applicabile alle operazioni manuali di gestione delle chiavi o laddove la gestione delle chiavi non è implementata dal prodotto di cifratura.</p> <p>Split knowledge è un metodo secondo cui due o più persone dispongono separatamente di componenti principali, ogni persona conosce solo il proprio componente principale e i singoli componenti principali non trasmettono alcuna informazione sulla chiave di crittografia originale.</p> <p>Il controllo duale richiede che due o più persone eseguano una funzione e che una persona sola non possa consultare o utilizzare i materiali di autenticazione di un'altra.</p>
	<p>3.6.6 b Consultare il personale e/o osservare i processi per verificare che le chiavi manuali con testo in chiaro vengano gestite con:</p> <ul style="list-style-type: none"> • split knowledge E • controllo duale 	
<p>3.6.7 Prevenzione di tentativi di sostituzione non autorizzata delle chiavi di crittografia.</p>	<p>3.6.7.a Verificare che le procedure di gestione delle chiavi specificano i processi per impedire la sostituzione non autorizzata delle chiavi.</p>	<p>La soluzione di cifratura non dovrebbe consentire o accettare la sostituzione delle chiavi provenienti da fonti non autorizzate o processi imprevisti.</p>
	<p>3.6.7.b Consultare il personale e/o osservare i processi per verificare che venga impedita la sostituzione non autorizzata delle chiavi.</p>	
<p>3.6.8 Obbligo per i custodi delle chiavi di crittografia di riconoscere in modo formale che accettano e confermano di conoscere le proprie responsabilità.</p>	<p>3.6.8.a Verificare che le procedure di gestione delle chiavi specifichino i processi con cui i custodi delle chiavi riconoscono (per iscritto o elettronicamente) che accettano e confermano di conoscere le proprie responsabilità.</p>	<p>Questo processo garantisce che gli individui che agiscono come custodi delle chiavi si impegnano a svolgere tale ruolo e accettano e confermano di conoscere le loro responsabilità.</p>
	<p>3.6.8.b Osservare la documentazione o altra prova che dimostri che i custodi delle chiavi hanno riconosciuto (per iscritto o elettronicamente) che accettano e confermano di conoscere le proprie responsabilità.</p>	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>3.7 Verificare che le politiche di sicurezza e le procedure operative per la protezione dei dati dei titolari di carta memorizzati siano documentate, in uso e note a tutte le parti coinvolte.</p>	<p>3.7 Esaminare la documentazione e consultare il personale per verificare che i criteri di protezione e le procedure operative per la protezione dei dati dei titolari di carta memorizzati siano:</p> <ul style="list-style-type: none"> • documentate • in uso • note a tutte le parti coinvolte 	<p>È necessario che il personale sia a conoscenza delle seguenti politiche di sicurezza e procedure operative documentate per la gestione continua della memorizzazione sicura dei dati dei titolari di carta.</p>

Requisito 4 - Cifrare i dati dei 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 prese di mira da utenti non autorizzati che sfruttano tali vulnerabilità per ottenere privilegi di accesso per ambienti di dati dei titolari di carta.

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>4.1 Utilizzare la crittografia avanzata e i protocolli di sicurezza per proteggere i dati sensibili dei titolari di carta quando vengono trasmessi su reti pubbliche aperte, incluso quando:</p> <ul style="list-style-type: none"> vengono accettati solo certificati e chiavi affidabili; il protocollo utilizzato supporta soltanto versioni o configurazioni sicure; il livello di cifratura è corretto per la metodologia di cifratura in uso. <p>Nota: laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.</p> <p><i>Esempi di reti pubbliche aperte includono, senza limitazioni:</i></p> <ul style="list-style-type: none"> Internet tecnologie wireless, incluso 802.11 e Bluetooth tecnologie mobili, ad esempio, comunicazioni GSM (Global System for Mobile), CDMA (code division multiple access) 	<p>4.1.a Individuare tutte le posizioni in cui vengono trasmessi o ricevuti i dati dei titolari di carta su reti pubbliche aperte. Esaminare gli standard documentati e confrontarli con le configurazioni di sistema per verificare l'uso dei protocolli di sicurezza e della crittografia avanzata per tutte le posizioni.</p> <p>4.1.b Esaminare le politiche e le procedure documentate per verificare che siano specificati i processi per:</p> <ul style="list-style-type: none"> l'accettazione di certificati e/o chiavi affidabili; il protocollo in uso, in modo che supporti solo versioni o configurazioni sicuri (e che le versioni e le configurazioni non sicure non siano supportate); l'implementazione del livello di cifratura corretto per la metodologia di cifratura in uso. <p>4.1.c Selezionare e osservare un campione di trasmissioni in ingresso e in uscita quando si verificano (ad esempio, osservando i processi di sistema o il traffico di rete) per verificare che tutti i dati dei titolari di carta siano cifrati con crittografia avanzata durante la transazione.</p> <p>4.1.d Esaminare chiavi e certificati per verificare che siano accettati solo certificati e/o chiavi affidabili.</p> <p>4.1.e Esaminare le configurazioni di sistema per verificare che il protocollo sia implementato per utilizzare solo configurazioni sicure e non supporti versioni o configurazioni non sicure.</p>	<p>Le informazioni sensibili devono essere cifrate durante la trasmissione su reti pubbliche, in quanto si verifica con facilità e frequenza che un utente non autorizzato intercetti e/o dirotti i dati in transito.</p> <p>La trasmissione sicura dei dati dei titolari di carta richiede l'uso di chiavi/certificati affidabili, un protocollo sicuro per il trasferimento e il livello di cifratura corretto per cifrare i dati dei titolari di carta. Le richieste di connessione da parte dei sistemi che non supportano il livello di cifratura necessario e che comporterebbero una connessione non sicura non vanno accettate.</p> <p>Tenere presente che alcune implementazioni di protocolli (come SSL, SSH v1.0 e TLS iniziale) presentano vulnerabilità note che un aggressore può utilizzare per ottenere il controllo del sistema interessato. Qualunque sia il protocollo di sicurezza utilizzato, verificare che sia configurato per usare solo versioni e configurazioni sicure per impedire l'utilizzo di una connessione non sicura, ad esempio sfruttando solo certificati attendibili e supportando solo la cifratura avanzata (non supportando metodi o protocolli non sicuri e più deboli).</p> <p>La verifica dell'affidabilità dei certificati (ad esempio, validità ed emissione da parte di una</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<ul style="list-style-type: none"> • <i>GPRS (General Packet Radio Service)</i> • <i>Comunicazioni satellitari</i> 	4.1.f Esaminare le configurazioni di sistema per verificare che sia implementato il livello di cifratura corretto per la metodologia di cifratura in uso. Controllare suggerimenti/migliori pratiche del fornitore.	fonte attendibile) consente di garantire l'integrità della connessione sicura.
	4.1.g Per le implementazioni SSL/TLS, esaminare le configurazioni di sistema per verificare che TLS sia abilitato durante la trasmissione o la ricezione dei dati dei titolari di carta. Ad esempio, per le implementazioni basate su browser: <ul style="list-style-type: none"> • "HTTPS" viene visualizzato come protocollo dell'URL del browser; • i dati dei titolari di carta vengono richiesti solo se "HTTPS" viene visualizzato come parte dell'URL. 	Solitamente, l'URL della pagina Web dovrebbe iniziare per "HTTPS" e/o nella finestra del browser Web dovrebbe comparire l'icona di un lucchetto. Molti fornitori di certificati TSL forniscono anche un sigillo di verifica altamente visibile (a volte denominato "sigillo di sicurezza" "sigillo di sito sicuro" o "sigillo di attendibilità sicura") su cui è possibile fare clic per ottenere informazioni sul sito Web.
	4.1.h Se si utilizza SSL/TLS iniziale, eseguire le procedure di test riportate nell' <i>Appendice A2: Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale</i> .	Per informazioni su crittografia avanzata e protocolli sicuri (ad es. NIST SP 800-52 e SP 800-57, OWASP, ecc.), fare riferimento alle migliori pratiche e agli standard di settore.
4.1.1 Garantire che le reti wireless che trasmettono i dati dei titolari di carta o connesse all'ambiente dei dati dei titolari di carta utilizzino le migliori pratiche di settore per implementare la cifratura avanzata per l'autenticazione e la trasmissione.	4.1.1 Individuare tutte le reti wireless che trasmettono i dati dei titolari di carta o connesse all'ambiente dei dati di titolari di carta. Esaminare gli standard documentati e confrontarli con le impostazioni delle configurazioni di sistema per verificare quanto segue per tutte le reti wireless individuate: <ul style="list-style-type: none"> • le migliori pratiche di settore vengano utilizzate per implementare la cifratura avanzata per l'autenticazione e la trasmissione; • la cifratura debole (ad esempio, WEP, SSL) non venga utilizzata come controllo di sicurezza per l'autenticazione o la trasmissione. 	Gli utenti non autorizzati utilizzano strumenti liberi e ampiamente disponibili per ascoltare le comunicazioni wireless. L'uso di crittografia avanzata può contribuire a limitare la divulgazione di informazioni sensibili attraverso le reti wireless. La crittografia avanzata per l'autenticazione e la trasmissione dei dati dei titolari di carta è necessaria per impedire agli utenti non autorizzati di ottenere accesso alla rete wireless o di utilizzare le reti wireless per accedere alle reti interne o ai dati.

Requisiti PCI DSS	Procedure di test	Istruzioni
4.2 Non inviare mai PAN non protetti mediante tecnologie di messaggistica degli utenti finali (ad esempio, e-mail, messaggistica istantanea, SMS, chat, ecc.).	4.2.a Se le tecnologie di messaggistica degli utenti finali vengono utilizzate per inviare i dati dei titolari di carta, osservare processi per l'invio di PAN ed esaminare un campione di trasmissioni in uscita mentre si verificano per verificare che il PAN sia stato reso illeggibile o sia protetto con crittografia avanzata ogni qual volta viene inviato mediante le tecnologie di messaggistica dell'utente finale.	L'e-mail, la messaggistica istantanea, l'SMS e la chat possono essere facilmente intercettati mediante packet-sniffing durante il recapito attraverso reti interne e pubbliche. Non utilizzare questi strumenti di messaggistica per inviare numeri PAN, a meno che siano configurate in modo da offrire cifratura avanzata.
	4.2.b Esaminare le politiche scritte per verificare l'esistenza di una politica in cui viene stabilito che i PAN non protetti non devono essere inviati tramite tecnologie di messaggistica degli utenti finali.	Inoltre, se un'entità richiede il PAN mediante tecnologie di messaggistica degli utenti finali, l'entità deve fornire uno strumento o un metodo per proteggere questi PAN utilizzando la crittografia avanzata o per rendere i PAN illeggibili prima della trasmissione.
4.3 Verificare che le politiche di sicurezza e le procedure operative per cifrare le trasmissioni dei dati dei titolari di carta siano documentate, in uso e note a tutte le parti coinvolte.	4.3 Esaminare la documentazione e consultare il personale per verificare che i criteri di protezione e le procedure operative per la cifratura delle trasmissioni dei dati dei titolari di carta siano: <ul style="list-style-type: none"> • documentate • in uso • note a tutte le parti coinvolte 	È necessario che il personale sia a conoscenza delle seguenti politiche di sicurezza e procedure operative per la gestione continua della trasmissione sicura dei dati dei titolari di carta.

Utilizzare un programma per la gestione delle vulnerabilità

Requisito 5 - Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software 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. Si potrebbero prendere in considerazione ulteriori soluzioni anti-malware come supplemento al software antivirus; tuttavia, tali soluzioni aggiuntive non sostituiscono l'esigenza di disporre di un software antivirus.

Requisiti PCI DSS	Procedure di test	Istruzioni
5.1 Distribuire il software antivirus su tutti i sistemi solitamente interessati 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.	Esiste un flusso costante di attacchi che utilizzano exploit pubblicati, spesso di tipo “zero day” (attacco che sfrutta vulnerabilità precedentemente sconosciute), contro sistemi altrimenti sicuri. Senza una soluzione antivirus aggiornata regolarmente, queste nuove forme di software dannoso possono attaccare i sistemi, disabilitare la rete o compromettere i dati.
5.1.1 Garantire che tutti i programmi antivirus siano in grado di rilevare, rimuovere e proteggere contro tutti i tipi di malware noto.	5.1.1 Esaminare la documentazione del fornitore e le configurazioni antivirus per verificare che i programmi antivirus: <ul style="list-style-type: none"> • rilevino tutti i tipi di malware noti; • rimuovano tutti i tipi di malware noti; • proteggano contro tutti i tipi di malware noti. <i>Esempio di tipi di malware includono virus, cavalli di Troia, worm, spyware, adware e rootkit.</i>	È importante proteggersi da TUTTI i tipi e le forme di software dannoso.

Requisiti PCI DSS	Procedure di test	Istruzioni
5.1.2 Effettuare valutazioni periodiche dei sistemi che non vengono comunemente interessati da malware per individuare e valutare l'evoluzione delle minacce malware e confermare o meno la necessità di software antivirus per tali sistemi.	5.1.2 Consultare il personale per verificare che venga effettuato il monitoraggio e la valutazione delle minacce malware in evoluzione per i sistemi che non vengono comunemente interessati da malware e confermare o meno la necessità di software antivirus per tali sistemi.	<p>Generalmente, è possibile che mainframe, computer di fascia media (quali AS/400) e sistemi analoghi non siano frequentemente presi di mira o interessati da malware. Tuttavia, è possibile che le tendenze del settore in merito al malware cambino in fretta, pertanto è fondamentale che le aziende siano consapevoli del nuovo malware che potrebbe interessare i propri sistemi (ad esempio, monitorando gli avvisi di sicurezza dei fornitori e i newsgroup sugli antivirus per capire se i loro sistemi potrebbero essere minacciati dal nuovo malware in evoluzione).</p> <p>Le tendenze del software dannoso dovrebbero essere incluse nell'identificazione delle nuove vulnerabilità della protezione e i metodi per gestire tali nuove tendenze dovrebbero essere integrati negli standard di configurazione dell'azienda e nei meccanismi di protezione, secondo necessità.</p>
5.2 Verificare che tutti i meccanismi antivirus siano: <ul style="list-style-type: none"> • aggiornati • inclusi in scansioni periodiche • in grado di generare log di audit da conservare in base al Requisito 10.7 PCI DSS 	5.2.a Esaminare le politiche e le procedure per verificare che il software antivirus e le definizioni siano mantenuti aggiornati.	<p>Anche le migliori soluzioni antivirus sono presentano un'efficacia limitata se non vengono aggiornate con gli ultimi aggiornamenti sulla sicurezza, i file di firme o le protezioni contro il malware.</p> <p>I log di audit consentono di monitorare l'attività di virus e malware e le reazioni dell'antivirus. Pertanto, è fondamentale che le soluzioni software antivirus siano configurate per generare log di audit e che questi log siano gestiti in conformità al Requisito 10.</p>
	5.2.b Esaminare le configurazioni antivirus, inclusa l'installazione principale del software per verificare che i meccanismi antivirus siano: <ul style="list-style-type: none"> • configurati per eseguire aggiornamenti automatici; • configurati per eseguire scansioni periodiche. 	
	5.2.c Esaminare un campione di componenti di sistema che include tutti i tipi di sistemi operativi comunemente interessati da malware e verificare che: <ul style="list-style-type: none"> • il software antivirus e le definizioni siano aggiornati; • vengano eseguite scansioni periodiche. 	
	5.2.d Esaminare le configurazioni antivirus, inclusa l'installazione principale del software e un campione di componenti di sistema, per verificare che: <ul style="list-style-type: none"> • la funzione di generazione di log del software antivirus sia attiva; • i log vengano memorizzati in conformità al Requisito 10.7 	

Requisiti PCI DSS	Procedure di test	Istruzioni
	PCI DSS.	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>5.3 Garantire che i meccanismi antivirus siano in esecuzione in modo attivo e che non possono essere disabilitati o alterati dagli utenti a meno che non siano stati specificatamente autorizzati dalla direzione per ogni singolo caso e per un periodo di tempo limitato.</p> <p><i>Nota: è possibile disattivare temporaneamente le soluzioni antivirus solo in caso di esigenza tecnica legittima, come autorizzato dalla direzione per ogni singolo caso. Se è necessario disattivare la protezione antivirus per un motivo specifico, è opportuno essere autorizzati formalmente. Potrebbe essere necessario implementare ulteriori misure di sicurezza per il periodo di tempo in cui la protezione antivirus non è attiva.</i></p>	<p>5.3.a Esaminare le configurazioni antivirus, inclusa l'installazione principale del software e un campione di componenti di sistema, per verificare che il software antivirus sia in funzione.</p> <p>5.3.b Esaminare le configurazioni antivirus, inclusa l'installazione principale del software e un campione di componenti di sistema, per verificare che il software antivirus non possa essere disattivato o modificato dagli utenti.</p> <p>5.3.c Consultare il personale responsabile e osservare i processi per verificare che il software antivirus non possa essere disabilitato o alterato dagli utenti a meno che non siano stati specificatamente autorizzati dalla direzione per ogni singolo caso e per un periodo di tempo limitato.</p>	<p>L'antivirus in continua esecuzione che non può essere modificato da nessuno offre una sicurezza costante contro il malware.</p> <p>L'uso di controlli basati su politiche su tutti i sistemi per impedire la modifica o la disattivazione delle protezioni anti-malware consente di impedire che i punti deboli del sistema vengano sfruttati dal malware.</p> <p>Potrebbe essere necessario implementare ulteriori misure di sicurezza per il periodo di tempo in cui la protezione antivirus non è attiva, ad esempio scollegando da Internet il sistema non protetto quando la protezione antivirus è disattiva ed eseguendo una scansione completa quando la protezione viene riattivata.</p>
<p>5.4 Verificare che le politiche di sicurezza e le procedure operative per la protezione dei sistemi contro il malware siano documentate, in uso e note a tutte le parti coinvolte.</p>	<p>5.4 Esaminare la documentazione e consultare il personale per verificare che le politiche di sicurezza e le procedure operative per la protezione dei sistemi contro il malware siano:</p> <ul style="list-style-type: none"> • documentate; • in uso • note a tutte le parti coinvolte. 	<p>È necessario che il personale sia a conoscenza delle seguenti politiche di sicurezza e procedure operative per garantire la protezione continua dei sistemi contro il malware.</p>

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 devono disporre delle patch di software corrette per proteggere contro lo sfruttamento e la compromissione dei dati dei titolari di carta da parte di utenti non autorizzati 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	Istruzioni
<p>6.1 Stabilire un processo per identificare le vulnerabilità della sicurezza, utilizzando fonti esterne attendibili per le informazioni sulle vulnerabilità della sicurezza e assegnare una classificazione dei rischi (ad esempio, "alta", "media" o "bassa") alle vulnerabilità della sicurezza recentemente rilevate.</p> <p>Nota: le classificazioni dei rischi devono essere basate sulle migliori pratiche di settore nonché sulla valutazione del potenziale impatto. Ad esempio, i criteri per la classificazione delle vulnerabilità possono tenere in considerazione il punteggio base CVSS e/o la classificazione del fornitore e/o il tipo di sistemi interessati.</p> <p>I metodi per la valutazione delle vulnerabilità e l'assegnazione delle valutazioni dei rischi variano in base all'ambiente aziendale e alla strategia di valutazione dei rischi. Le classificazioni dei rischi devono almeno identificare tutte le vulnerabilità ad "alto rischio" per l'ambiente. Oltre alla classificazione dei rischi, le vulnerabilità possono essere considerate "critiche" se rappresentano una minaccia imminente per l'ambiente, influiscono sui sistemi critici e/o comportano una potenziale compromissione se non risolte. Esempi di sistemi critici includono sistemi di sicurezza, dispositivi e sistemi rivolti al pubblico, database e altri</p>	<p>6.1.a Esaminare le politiche e le procedure per verificare che siano stati definiti i processi per:</p> <ul style="list-style-type: none"> identificare le nuove vulnerabilità della sicurezza; assegnare una classificazione dei rischi alle vulnerabilità che include l'identificazione di tutte le vulnerabilità ad "alto rischio" e "critiche"; utilizzare fonti esterne attendibili di informazioni sulle vulnerabilità della sicurezza. <p>6.1.b Consultare il personale responsabile e osservare i processi per verificare che:</p> <ul style="list-style-type: none"> vengano individuate le nuove vulnerabilità della sicurezza; venga assegnata una classificazione dei rischi alle vulnerabilità che include l'identificazione di tutte le vulnerabilità ad "alto rischio" e "critiche"; i processi per identificare le nuove vulnerabilità della sicurezza comprendano l'uso di fonti esterne per informazioni sulle vulnerabilità della sicurezza. 	<p>Lo scopo di questo requisito è l'aggiornamento delle organizzazioni in relazione alle nuove vulnerabilità che possono influire sul loro ambiente.</p> <p>Le fonti di informazioni sulle vulnerabilità devono essere affidabili e spesso includono siti Web dei fornitori, newsgroup di settore, mailing list o feed RSS.</p> <p>Una volta che un'organizzazione identifica una vulnerabilità che potrebbe incidere sul suo ambiente, è necessario valutare e classificare il rischio che la vulnerabilità comporta. Pertanto, l'organizzazione deve disporre di un metodo per valutare le vulnerabilità in maniera costante e assegnare le classificazioni dei rischi a tali vulnerabilità. A tale scopo non è possibile utilizzare la scansione ASV né la scansione vulnerabilità interne, piuttosto è necessario un processo che monitori attivamente le fonti di informazione del settore sulle vulnerabilità.</p> <p>La classificazione dei rischi (ad esempio come "alta", "media" o "bassa") consente alle organizzazioni di individuare, assegnare priorità e risolvere gli elementi a rischio maggiore più rapidamente e ridurre la probabilità che vengano sfruttate le vulnerabilità che costituiscono i rischi più elevati.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<i>sistemi che memorizzano, elaborano o trasmettono i dati dei titolari di carta.</i>		
<p>6.2 Assicurare che tutti i componenti di sistema ed il software siano protetti dalle vulnerabilità note mediante l'installazione delle patch di sicurezza dei fornitori. Installare patch di sicurezza critiche entro un mese dalla release.</p> <p>Nota: le patch di sicurezza critiche vanno identificate in conformità al processo di classificazione dei rischi definito nel Requisito 6.1.</p>	<p>6.2.a Esaminare le politiche e le procedure connesse all'installazione delle patch di sicurezza per verificare i processi definiti per:</p> <ul style="list-style-type: none"> l'installazione di patch di sicurezza critiche del fornitore entro un mese dalla release; l'installazione di tutte le patch di sicurezza del fornitore entro un adeguato arco temporale (ad esempio, entro tre mesi). <p>6.2.b 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:</p> <ul style="list-style-type: none"> le patch di sicurezza critiche del fornitore siano state installate entro un mese dalla release; tutte le patch di sicurezza del fornitore siano state installate entro un adeguato arco temporale (ad esempio, entro tre mesi). 	<p>Esiste un flusso costante di attacchi che utilizzano exploit pubblicati, spesso di tipo "zero day" (attacco che sfrutta vulnerabilità precedentemente sconosciute), contro sistemi altrimenti sicuri. Se le patch più recenti non vengono implementate sui sistemi critici nel minor tempo possibile, un utente non autorizzato può utilizzare questi exploit per attaccare o disabilitare la rete e accedere ai dati sensibili.</p> <p>L'assegnazione della massima priorità alle patch per l'infrastruttura critica assicura la protezione di sistemi e dispositivi ad alta priorità da vulnerabilità nel minor tempo possibile, in seguito alla release della patch. È opportuno assegnare una priorità alle installazioni di patch per garantire l'installazione delle patch di sicurezza sui sistemi critici o ad alto rischio entro 30 giorni e l'installazione delle altre patch a basso rischio entro 2-3 mesi.</p> <p>Questo requisito è applicabile alle patch valide per tutto il software installato, incluse le applicazioni di pagamento (sia quelle convalidate PA-DSS e quelle che non lo sono).</p>
<p>6.3 Sviluppare applicazioni software interne ed esterne (incluso l'accesso amministrativo basato su Web alle applicazioni) in maniera sicura, come segue:</p> <ul style="list-style-type: none"> in conformità allo standard PCI DSS (ad esempio autenticazione e registrazione sicure); sulla base di standard e/o migliori pratiche di settore; includendo la sicurezza delle 	<p>6.3.a 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.</p> <p>6.3.c Esaminare i processi di sviluppo del software scritti per verificare che le applicazioni del software siano sviluppate in conformità allo standard PCI DSS.</p>	<p>Senza l'inclusione della sicurezza durante le fasi di definizione dei requisiti, progettazione, analisi e test dello sviluppo del software, le vulnerabilità di protezione possono essere introdotte inavvertitamente o con cattive intenzioni nell'ambiente di produzione.</p> <p>Sapere in che modo l'applicazione gestisce i dati sensibili, anche in fase di memorizzazione, trasmissione quando sono in memoria, consente di</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>informazioni per l'intera durata del ciclo di sviluppo del software.</p> <p>Nota: <i>valido per tutto il software sviluppato internamente, nonché per il software su misura o personalizzato, sviluppato da terzi.</i></p>	<p>6.3.d Consultare gli sviluppatori del software per verificare che i processi di sviluppo del software scritti siano stati implementati.</p>	<p>identificare i luoghi in cui è necessaria la protezione.</p>
<p>6.3.1 Rimozione di sviluppo, test e/o account, ID utente e password di applicazioni personalizzate prima dell'attivazione o della release di tali applicazioni ai clienti.</p>	<p>6.3.1 Esaminare le procedure di sviluppo del software scritte e consultare il personale responsabile per verificare che la pre-produzione e/o gli account, gli ID utente e/o le password delle applicazioni personalizzate vengano rimossi prima della produzione o della release di tali applicazioni ai clienti.</p>	<p>Lo sviluppo, il test e/o gli account, gli ID utente e le password delle applicazioni personalizzate devono essere rimossi dal codice di produzione prima dell'attivazione o della release dell'applicazione ai clienti, in quanto questi elementi possono fornire informazioni sul funzionamento dell'applicazione. Il possesso di tali informazioni potrebbe facilitare la compromissione dell'applicazione e dei dati dei titolari di carta correlati.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>6.3.2 Analizzare il codice personalizzato prima della release in produzione o della distribuzione ai clienti per individuare eventuali vulnerabilità del codice (mediante processi manuali o automatici) e accertarsi almeno che:</p> <ul style="list-style-type: none"> le modifiche del codice siano 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; le analisi del codice garantiscano che il codice venga sviluppato in base a linee guida di codifica sicure; le correzioni appropriate vengono implementate prima della release; i risultati dell'analisi del codice vengono esaminati e approvati dalla direzione prima della release; <p><i>(continua alla pagina successiva)</i></p>	<p>6.3.2.a Esaminare le procedure di sviluppo di software scritte e consultare il personale responsabile per verificare che tutte le modifiche del codice dell'applicazione personalizzata siano state analizzate (utilizzando 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 della release; i risultati dell'analisi del codice vengono esaminati e approvati dalla direzione prima della release; 	<p>Le vulnerabilità di protezione nel codice personalizzato vengono comunemente sfruttate da utenti non autorizzati per accedere a una rete e compromettere i dati dei titolari di carta.</p> <p>Nel processo di analisi deve essere coinvolto un utente esperto in tecniche di analisi del codice. Le analisi del codice vanno eseguite da una persona diversa dallo sviluppatore del codice per garantire un'analisi obiettiva e indipendente. È possibile utilizzare anche strumenti o processi automatici al posto delle analisi manuali, ma occorre tener presente che per uno strumento automatico potrebbe rivelarsi difficile se non impossibile identificare i problemi di codifica.</p> <p>La correzione degli errori di codifica prima dell'implementazione del codice nell'ambiente di produzione o prima della release ai clienti impedisce al codice di esporre gli ambienti a un potenziale sfruttamento. Il codice errato è più difficile e costoso da risolvere dopo essere stato implementato o distribuito negli ambienti di produzione.</p> <p>L'analisi e l'approvazione formali da parte della direzione prima della release consentono di garantire che il codice è approvato ed è stato sviluppato in conformità alle politiche e alle procedure.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>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.</p> <p>Le analisi del codice possono essere condotte da personale interno preparato o da terze parti. Le applicazioni Web rivolte al pubblico sono anche soggette a controlli aggiuntivi, per risolvere le minacce costanti e le vulnerabilità dopo l'implementazione, secondo quanto definito nel Requisito 6.6 PCI DSS.</p>	<p>6.3.2.b Selezionare un campione di modifiche di applicazioni personalizzate recenti e verificare che il codice dell'applicazione personalizzata 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 Esaminare le politiche e le procedure per verificare che sia stato definito quanto segue:</p> <ul style="list-style-type: none"> • gli ambienti di sviluppo/test sono separati dagli ambienti di produzione con controllo dell'accesso in atto per garantire la separazione; • una separazione di responsabilità tra il personale assegnato agli ambienti di sviluppo/test e il personale assegnato all'ambiente di produzione; • i dati di produzione (PAN attivi) sono esclusi dalle attività di test o sviluppo; • i dati e gli account di test vengono rimossi prima dell'attivazione di un sistema di produzione; • le procedure di controllo delle modifiche correlate all'implementazione di patch di sicurezza e di modifiche del software sono documentate. 	<p>Senza controlli di modifica opportunamente documentati e implementati, le funzionalità di protezione possono essere inavvertitamente o deliberatamente omesse o rese inattive, possono verificarsi problemi di elaborazione o è possibile che venga introdotto codice dannoso.</p>
<p>6.4.1 Separare gli ambienti di sviluppo/test dagli ambienti di produzione e garantire tale separazione con i controlli di accesso.</p>	<p>6.4.1.a Esaminare la documentazione di rete e le configurazioni del dispositivo di rete per verificare che gli ambienti di sviluppo/test siano separati da quelli di produzione.</p> <p>6.4.1.b Esaminare i controlli di accesso per verificare che siano presenti per garantire la separazione tra gli ambienti di sviluppo/test e quelli di produzione.</p>	<p>In considerazione dello stato di costante cambiamento degli ambienti di test e sviluppo, questi tendono ad essere meno sicuri rispetto all'ambiente di produzione. In assenza di un'adeguata separazione tra gli ambienti potrebbe verificarsi la compromissione dell'ambiente di produzione e dei dati dei titolari di carta a causa delle configurazioni di sicurezza meno rigorose e delle possibili vulnerabilità in un ambiente di test o di sviluppo.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
6.4.2 Separare le responsabilità tra ambienti di sviluppo/test e ambienti di produzione	6.4.2 Osservare i processi e consultare il personale assegnato agli ambienti di sviluppo/test e il personale assegnato agli ambienti di produzione per verificare che le responsabilità degli ambienti di sviluppo/test siano separate da quelle dell'ambiente di produzione.	Riducendo il numero di membri del personale con accesso all'ambiente di produzione e ai dati dei titolari di carta si limita il rischio e si contribuisce a garantire che l'accesso sia limitato a coloro per i quali è effettivamente necessario. Lo scopo di questo requisito è di separare le funzioni di sviluppo e test dalle funzioni di produzione. Ad esempio, uno sviluppatore può usare un account a livello di amministratore con privilegi elevati per l'ambiente di sviluppo e avere un account separato con accesso a livello utente per l'ambiente di produzione.
6.4.3 I dati di produzione (PAN attivi) sono esclusi dalle attività di test o sviluppo	6.4.3.a Osservare i processi di test e consultare il personale per verificare che vengano adottate le procedure che garantiscono che i dati di produzione (PAN attivi) sono esclusi dalle attività di test o sviluppo.	I controlli di protezione di solito non sono particolarmente rigorosi negli ambienti di test o produzione. L'uso dei dati di produzione permette agli utenti non autorizzati di accedere ai dati di produzione (dati dei titolari di carta).
	6.4.3.b Esaminare un campione di dati di test per verificare che i dati di produzione (PAN attivi) siano esclusi dalle attività di test o sviluppo.	
6.4.4 Rimuovere dai componenti di sistema dati e account di test prima che il sistema diventi attivo/entri in produzione.	6.4.4.a Osservare i processi di test e consultare il personale per verificare che i dati e gli account di test vengano rimossi prima dell'attivazione di un sistema di produzione.	I dati e gli account di test devono essere rimossi prima che il componente di sistema diventi attivo (in produzione), in quanto questi elementi possono fornire informazioni sul funzionamento dell'applicazione o del sistema. Il possesso di tali informazioni potrebbe facilitare la compromissione del sistema e dei relativi dati dei titolari di carta.
	6.4.4.b Esaminare un campione di dati e account provenienti da sistemi di produzione recentemente installati o aggiornati per verificare che i dati e gli account dei dati vengano rimossi prima dell'attivazione del sistema.	

Requisiti PCI DSS	Procedure di test	Istruzioni
6.4.5 Le procedure di controllo delle modifiche devono includere quanto segue:	6.4.5.a Esaminare le procedure di controllo delle modifiche documentate e verificare che siano definite le procedure per: <ul style="list-style-type: none"> documentazione dell'impatto; approvazione documentata delle modifiche da parte di parti autorizzate; test della funzionalità per verificare che la modifica non influisca negativamente sulla sicurezza del sistema; procedure di back-out. 	Se non adeguatamente gestito, l'impatto delle modifiche del sistema, come gli aggiornamenti software o hardware e l'installazione delle patch di sicurezza, potrebbe non essere pienamente realizzato e potrebbe avere conseguenze non previste.
	6.4.5.b Per un campione di componenti di sistema, consultare il personale responsabile per determinare modifiche recenti. 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.	L'impatto della modifica dovrebbe essere documentato in modo che tutte le parti interessate siano in grado di pianificare accuratamente qualsiasi modifica di elaborazione.
6.4.5.2 Approvazione documentata delle modifiche da parte di parti autorizzate.	6.4.5.2 Verificare la presenza dell'approvazione documentata delle parti autorizzate per ogni modifica inserita nel campione.	L'approvazione delle parti autorizzate indica che una modifica è legittima e autorizzata dall'organizzazione.
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.	Un test approfondito consente di verificare che l'introduzione della modifica non comporti una riduzione della sicurezza dell'ambiente. I test dovrebbero convalidare che, dopo ogni modifica apportata all'ambiente, tutti i controlli di sicurezza esistenti rimangano attivi, siano sostituiti con controlli ugualmente efficaci oppure siano intensificati.
	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 dell'implementazione in produzione.	

Requisiti PCI DSS	Procedure di test	Istruzioni
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.	Per ogni modifica devono esistere procedure di back-out documentate nel caso in cui la modifica non riesca o influisca negativamente sulla sicurezza dell'applicazione o del sistema, in modo da consentire il ripristino del sistema allo stato precedente.

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>6.4.6 Al completamento di una modifica significativa, tutti i requisiti PCI DSS pertinenti devono essere implementati su tutte le reti e tutti i sistemi nuovi o modificati e la documentazione deve essere aggiornata come applicabile.</p> <p><i>Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.</i></p>	<p>6.4.6 Per un campione di modifiche significative, esaminare i record delle modifiche, consultare il personale e osservare le reti/i sistemi interessati per verificare che i requisiti PCI DSS applicabili siano stati implementati e la documentazione aggiornata in base alle modifiche.</p>	<p>Predisporre di processi per analizzare modifiche significative assicura che tutti i controlli PCI DSS appropriati vengano applicati a eventuali reti o sistemi aggiunti o modificati nell'ambiente che rientra nell'ambito.</p> <p>Introdurre questa convalida nei processi di gestione delle modifiche garantisce che gli inventari di dispositivi e gli standard di configurazione siano aggiornati e che i controlli di sicurezza siano applicati laddove necessario.</p> <p>Un processo di gestione delle modifiche deve includere la prova che i requisiti PCI DSS vengano implementati o preservati nell'intero processo iterativo. Esempi di requisiti PCI DSS che potrebbero essere influenzati includono, senza limitazioni, quanto segue:</p> <ul style="list-style-type: none"> • il diagramma di rete viene aggiornato in base alle modifiche; • i sistemi vengono configurati in base agli standard di configurazione, con tutte le password predefinite modificate e i servizi non necessari disabilitati; • i sistemi vengono protetti con i controlli richiesti, ad es. monitoraggio dell'integrità dei file (FIM), antivirus, patch, log di audit; • i dati sensibili di autenticazione (SAD) non vengono memorizzati e la memorizzazione dei dati dei titolari di carta (CHD) è documentata e incorporata nelle procedure e nei criteri di di conservazione dei dati; • vengono inclusi nuovi sistemi nel processo di scansione delle vulnerabilità trimestrale.
<p>6.5 Risoluzione delle vulnerabilità di codifica comuni nei processi di sviluppo software come segue:</p> <ul style="list-style-type: none"> • formare gli sviluppatori almeno una volta all'anno sulle tecniche di codifica sicura 	<p>6.5.a Esaminare le politiche e le procedure di sviluppo software per verificare che la formazione aggiornata sulle tecniche di codifica sicura sia richiesta per gli sviluppatori almeno una volta all'anno, in base alle istruzioni e alle migliori pratiche di settore.</p>	<p>Lo strato applicazione è ad alto rischio e può divenire bersaglio di minacce interne ed esterne.</p> <p>I requisiti da 6.5.1 a 6.5.10 costituiscono i controlli minimi da adottare e le organizzazioni dovrebbero incorporare le relative pratiche di codifica sicure in</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>aggiornate, inclusi i metodi per evitare le vulnerabilità di codifica comuni;</p> <ul style="list-style-type: none"> sviluppare applicazioni in base a linee guida di codifica sicura. <p>Nota: le vulnerabilità elencate dal punto 6.5.1 al punto 6.5.10 erano presenti nelle migliori pratiche di settore al momento della pubblicazione di questa versione dello standard PCI DSS. Tuttavia, poiché le migliori pratiche di settore per la gestione delle vulnerabilità sono state aggiornate (ad esempio, la Guide, SANS CWE Top 25, CERT Secure Coding, ecc.), per questi requisiti è necessario utilizzare le migliori pratiche più recenti.</p>	<p>6.5.b Esaminare i record della formazione per verificare che gli sviluppatori software abbiano ricevuto la formazione aggiornata sulle tecniche di codifica sicura almeno una volta all'anno, inclusi i metodi per evitare le comuni vulnerabilità di codifica.</p> <p>6.5.c Verificare che siano in atto processi per proteggere le applicazioni almeno dalle seguenti vulnerabilità:</p>	<p>base alla particolare tecnologia del proprio ambiente.</p> <p>Gli sviluppatori delle applicazioni andrebbero adeguatamente formati per individuare e risolvere i problemi connessi a queste (e altre) vulnerabilità di codifica comuni. Se il personale è a conoscenza delle linee guida di codifica, il numero di vulnerabilità della sicurezza introdotte tramite pratiche di codifica carenti diminuisce notevolmente. La formazione degli sviluppatori può essere fornita dall'azienda o da terzi e deve essere valida per la tecnologia utilizzata.</p> <p>Non appena le pratiche di codifica sicure accettate nel settore cambiano, è necessario aggiornare le pratiche di codifica aziendali e la formazione degli sviluppatori in modo da risolvere nuove minacce, ad esempio, gli attacchi che intaccano la memoria.</p> <p>Le vulnerabilità individuate da 6.5.1 a 6.5.10 offrono un punto di riferimento minimo. Spetta all'organizzazione restare aggiornata sulle tendenze delle vulnerabilità e incorporare le misure appropriate nelle proprie pratiche di codifica sicure.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
Nota: i requisiti da 6.5.1 a 6.5.6, riportati di seguito, si riferiscono a tutte le applicazioni (interne o esterne).		
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 Esaminare le politiche e le procedure di sviluppo software e consultare il personale responsabile per verificare che le injection flaw siano state risolte con tecniche di codifica che includono: <ul style="list-style-type: none"> • convalida dell'input per verificare che i dati dell'utente non possano modificare il significato di comandi e query; • utilizzo di query con parametri. 	<p>Injection flaw, in particolare SQL injection, rappresentano il metodo comunemente usato per compromettere le applicazioni. L'injection avviene quando i dati forniti dall'utente vengono inviati a un interprete durante un comando o una query. I dati ostili dell'aggressore inducono l'interprete a eseguire comandi indesiderati o a modificare i dati, e consentono all'aggressore di attaccare i componenti all'interno della rete attraverso l'applicazione, per dare il via ad attacchi di tipo buffer overflow o per rivelare informazioni riservate e funzionalità dell'applicazione server.</p> <p>Le informazioni devono essere convalidate prima dell'invio all'applicazione, ad esempio controllando tutti i caratteri alfabetici, un insieme di caratteri alfabetici e numerici, ecc.</p>
6.5.2 Buffer overflow	6.5.2 Esaminare le politiche e le procedure di sviluppo software e consultare il personale responsabile per verificare che i buffer overflow siano stati risolti con tecniche di codifica che includono: <ul style="list-style-type: none"> • convalida dei limiti del buffer; • Troncatura delle stringhe di input 	<p>I buffer overflow si verificano quando un'applicazione non dispone degli adeguati controlli di limite sul suo spazio buffer. Ciò può causare che le informazioni nel buffer vengano spinte fuori dallo spazio di memoria del buffer e collocate nello spazio di memoria eseguibile. Quando ciò si verifica, l'aggressore è in grado di inserire un codice dannoso alla fine del buffer e quindi spingere tale codice nello spazio di memoria eseguibile causando un buffer overflow. Questo codice dannoso viene quindi eseguito e spesso consente all'aggressore di accedere in remoto all'applicazione e/o al sistema infetto.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
6.5.3 Memorizzazione di dati crittografici non sicura	6.5.3 Esaminare le politiche e le procedure di sviluppo software e consultare il personale responsabile per verificare che la memorizzazione di dati crittografici non sicura sia stata risolta con tecniche di codifica che includono: <ul style="list-style-type: none"> • prevenzione degli errori di crittografia; • utilizzano algoritmi e chiavi di crittografia avanzata. 	Le applicazioni che non usano funzioni di crittografia avanzata in modo corretto per la memorizzazione dei dati sono esposte a un maggiore rischio di essere compromesse e di esporre le credenziali e/i dati dei titolari di carta. Nel caso in cui un aggressore sia in grado di sfruttare i processi crittografici deboli, può ottenere l'accesso con testo in chiaro ai dati cifrati.
6.5.4 Comunicazioni non sicure	6.5.4 Esaminare le politiche e le procedure di sviluppo software e consultare il personale responsabile per verificare che le comunicazioni non sicure siano state risolte con tecniche di codifica che autenticano e cifrano correttamente tutte le comunicazioni sensibili.	Le applicazioni che non riescono a cifrare in modo appropriato il traffico di rete usando la crittografia avanzata sono esposte ad un rischio maggiore di compromissione e di esposizione dei dati dei titolari di carta. Nel caso in cui un aggressore sia in grado di sfruttare i processi crittografici deboli, può ottenere il controllo di un'applicazione o addirittura l'accesso con testo in chiaro ai dati cifrati.
6.5.5 Gestione degli errori non corretta	6.5.5 Esaminare le politiche e le procedure di sviluppo software e consultare il personale responsabile per verificare che la gestione degli errori appropriata sia stata risolta con tecniche di codifica che non perdono informazioni mediante messaggi di errore (ad esempio, generando messaggi di errore generici anziché specifici).	Le applicazioni possono involontariamente perdere informazioni sulla relativa configurazione e sulle procedure interne, o esporre le informazioni con privilegi tramite metodi di errata gestione degli errori. Gli aggressori utilizzano questi punti deboli per sottrarre dati sensibili o compromettere il sistema. Se un utente non autorizzato può creare errori che l'applicazione non è in grado di gestire correttamente, può ottenere informazioni dettagliate sul sistema, creare interruzioni denial-of-service, provocare il fallimento della protezione o causare l'arresto anomalo del server. Ad esempio, il messaggio "password non corretta" segnala all'aggressore che l'ID utente fornito è corretto e che gli sforzi devono essere concentrati solamente sulla password. Utilizzare messaggi d'errore più generici, come "Impossibile verificare i dati".

Requisiti PCI DSS	Procedure di test	Istruzioni
6.5.6 Tutte le vulnerabilità ad “alto rischio” identificate nel processo di identificazione delle vulnerabilità (come definito nel Requisito 6.1 PCI DSS).	6.5.6 Esaminare le politiche e le procedure di sviluppo software e consultare il personale responsabile per verificare che le tecniche di codifica risolvano le vulnerabilità ad “alto rischio” che potrebbero incidere sull'applicazione, come descritto nel Requisito PCI DSS 6.1.	Durante lo sviluppo dell'applicazione è necessario identificare e risolvere tutte le vulnerabilità che mediante il processo di classificazione dei rischi delle vulnerabilità di un'organizzazione (definito nel Requisito 6.1) risultano essere ad “alto rischio” e potrebbero incidere sull'applicazione.
Nota: i requisiti da 6.5.7 a 6.5.10, riportati di seguito, si riferiscono ad applicazioni Web e interfacce di applicazioni (interne o esterne):		Applicazioni Web, interne ed esterne (rivolte al pubblico), presentano dei rischi di sicurezza univoci sulla base della loro architettura nonché della loro relativa facilità e del verificarsi di compromissioni.
6.5.7 XSS (Cross-Site Scripting)	6.5.7 Esaminare le politiche e le procedure di sviluppo software e consultare il personale responsabile per verificare che il cross-site scripting (XSS) sia stato risolto con tecniche di codifica che includono: <ul style="list-style-type: none"> • convalida di tutti i parametri prima dell'inclusione; • utilizzo di escape sensibile al contesto. 	Le falle XSS si verificano quando un'applicazione prende i dati forniti dall'utente e li invia a un browser Web senza prima convalidarli o codificarne il contenuto. XSS consente agli aggressori di eseguire script sul browser della vittima, che possono dirottare le sessioni utente, alterare i siti Web, introdurre worm, ecc.

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>6.5.8 Controllo di accesso non corretto (quali riferimenti a oggetti diretti non sicuri, errore di limitazione dell'accesso URL, errore di scansione trasversale directory ed errore di limitazione dell'accesso utente alle funzioni).</p>	<p>6.5.8 Esaminare le politiche e le procedure di sviluppo software e consultare il personale responsabile per verificare che il controllo dell'accesso non corretto, quali riferimenti a oggetti diretti non sicuri, errore di limitazione dell'accesso URL ed errore di scansione trasversale directory, sia stato risolto con tecniche di codifica che includono:</p> <ul style="list-style-type: none"> • corretta autenticazione degli utenti; • purificazione degli input; • mancata esposizione di riferimenti a oggetti interni agli utenti; • interfacce utente che non consentono l'accesso alle funzioni non autorizzate. 	<p>Un riferimento a oggetto diretto si verifica quando uno sviluppatore espone un riferimento a un oggetto di implementazione interno, come un file, una directory, un record di database o una chiave, sotto forma di parametro URL o di modulo. Gli aggressori possono manipolare questi riferimenti per accedere ad altri oggetti senza autorizzazione.</p> <p>Applicare in modo coerente il controllo dell'accesso a livello di presentazione e business logic per tutti gli URL. Spesso l'unico modo in cui un'applicazione protegge le funzionalità sensibili consiste nell'impedire la visualizzazione di collegamenti o URL agli utenti non autorizzati. Gli aggressori possono utilizzare questi punti deboli per accedere ed eseguire operazioni non autorizzate mediante accesso diretto a questi URL.</p> <p>Un aggressore può essere in grado di elencare e navigare la struttura della directory (scansione trasversale directory) di un sito Web e quindi ottenere accesso a informazioni non autorizzate ed anche acquisire un'ulteriore comprensione approfondita delle procedure interne del sito per un successivo sfruttamento.</p> <p>Se le interfacce utente consentono l'accesso a funzioni non autorizzate, tale accesso potrebbe determinare l'accesso da parte di utenti non autorizzati a credenziali con privilegi o dati dei titolari di carta. È necessario consentire solo agli utenti autorizzati di accedere ai riferimenti di oggetti diretti a risorse sensibili. La limitazione dell'accesso alle risorse di dati consente di impedire che i dati dei titolari di carta vengano presentati a risorse non autorizzate.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
6.5.9 Cross-site request forgery (CSRF)	6.5.9 Esaminare le politiche e le procedure di sviluppo software e consultare il personale responsabile per verificare che il cross-site request forgery (CSRF) sia stato risolto con tecniche di codifica che garantiscono che le applicazioni non facciano affidamento su credenziali e token di autorizzazione inviate automaticamente dai browser.	Un attacco CSRF impone al browser di una vittima connessa di inviare una richiesta pre-autenticata a un'applicazione Web vulnerabile che permette all'aggressore di eseguire tutte le operazioni di modifica di stato che la vittima è autorizzata ad eseguire, quali l'aggiornamento dei dettagli dell'account, acquisti o l'autenticazione su un'applicazione.
6.5.10 Violazione dell'autenticazione e gestione delle sessioni	6.5.10 Esaminare le politiche e le procedure di sviluppo software e consultare il personale responsabile per verificare che la violazione dell'autenticazione e la gestione delle sessioni siano state risolte con tecniche di codifica che includono: <ul style="list-style-type: none"> • contrassegnare i token delle sessioni (ad esempio, i cookie) come "sicuri"; • non esporre gli ID sessione nell'URL; • incorporare timeout appropriati e rotazione di ID sessione dopo l'accesso. 	L'autenticazione sicura e la gestione delle sessioni impediscono agli utenti non autorizzati di compromettere credenziali degli account, chiavi o token di sessione che altrimenti consentirebbero loro di impossessarsi dell'identità degli utenti autorizzati.

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>6.6 Per le applicazioni Web esterne, risolvere costantemente le nuove minacce e vulnerabilità e garantire che queste applicazioni siano protette da attacchi noti mediante uno 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; <p>Nota: la valutazione non corrisponde alle scansioni delle vulnerabilità eseguite in base al Requisito 11.2.</p> <ul style="list-style-type: none"> installazione di una soluzione tecnica automatica che rileva e impedisce gli attacchi basati sul Web (ad esempio, un firewall per applicazioni Web) davanti alle applicazioni Web rivolte al pubblico per monitorare costantemente tutto il traffico. 	<p>6.6 Per le applicazioni Web rivolte al pubblico, garantire che uno dei seguenti metodi sia in atto:</p> <ul style="list-style-type: none"> Esaminare i processi documentati, consultare il personale ed esaminare i record delle valutazioni della sicurezza delle applicazioni per verificare che le applicazioni Web rivolte al pubblico vengano analizzate (tramite strumenti o metodi di valutazione della sicurezza delle vulnerabilità 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 almeno tutte le vulnerabilità elencate nel Requisito 6.5 vengano incluse nella valutazione; che tutte le vulnerabilità vengano corrette; Che l'applicazione venga nuovamente valutata dopo le correzioni. Esaminare le impostazioni di configurazione del sistema e consultare il personale responsabile per verificare che la soluzione tecnica automatica che rileva e impedisce gli attacchi basati sul Web (ad esempio, un firewall per applicazioni Web) sia implementata come segue: <ul style="list-style-type: none"> posta davanti alle applicazioni Web rivolte al pubblico per rilevare ed evitare attacchi basati su Web; in esecuzione e aggiornata secondo necessità; in grado di generare log di audit; configurata in modo da bloccare gli attacchi basati sul Web o da generare un avviso investigato immediatamente. 	<p>Le applicazioni Web rivolte al pubblico sono gli obiettivi principali degli aggressori che riescono facilmente ad accedere ai dati sensibili e ai sistemi in presenza di applicazioni Web codificate in modo scadente. Il requisito di revisione delle applicazioni o di installazione di firewall per le applicazioni Web mira a ridurre il numero di compromissioni sulle applicazioni Web rivolte al pubblico, dovute a codifica o pratiche di gestione delle applicazioni scadenti.</p> <ul style="list-style-type: none"> Metodi o strumenti di valutazione della protezione dalle vulnerabilità automatici o manuali analizzano e/o sottopongono a test le vulnerabilità dell'applicazione. I firewall delle applicazioni Web filtrano e bloccano il traffico non essenziale nello strato applicazione. Utilizzato insieme a un firewall di rete, un firewall di applicazioni Web correttamente configurato impedisce gli attacchi dallo strato applicazione nel caso in cui le applicazioni siano configurate o scritte in modo improprio. Questo obiettivo viene realizzato tramite una combinazione di tecnologia e processo. Le soluzioni basate su processi devono prevedere meccanismi che facilitano risposte tempestive agli avvisi al fine di soddisfare lo scopo di questo requisito, che è quello di prevenire gli attacchi. <p>Nota: per "organizzazione specializzata nella sicurezza delle applicazioni" si intende una società esterna o un'organizzazione interna specializzata nella sicurezza delle applicazioni e in grado di dimostrare indipendenza dal team di sviluppo.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
6.7 Verificare che le politiche di sicurezza e le procedure operative per lo sviluppo e la manutenzione di applicazioni e sistemi sicuri siano documentate, in uso e note a tutte le parti coinvolte.	6.7 Esaminare la documentazione e consultare il personale per verificare che le politiche di sicurezza e le procedure operative per lo sviluppo e la manutenzione di applicazioni e sistemi sicuri siano: <ul style="list-style-type: none">• documentate• in uso• note a tutte le parti coinvolte	È necessario che il personale sia a conoscenza delle seguenti politiche di sicurezza e procedure operative per garantire lo sviluppo e la protezione continui dei sistemi e delle applicazioni contro le vulnerabilità.

Implementazione di rigide misure di controllo dell'accesso

Requisito 7 *Limitare l'accesso ai dati dei 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	Istruzioni
7.1 Limitare l'accesso ai componenti di sistema e ai dati dei titolari di carta solo alle persone che svolgono mansioni per le quali tale accesso risulta realmente necessario.	7.1 Esaminare la politica scritta per il controllo dell'accesso e verificare che tale politica comprenda i requisiti da 7.1.1 a 7.1.4 come segue: <ul style="list-style-type: none"> Definizione delle esigenze di accessi e assegnazioni dei privilegi per ogni ruolo limitazione dell'accesso a ID utente privilegiati alla quantità minima necessaria per le responsabilità di ruolo; assegnazione dell'accesso basata sulla classificazione e sulla funzione del ruolo del personale; approvazione documentata (elettronicamente o per iscritto) da parte di terzi autorizzati per tutti gli accessi, incluso l'elenco di privilegi specifici approvati. 	Quanto maggiore è il numero di persone che hanno accesso ai dati dei titolari di carta, tanto maggiore è il rischio di utilizzo fraudolento di un account utente. Limitando l'accesso alle persone che presentano ragioni aziendali legittime per l'accesso, l'organizzazione può impedire l'abuso dei dati dei titolari di carta a causa di inesperienza o premeditazione.
7.1.1 Definizione delle esigenze di accesso per ogni ruolo, incluso: <ul style="list-style-type: none"> componenti di sistema e risorse dati di cui ogni ruolo ha bisogno per accedere alla relativa funzione; Livello di privilegio necessario (ad esempio, utente, amministratore, ecc.) per accedere alle risorse. 	7.1.1 Selezionare un campione di ruoli e verificare che le esigenze di accesso per ciascun ruolo siano definite e includano: <ul style="list-style-type: none"> componenti di sistema e risorse dati di cui ogni ruolo ha bisogno per accedere alla relativa funzione; identificazione del privilegio necessario a ciascun ruolo per eseguire la relativa funzione. 	Al fine di limitare l'accesso ai dati dei titolari di carta solo agli utenti che necessitano di tale accesso, è necessario definire le esigenze di accesso per ogni ruolo (ad esempio, amministratore di sistema, addetti al call center, addetto alle vendite), i sistemi/dispositivi/dati a cui ciascun ruolo deve poter accedere e il livello di privilegio necessario a ciascun ruolo per eseguire in modo efficiente le operazioni assegnate. Dopo aver definito ruoli e relative esigenze di accesso, gli utenti possono ottenere l'accesso di conseguenza.

Requisiti PCI DSS	Procedure di test	Istruzioni
7.1.2 Limitazione dell'accesso a ID utente privilegiati alla quantità minima necessaria per le responsabilità di ruolo.	7.1.2.a Consultare il personale responsabile dell'assegnazione dell'accesso per verificare che i privilegi di accesso degli ID utente siano: <ul style="list-style-type: none"> • assegnati solo a ruoli che necessitano specificatamente tale accesso privilegiato; • limitati alla quantità minima necessaria per le responsabilità di ruolo. 	Nell'assegnare gli ID con privilegi, è importante assegnare agli utenti soltanto i privilegi di cui hanno bisogno per svolgere la propria attività (la "quantità minima necessaria"). Ade esempio, all'amministratore del database e all'amministratore del backup non vanno assegnati gli stessi privilegi dell'amministratore di tutti i sistemi.
	7.1.2.b Selezionare un campione di ID utente con accesso privilegiato e consultare il management per verificare che i privilegi assegnati siano: <ul style="list-style-type: none"> • necessari allo svolgimento delle mansioni dell'utente; • limitati alla quantità minima necessaria per le responsabilità di ruolo. 	Assegnare il minor numero di privilegi possibile aiuta a prevenire che utenti con le giuste conoscenze sull'applicazione modifichino in modo errato o accidentale la configurazione dell'applicazione o alterino le sue impostazioni di sicurezza. L'applicazione del privilegio più limitato possibile contribuisce inoltre a ridurre al minimo la portata del danno nel caso in cui un utente non autorizzato riesca ad accedere a un ID utente.
7.1.3 Assegnazione dell'accesso basata sulla classificazione e sulla funzione del ruolo del personale.	7.1.3 Selezionare un campione di ID utente e consultare il management per verificare che i privilegi assegnati siano basati sulla classificazione e la funzione delle mansioni dell'utente.	Dopo aver definito le esigenze dei ruoli degli utenti (in base al Requisito 7.1.1 PCI DSS), è possibile concedere agli utenti l'accesso in base alla relativa classificazione e funzione delle mansioni utilizzando i ruoli già creati.
7.1.4 Richiedere l'approvazione documentata delle parti autorizzate specificando i privilegi necessari.	7.1.4 Selezionare un campione di ID utente e metterlo a confronto con le approvazioni documentate per verificare che: <ul style="list-style-type: none"> • sia presente l'approvazione documentata per i privilegi assegnati; • l'approvazione è stata rilasciata da parti autorizzate; • i privilegi specifici corrispondono ai ruoli assegnati all'utente. 	L'approvazione documentata (scritta o elettronica) garantisce che gli utenti che dispongono di accesso e privilegi sono persone note e autorizzate dalla direzione e che il loro accesso è necessario per lo svolgimento delle relative mansioni.

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>7.2 Stabilire un sistema di controllo dell'accesso per i componenti di sistema 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.</p> <p>Il sistema di controllo dell'accesso deve includere quanto segue:</p>	<p>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:</p>	<p>Senza un meccanismo che limiti l'accesso in base all'effettiva esigenza di un utente, l'utente potrebbe inconsapevolmente ottenere accesso ai dati dei titolari di carta. I sistemi di controllo dell'accesso automatizzano il processo di limitazione dell'accesso e assegnazione dei privilegi. Inoltre, un'impostazione predefinita "deny all" garantisce che a nessuno venga consentito l'accesso fino a quando non è stata stabilita una regola che concede in modo specifico tale accesso. Le entità possono disporre di uno o più sistemi di controllo dell'accesso per gestire l'accesso utente.</p>
<p>7.2.1 Copertura di tutti i componenti di sistema</p>	<p>7.2.1 Confermare che siano in atto sistemi di controllo dell'accesso su tutti i componenti di sistema.</p>	<p>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.</p>
<p>7.2.2 Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale.</p>	<p>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.</p>	
<p>7.2.3 Impostazione predefinita "deny all".</p>	<p>7.2.3 Confermare che i sistemi di controllo dell'accesso abbiano un'impostazione predefinita "deny all".</p>	
<p>7.3 Verificare che le politiche di sicurezza e le procedure operative per la limitazione dell'accesso ai dati dei titolari di carta siano documentate, in uso e note a tutte le parti coinvolte.</p>	<p>7.3 Esaminare la documentazione e consultare il personale per verificare che i criteri di protezione e le procedure operative per la limitazione dell'accesso ai dati dei titolari di carta siano:</p> <ul style="list-style-type: none"> • documentate; • in uso • note a tutte le parti coinvolte. 	<p>È necessario che il personale sia a conoscenza delle seguenti politiche di sicurezza e procedure operative per garantire che l'accesso sia continuamente controllato e basato sul minor numero di privilegi necessari.</p>

Requisito 8 - Individuare e autenticare l'accesso ai componenti di sistema

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 e processi noti e autorizzati e possono essere registrate come tali.

L'efficacia di una password dipende soprattutto dal design e dall'implementazione del sistema di autenticazione, in particolare dalla frequenza dei tentativi di inserimento di password da parte di aggressori e dai metodi di sicurezza utilizzati per proteggere le password degli utenti nel punto di ingresso, durante la trasmissione e l'archiviazione.

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. Sono inclusi gli account utilizzati dai fornitori e da terzi (ad esempio, per assistenza o manutenzione). Questi requisiti non si applicano agli account utilizzati dai consumatori (ad es., titolari di carta).

Tuttavia, i Requisiti 8.1.1, 8.2, 8.5 e da 8.2.3 a 8.2.5 e da 8.1.6 a 8.1.8 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	Istruzioni
8.1 Definizione e implementazione di politiche e procedure per garantire una corretta gestione dell'identificazione degli utenti non consumatori e amministratori su tutti i componenti di sistema nel seguente modo:	8.1.a Esaminare le procedure e confermare che definiscano i processi per ciascuno degli elementi seguenti da 8.1.1 a 8.1.8. 8.1.c Verificare che le procedure siano implementate per la gestione dell'autenticazione utente, effettuando quanto segue:	Garantendo l'identificazione univoca di ogni utente (invece di utilizzare un solo ID per diversi dipendenti), un'organizzazione può mantenere la responsabilità delle azioni e disporre di un effettivo audit trail per ogni dipendente. In questo modo i problemi vengono risolti più velocemente ed è possibile attuare un contenimento quando si rilevano abusi o cattive intenzioni.
8.1.1 Assegnare a tutti gli utenti un ID univoco prima di consentire l'accesso ai componenti di sistema o ai dati dei titolari di carta.	8.1.1 Consultare il personale amministrativo per confermare che tutti gli utenti dispongano di un ID univoco per l'accesso ai componenti di sistema o ai dati dei titolari di carta.	
8.1.2 Controllare le operazioni di aggiunta, eliminazione e modifica di ID utente, credenziali e altri oggetti identificativi.	8.1.2 Per un campione di ID utente con privilegi e ID utente generici, esaminare le autorizzazioni associate e osservare le impostazioni di sistema per verificare che tutti gli ID utente e gli ID utente con privilegi siano stati implementati solo con i privilegi specificati nell'approvazione documentata.	Per verificare che gli account utente che hanno accesso ai sistemi appartengano a utenti validi e riconosciuti, è necessario che i processi avanzati gestiscano tutte le modifiche apportate agli ID utente e alle altre credenziali di autenticazione, incluse le operazioni di aggiunta, modifica o eliminazione.

Requisiti PCI DSS	Procedure di test	Istruzioni
8.1.3 Revocare immediatamente l'accesso per gli utenti non attivi.	8.1.3.a Selezionare un campione di utenti non attivi negli ultimi sei mesi e analizzare gli elenchi di accesso utente attuali (per <i>l'accesso in locale</i> e in remoto) per verificare che gli ID relativi a tali utenti siano stati disattivati o rimossi dagli elenchi di accesso.	Se un dipendente ha lasciato l'azienda e ha tuttora accesso alla rete tramite il suo account utente, è possibile che si verifichi l'accesso inutile o pericoloso ai dati dei titolari di carta da parte dell'ex dipendente o di un utente non autorizzato che sfrutta l'account vecchio e/o inutilizzato. Per impedire l'accesso non autorizzato, è necessario revocare tempestivamente (non appena possibile) le credenziali dell'utente e gli altri metodi di autenticazione quando il dipendente lascia l'azienda.
	8.1.3.b Verificare che tutti i metodi di autenticazione fisici, quali smartcard, token, ecc., siano stati ripristinati o disattivati.	
8.1.4 Rimuovere/disabilitare gli account utente non attivi entro 90 giorni.	8.1.4 Osservare gli account utente per verificare che gli eventuali account non attivi da oltre 90 giorni siano stati rimossi o disabilitati.	Gli account che non vengono utilizzati regolarmente sono spesso oggetto di attacco, poiché è meno probabile che le eventuali modifiche (ad esempio, password modificata) vengano notate. In tal senso, questi account potrebbero essere sfruttati e utilizzati più facilmente per accedere ai dati dei titolari di carta.
8.1.5 Gestire gli ID utilizzati da terzi per accedere, fornire supporto o manutenzione dei componenti di sistema tramite accesso remoto come segue: <ul style="list-style-type: none"> abilitati solo durante il periodo di tempo necessario e disabilitati se non in uso; monitorati quando in uso. 	8.1.5.a Consultare il personale e osservare i processi per la gestione degli account utilizzati da terzi per accedere, fornire supporto o manutenzione ai componenti di sistema per verificare che gli account utilizzati per l'accesso remoto siano: <ul style="list-style-type: none"> disabilitati se non in uso; abilitati solo se necessari per la terza parte e disabilitati se non in uso. 	Consentendo ai fornitori di disporre di accesso 24/7 alla rete nel caso debbano fornire supporto ai sistemi, si aumentano le possibilità di accesso non autorizzato, sia da parte di un utente nell'ambiente del fornitore sia da parte di un utente non autorizzato che trova e utilizza questo punto di ingresso esterno alla rete sempre disponibile. È possibile impedire l'uso improprio delle connessioni fornendo l'accesso solo per il periodo necessario e disabilitandolo quando non serve più. Con il monitoraggio dell'accesso del fornitore è possibile verificare che i fornitori accedano solo ai sistemi necessari durante archi temporali approvati.
	8.1.5.b Consultare il personale e osservare i processi per verificare che gli account per l'accesso remoto di terzi siano monitorati durante l'uso.	
8.1.6 Limitare i tentativi di accesso ripetuti bloccando l'ID utente dopo un massimo di sei tentativi.	8.1.6.a Per un campione di componenti di sistema, 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.	Senza i meccanismi di blocco dell'account, un aggressore può tentare in modo continuo di indovinare una password mediante strumenti manuali o automatici (cracking delle password), fino ad avere successo e accedere all'account di un utente.
	8.1.6.b <i>Ulteriore procedura di test solo per le valutazioni</i>	

Requisiti PCI DSS	Procedure di test	Istruzioni
	dei provider di servizi: esaminare i processi interni e la documentazione per clienti/utenti e osservare i processi implementati per verificare che gli account utente dei clienti non consumatori siano temporaneamente bloccati dopo un massimo di sei tentativi di accesso non validi.	Nota: la procedura di test 8.1.6.b è una procedura aggiuntiva applicabile solo se l'entità in corso di valutazione è un provider di servizi.
8.1.7 Impostare la durata del blocco a un minimo di 30 minuti o finché l'amministratore non abilita l'ID utente.	8.1.7 Per un campione di componenti di sistema, 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.	Se un account è bloccato a causa di un tentativo continuo di indovinare una password, i controlli per ritardare la riattivazione degli account bloccati impediscono all'utente non autorizzato di tentare continuamente di individuare una password (l'interruzione minima prima della riattivazione dell'account è di 30 minuti). Inoltre, se è necessario richiedere la riattivazione, l'amministratore o l'help desk può verificare che sia il proprietario dell'account a richiedere la riattivazione.
8.1.8 Se una sessione è inattiva per più di 15 minuti, è necessario che l'utente effettui di nuovo l'autenticazione per riattivare il terminale o la sessione.	8.1.8 Per un campione di componenti di sistema, 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.	Quando gli utenti si allontanano da un computer attivo con accesso a dati dei titolari di carta o di sistema critici, il computer può essere utilizzato da altri in loro assenza, dando luogo all'accesso non autorizzato all'account e/o all'abuso dell'account. È possibile richiedere di effettuare di nuovo l'autenticazione sia a livello di sistema per proteggere tutte le sessioni in esecuzione su quel computer o a livello dell'applicazione.
8.2 Oltre ad assegnare un ID univoco, garantire la corretta gestione dell'autenticazione degli utenti non cliente e amministratori su tutti i componenti di sistema adottando almeno uno dei seguenti metodi per autenticare 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 un elemento biometrico. 	8.2 Per verificare che gli utenti vengano autenticati tramite un ID univoco e un altro elemento di autenticazione (ad esempio, una password/frase) per l'accesso all'ambiente dei dati dei titolari di carta, effettuare quanto segue: <ul style="list-style-type: none"> 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. 	Questi metodi di autenticazione, se usati in aggiunta agli ID univoci, aiutano a proteggere gli ID univoci degli utenti dalla compromissione (in quanto per un tentativo di compromissione è necessario conoscere sia l'ID univoco che la password o l'altro metodo di autenticazione). Tenere presente che un certificato digitale è una valida opzione per "qualcosa in possesso dell'utente" fin quando è univoco per un utente specifico. Poiché uno di primi passi compiuti da un utente non autorizzato per compromettere un sistema è sfruttare le password deboli o inesistenti, è importante implementare validi processi di gestione dell'autenticazione.

Requisiti PCI DSS	Procedure di test	Istruzioni
8.2.1 Utilizzando la crittografia avanzata, rendere illeggibili tutte le credenziali di autenticazione (quali password/passphrase) durante la trasmissione e la memorizzazione su tutti i componenti di sistema.	8.2.1.a Esaminare la documentazione del fornitore e le impostazioni di configurazione dei sistemi per verificare che le password siano protette con crittografia avanzata durante la trasmissione e la memorizzazione.	<p>Molti dispositivi e applicazioni di rete trasmettono password non cifrate e leggibili sulla rete e/o le memorizzano senza cifratura. Un utente non autorizzato può facilmente intercettare le password non cifrate utilizzando uno “sniffer” durante la trasmissione o accedendo direttamente a password non cifrate nei file in cui sono memorizzate, utilizzando i dati sottratti per l'accesso non autorizzato.</p> <p>Nota: le procedure di test 8.2.1.d e 8.2.1.e sono procedure aggiuntive applicabili solo se l'entità in corso di valutazione è un provider di servizi.</p>
	8.2.1.b Per un campione di componenti di sistema, esaminare i file di password per verificare che le password siano illeggibili durante la memorizzazione.	
	8.2.1.c Per un campione di componenti di sistema, esaminare le trasmissioni di dati per verificare che le password siano illeggibili durante la trasmissione.	
	8.2.1.d Ulteriore procedura di test solo per le valutazioni dei provider di servizi: osservare i file di password per verificare che le password dei clienti non consumatori siano illeggibili durante la memorizzazione.	
	8.2.1.e Ulteriore procedura di test solo per le valutazioni dei provider di servizi: osservare le trasmissioni di dati per verificare che le password dei clienti non consumatori siano illeggibili durante la trasmissione.	
8.2.2 Verificare l'identità dell'utente prima di modificare le credenziali di autenticazione, ad esempio ripristinando la password, fornendo nuovi token o generando nuove chiavi.	8.2.2 Esaminare le procedure delle di autenticazione per la modifica delle credenziali di autenticazione e osservare il personale responsabile della sicurezza per verificare che, se l'utente richiede il ripristino di una credenziale di autenticazione per telefono, e-mail, Web o in altra forma non diretta, l'identità di tale utente venga controllata prima di modificare tale credenziale di autenticazione.	<p>Molti utenti non autorizzati utilizzano l'ingegneria sociale, ad esempio chiamando un help desk e fingendosi un utente legittimo, per cambiare la loro password in modo da poter utilizzare un ID utente. Prendere in considerazione l'uso di una “domanda segreta” a cui solo l'utente legittimo può rispondere per aiutare gli amministratori a identificare l'utente prima di reimpostare o modificare le credenziali di autenticazione.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>8.2.3 Le password/passphrase devono soddisfare i seguenti parametri:</p> <ul style="list-style-type: none"> • Lunghezza minima di almeno 7 caratteri • Presenza di caratteri numerici e alfabetici <p>In alternativa, le password/passphrase devono presentare una complessità e solidità pari almeno ai parametri specificati sopra.</p>	<p>8.2.3.a Per un campione di componenti di sistema, ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password/passphrase dell'utente siano impostati in modo che venga richiesta almeno la seguente solidità/complessità:</p> <ul style="list-style-type: none"> • Lunghezza minima di almeno 7 caratteri • Presenza di caratteri numerici e alfabetici 	<p>Le password/passphrase avanzate sono la prima linea di difesa nella rete, in quanto un utente non autorizzato spesso tenta in primo luogo di trovare account con password deboli o inesistenti. Se le password sono corte o facili da indovinare, è abbastanza semplice per un utente non autorizzato individuare account deboli e compromettere una rete utilizzando un ID utente valido.</p> <p>Questo requisito indica che le password/passphrase devono contenere almeno sette caratteri e devono essere composte sia da caratteri numerici che alfabetici. Nei casi in cui questi requisiti minimi non possono essere soddisfatti a causa di limiti tecnici, le entità possono utilizzare la "potenza equivalente" per valutare la propria alternativa. Per informazioni sulla variabilità e sull'equivalenza della solidità delle password (anche definita entropia) per le password/passphrase di formati differenti, fare riferimento agli standard di settore (ad es., la versione corrente di NIST SP 800-63.)</p> <p>Nota: la procedura di test 8.2.3.b è una procedura aggiuntiva applicabile solo se l'entità in corso di valutazione è un provider di servizi.</p>
	<p>8.2.3.b Ulteriore procedura di test solo per le valutazioni dei provider di servizi: esaminare i processi interni e la documentazione per clienti/utenti per verificare che venga richiesta almeno la seguente solidità/complessità per le password/passphrase dei clienti non consumatori:</p> <ul style="list-style-type: none"> • Lunghezza minima di almeno 7 caratteri • Presenza di caratteri numerici e alfabetici 	
<p>8.2.4 Modificare le password/passphrase dell'utente almeno una volta ogni 90 giorni.</p>	<p>8.2.4.a Per un campione di componenti di sistema, ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password/passphrase dell'utente siano impostati in modo che ne venga richiesta la modifica almeno ogni 90 giorni.</p>	<p>Le password/passphrase in uso da lungo tempo senza essere state modificate forniscono agli utenti non autorizzati più tempo per tentare di violarle.</p> <p>Nota: la procedura di test 8.2.4.b è una procedura aggiuntiva applicabile solo se l'entità in corso di valutazione è un provider di servizi.</p>
	<p>8.2.4.b Ulteriore procedura di test solo per le valutazioni dei provider di servizi: Esaminare i processi interni e la documentazione per clienti/utenti per verificare che:</p> <ul style="list-style-type: none"> • venga richiesta periodicamente la modifica delle password/passphrase degli utenti clienti non consumatori; • vengano fornite agli utenti clienti non consumatori istruzioni relativamente a quando e in quali circostanze occorre modificare le password/passphrase. 	
<p>8.2.5 Non consentire l'invio di una</p>	<p>8.2.5.a Per un campione di componenti di sistema, richiedere e</p>	<p>Se non si conserva la cronologia password, si riduce</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
nuova password/passphrase uguale a una delle ultime quattro password/passphrase utilizzate.	<p>ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password siano impostati in modo che vengano richieste nuove password/passphrase diverse dalle ultime quattro password/passphrase utilizzate.</p> <p>8.2.5.b Ulteriore procedura di test solo per le valutazioni dei provider di servizi: esaminare i processi interni e la documentazione per clienti/utenti per verificare che le nuove password/passphrase degli utenti clienti non consumatori siano diverse dalle ultime quattro password utilizzate.</p>	<p>l'efficacia della modifica della password, poiché le password precedenti possono essere riutilizzate in continuazione. La richiesta di non riutilizzare le password per un periodo di tempo riduce il rischio di adottare in futuro password individuate o violate.</p> <p>Nota: la procedura di test 8.2.5.b è una procedura aggiuntiva applicabile solo se l'entità in corso di valutazione è un provider di servizi.</p>
8.2.6 Impostare le password/passphrase per il primo accesso e il ripristino su un valore univoco per ogni utente e modificarlo immediatamente dopo il primo uso.	8.2.6 Esaminare le procedure delle password e osservare il personale responsabile della sicurezza per verificare che le password/passphrase per il primo accesso per i nuovi utenti e le password/passphrase di ripristino per gli utenti esistenti siano impostate su un valore univoco per ogni utente e modificate dopo il primo uso.	Se viene utilizzata la stessa password per ogni nuovo utente, un utente interno, un ex-dipendente o un utente non autorizzato può conoscere o scoprire facilmente la password e utilizzarla per ottenere l'accesso agli account.
<p>8.3 Proteggere tutto il singolo accesso amministrativo non da console e tutto l'accesso remoto al CDE utilizzando l'autenticazione a più fattori.</p> <p>Nota: l'autenticazione a più fattori richiede l'utilizzo di almeno due dei tre metodi di autenticazione (fare riferimento al Requisito 8.2 per le descrizioni dei metodi di autenticazione). Utilizzare due volte un fattore (ad esempio, l'uso di due password separate) non viene considerato come un'autenticazione a più fattori.</p>		<p>L'autenticazione a più fattori richiede l'utilizzo di almeno due metodi separati di autenticazione (come descritto nel Requisito 8.2) prima che venga concesso l'accesso.</p> <p>L'autenticazione a più fattori garantisce inoltre l'identità dell'utente che tenta di ottenere l'accesso. Con l'autenticazione a più fattori, un aggressore dovrebbe compromettere almeno due meccanismi di autenticazione differenti, aumentando la difficoltà di compromissione e quindi riducendo il rischio.</p> <p>L'autenticazione a più fattori non è richiesta né a livello di sistema né a livello di applicazione per un determinato componente di sistema.</p> <p>L'autenticazione a più fattori può essere eseguita dopo l'autenticazione a un determinato componente di sistema o rete.</p> <p>Esempi di tecnologie a più fattori includono, senza limitazioni, 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 più fattori.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
8.3.1 Incorporare l'autenticazione a più fattori per tutto l'accesso non da console al CDE per il personale con accesso amministrativo. <i>Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.</i>	8.3.1.a Esaminare le configurazioni di sistema e/o di rete, come applicabile, per verificare che l'autenticazione a più fattori sia richiesta per tutto l'accesso amministrativo non da console al CDE.	<p>Questo requisito è valido per tutto il personale con accesso amministrativo al CDE. Questo requisito si applica solo al personale con accesso amministrativo e solo per l'accesso non da console al CDE; non si applica agli account di applicazioni o sistemi che eseguono funzioni automatiche.</p> <p>Se l'entità non utilizza la segmentazione per separare il CDE dal resto della rete, un amministratore potrebbe utilizzare l'autenticazione a più fattori per l'accesso alla rete CDE o a un sistema.</p> <p>Se il CDE è segmentato dal resto della rete dell'entità, un amministratore dovrebbe utilizzare l'autenticazione a più fattori quando si connette a un sistema CDE da una rete non CDE. L'autenticazione a più fattori può essere implementata a livello di rete o a livello di sistema/applicazione, ma non entrambi. Se l'amministratore utilizza MFA per l'accesso alla rete CDE, non deve utilizzarlo anche per l'accesso a un determinato sistema o applicazione nel CDE.</p>
	8.3.1.b Osservare un campione del personale (amministratori) che accede al CDE e verificare che almeno due dei tre metodi di autenticazione vengano utilizzati.	
8.3.2 Incorporare l'autenticazione a più fattori per tutto l'accesso remoto alla rete (sia utente che amministratore e incluso l'accesso di terzi per supporto o manutenzione) originato al di fuori della rete dell'entità.	8.3.2.a Esaminare le configurazioni di sistema per i server e i sistemi ad accesso remoto per verificare che venga richiesta l'autenticazione a più fattori per: <ul style="list-style-type: none"> tutto l'accesso remoto da parte del personale, sia utente che amministratore; tutti gli accessi in remoto da parte di terzi/fornitori (incluso l'accesso ad applicazioni e componenti di sistema per fini di assistenza o manutenzione). 	<p>Questo requisito è valido per tutto il personale, inclusi gli utenti generici, gli amministratori e i fornitori (per supporto o manutenzione) con accesso remoto alla rete, che potrebbe comportare l'accesso al CDE. Se l'accesso remoto avviene alla rete di un'entità dotata di adeguata segmentazione, tale che gli utenti in remoto non possono accedere o influire sull'ambiente dei dati dei titolari di carta, non sarebbe necessaria l'autenticazione a più fattori per l'accesso remoto a tale rete. Tuttavia, un'autenticazione a più fattori è richiesta per qualsiasi accesso remoto alle reti con accesso all'ambiente dei dati dei titolari di carta ed è consigliata per tutto l'accesso remoto alle reti dell'entità.</p>
	8.3.2.b Osservare un campione del personale (ad esempio, utenti e amministratori) che si connette in remoto alla rete e verificare che almeno due dei tre metodi di autenticazione vengano utilizzati.	

Requisiti PCI DSS	Procedure di test	Istruzioni
8.4 Documentare e comunicare le procedure e le politiche di autenticazione a tutti gli utenti inclusi: <ul style="list-style-type: none"> Istruzioni sulla selezione di credenziali di autenticazione avanzata Istruzioni su come gli utenti dovrebbero proteggere le proprie credenziali di autenticazione Istruzioni per non riutilizzare le password utilizzate precedentemente istruzioni per modificare le password in caso di sospetta compromissione delle password. 	8.4.a Esaminare le procedure e consultare il personale per verificare che le procedure e le politiche di autenticazione siano distribuite a tutti gli utenti.	<p>La comunicazione delle procedure e delle politiche per password/autenticazione a tutti gli utenti aiuta questi utenti a comprendere e rispettare le politiche.</p> <p>Ad esempio, le istruzioni sulla selezione di password complesse possono includere suggerimenti che aiutano il personale a scegliere password difficili da indovinare che non contengono termini presenti nel dizionario o informazioni sull'utente (quali l'ID utente, i nomi dei componenti della famiglia, la data di nascita, ecc.). Le istruzioni sulla protezione delle credenziali di autenticazione includono: non annotare le password né salvarle in file non sicuri ed essere avvisati gli utenti non autorizzati tentano di sfruttare le password (ad esempio, chiamando un dipendente e domandando la sua password in modo che il chiamante possa "risolvere un problema").</p> <p>Fornire agli utenti le istruzioni su come modificare le password nell'eventualità in cui la password non sia più sicura per impedire agli utenti non autorizzati di utilizzare password legittime per ottenere accesso non autorizzato.</p>
	8.4.b Analizzare le procedure e le politiche di autenticazione distribuite agli utenti e verificare che includano: <ul style="list-style-type: none"> Istruzioni sulla selezione di credenziali di autenticazione avanzata istruzioni su come gli utenti dovrebbero proteggere le proprie credenziali di autenticazione; istruzioni per gli utenti per non riutilizzare le password utilizzate precedentemente; istruzioni per modificare le password in caso di sospetta compromissione delle password. 	
	8.4.c Consultare un campione di utenti per verificare che siano a conoscenza delle procedure e delle politiche di autenticazione.	
8.5 Non utilizzare ID e password di gruppo, condivisi o generici né altri metodi di autenticazione, come segue: <ul style="list-style-type: none"> gli ID 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. 	8.5.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 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. 	<p>Se più utenti condividono le medesime credenziali di autenticazione (ad esempio, account utente e password), diventa impossibile tenere traccia dell'accesso e delle attività del sistema. A sua volta l'entità non riesce ad assegnare le responsabilità delle azioni degli utenti o a tenerne traccia in modo efficace, in quanto una determinata azione potrebbe essere stata eseguita da qualunque componente del gruppo a conoscenza delle credenziali di autenticazione.</p>
	8.5.b Esaminare le politiche e le procedure di autenticazione per verificare che siano espressamente vietati gli ID e/o le password di gruppo e condivisi o altri metodi di autenticazione.	
	8.5.c Consultare gli amministratori di sistema per verificare che non vengano distribuiti, anche se richiesto, ID e/o password di gruppo o condivisi o altri metodi di autenticazione.	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>8.5.1 Requisito aggiuntivo solo per provider di servizi: i provider di servizi con accesso remoto alle sedi dei clienti (ad esempio, per fornire assistenza a sistemi o server POS) devono utilizzare credenziali di autenticazione univoche (quali password/passphrase) per ogni cliente.</p> <p>Nota: questo requisito non è valido per i provider di hosting condiviso che accedono al proprio ambiente di hosting in cui sono ospitati più ambienti dei clienti.</p>	<p>8.5.1 Ulteriore procedura di test solo per le valutazioni dei provider di servizi: esaminare le politiche e le procedure di autenticazione e consultare il personale per verificare che vengano utilizzate credenziali di autenticazione diverse per l'accesso a ciascun cliente.</p>	<p>Nota: questo requisito si applica solo quando l'entità in corso di valutazione è un provider di servizi.</p> <p>Per evitare il problema della gestione di più ambienti dei clienti con un unico gruppo di credenziali, i fornitori con account di accesso remoto agli ambienti dei clienti devono utilizzare credenziali di autenticazione diverse per ogni cliente.</p> <p>Tecnologie, quali i meccanismi di autenticazione a più fattori, che forniscono un'unica credenziale per ciascuna connessione (ad esempio, tramite password monouso) potrebbero anche soddisfare lo scopo di questo requisito.</p>
<p>8.6 Laddove vengano utilizzati altri meccanismi di autenticazione (ad esempio, token di sicurezza fisici o logici, smart card, certificati, ecc.), l'uso di questi meccanismi deve essere assegnato come segue:</p> <ul style="list-style-type: none"> • i meccanismi di autenticazione devono essere assegnati a un singolo account e non vanno condivisi tra più account; • vanno adottati controlli fisici e/o logici per assicurare che solo un account determinato possa utilizzare tale meccanismo di accesso. 	<p>8.6.a Esaminare le politiche e le procedure di autenticazione per verificare che le procedure per l'utilizzo dei meccanismi di autenticazione, quali token, smartcard e certificati per la sicurezza fisica siano definiti e includano:</p> <ul style="list-style-type: none"> • meccanismi di autenticazione assegnati a un singolo account e non condivisi tra più account; • controlli fisici e/o logici definiti per assicurare che solo un account determinato possa utilizzare tale meccanismo di accesso. 	<p>Se i meccanismi di autenticazione dell'utente quali token, smartcard e certificati vengono utilizzati da più account, potrebbe essere impossibile identificare l'utente che utilizza il meccanismo di autenticazione. Disporre di controlli fisici e/o logici (ad esempio, PIN, dati biometrici o password) per identificare in maniera univoca l'utente dell'account consente di impedire agli utenti non autorizzati di accedere mediante l'uso di meccanismi di autenticazione condivisa.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
	<p>8.6.b Consultare il personale di sicurezza per verificare che i meccanismi di autenticazione vengano assegnati a un singolo account e non condivisi tra più account.</p> <p>8.6.c Esaminare le impostazioni di configurazione del sistema e/o i controlli fisici, secondo necessità, per verificare che i controlli vengano implementati e assicurare che solo l'account prestabilito possa utilizzare un determinato meccanismo di accesso.</p>	
<p>8.7 L'accesso a eventuali database contenenti dati dei titolari di carta (incluso l'accesso da parte di applicazioni, amministratori e altri utenti) è limitato come segue:</p> <ul style="list-style-type: none"> • Tutti gli accessi, le query e le azioni dell'utente sul database si verificano tramite metodi programmatici. • Solo gli amministratori del database hanno la possibilità di accedere o eseguire query direttamente sui database. • Gli ID di applicazione per le applicazioni del database possono essere utilizzati esclusivamente dalle applicazioni e non da utenti singoli o altri processi non relativi alle applicazioni. 	<p>8.7.a Analizzare le impostazioni di configurazione del database e dell'applicazione e verificare che venga eseguita l'autenticazione di tutti gli utenti prima dell'accesso.</p> <p>8.7.b Esaminare le impostazioni di configurazione del database e dell'applicazione per verificare 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).</p> <p>8.7.c Esaminare le impostazioni di controllo dell'accesso al database e le impostazioni di configurazione dell'applicazione del database per verificare che l'accesso diretto dell'utente e le query ai database siano consentite solo agli amministratori del database.</p> <p>8.7.d Esaminare le impostazioni di controllo dell'accesso al database, le impostazioni di configurazione delle 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.</p>	<p>Senza l'autenticazione utente per l'accesso a database e applicazioni, il potenziale di accessi non autorizzati o pericolosi aumenta; inoltre, tale accesso non può essere registrato in quando l'utente non è stato autenticato e quindi non è noto al sistema. Inoltre, l'accesso ai database deve essere consentito solo tramite metodi programmatici (ad esempio procedure memorizzate), anziché mediante accesso diretto al database da parte degli utenti finali (con l'eccezione dei DBA che possono avere accesso diretto al database per i loro compiti amministrativi).</p>
<p>8.8 Verificare che le politiche di sicurezza e le procedure operative per l'identificazione e l'autenticazione siano documentate, in uso e note a tutte le parti coinvolte.</p>	<p>8.8 Esaminare la documentazione e consultare il personale per verificare che i criteri di protezione e le procedure operative per l'identificazione e l'autenticazione siano:</p> <ul style="list-style-type: none"> • documentate; • in uso • note a tutte le parti coinvolte 	<p>È necessario che il personale sia a conoscenza delle seguenti politiche di sicurezza e procedure operative per la gestione continua dell'identificazione e dell'autorizzazione.</p>

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

Gli accessi fisici ai dati o ai sistemi che ospitano i dati dei 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	Istruzioni
9.1 Utilizzare i controlli dell'accesso alle strutture appropriati per limitare e monitorare gli accessi fisici ai sistemi nell'ambiente dei dati dei titolari di carta.	9.1 Verificare la presenza di controlli di sicurezza fisica per ogni sala computer, centro dati e altre aree fisiche con sistemi nell'ambiente dei dati dei titolari di carta. <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 di sistema a console per sistemi selezionati casualmente nell'ambiente dei dati dei titolari di carta e verificare che siano "sotto chiave" per impedire l'uso non autorizzato. 	Senza i controlli dell'accesso fisici, quali sistemi di tessere magnetiche e controlli all'ingresso, gli utenti non autorizzati possono facilmente accedere all'edificio per rubare, disattivare, interrompere o distruggere sistemi critici e dati dei titolari di carta. Il blocco delle schermate di accesso alla console consente di impedire agli utenti non autorizzate di accedere a informazioni sensibili, alterare le configurazioni di sistema, introdurre vulnerabilità nella rete o distruggere i record.
9.1.1 Utilizzare videocamere o meccanismi di controllo dell'accesso per monitorare il singolo accesso fisico 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>Nota: per "aree sensibili" si intendono centri dati, aree server e aree che ospitano sistemi di memorizzazione, elaborazione o trasmissione dei dati dei titolari di carta. Ciò esclude le aree rivolte al pubblico in cui vi sono i terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio.</p>	9.1.1.a Verificare che siano presenti videocamere o meccanismi di controllo dell'accesso per monitorare i punti di ingresso/uscita ad aree sensibili. <p>9.1.1.b Verificare che videocamere o meccanismi di controllo dell'accesso (o entrambi) siano protetti da manomissione o disabilitazione.</p>	Durante l'analisi delle violazioni alla protezione, questi controlli possono aiutare a identificare gli individui che hanno effettuato l'accesso a queste aree sensibili, quando sono entrati e quando sono usciti. <p>I criminali che cercano di ottenere l'accesso fisico alle aree sensibili spesso cercano di disattivare o eludere i controlli di monitoraggio. Per proteggere tali controlli contro manomissioni, è possibile utilizzare videocamere in modo da renderli irraggiungibili e/o monitorati per rilevare la manomissione. Analogamente, è possibile monitorare i meccanismi di controllo dell'accesso o installare protezioni fisiche per impedire che vengano danneggiati o disattivati da utenti non autorizzati.</p> <p style="text-align: right;"><i>(continua alla pagina successiva)</i></p>

Requisiti PCI DSS	Procedure di test	Istruzioni
	9.1.1.c Verificare che videocamere e/o meccanismi di controllo dell'accesso siano monitorati e che i dati vengano conservati per almeno tre mesi.	Esempi di aree sensibili comprendono aree server di database aziendali, aree back-office di sedi di punti vendita che memorizzano dati dei titolari di carta e aree di memorizzazione per grandi quantità di dati dei titolari di carta. Le aree sensibili dovrebbero essere identificate da ciascuna organizzazione per assicurare l'adeguata implementazione dei controlli di monitoraggio fisici.
9.1.2 Implementare controlli fisici e/o logici per limitare l'accesso ai connettori di rete pubblicamente accessibili. <i>Ad esempio, i connettori di rete che si trovano nelle aree pubbliche e nelle aree accessibili ai visitatori potrebbero essere disattivati e attivati solo quando l'accesso alla rete è autorizzato esplicitamente. In alternativa, è possibile implementare i processi per garantire che i visitatori siano scortati costantemente nelle aree con connettori di rete attivi.</i>	9.1.2 Consultare il personale responsabile e osservare le posizioni dei connettori di rete accessibili pubblicamente per verificare l'implementazione dei controlli fisici e/o logici per limitare l'accesso ai connettori di rete pubblicamente accessibili.	Limitando l'accesso ai connettori di rete (o porte di rete) è possibile impedire che utenti non autorizzati effettuino il collegamento a tali connettori disponibili, ottenendo accesso alle risorse della rete interna. Indipendentemente dal fatto che vengano utilizzati controlli logici o fisici, o un mix dei due, dovrebbero essere sufficienti a impedire a un utente o a un dispositivo non esplicitamente autorizzato di connettersi alla rete.
9.1.3 Limitare l'accesso fisico a punti di accesso wireless, gateway, dispositivi portatili, hardware di rete e comunicazione e linee di telecomunicazione.	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.	Senza la protezione dell'accesso a componenti e dispositivi wireless, gli utenti non autorizzati possono utilizzare i dispositivi wireless incustoditi dell'organizzazione per accedere alle risorse di rete, o persino per connettere i loro dispositivi alla rete wireless, ottenendo accesso non autorizzato. Inoltre, la protezione di hardware di comunicazione e di rete impedisce agli utenti non autorizzati di intercettare il traffico di rete o di collegare fisicamente i loro dispositivi alle risorse di rete cablate.

Requisiti PCI DSS	Procedure di test	Istruzioni
9.2 Sviluppare procedure per consentire di distinguere facilmente tra personale in sede e visitatori e includere: <ul style="list-style-type: none"> individuazione di personale in sede e visitatori (ad esempio, assegnando tessere magnetiche); modifiche ai requisiti di accesso; revoca o disattivazione dell'identificazione scaduta del personale in sede e dei visitatori (quali tessere magnetiche). 	9.2.a Analisi dei processi documentati per verificare che siano state definite le procedure per l'identificazione e la distinzione di personale in sede e visitatori. <ul style="list-style-type: none"> Verificare che le procedure includano quanto segue: individuazione di personale in sede e visitatori (ad esempio, assegnando tessere magnetiche); modifica dei requisiti di accesso; revoca dell'identificazione scaduta del personale in sede o dei visitatori (ad esempio, tessere magnetiche). 	La predisposizione dell'identificazione dei visitatori autorizzati in modo da poterli facilmente distinguerli dal personale in sede impedisce che a visitatori non autorizzati venga concesso l'accesso ad aree contenenti dati dei titolari di carta.
	9.2.b Esaminare metodi di identificazione (ad esempio, tessere magnetiche) e osservare i processi per l'identificazione e la distinzione tra personale in sede e visitatori per verificare che: <ul style="list-style-type: none"> i visitatori vengano identificati in modo chiaro; sia facile distinguere il personale in sede dai visitatori. 	
	9.2.c Verificare che l'accesso al processo di identificazione (quale un sistema di tessere magnetiche) sia limitato al personale autorizzato.	
9.3 Controllare l'accesso fisico per il personale in sede alle aree sensibili come segue: <ul style="list-style-type: none"> l'accesso deve essere autorizzato e basato sulla mansione dell'utente; l'accesso viene revocato immediatamente al termine del rapporto di lavoro e tutti i meccanismi di accesso fisici, quali chiavi, schede di accesso, ecc., vengono restituiti o disattivati. 	9.3.a Per un campione del personale in sede con accesso fisico ad aree sensibili, consultare il personale responsabile e osservare gli elenchi di controllo dell'accesso per verificare che: <ul style="list-style-type: none"> l'accesso all'area sensibile sia autorizzato; l'accesso sia necessario per lo svolgimento della mansione dell'utente. 	Il controllo dell'accesso fisico ad aree sensibili aiuta a garantire che solo il personale autorizzato con un'esigenza aziendale legittima ottenga l'accesso. Al termine del rapporto di lavoro, tutti i meccanismi di accesso fisico devono essere restituiti o disabilitati tempestivamente (non appena possibile), per garantire che il personale non possa più accedere fisicamente alle aree sensibili.
	9.3.b Osservare l'accesso del personale ad aree sensibili per verificare che tutto il personale abbia l'autorizzazione prima di poter accedere.	
	9.3.c Selezionare un campione di dipendenti il cui rapporto di lavoro con l'azienda è terminato di recente ed esaminare gli elenchi di controllo dell'accesso per verificare che il personale non abbia più accesso fisico alle aree sensibili.	

Requisiti PCI DSS	Procedure di test	Istruzioni
9.4 Implementare le procedure per identificare e autorizzare i visitatori. Le procedure devono includere quanto segue:	9.4 Verificare che siano in atto i controlli delle autorizzazioni e degli accessi dei visitatori come segue:	I controlli sui visitatori sono importanti per ridurre la capacità degli utenti non autorizzati di accedere agli edifici (e, potenzialmente, ai dati dei titolari di carta).
9.4.1 I visitatori ricevono l'autorizzazione prima di accedere e devono essere sempre scortati nelle aree in cui i dati dei titolari di carta sono elaborati o custoditi.	9.4.1.a Osservare le procedure e consultare il personale per verificare che i visitatori abbiano ricevuto l'autorizzazione prima di accedere e siano sempre scortati nelle aree in cui i dati dei titolari di carta sono elaborati o custoditi.	I controlli sui visitatori garantiscono che i visitatori siano identificabili in modo che il personale possa controllarne le attività e che il loro accesso sia limitato solo alla durata della visita legittima. La restituzione delle tessere magnetiche dei visitatori alla scadenza o al termine della visita consente di impedire agli utenti non autorizzati di utilizzare un pass precedentemente autorizzato e accedere all'edificio al termine della visita.
	9.4.1.b Osservare l'uso delle tessere magnetiche dei visitatori o degli altri strumenti di identificazione per verificare che il token fisico non permetta l'accesso non scortato alle aree fisiche in cui i dati dei titolari di carta vengono elaborati o custoditi.	
9.4.2 I visitatori vengono identificati e ricevono una tessera magnetica o altro strumento di identificazione che scade e che consente di distinguere visivamente i visitatori dal personale in sede.	9.4.2.a Osservare le persone all'interno della struttura per verificare l'uso di tessere magnetiche o altro strumento di identificazione per i visitatori e che sia possibile distinguere facilmente i visitatori dal personale in sede.	Un registro dei visitatori che documenta informazioni minime sul visitatore è facile ed economico da mantenere e può offrire assistenza nell'identificazione dell'accesso fisico a un edificio o un locale e potenzialmente ai dati dei titolari di carta.
	9.4.2.b Verificare che le tessere magnetiche dei visitatori o gli altri strumenti di identificazione abbiano una scadenza.	
9.4.3 Ai visitatori viene chiesto di restituire la tessera magnetica o altro strumento di identificazione prima di lasciare la struttura o in corrispondenza della data di scadenza.	9.4.3 Osservare i visitatori che lasciano la struttura per verificare che venga loro richiesta la restituzione della tessera magnetica o altro strumento di identificazione all'uscita o al momento della scadenza.	
9.4.4 Il registro dei visitatori viene utilizzato per mantenere un audit trail fisico dell'attività dei visitatori nella struttura nonché nelle aree computer e nei centri dati in cui vengono memorizzati o trasmessi i dati dei titolari di carta. Documentare il nome del visitatore, l'azienda rappresentata e il personale	9.4.4.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 dei titolari di carta.	
	9.4.4.b Verificare che il registro contenga: <ul style="list-style-type: none"> • nome del visitatore; • azienda rappresentata; • personale in sede che autorizza l'accesso fisico. 	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>in sede che autorizza l'accesso fisico sul registro.</p> <p>Conservare questo registro per almeno tre mesi, se non diversamente richiesto dalla legge.</p>	<p>9.4.4.c Verificare che il registro venga conservato per almeno tre mesi.</p>	
<p>9.5 Proteggere fisicamente tutti i supporti.</p>	<p>9.5 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).</p>	<p>I controlli per proteggere fisicamente i supporti hanno lo scopo di impedire agli utenti non autorizzati di accedere ai dati dei titolari di carta su tutti i tipi di supporto. I dati dei titolari di carta sono soggetti a visualizzazione, copia o scansione non autorizzate se sono trasferiti senza protezione su supporti portatili o rimovibili, stampati o lasciati sulla scrivania.</p>
<p>9.5.1 Conservare i backup dei supporti in un luogo sicuro, preferibilmente in una struttura esterna, come un luogo alternativo o di backup oppure un magazzino. Controllare la sicurezza del luogo almeno una volta all'anno.</p>	<p>9.5.1 Verificare che la sicurezza del luogo di conservazione sia rivista almeno una volta all'anno per confermare che la conservazione dei supporti di backup è sicura.</p>	<p>Se conservati in un ambiente non sicuro, i backup contenenti i dati dei titolari di carta possono essere facilmente persi, rubati o copiati per scopi pericolosi.</p> <p>L'analisi periodica del luogo di conservazione consente all'organizzazione di risolvere i problemi di sicurezza identificati in maniera tempestiva, riducendo al minimo il rischio potenziale.</p>
<p>9.6 Mantenere un rigido controllo sulla distribuzione interna o esterna di qualsiasi tipo di supporto, incluso quanto segue:</p>	<p>9.6 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.</p>	<p>Procedure e processi che aiutano a proteggere i dati dei titolari di carta sui supporti distribuiti agli utenti interni e/o esterni. Senza tali procedure i dati possono essere persi o rubati e utilizzati per scopi fraudolenti.</p>
<p>9.6.1 Classificare i supporti in modo che si possa determinare la sensibilità dei dati.</p>	<p>9.6.1 Verificare che tutti i supporti siano classificati in modo da poter determinare la sensibilità dei dati.</p>	<p>È importante che i supporti siano identificati in modo che il loro stato di classificazione possa essere facilmente rilevato. I supporti non identificati come riservati potrebbero non disporre di una protezione adeguata o potrebbero essere persi o rubati.</p> <p>Nota: questo non significa che sui supporti deve essere presente l'etichetta "Riservato", lo scopo è quello di permettere all'organizzazione che ha identificato i supporti contenenti dati sensibili di proteggerli.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
9.6.2 Inviare i supporti tramite un corriere affidabile o un altro metodo di consegna che possa essere monitorato in modo appropriato.	9.6.2.a Consultare il personale e esaminare i record per verificare che tutti i supporti inviati all'esterno della struttura siano registrati e vengano inviati tramite corriere affidabile o un altro metodo di consegna monitorato.	I supporti possono essere rubati o persi se inviati tramite un metodo non rintracciabile, ad esempio la posta tradizionale. L'uso di corrieri affidabili per consegnare i supporti che contengono i dati dei titolari di carta consentono alle organizzazioni di utilizzare i loro sistemi di tracking per mantenere l'inventario e la posizione delle spedizioni.
	9.6.2.b 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.	
9.6.3 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).	9.6.3 Selezionare un campione recente di alcuni giorni dei registri di controllo fuori sede per tutti i supporti. Sulla base dell'analisi dei registri e dei colloqui con il personale responsabile, verificare che sia stata ottenuta l'opportuna autorizzazione del management ogniqualvolta vengono spostati i supporti da un'area protetta (in particolare quando i supporti vengono distribuiti a singoli utenti).	In assegni di un solido processo che garantisce l'approvazione di tutti gli spostamenti dei supporti prima della loro rimozione dalle aree sicure, i supporti non verrebbero monitorati né adeguatamente protetti e la loro posizione sarebbe sconosciuta, facilitando lo smarrimento o il furto dei supporti.
9.7 Mantenere un rigido controllo sulla conservazione e sull'accessibilità dei supporti.	9.7 Ottenere 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.	Senza metodi di inventario attenti e controlli di storage, potrebbe non essere possibile accorgersi del furto o della mancanza di supporti per diverso tempo.
9.7.1 Conservare in modo appropriato i registri di inventario per tutti i supporti ed eseguire tali inventari almeno una volta all'anno.	9.7.1 Richiedere ed esaminare i registri di inventario dei supporti per verificare che vengano conservati ed eseguiti periodicamente inventari dei supporti almeno una volta all'anno.	Se i supporti non vengono inventariati, potrebbe non essere possibile accorgersi del furto o della mancanza di supporti per diverso tempo oppure non accorgersene affatto.
9.8 Distruggere i supporti quando non sono più necessari per scopi aziendali o legali, come segue:	9.8 Esaminare la politica di distruzione dei supporti periodica e verificare che tale politica copra tutti i supporti e definisca o requisiti per quanto riportato di seguito: <ul style="list-style-type: none"> • Verificare che i materiali cartacei vengano stracciati tramite trinciatrice, bruciati o macerati in modo da garantire ragionevolmente che tali materiali non potranno essere ricostruiti. • I contenitori utilizzati per il materiale da distruggere devono essere sicuri. • I dati dei titolari di carta su supporti elettronici devono essere resi irrecuperabili (ad es. tramite un programma di cancellazione sicura basato su standard di settore accettati per l'eliminazione sicura oppure distruggendo fisicamente i supporti). 	La mancata adozione di misure per distruggere le informazioni contenute sui dischi rigidi, unità portatili, CD/DVD o su carta prima dell'eliminazione, può dar modo ad utenti non autorizzati di recuperare le informazioni dai supporti eliminati, determinando una compromissione dei dati. Ad esempio, gli individui non autorizzati possono utilizzare una tecnica chiamata "dumpster diving", con la quale ricercano nei cestini e nella spazzatura informazioni che possono usare per lanciare un attacco. Proteggendo i contenitori utilizzati per il materiale da distruggere impedisce l'acquisizione delle informazioni sensibili durante la raccolta del

Requisiti PCI DSS	Procedure di test	Istruzioni
9.8.1 Stracciare, bruciare o mandare al macero i materiali cartacei in modo che i dati dei titolari di carta non possano essere ricostruiti. Proteggere i contenitori utilizzati per il materiale da distruggere.	9.8.1.a Consultare il personale ed esaminare le procedure per verificare che i materiali cartacei vengano stracciati tramite trinciatrice, bruciati o macerati in modo da garantire ragionevolmente che tali materiali non potranno essere ricostruiti.	<p>materiale. Ad esempio, i contenitori di “informazioni da distruggere” potrebbero disporre di un dispositivo di blocco che impedisce l’accesso ai contenuti o impedisce l’accesso fisico al contenuto.</p> <p>Esempi di metodi che consentono una distruzione sicura dei supporti elettronici comprendono cancellazione, smagnetizzazione o distruzione fisica (come tritare o distruggere i dischi rigidi).</p>
	9.8.1.b Esaminare i contenitori utilizzati per i materiali che contengono le informazioni da distruggere per verificare che siano sicuri.	
9.8.2 Rendere i dati dei titolari di carta su supporti elettronici non recuperabili, in modo che non sia possibile ricostruirli.	9.8.2 Verificare che i dati dei titolari di carta su supporti elettronici vengano resi irrecuperabili (ad es. tramite un programma di cancellazione sicura basato su standard di settore accettati per l’eliminazione sicura oppure distruggendo fisicamente i supporti).	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>9.9 Proteggere conto manomissioni e sostituzioni i dispositivi che acquisiscono i dati delle carte di pagamento attraverso un'interazione fisica diretta con la carta.</p> <p>Nota: questi requisiti si applicano ai dispositivi che leggono le carte utilizzati nelle transazioni con carta presente (ovvero, tessera magnetica o dip) nel punto vendita. Questo requisito non si applica ai componenti per l'immissione manuale, quali tastiere di computer o tastierini di POS.</p>	<p>9.9 Esaminare le politiche e le procedure per verificare che includano:</p> <ul style="list-style-type: none"> la conservazione di un elenco di dispositivi; l'ispezione periodica dei dispositivi per verificare la presenza di manomissioni o sostituzioni; la formazione del personale che deve essere a conoscenza del comportamento sospetto e segnalare le manomissioni o le sostituzioni dei dispositivi. 	<p>I criminali tentano di sottrarre i dati dei titolari di carta appropriandosi e/o manipolando i dispositivi e i terminali che leggono le carte. Ad esempio, cercano di rubare i dispositivi per capire come accedervi e spesso tentano di sostituire i dispositivi legittimi con dispositivi fraudolenti con cui acquisiscono le informazioni delle carte di pagamento ogniquale volta viene inserita una carta. I criminali cercano anche di aggiungere componenti di "skimming" all'esterno dei dispositivi, in grado di acquisire i dettagli delle carte di pagamento ancor prima di introdursi nel dispositivo, ad esempio collegando un ulteriore lettore di carte sopra al lettore di carte legittimo in modo che da acquisire due volte i dettagli delle carte di pagamento: una volta dal componente del criminale e un'altra dal componente legittimo del dispositivo. In questo modo, le transazioni vengono concluse senza interruzioni mentre il criminale effettua lo "skimming" delle informazioni delle carte di pagamento durante il processo.</p> <p>Questo requisito è consigliato, ma non obbligatorio, per i componenti per l'immissione manuale, quali tastiere di computer o tastierini di POS.</p> <p>Altre migliori pratiche sulla prevenzione dello skimming sono disponibili sul sito Web PCI SSC.</p>
<p>9.9.1 Conservare un elenco aggiornato di dispositivi. L'elenco deve includere quanto segue:</p> <ul style="list-style-type: none"> Marca, modello del dispositivo Posizione del dispositivo (ad esempio, l'indirizzo della sede o della struttura in cui si trova il dispositivo) numero di serie del dispositivo o altro metodo di identificazione 	<p>9.9.1.a Esaminare l'elenco dei dispositivi per verificare che includano:</p> <ul style="list-style-type: none"> Marca, modello del dispositivo Posizione del dispositivo (ad esempio, l'indirizzo della sede o della struttura in cui si trova il dispositivo) numero di serie del dispositivo o altro metodo di identificazione univoca. <p>9.9.1.b Selezionare un campione di dispositivi dall'elenco e osservare i dispositivi e le relative posizioni per verificare che l'elenco sia accurato e aggiornato.</p>	<p>L'elenco aggiornato dei dispositivi consente all'organizzazione di registrare la posizione in cui dovrebbero essere i dispositivi e di individuare velocemente se un dispositivo manca o è andato perso.</p> <p>Il metodo utilizzato per conservare un elenco di dispositivi può essere automatico (ad esempio, un sistema di gestione dei dispositivi) o manuale (ad esempio, documentato in record elettronici o cartacei). Per i dispositivi in movimento, la posizione può includere il nome del personale a cui</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
univoca.	9.9.1.c Consultare il personale per verificare che l'elenco di dispositivi sia aggiornato quando i dispositivi vengono aggiunti, riposizionato, messi fuori uso, ecc.	è stato assegnato il dispositivo.
<p>9.9.2 Ispezionare periodicamente le superfici del dispositivo per rilevare manomissioni (ad esempio, aggiunta di skimmer di carte ai dispositivi) o sostituzioni (ad esempio, controllando il numero di serie o le caratteristiche del dispositivo per verificare che non sia stato sostituito con un dispositivo fraudolento).</p> <p>Nota: esempi di indicazioni che un dispositivo potrebbe essere stato alterato o sostituito includono raccordi o cavi innestati nel dispositivo, etichette di sicurezza mancanti o modificate, involucri rotti o di colori diversi o modifiche al numero di serie o altri contrassegni esterni.</p>	<p>9.9.2.a Esaminare le procedure documentate per verificare che la definizione dei processi preveda gli elementi seguenti:</p> <ul style="list-style-type: none"> • procedure per ispezionare i dispositivi; • frequenza delle ispezioni. <p>9.9.2.b Consultare il personale responsabile e osservare i processi di ispezione per verificare che:</p> <ul style="list-style-type: none"> • il personale sia a conoscenza delle procedure per ispezionare i dispositivi; • tutti i dispositivi vengano periodicamente ispezionati per rilevare la prova di alterazioni o sostituzioni. 	<p>Le ispezioni regolari dei dispositivi consentono alle organizzazioni di rilevare più rapidamente le alterazioni o sostituzioni di un dispositivo e di contenere quindi l'impatto potenziale dell'uso di dispositivi fraudolenti.</p> <p>Il tipo di ispezione dipende dal dispositivo; ad esempio, è possibile utilizzare le fotografie di dispositivi noti come dispositivi protetti per confrontare l'aspetto attuale del dispositivo con il suo aspetto originario e vedere se sia cambiato. Un'altra opzione prevede l'uso di un evidenziatore sicuro, come una penna con luce ultravioletta, per contrassegnare le superfici e gli orifizi del dispositivo ed evidenziare eventuali alterazioni o sostituzioni. I criminali spesso sostituiscono l'involucro esterno di un dispositivo per celarne l'alterazione; tali metodi possono consentire di rilevare queste attività. I fornitori di dispositivi possono anche fornire indicazioni di sicurezza e guide sulle procedure per poter determinare se il dispositivo sia stato alterato.</p> <p>La frequenza delle ispezioni dipende da fattori come la posizione del dispositivo e se il dispositivo sia custodito o incustodito. Ad esempio, i dispositivi situati in aree pubbliche senza la supervisione del personale dell'organizzazione possono essere soggetti a ispezioni più frequenti rispetto ai dispositivi collocati in aree protette o supervisionati quando sono accessibili al pubblico. Il tipo e la frequenza delle ispezioni è determinato dall'esercente, secondo la definizione del rispettivo processo di valutazione dei rischi.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>9.9.3 Garantire la formazione del personale che deve essere a conoscenza dei tentativi di alterazione o sostituzione dei dispositivi. La formazione deve comprendere quanto segue:</p> <ul style="list-style-type: none"> • Verifica dell'identità di eventuali terzi che sostengono di essere addetti alle riparazioni o alla manutenzione, prima di consentire loro l'autorizzazione a modificare o risolvere i problemi dei dispositivi. • Divieto di installare, sostituire o restituire dispositivi in assenza di verifica. • Massima attenzione al comportamento sospetto in prossimità dei dispositivi (ad esempio, tentativi di persone sconosciute di disconnettere o aprire i dispositivi). • Segnalazione di comportamento sospetto e indicazioni di alterazione o sostituzione del dispositivo al personale appropriato (ad esempio, un manager o un addetto alla sicurezza). 	<p>9.9.3.a Esaminare il materiale formativo per il personale dei punti vendita per accertarsi che comprenda la formazione sui seguenti aspetti:</p> <ul style="list-style-type: none"> • verifica dell'identità di eventuali terzi che sostengono di essere addetti alle riparazioni o alla manutenzione, prima di consentire loro l'autorizzazione a modificare o risolvere i problemi dei dispositivi; • divieto di installare, sostituire o restituire dispositivi in assenza di verifica; • massima attenzione al comportamento sospetto in prossimità dei dispositivi (ad esempio, tentativi di persone sconosciute di disconnettere o aprire i dispositivi); • segnalazione di comportamento sospetto e indicazioni di alterazione o sostituzione del dispositivo al personale appropriato (ad esempio, un manager o un addetto alla sicurezza). <p>9.9.3.b Consultare un campione del personale presso il punto vendita per verificare che abbia ricevuto la formazione e che sia a conoscenza delle procedure per quanto segue:</p> <ul style="list-style-type: none"> • verifica dell'identità di eventuali terzi che sostengono di essere addetti alle riparazioni o alla manutenzione, prima di consentire loro l'autorizzazione a modificare o risolvere i problemi dei dispositivi; • divieto di installare, sostituire o restituire dispositivi in assenza di verifica; • massima attenzione al comportamento sospetto in prossimità dei dispositivi (ad esempio, tentativi di persone sconosciute di disconnettere o aprire i dispositivi); • segnalazione di comportamento sospetto e indicazioni di alterazione o sostituzione del dispositivo al personale appropriato (ad esempio, un manager o un addetto alla sicurezza). 	<p>I criminali si fanno spesso passare per addetti autorizzati alla manutenzione per poter accedere ai dispositivi POS. Tutti i terzi che richiedono di accedere ai dispositivi devono venire sottoposti a verifica prima di essere autorizzati, ad esempio controllando presso la direzione o telefonando alla società di manutenzione del POS (il fornitore o l'acquirente) per verifica. Molti criminali tentano di ingannare il personale adottando un abbigliamento consono (ad esempio, portando con sé cassette degli attrezzi e indossando abiti da lavoro) e potrebbero anche avere una certa conoscenza delle ubicazioni dei dispositivi; è pertanto importante che il personale sia addestrato a seguire le procedure in ogni circostanza.</p> <p>Un altro trucco adottato spesso dai criminali prevede l'invio di un "nuovo" sistema POS con istruzioni per scambiarlo con un sistema legittimo e "restituire" il sistema legittimo a un indirizzo dato. I criminali possono persino arrivare a fornire l'affrancatura di ritorno poiché sono particolarmente ansiosi di mettere le mani sui dispositivi. Il personale è tenuto a verificare sempre con il proprio manager o fornitore che il dispositivo sia legittimo e provenga da una fonte affidabile prima di installarlo o utilizzarlo per l'azienda.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
9.10 Verificare che le politiche di sicurezza e le procedure operative per la limitazione dell'accesso fisico ai dati dei titolari di carta siano documentate, in uso e note a tutte le parti coinvolte.	9.10 Esaminare la documentazione e consultare il personale per verificare che le politiche di sicurezza e le procedure operative per la limitazione dell'accesso fisico ai dati dei titolari di carta siano: <ul style="list-style-type: none">• documentate;• in uso• note a tutte le parti coinvolte	È necessario che il personale sia a conoscenza delle seguenti politiche di sicurezza e procedure operative per limitare continuamente l'accesso fisico ai dati dei titolari di carta e ai sistemi nell'ambiente dei dati dei titolari di carta.

Monitoraggio e test delle reti regolari

Requisito 10 - Registrare e monitorare tutti gli accessi a risorse di rete e dati dei 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, se non impossibile, determinare la causa di una compromissione di dati.

Requisiti PCI DSS	Procedure di test	Istruzioni
10.1 Implementare audit trail per collegare l'accesso ai componenti di sistema a ogni singolo utente.	10.1 Verificare tramite osservazione e consultazione dell'amministratore di sistema che: <ul style="list-style-type: none"> gli audit trail siano attivi e funzionanti per i componenti di sistema; l'accesso ai componenti di sistema sia collegato ad ogni singolo utente. 	È fondamentale disporre di un processo o di un sistema che colleghi l'accesso dell'utente ai componenti di sistema. Questo sistema genera log di audit e consente di ricondurre le attività sospette a un utente specifico.
10.2 Implementare audit trail automatizzati per tutti i componenti del sistema per ricostruire i seguenti eventi:	10.2 Tramite consultazioni con il personale responsabile, osservazione dei log di audit ed esame delle relative impostazioni, eseguire quanto segue:	La generazione di audit trail sulle attività sospette avverte l'amministratore di sistema, invia dati ad altri meccanismi di monitoraggio (ad esempio i sistemi di rilevamento delle intrusioni) e fornisce una cronologia da utilizzare a seguito di un incidente. La registrazione dei seguenti eventi consente ad un'organizzazione di identificare e tenere traccia delle attività potenzialmente dannose.
10.2.1 Tutti gli accessi utente ai dati dei titolari di carta	10.2.1 Verificare che tutti gli accessi utente ai dati dei titolari di carta siano registrati.	Gli utenti non autorizzati potrebbero arrivare a conoscere un account utente con accesso ai sistemi nell'ambiente dei dati dei titolari di carta, oppure potrebbero creare un nuovo account non autorizzato per accedere ai dati dei titolari di carta. La registrazione di tutti gli accessi individuali ai dati dei titolari di carta può individuare quali account possono essere stati compromessi o usati in modo improprio.

Requisiti PCI DSS	Procedure di test	Istruzioni
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.	Account con maggiori privilegi, come di “amministratore” o “root”, hanno il potenziale di influire in modo significativo sulla sicurezza o sulla funzionalità operativa di un sistema. Senza un registro delle attività eseguite, un’organizzazione non è in grado di ricondurre ogni questione risultante da un errore amministrativo o dall’uso improprio di privilegi all’individuo o all’azione specifici.
10.2.3 Accesso a tutti gli audit trail	10.2.3 Verificare che l’accesso a tutti gli audit trail sia registrato.	Gli utenti non autorizzati spesso cercano di modificare i log di audit per nascondere le loro azioni e con la registrazione degli accessi un’organizzazione può ricondurre eventuali incongruenze o potenziali manomissioni dei registri ad un singolo account. Il potere accedere ai registri che identificano modifiche, aggiunte ed eliminazioni consente di ricostruire i passaggi intrapresi dal personale non autorizzato.
10.2.4 Tentativi di accesso logico non validi	10.2.4 Verificare che siano registrati i tentativi di accesso logico non riusciti.	Gli utenti non autorizzati sulla rete spesso eseguono più tentativi di accesso sui sistemi di destinazione. Vari tentativi di accesso non riusciti possono rappresentare un’indicazione dei tentativi di accesso di un utente non autorizzato facendo ricorso a “forza bruta” o cercando di indovinare una password.
10.2.5 Uso e modifiche dei meccanismi di identificazione e autenticazione (compresi, a titolo esemplificativo, creazione di nuovi account, incremento dei privilegi) e tutte le modifiche, le aggiunte e le eliminazioni agli account con privilegi root o di amministratore.	10.2.5.a Verificare che l’uso dei meccanismi di identificazione e autenticazione sia registrato.	Se non è possibile sapere chi erano gli utenti presenti al momento in cui si è verificato un incidente, non è possibile identificare gli account che potrebbero essere stati utilizzati. Inoltre, gli utenti non autorizzati possono tentare di manipolare i controlli di autenticazione per cercare di superarli o di spacciarsi per un account valido.
	10.2.5.b Verificare che l’aumento dei privilegi sia stato registrato.	
	10.2.5.c Verificare che siano registrate tutte le modifiche, le aggiunte o le eliminazioni a qualsiasi account con privilegi di utente root o amministratore.	

Requisiti PCI DSS	Procedure di test	Istruzioni
10.2.6 Inizializzazione, arresto o pausa dei log di audit	10.2.6 Verificare che vengano registrati i seguenti elementi: <ul style="list-style-type: none"> • inizializzazione di log di audit; • blocco o sospensione dei log di audit. 	La disattivazione (o la sospensione) dei log di audit prima di eseguire delle attività illecite è una prassi comune degli utenti non autorizzati che non vogliono essere scoperti. L'inizializzazione dei log di audit potrebbe indicare che la funzione di registrazione è stata disattivata da un utente per nascondere le sue azioni.
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.	Software dannoso, come il malware, spesso crea o sostituisce oggetti a livello di sistema sul sistema di destinazione per controllarne una determinata funzione o operazione in tale sistema. Grazie alla registrazione della creazione e dell'eliminazione degli oggetti a livello di sistema, come tabelle di database o procedure memorizzate, sarà più facile determinare se tali modifiche sono state autorizzate o meno.
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 dei log di audit, per ogni evento inseribile nell'audit (da 10.2):	Registrando queste voci per gli eventi registrabili nel punto 10.2, è possibile identificare rapidamente una potenziale compromissione e disporre di dettagli sufficienti per sapere chi, cosa, dove, come e quando.
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 l'indicazione di data e ora sia inclusa 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 dei dati, del componente di sistema o delle risorse interessati siano inclusi nelle voci di registro.	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>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.</p> <p>Nota: NTP (Network Time Protocol) è un esempio di tecnologia per la sincronizzazione dell'ora.</p>	<p>10.4 Esaminare gli standard e i processi di configurazione per verificare che la tecnologia per la sincronizzazione dell'ora sia implementata e tenuta aggiornata in base ai Requisiti 6.1 e 6.2 PCI DSS.</p>	<p>La tecnologia per la sincronizzazione dell'ora viene utilizzata per sincronizzare gli orologi su sistemi multipli. Quando gli orologi non sono sincronizzati in modo corretto può risultare difficile se non impossibile il confronto di file di log di diversi sistemi e stabilire la sequenza esatta di eventi (elemento fondamentale per l'analisi forense nel caso di una violazione). Per i team legali attivati dopo un incidente, la precisione e l'uniformità dell'ora tra tutti i sistemi e l'ora di ciascuna attività è fondamentale per determinare come sono stati compromessi i sistemi.</p>
<p>10.4.1 I sistemi critici hanno l'ora esatta e uniforme.</p>	<p>10.4.1.a Esaminare il processo di acquisizione, distribuzione e archiviazione dell'ora esatta all'interno dell'organizzazione per verificare che:</p> <ul style="list-style-type: none"> • solo i server di rilevamento dell'orario centrali designati ricevano i segnali orari da sorgenti esterne e che tali segnali si basino su International Atomic Time o UTC; • laddove esiste più di un server di riferimento orario, i server comunichino tra loro per mantenere un orario esatto; • i sistemi ricevano le informazioni orarie soltanto dai server centrali di riferimento orario designati. 	
	<p>10.4.1.b Osservare le impostazioni dei parametri di sistema legati all'ora per un campione dei componenti di sistema per verificare che:</p> <ul style="list-style-type: none"> • solo i server di rilevamento dell'orario centrali designati ricevano i segnali orari da sorgenti esterne e che tali segnali si basino su International Atomic Time o UTC; • laddove esiste più di un server di riferimento orario, i server centrali designati comunichino tra loro per mantenere un orario esatto; • i sistemi ricevano le informazioni orarie soltanto dai server centrali designati. 	
<p>10.4.2 I dati dell'ora sono protetti.</p>	<p>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.</p>	

Requisiti PCI DSS	Procedure di test	Istruzioni
	10.4.2.b Esaminare le configurazioni di sistema e le impostazioni e i log per la sincronizzazione dell'ora e i processi 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 Esaminare le configurazioni di sistema per 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 configurazioni di sistema e le autorizzazioni per verificare che gli audit trail siano protetti e non possano essere modificati, come segue:	Spesso un utente non autorizzato che ha ottenuto accesso alla rete tenta di modificare i log di audit per celare le sue attività. Senza un'adeguata protezione dei log di audit non è possibile garantirne la completezza, la precisione e l'integrità; inoltre, i log di audit possono rivelarsi uno strumento di indagine inutile dopo una compromissione.
10.5.1 Limitare la visualizzazione degli audit trail a coloro che realmente necessitano di tali informazioni per scopi aziendali.	10.5.1 Solo coloro che necessitano di tali informazioni per scopi aziendali possano visualizzare i file di audit trail.	Una protezione adeguata dei log di audit comprende un solido controllo degli accessi (che limita l'accesso ai registri "solo se effettivamente necessario") e l'uso della separazione fisica o di rete (per rendere più difficile l'individuazione e la modifica dei registri). Eseguire immediatamente il backup dei log su un server di registro centralizzato o un supporto difficile da modificare consente di proteggere i log anche se il sistema che li ha generati è stato compromesso.
10.5.2 Proteggere i file di audit trail da modifiche non autorizzate.	10.5.2 I file di audit trail correnti siano protetti da modifiche non autorizzate tramite meccanismi di controllo dell'accesso e 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 Il backup dei file di audit trail viene prontamente eseguito su un server di registro centralizzato o un supporto difficile da modificare.	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>10.5.4 Scrivere registri per tecnologie rivolte al pubblico su un server di registro o un dispositivo per supporti sicuro, centralizzato e interno.</p>	<p>10.5.4 I registri per le tecnologie rivolte al pubblico (ad esempio wireless, firewall, DNS, e-mail) vengono scritti su un server di registro o un supporto sicuro, centralizzato e interno.</p>	<p>Scrivendo i log da tecnologie rivolte al pubblico, quali wireless, firewall, DNS e server di posta, il rischio di modifica dei registri è ridotto, in quanto sono più sicuri all'interno della rete interna.</p> <p>I registri possono venire scritti direttamente o scaricati o copiati da sistemi esterni sul sistema o supporto interno sicuro.</p>
<p>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).</p>	<p>10.5.5 Esaminare le impostazioni di sistema, i file monitorati e i risultati delle attività di monitoraggio per verificare l'uso del software di monitoraggio dell'integrità dei file o di rilevamento delle modifiche per i registri.</p>	<p>I sistemi di monitoraggio dell'integrità dei file o i sistemi di rilevamento delle modifiche controllano e segnalano le modifiche ai file critici. Ai fini del monitoraggio dell'integrità dei file, un'entità di solito controlla i file che in genere non cambiano, ma che se sono modificati indicano una potenziale compromissione.</p>
<p>10.6 Esaminare i registri e gli eventi di sicurezza per tutti i componenti di sistema al fine di identificare anomalie o attività sospette.</p> <p>Nota: strumenti di raccolta, analisi e generazione di avvisi per i registri possono essere utilizzati ai fini della conformità a questo Requisito.</p>	<p>10.6 Eseguire le seguenti operazioni:</p>	<p>Molte violazioni avvengono per giorni o mesi prima di essere rilevate. Regolari revisioni dei registri da parte del personale o con mezzi automatizzati possono individuare e risolvere proattivamente l'accesso non autorizzato all'ambiente dei dati dei titolari di carta.</p> <p>Il processo di revisione dei registri non deve necessariamente essere manuale. L'uso di strumenti di raccolta, analisi e generazione di avvisi può contribuire a facilitare il processo tramite l'identificazione degli eventi di registro che devono essere revisionati.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
10.6.1 Rivedere i seguenti elementi almeno quotidianamente: <ul style="list-style-type: none"> Tutti gli eventi di sicurezza. Registri di tutti i componenti di sistema che memorizzano, elaborano o trasmettono CHD e/o SAD. Registri di tutti i componenti di sistema critici. registri di tutti i server e componenti di sistema che eseguono funzioni di sicurezza (ad esempio, firewall, sistemi di rilevamento intrusioni/sistemi di prevenzione intrusioni IDS/IPS, server di autenticazione, server di ridirezionamento e-commerce). 	10.6.1.a Esaminare le politiche e le procedure di sicurezza per verificare che nelle procedure siano stati definiti i processi per rivedere gli elementi seguenti almeno quotidianamente, manualmente o tramite strumenti di registro: <ul style="list-style-type: none"> Tutti gli eventi di sicurezza. Registri di tutti i componenti di sistema che memorizzano, elaborano o trasmettono CHD e/o SAD. Registri di tutti i componenti di sistema critici. Registri di tutti i server e componenti di sistema che eseguono funzioni di sicurezza (ad esempio, firewall, sistemi di rilevamento intrusioni/sistemi di prevenzione intrusioni IDS/IPS, server di autenticazione, server di ridirezionamento e-commerce). 	<p>Il controllo quotidiano dei registri riduce al minimo la durata e l'esposizione di una potenziale violazione.</p> <p>Per identificare problemi potenziali occorrono la revisione quotidiana degli eventi di sicurezza, ad esempio notifiche o avvisi che identificano attività sospette o anomale, e dei registri dei componenti dei sistemi critici e dei registri dei sistemi che eseguono funzioni di sicurezza, tra cui firewall, IDS/IPS, sistemi di monitoraggio dell'integrità dei file (FIM), ecc. La determinazione degli "eventi di sicurezza" varia per ciascuna organizzazione e può prevedere di tenere conto di tipo di tecnologia, posizione e funzioni del dispositivo. Le aziende possono anche preferire mantenere una base di traffico "normale" per contribuire a identificare il comportamento anomalo.</p>
	10.6.1.b Osservare i processi e consultare il personale per verificare che gli elementi seguenti vengano rivisti almeno quotidianamente: <ul style="list-style-type: none"> Tutti gli eventi di sicurezza. Registri di tutti i componenti di sistema che memorizzano, elaborano o trasmettono CHD e/o SAD. Registri di tutti i componenti di sistema critici. registri di tutti i server e componenti di sistema che eseguono funzioni di sicurezza (ad esempio, firewall, sistemi di rilevamento intrusioni/sistemi di prevenzione intrusioni IDS/IPS, server di autenticazione, server di ridirezionamento e-commerce). 	
10.6.2 Rivedere periodicamente i registri di tutti gli altri componenti di sistema in base alle politiche e alla strategia di gestione del rischio dell'azienda, secondo quanto stabilito dalla valutazione annuale dei rischi dell'azienda.	10.6.2.a Esaminare le politiche e le procedure di sicurezza per verificare che nelle procedure siano stati definiti i processi per rivedere periodicamente i registri e tutti gli altri componenti di sistema, manualmente o tramite strumenti di registro, in base alle politiche e alla strategia di gestione del rischio dell'azienda.	<p>I registri di tutti gli altri componenti di sistema devono essere rivisti periodicamente per identificare le indicazioni di potenziali problemi o tentativi di ottenere l'accesso ai sistemi sensibili tramite sistemi meno sensibili. La frequenza delle revisioni deve essere determinata dalla valutazione annuale dei rischi dell'entità.</p>
	10.6.2.b Esaminare la documentazione dell'azienda relativa alla valutazione dei rischi e consultare il personale per verificare che le revisioni vengano eseguite in conformità alle politiche e alla strategia di gestione del rischio dell'azienda.	

Requisiti PCI DSS	Procedure di test	Istruzioni
10.6.3 Eseguire il follow-up di eccezioni e anomalie individuate durante il processo di revisione.	10.6.3.a Esaminare le politiche e le procedure di sicurezza per verificare che nelle procedure sia stato definito il follow-up di eccezioni o anomalie identificate durante il processo di revisione.	Se le eccezioni o anomalie identificate durante il processo di revisione dei registri non vengono investigate, l'entità potrebbe non essere a conoscenza delle attività non autorizzate e potenzialmente dannose che si verificano nella sua rete.
	10.6.3.b Osservare i processi e consultare il personale per verificare che venga eseguito il follow-up di eccezioni e anomalie.	
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 Esaminare le politiche e le procedure di sicurezza per verificare che siano stati definiti i seguenti elementi: <ul style="list-style-type: none"> politiche per la conservazione dei log di audit; procedure per la conservazione dei log di audit per almeno un anno, con un minimo di tre mesi di disponibilità immediata online. 	La conservazione dei registri per almeno un anno è dovuta al fatto che spesso serve tempo per individuare una compromissione avvenuta o in corso, e consente agli investigatori di disporre di una cronologia sufficiente per determinare il periodo interessato da una potenziale violazione e i sistemi coinvolti. Con la disponibilità immediata dei registri di tre mesi, un'entità può identificare rapidamente e ridurre al minimo l'impatto di una violazione dei dati. La conservazione dei registri fuori sede può impedire la disponibilità immediata, con conseguenti tempi superiori per il ripristino dei dati, l'analisi e l'identificazione dei dati o dei sistemi interessati.
	10.7.b Consultare il personale ed esaminare i log di audit per verificare che questi ultimi siano disponibili per almeno un anno.	
	10.7.c Consultare il personale e osservare i processi per verificare che almeno i registri degli ultimi tre mesi possano essere immediatamente disponibili per l'analisi.	
10.8 <i>Requisito aggiuntivo solo per provider di servizi:</i> implementare un processo per il rilevamento tempestivo e il reporting di errori dei sistemi di controllo di sicurezza critici, inclusi, senza limitazione, errori di: <ul style="list-style-type: none"> Firewall IDS/IPS FIM Antivirus Controlli dell'accesso fisico Controlli dell'accesso logico Meccanismi di log di audit 	10.8.a Esaminare le procedure e le politiche documentate per verificare che i processi siano definiti per il rilevamento tempestivo e il reporting di errori dei sistemi di controllo di sicurezza critici, inclusi, senza limitazione, errori di: <ul style="list-style-type: none"> Firewall IDS/IPS FIM Antivirus Controlli dell'accesso fisico Controlli dell'accesso logico Meccanismi di log di audit Controlli di segmentazione (se utilizzati) 	<p>Nota: questo requisito si applica solo quando l'entità in corso di valutazione è un provider di servizi.</p> <p>Senza processi formali per rilevare e avvisare quando i controlli di sicurezza critici hanno esito negativo, gli errori possono risultare non rilevati per periodi prolungati e fornire agli aggressori molto tempo per compromettere sistemi e rubare dati sensibili dall'ambiente dei dati dei titolari di carta.</p> <p>I tipi specifici di errori possono variare a seconda della funzione del dispositivo e della tecnologia in uso. Errori tipici includono un sistema che smette di eseguire la sua funzione di sicurezza o non</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<ul style="list-style-type: none"> Controlli di segmentazione (se utilizzati) <p>Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.</p>	<p>10.8.b Esaminare i processi di rilevamento e generazione di avvisi e consultare il personale per verificare che i processi siano implementati per tutti i controlli di sicurezza critici e che l'errore di un controllo di sicurezza critico determini la generazione di un avviso.</p>	<p>funziona nella maniera prevista; ad esempio, un firewall che cancella tutte le relative regole o entra in modalità offline.</p>
<p>10.8.1 Requisito aggiuntivo solo per provider di servizi: risolvere gli errori di eventuali controlli di sicurezza critici in maniera tempestiva. I processi di risoluzione degli errori presenti nei controlli di sicurezza devono includere:</p> <ul style="list-style-type: none"> ripristino delle funzioni di sicurezza; identificazione e documentazione della durata (data e ora dell'inizio e della fine) dell'errore della sicurezza; identificazione e documentazione delle cause dell'errore, inclusa la causa principale, e documentazione delle attività di correzione richieste per identificare ed eliminare la causa principale; identificazione e risoluzione di 	<p>10.8.1.a Esaminare le procedure e le politiche documentate e consultare il personale per verificare che i processi siano definiti e implementati per risolvere un errore del controllo di sicurezza e includano:</p> <ul style="list-style-type: none"> ripristino delle funzioni di sicurezza; identificazione e documentazione della durata (data e ora dell'inizio e della fine) dell'errore della sicurezza; identificazione e documentazione delle cause dell'errore, inclusa la causa principale, e documentazione delle attività di correzione richieste per identificare ed eliminare la causa principale; identificazione e risoluzione di eventuali problemi di sicurezza che insorgono durante l'errore; esecuzione di una valutazione dei rischi per determinare se sono richieste ulteriori azioni come conseguenza dell'errore della sicurezza; implementazione di controlli per impedire il ripetersi della causa dell'errore; ripresa del monitoraggio dei controlli di sicurezza. 	<p>Nota: questo requisito si applica solo quando l'entità in corso di valutazione è un provider di servizi.</p> <p>Se non si risponde in modo rapido ed efficiente agli avvisi degli errori dei controlli di sicurezza critici, gli aggressori possono utilizzare questo periodo di tempo per inserire software dannoso, ottenere il controllo di un sistema o rubare i dati dall'ambiente dell'entità.</p> <p>La prova documentata (ad es. i record in un sistema di gestione dei problemi) deve supportare che sono in atto processi e procedure per risolvere gli errori della sicurezza. Inoltre, il personale deve essere a conoscenza delle sue responsabilità nel caso di un errore. Azioni e risoluzioni dell'errore devono essere acquisite nella prova documentata.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>eventuali problemi di sicurezza che insorgono durante l'errore;</p> <ul style="list-style-type: none"> • esecuzione di una valutazione dei rischi per determinare se sono richieste ulteriori azioni come conseguenza dell'errore della sicurezza; • implementazione di controlli per impedire il ripetersi della causa dell'errore; • ripresa del monitoraggio dei controlli di sicurezza. <p>Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.</p>	<p>10.8.1.b Esaminare i record per verificare che gli errori dei controlli di sicurezza siano documentati per includere:</p> <ul style="list-style-type: none"> • identificazione delle cause dell'errore, inclusa la causa principale; • durata (data e ora dell'inizio e della fine) dell'errore della sicurezza; • dettagli delle attività di correzione richieste per identificare ed eliminare la causa principale. 	
<p>10.9 Verificare che i criteri di protezione e le procedure operative per il monitoraggio di tutto l'accesso alle risorse di rete e ai dati dei titolari di carta siano documentati, in uso e noti a tutte le parti coinvolte.</p>	<p>10.9 Esaminare la documentazione e consultare il personale per verificare che i criteri di protezione e le procedure operative per il monitoraggio di tutto l'accesso alle risorse di rete e ai dati dei titolari di carta siano:</p> <ul style="list-style-type: none"> • documentati; • in uso • note a tutte le parti coinvolte 	<p>È necessario che il personale sia sempre a conoscenza delle seguenti politiche di sicurezza e delle procedure operative per il monitoraggio di tutti gli accessi alle risorse di rete e ai dati dei titolari di carta.</p>

Requisito 11 - Eseguire regolarmente test dei 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	Istruzioni
<p>11.1 Implementare i processi per accertare la presenza di punti di accesso wireless (802.11) e rilevare e identificare tutti i punti di accesso wireless autorizzati e non autorizzati almeno a cadenza trimestrale.</p> <p>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.</p> <p>Qualunque sia il metodo adottato, questo deve essere in grado di rilevare e identificare sia i dispositivi autorizzati che quelli non autorizzati.</p>	<p>11.1.a Esaminare le politiche e le procedure per verificare che siano definiti i processi per il rilevamento e l'identificazione di punti di accesso wireless autorizzati e non autorizzati almeno a cadenza trimestrale.</p>	<p>L'implementazione e/o lo sfruttamento della tecnologia wireless all'interno di una rete rappresentano uno dei percorsi più noti agli utenti non autorizzati per ottenere l'accesso alla rete e ai dati dei titolari di carta. Se viene installato un dispositivo o una rete wireless senza che l'azienda ne sia a conoscenza, un aggressore potrebbe accedere alla rete con facilità e in modo "invisibile". Dispositivi wireless non autorizzati possono essere nascosti all'interno di un computer o di un altro componente di sistema o collegati ad esso, oppure essere collegati direttamente ad una porta o a un dispositivo di rete, come uno switch o un router. Ogni dispositivo non autorizzato di questo tipo potrebbe costituire un punto di accesso non autorizzato all'ambiente.</p> <p>Sapere quali sono i dispositivi wireless autorizzati può consentire agli amministratori di identificare rapidamente i dispositivi wireless non autorizzati; rispondere all'identificazione di punti di accesso wireless non autorizzati consente di contenere in modo proattivo l'esposizione dell'ambiente dei dati dei titolari di carta agli utenti non autorizzati.</p> <p>In considerazione della facilità con cui un punto di accesso wireless può essere unito alla rete, della difficoltà a rilevarne la presenza e del maggiore rischio posto dai dispositivi wireless non autorizzati, queste scansioni vanno eseguite anche in presenza di una politica che impedisce l'uso della tecnologia wireless.</p> <p>Le dimensioni e la complessità di un determinato ambiente stabiliranno gli strumenti ed i processi</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 o mobili collegati ai componenti di sistema per creare un punto di accesso wireless (ad esempio, con USB, ecc.); • Dispositivi wireless collegati a una porta o a un dispositivo di rete 	
	<p>11.1.c Se viene utilizzata la scansione wireless, esaminare l'output delle scansioni wireless recenti per verificare che:</p> <ul style="list-style-type: none"> • vengano identificati i punti di accesso wireless autorizzati e non autorizzati; • la scansione venga eseguita almeno a cadenza trimestrale per tutti i componenti e le strutture di sistema. 	
	<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>	

Requisiti PCI DSS	Procedure di test	Istruzioni
		adeguati da utilizzare per fornire un'assicurazione sufficiente che nell'ambiente non sia stato installato un punto di accesso wireless non autorizzato.
11.1.1 Mantenere un inventario dei punti di accesso wireless autorizzati, compresa una giustificazione aziendale documentata.	11.1.1 Esaminare i record documentati per verificare che venga mantenuto un inventario dei punti di accesso wireless autorizzati e che venga documentata una giustificazione aziendale per tutti i punti di accesso wireless autorizzati.	Ad esempio: nel caso di un singolo chiosco di vendita indipendente in un centro commerciale, dove tutti i componenti di comunicazione sono inseriti in contenitori a prova di manomissione e con chiusura di garanzia, l'esecuzione di un'accurata ispezione fisica del chiosco spesso può essere sufficiente per garantire che non sia stato installato o connesso un punto di accesso wireless non autorizzato. Tuttavia, in un ambiente con più nodi (ad esempio, un grande centro commerciale, un call center, una sala server o un data center), eseguire ispezioni fisiche dettagliate è difficile. In questo caso, è possibile combinare più metodi per soddisfare il requisito, ad esempio abbinando l'esecuzione di ispezioni fisiche del sistema ai risultati di un analizzatore wireless.
11.1.2 Implementare le procedure di risposta agli incidenti in caso di rilevamento di punti di accesso wireless non autorizzati.	<p>11.1.2.a Esaminare il piano di risposta agli incidenti aziendale (Requisito 12.10) per accertarsi che definisca e richieda una risposta in caso di rilevamento di punti di accesso wireless non autorizzati.</p> <p>11.1.2.b Consultare il personale responsabile e/o ispezionare scansioni wireless recenti per verificare che vengano presi provvedimenti in caso di rilevamento di punti di accesso wireless non autorizzati.</p>	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>11.2 Eseguire scansioni interne ed esterne della rete almeno una volta ogni tre mesi e dopo ogni cambiamento significativo apportato alla rete (ad esempio, l'installazione di nuovi componenti di sistema, la modifica della topologia della rete, la modifica delle regole del firewall o l'aggiornamento di un prodotto).</p> <p>Nota: è possibile unire più rapporti delle scansioni per il processo di scansione trimestrale per accertarsi che sia stata eseguita la scansione di tutti i sistemi e siano state risolte tutte le vulnerabilità applicabili. Potrebbe essere necessaria una documentazione ulteriore per verificare che le vulnerabilità non corrette siano in fase di correzione.</p> <p>Per la conformità iniziale a PCI DSS, non è necessario che vengano completati quattro scansioni trimestrali positive 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) le vulnerabilità rilevate nei risultati della scansione sono state corrette nel modo dimostrato da una nuova scansione. Per gli anni successivi alla revisione PCI DSS iniziale, è necessario eseguire quattro scansioni trimestrali con esito positivo.</p>	<p>11.2 Esaminare i rapporti delle scansioni e la documentazione di supporto per verificare che le scansioni della vulnerabilità interna ed esterna vengano eseguite come segue:</p>	<p>Una scansione delle vulnerabilità è una combinazione di metodi, tecniche e/o strumenti automatici o manuali eseguiti su server e dispositivi di rete interni ed esterni, studiati per esporre le potenziali vulnerabilità che potrebbero essere individuate e sfruttate da utenti non autorizzati.</p> <p>Sono tre i tipi di scansione delle vulnerabilità obbligatori per PCI DSS:</p> <ul style="list-style-type: none"> • scansione trimestrale delle vulnerabilità interna eseguite da personale qualificato (non occorre avvalersi di un fornitore di prodotti di scansione approvato o ASV PCI SSC); • scansione trimestrale delle vulnerabilità esterna, che deve essere eseguita da un ASV; • scansione interna ed esterna secondo esigenza dopo sostanziali modifiche. <p>Una volta identificati questi punti deboli, l'entità li corregge e ripete la scansione fino a quando le vulnerabilità sono state corrette.</p> <p>L'identificazione e la risoluzione delle vulnerabilità in modo tempestivo, riduce le probabilità che una vulnerabilità venga sfruttata e quindi la potenziale compromissione di un componente di sistema o dei dati dei titolari di carta.</p>
<p>11.2.1 Eseguire scansioni delle vulnerabilità interne trimestrali. Identificare le vulnerabilità ed eseguire</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>Un processo definito per l'identificazione delle vulnerabilità sui sistemi interni richiede l'esecuzione di scansioni di vulnerabilità trimestrali.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>nuove scansioni per verificare che tutte le vulnerabilità “ad alto rischio” siano risolte in base alla classificazione di vulnerabilità dell’entità (secondo il Requisito 6.1). le scansioni devono essere eseguite da personale qualificato.</p>	<p>11.2.1.b Esaminare i rapporti delle scansioni e verificare che vengano identificate tutte le vulnerabilità “ad alto rischio” e il processo di scansione preveda l’esecuzione di ulteriori scansioni per verificare che le vulnerabilità “ad alto rischio” (come definito nel Requisito 6.1 PCI DSS) siano risolte.</p>	<p>Le vulnerabilità che costituiscono i rischi più elevati per l’ambiente (ad esempio, classificate come “Elevate” in base al Requisito 6.1) dovrebbero essere risolte con la massima priorità.</p> <p>Le scansioni per le vulnerabilità interne possono essere eseguite da personale interno qualificato che sia ragionevolmente indipendente dai componenti di sistema sottoposti a scansione (ad esempio, un amministratore del firewall non dovrebbe eseguire la scansione del firewall), oppure un’entità può scegliere di far eseguire queste scansioni delle vulnerabilità interne da un’altra azienda specializzata in scansioni delle vulnerabilità.</p>
	<p>11.2.1.c Consultare il personale per verificare che la scansione sia stata eseguita da una risorsa interna o da terzi esterni qualificati e che chi esegue la scansione sia indipendente dall’organizzazione, ove possibile (non necessariamente un QSA o un ASV).</p>	
<p>11.2.2 Eseguire scansioni esterne della vulnerabilità trimestrali tramite un fornitore di prodotti di scansione approvato (ASV) autorizzato dall’Ente responsabile degli standard di protezione PCI (PCI SSC). Ripetere le scansioni secondo esigenza, fino a che non si ottengono scansioni positive.</p> <p>Nota: le scansioni esterne delle vulnerabilità trimestrali devono essere eseguite da un fornitore di prodotti di scansione approvato (ASV) e autorizzato dall’Ente responsabile degli standard di protezione PCI (PCI SSC).</p> <p>Fare riferimento alla Guida del programma ASV pubblicata sul sito Web PCI SSC per le responsabilità dei clienti relative alle scansioni, la preparazione delle scansioni, ecc.</p>	<p>11.2.2.a Esaminare l’output dei quattro trimestri più recenti di scansioni esterne delle vulnerabilità e verificare che siano state realizzate quattro scansioni trimestrali esterne negli ultimi 12 mesi.</p>	<p>Poiché le reti esterne sono esposte ad un rischio più elevato di compromissione, le scansioni esterne delle vulnerabilità devono essere eseguita da ASV di PCI SSC.</p> <p>Un programma di scansione valido assicura che le scansioni vengano eseguite e le vulnerabilità risolte in maniera tempestiva.</p>
	<p>11.2.2.b Esaminare i risultati di ogni scansione trimestrale per verificare che soddisfino i requisiti della Guida del programma ASV per una scansione con esito positivo (ad esempio, nessuna vulnerabilità classificata a 4.0 o superiore 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 fornitore di prodotti di scansione approvato (ASV) da PCI SSC.</p>	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>11.2.3 Eseguire scansioni interne ed esterne, e ripeterle se necessario, dopo ogni modifica significativa. Le scansioni devono essere eseguite da personale qualificato.</p>	<p>11.2.3.a Ispezionare e mettere in relazione 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>La determinazione di cosa costituisca una modifica significativa dipende strettamente dalla configurazione di un determinato ambiente. Se un aggiornamento o una modifica potessero consentire l'accesso ai dati dei titolari di carta o avere conseguenze sulla sicurezza dell'ambiente dei dati dei titolari di carta, allora devono essere considerati significativi.</p> <p>La scansione di un ambiente, successivamente all'introduzione di una modifica significativa, assicura che le modifiche siano state apportate in modo adeguato così da non compromettere la sicurezza dell'ambiente a seguito della modifica. Tutti i componenti di sistema interessati dalla modifica dovranno essere sottoposti a scansione.</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, vengono risolte tutte le vulnerabilità "ad alto rischio" in base alla definizione contenuta nel Requisito 6.1 PCI DSS. 	
	<p>11.2.3.c Convalidare che la scansione sia stata eseguita da una risorsa interna o da terzi esterni qualificati e che chi esegue la scansione sia indipendente dall'organizzazione, ove possibile (non necessariamente un QSA o un ASV).</p>	
<p>11.3 Implementare una metodologia per il test di penetrazione che preveda quanto segue:</p> <ul style="list-style-type: none"> • È basata sugli approcci ai test di penetrazione accettati dal settore (ad esempio, NIST SP800-115). • Include la copertura dell'intero perimetro dell'ambiente dei dati dei titolari di carta e i dei sistemi critici. • Include i test dall'interno e dall'esterno della rete. • Comprende i test per convalidare eventuali controlli di segmentazione e riduzione della portata. • Definisce i test di penetrazione a livello di applicazione affinché includano almeno le vulnerabilità elencate nel 	<p>11.3 Esaminare la metodologia dei test di penetrazione e consultare il personale responsabile per verificare che venga implementata una metodologia che:</p> <ul style="list-style-type: none"> • È basata sugli approcci ai test di penetrazione accettati dal settore (ad esempio, NIST SP800-115). • Include la copertura dell'intero perimetro dell'ambiente dei dati dei titolari di carta e i dei sistemi critici. • esegua i test dall'interno e dall'esterno della rete; • Comprende i test per convalidare eventuali controlli di segmentazione e riduzione della portata. • Definisce i test di penetrazione a livello di applicazione affinché includano almeno le vulnerabilità elencate nel Requisito 6.5. • Definisce i test di penetrazione a livello di rete affinché includano componenti che supportano le funzioni di rete nonché i sistemi operativi. • Include la revisione e la valutazione delle minacce e delle 	<p>Il test di penetrazione ha come scopo la simulazione di una situazione di attacco nel mondo reale con l'obiettivo di stabilire fino a che punto un aggressore sarebbe in grado di penetrare nell'ambiente. In questo modo un'entità, disponendo di un'idea più chiara dell'esposizione potenziale, può elaborare una strategia per difendersi dagli attacchi.</p> <p>Un test di penetrazione è diverso da una scansione della vulnerabilità, essendo esso un processo attivo che può comprendere lo sfruttamento delle vulnerabilità identificate. L'esecuzione di una scansione delle vulnerabilità rappresenta uno dei primi passaggi che una persona che esegue test di penetrazione effettua per pianificare la strategia di attacco, pur non essendo l'unico passaggio. Anche se una scansione delle vulnerabilità non rileva alcuna</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>Requisito 6.5.</p> <ul style="list-style-type: none"> Definisce i test di penetrazione a livello di rete affinché includano componenti che supportano le funzioni di rete nonché i sistemi operativi. Include la revisione e la valutazione delle minacce e delle vulnerabilità verificatesi negli ultimi 12 mesi. specifichi la conservazione dei risultati dei test di penetrazione e dei risultati delle attività di correzione. 	<p>vulnerabilità verificatesi negli ultimi 12 mesi.</p> <ul style="list-style-type: none"> specifichi la conservazione dei risultati dei test di penetrazione e dei risultati delle attività di correzione. 	<p>vulnerabilità conosciuta, la persona che esegue il test di penetrazione spesso acquisirà una conoscenza sufficiente del sistema per identificare eventuali lacune della sicurezza.</p> <p>I test di penetrazione sono generalmente un processo estremamente manuale. Sebbene possano essere utilizzati alcuni strumenti automatici, la persona che esegue il test deve utilizzare la propria conoscenza dei sistemi per penetrare in un ambiente. Spesso la persona che esegue i test incatena insieme vari tipi di exploit con l'obiettivo di bucare gli strati di difesa. Ad esempio, se la persona che esegue i test individua un modo per accedere al server di un'applicazione, userà il server compromesso come punto per organizzare un nuovo attacco sulla base delle risorse a cui il server ha accesso. In questo modo l'esecutore del test è in grado di simulare i metodi cui ricorre un aggressore per identificare le aree che presentano potenziali punti deboli nell'ambiente.</p> <p><i>Le tecniche dei test di penetrazione variano da un'organizzazione all'altra e il tipo, la profondità e la complessità dei test dipenderanno dall'ambiente specifico e della valutazione dei rischi dell'organizzazione.</i></p>
<p>11.3.1 Eseguire test di penetrazione <i>esterna</i> 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).</p>	<p>11.3.1.a Esaminare la portata del lavoro e i risultati dell'ultimo test di penetrazione esterna per verificare che il test di penetrazione sia stato eseguito come segue:</p> <ul style="list-style-type: none"> in base alla metodologia definita; Almeno una volta all'anno dopo ogni modifica significativa all'ambiente. <p>11.3.1.b Verificare che il test sia stato eseguito da una risorsa interna o da terzi esterni qualificati e che chi esegue il test sia indipendente dall'organizzazione, ove possibile (non necessariamente un QSA o un ASV).</p>	<p>I test di penetrazione condotti con regolarità e dopo modifiche significative all'ambiente sono una misura di sicurezza proattiva che consente di contenere l'accesso potenziale all'ambiente dei dati dei titolari di carta da parte di utenti non autorizzati.</p> <p>La determinazione di cosa costituisca un aggiornamento o una modifica significativi dipende strettamente dalla configurazione di un determinato ambiente. Se un aggiornamento o una modifica potessero consentire l'accesso ai dati dei</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
11.3.2 Eseguire test di penetrazione <i>interna</i> 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).	11.3.1.a Esaminare la portata del lavoro e i risultati del test di penetrazione interna più recente per verificare che il test di penetrazione sia stato eseguito come segue: <ul style="list-style-type: none"> • in base alla metodologia definita; • Almeno una volta all'anno • dopo ogni modifica significativa all'ambiente. 	titolari di carta o avere conseguenze sulla sicurezza dell'ambiente dei dati dei titolari di carta, allora devono essere considerati significativi. Eseguire test di penetrazione dopo l'aggiornamento e la modifica alla rete garantisce che i controlli presumibilmente in atto funzionino in modo efficace dopo l'aggiornamento o la modifica.
	11.3.2.b Verificare che il test sia stato eseguito da una risorsa interna o da terzi esterni qualificati e che chi esegue il test sia indipendente dall'organizzazione, ove possibile (non necessariamente un QSA o un ASV).	
11.3.3 Le vulnerabilità sfruttabili individuate durante il test di penetrazione vengono corrette e il test viene ripetuto per verificare le correzioni.	11.3.3 Esaminare i risultati dei test di penetrazione per verificare che le vulnerabilità sfruttabili note siano state corrette e che la ripetizione dei test abbia confermato che la vulnerabilità è stata corretta.	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>11.3.4 Se si utilizza la segmentazione per isolare il CDE dalle altre reti, eseguire i test di penetrazione almeno una volta all'anno e dopo eventuali modifiche ai controlli/metodi di segmentazione per verificare che i metodi di segmentazione siano funzionali ed efficaci e isolare tutti i sistemi che non rientrano nell'ambito dai sistemi che rientrano nel CDE.</p>	<p>11.3.4.a Esaminare i controlli di segmentazione e rivedere la metodologia dei test di penetrazione per verificare che le relative procedure siano definite per testare tutti i metodi di segmentazione e confermare che sono funzionali ed efficaci e isolare tutti i sistemi che non rientrano nell'ambito dai sistemi che rientrano nel CDE.</p>	<p>I test di penetrazione sono uno strumento importante per confermare l'efficacia delle eventuali segmentazioni applicate per isolare l'ambiente dei dati dei titolari di carta dalle altre reti. Il test di penetrazione dovrebbe focalizzarsi sui controlli di segmentazione, sia dall'esterno della rete dell'entità sia dall'interno della rete ma all'esterno dell'ambiente dei dati dei titolari di carta, per confermare che i controlli non siano in grado di superare i controlli di segmentazione per accedere all'ambiente dei dati dei titolari di carta. Ad esempio, i test e/o la scansione della rete alla ricerca di porte aperte, per verificare che non vi sia connettività tra le reti che rientrano e le reti che rientrano nell'ambito.</p>
	<p>11.3.4.b Esaminare i risultati del test di penetrazione più recente per verificare che:</p> <ul style="list-style-type: none"> • il test di penetrazione per verificare i controlli di segmentazione venga eseguito almeno una volta all'anno e dopo eventuali modifiche ai controlli/metodi di segmentazione; • il test di penetrazione copra tutti i controlli/metodi di segmentazione in uso; • il test di penetrazione verifichi che i controlli/metodi di segmentazione siano funzionali ed efficaci e isolino tutti i sistemi che non rientrano nell'ambito dai sistemi che rientrano nel CDE. 	
	<p>11.3.2.c Verificare che il test sia stato eseguito da una risorsa interna o da una terza parte esterna qualificata e, se applicabile, l'esecutore del test sia indipendente dall'organizzazione (non necessariamente un QSA o un ASV).</p>	
<p>11.3.4.1 Requisito aggiuntivo solo per provider di servizi: se si utilizza la segmentazione, confermare l'ambito PCI DSS eseguendo test di penetrazione nei controlli di segmentazione almeno ogni sei mesi e dopo eventuali modifiche ai controlli/metodi di segmentazione.</p> <p>Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.</p>	<p>11.3.4.1.a Esaminare i risultati del test di penetrazione più recente per verificare che:</p> <ul style="list-style-type: none"> • il test di penetrazione venga eseguito per verificare i controlli di segmentazione almeno ogni sei mesi e dopo eventuali modifiche ai controlli/metodi di segmentazione; • il test di penetrazione copra tutti i controlli/metodi di segmentazione in uso; • il test di penetrazione verifichi che i controlli/metodi di segmentazione siano funzionali ed efficaci e isolino tutti i sistemi che non rientrano nell'ambito dai sistemi che rientrano nel CDE. 	<p>Nota: questo requisito si applica solo quando l'entità in corso di valutazione è un provider di servizi.</p> <p>Per i provider di servizi, la convalida dell'ambito PCI DSS deve essere eseguita il più frequentemente possibile per accertarsi che l'ambito PCI DSS sia aggiornato e allineato agli obiettivi aziendali mutevoli.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
	11.3.4.1.b Verificare che il test sia stato eseguito da una risorsa interna o da una terza parte esterna qualificata e, se applicabile, l'esecutore del test sia indipendente dall'organizzazione (non necessariamente un QSA o un ASV).	
11.4 Utilizzare tecniche di rilevamento intrusioni e/o prevenzione delle intrusioni per rilevare e/o prevenire le intrusioni nella rete. Monitorare tutto il traffico in corrispondenza del perimetro dell'ambiente dei dati dei titolari di carta nonché dei punti critici all'interno dell'ambiente stesso e segnalare possibili compromissioni al personale addetto. Mantenere aggiornati tutti i motori, basi e firme di rilevamento e prevenzione delle intrusioni.	11.4.a Esaminare le configurazioni di sistema e i diagrammi di rete per verificare che le tecniche (come i sistemi di rilevamento delle intrusioni e/o i sistemi di prevenzione delle intrusioni) siano in atto per monitorare tutto il traffico: <ul style="list-style-type: none"> in corrispondenza del perimetro dell'ambiente dei dati dei titolari di carta; in corrispondenza dei punti critici nell'ambiente dei dati dei titolari di carta. 11.4.b Esaminare le configurazioni di sistema e consultare il personale responsabile per confermare che le tecniche di rilevamento intrusioni e/o prevenzione delle intrusioni segnalino possibili compromissioni al personale addetto.	Le tecniche di rilevamento intrusioni e/o prevenzione delle intrusioni (come IDS/IPS) operano un confronto del traffico in entrata nella rete con "firme" e/o comportamenti conosciuti di migliaia di tipi di compromissione (strumenti per hacker, cavalli di Troia e altro malware) e inviano avvisi e/o fermano il tentativo in corso. Senza un approccio proattivo al rilevamento di attività non autorizzate, gli attacchi alle risorse del computer (o l'abuso di tali risorse) potrebbero non essere rilevati in tempo reale. Gli avvisi di protezione generati da queste tecniche dovrebbero essere monitorati, al fine di fermare i tentativi di intrusione.
	11.4.c Esaminare le configurazioni IDS/IPS e la documentazione del fornitore per verificare che le tecniche di rilevamento intrusioni e/o prevenzione delle intrusioni vengano configurate, conservate e aggiornate secondo le istruzioni del fornitore per garantire una protezione ottimale.	
11.5 Distribuire un meccanismo di rilevamento delle modifiche (ad esempio, gli strumenti di monitoraggio dell'integrità dei file) per segnalare al personale modifiche non autorizzate (incluse modifiche, aggiunte ed eliminazioni) di file system, file di configurazione o file di contenuto critici e per configurare il software in modo che esegua confronti di file critici almeno una volta alla settimana.	11.5.a Verificare l'uso del meccanismo di rilevamento delle modifiche osservando le impostazioni del sistema e i file monitorati ed esaminando i risultati delle attività di monitoraggio. Esempi di file che devono essere monitorati: <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 File critici ulteriori determinati dall'entità (ad esempio, tramite la valutazione dei rischi o altri mezzi) 	Le soluzioni di rilevamento delle modifiche come gli strumenti di monitoraggio dell'integrità dei file (FIM) controllano e segnalano le modifiche, le aggiunte e le eliminazioni ai file critici. Se non vengono implementati correttamente e l'output della soluzione di rilevamento delle modifiche non è monitorato, un utente non autorizzato potrebbe aggiungere, rimuovere o modificare il contenuto dei file di configurazione, i programmi del sistema operativo o i file eseguibili delle applicazioni. Le modifiche non autorizzate, se non vengono rilevate, possono rendere inefficaci i controlli di protezione esistenti e/o dare luogo al furto dei dati

Nota: ai fini del meccanismo di rilevamento

Requisiti PCI DSS	Procedure di test	Istruzioni
<i>modifiche, i file critici sono solitamente file che non cambiano frequentemente, ma la cui modifica può indicare la compromissione, effettiva o potenziale, del sistema. I meccanismi di rilevamento modifiche come i prodotti per il monitoraggio dell'integrità dei file sono generalmente 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>	11.5.b Verificare che il meccanismo sia configurato per segnalare al personale modifiche non autorizzate (incluse modifiche, aggiunte ed eliminazioni) a file critici e per eseguire confronti di file critici almeno una volta alla settimana.	dei titolari di carta senza impatto percettibile sulla normale elaborazione.
11.5.1 Implementare una procedura per rispondere a eventuali avvisi generati dalla soluzione di rilevamento modifiche.	11.5.1 Consultare il personale per verificare che tutti gli avvisi vengano investigati e risolti.	
11.6 Garantire che le politiche di sicurezza e le procedure operative per il monitoraggio e i test della sicurezza siano documentate, in uso e note a tutte le parti coinvolte.	11.6 Esaminare la documentazione e consultare il personale per verificare che i criteri di protezione e le procedure operative per il monitoraggio e il test siano: <ul style="list-style-type: none"> • documentate • in uso • note a tutte le parti coinvolte 	È necessario che il personale sia a conoscenza delle seguenti politiche di sicurezza e procedure operative per il monitoraggio e il test della sicurezza continui.

Gestione di 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	Istruzioni
12.1 Stabilire, pubblicare, conservare e rendere disponibile una politica di sicurezza.	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).	Una politica di sicurezza delle informazioni dell'azienda crea la roadmap per l'implementazione delle misure di protezione per proteggere le sue risorse più preziose. Tutto il personale deve essere a conoscenza della sensibilità dei dati e delle proprie responsabilità in termini di protezione.
12.1.1 Rivedere la politica di sicurezza almeno una volta all'anno e aggiornarla quando l'ambiente cambia.	12.1.1 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.	Le minacce alla sicurezza e i metodi di protezione si evolvono rapidamente. Senza l'aggiornamento della politica di sicurezza per riflettere le modifiche di rilievo, le nuove misure di protezione per combattere queste minacce non vengono applicate.
12.2 Implementare un processo di valutazione dei rischi che: <ul style="list-style-type: none"> venga eseguito almeno una volta all'anno e in occasione di modifiche significative all'ambiente (ad esempio, acquisizione, 	12.2.a Verificare che sia documentato un processo di valutazione dei rischi annuale che: <ul style="list-style-type: none"> identifichi risorse critiche, minacce e vulnerabilità; consenta di ottenere una formale analisi dei rischi documentata. 	Una valutazione dei rischi consente all'organizzazione di individuare le minacce e le vulnerabilità connesse che hanno il potenziale di influire negativamente sulla sua attività. Esempi di differenti considerazioni dei

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>fusione, trasferimento, ecc.);</p> <ul style="list-style-type: none"> identifichi risorse critiche, minacce e vulnerabilità; consenta di ottenere una formale analisi dei rischi documentata. <p><i>Esempi di metodologie per la valutazione dei rischi includono, senza limitazioni, OCTAVE, ISO 27005 e NIST SP 800-30.</i></p>	<p>12.2.b Esaminare la documentazione per la valutazione dei rischi per verificare che il processo di valutazione dei rischi venga eseguito con cadenza almeno annuale e in occasione di significative modifiche all'ambiente.</p>	<p>rischi includono crimini informatici, attacchi Web e malware POS. Si può quindi procedere ad assegnare in modo efficace le risorse per implementare controlli volti a ridurre la probabilità e/o il potenziale impatto della minaccia che si verifica.</p> <p>L'esecuzione di valutazioni dei rischi con cadenza almeno annuale consente all'organizzazione di tenersi aggiornata sulle modifiche organizzative e sulle minacce, tendenze e tecnologie in evoluzione.</p>
<p>12.3 Sviluppare politiche che regolano l'uso per tecnologie critiche e definire l'uso corretto di queste tecnologie.</p> <p>Nota: esempi di tecnologie critiche comprendono, senza limitazioni, accesso remoto e tecnologie wireless, laptop, tablet, supporti elettronici rimovibili, uso della posta elettronica e di Internet.</p> <p>Accertarsi che tali politiche richiedano quanto segue:</p>	<p>12.3 Esaminare le politiche che regolano l'uso per le tecnologie critiche e consultare il personale responsabile per verificare che le seguenti politiche vengano implementate e seguite:</p>	<p>Le politiche che regolano l'uso del personale possono sia vietare l'uso di determinati dispositivi e altre tecnologie in base alla politica dell'azienda, sia fornire una guida all'uso e all'implementazione corretti per il personale. Se non sono disponibili politiche che regolano l'uso, il personale può utilizzare le tecnologie in violazione delle politiche dell'azienda, consentendo pertanto agli utenti non autorizzati di accedere ai sistemi critici e ai dati dei titolari di carta.</p>
<p>12.3.1 Approvazione esplicita delle parti autorizzate</p>	<p>12.3.1 Verificare che le politiche che regolano l'uso richiedano l'approvazione esplicita delle parti autorizzare per usare le tecnologie.</p>	<p>Senza la richiesta dell'approvazione esplicita per l'implementazione di queste tecnologie, un singolo membro del personale può implementare una soluzione per un'esigenza aziendale percepita aprendo inconsapevolmente un enorme falla che mette sistemi critici e dati a disposizione degli utenti non autorizzati.</p>
<p>12.3.2 Autenticazione per l'uso della tecnologia</p>	<p>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).</p>	<p>Se la tecnologia viene implementata senza la corretta autenticazione (ID utente e password, token, VPN, ecc.), gli individui non autorizzati possono facilmente utilizzare questa tecnologia non protetta per accedere a sistemi critici e dati dei titolari di carta.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
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 di utilizzo definiscano: <ul style="list-style-type: none"> un elenco di tutti i dispositivi critici; un elenco del personale autorizzato a utilizzare i dispositivi. 	Gli individui non autorizzati possono violare la sicurezza fisica e inserire i loro dispositivi nella rete come "back door". Il personale può inoltre bypassare procedure e dispositivi di installazione. Un inventario accurato con una corretta etichettatura dei dispositivi consente una rapida identificazione delle installazioni non approvate.
12.3.4 Un metodo per determinare accuratamente e rapidamente proprietario, informazioni di contatto e scopo (ad esempio, etichettatura, codifica e/o inventariazione dei dispositivi)	12.3.4 Verificare che le politiche che regolano l'uso definiscano un metodo per determinare accuratamente e rapidamente proprietario, informazioni di contatto e scopo (ad esempio, etichettatura, codifica e/o inventariazione dei dispositivi).	Gli individui non autorizzati possono violare la sicurezza fisica e inserire i loro dispositivi nella rete come "back door". Il personale può inoltre bypassare procedure e dispositivi di installazione. Un inventario accurato con una corretta etichettatura dei dispositivi consente una rapida identificazione delle installazioni non approvate. Prendere in considerazione l'applicazione di una convenzione di denominazione ufficiale per i dispositivi, quindi registrare tutti i dispositivi insieme a controlli dell'inventario ben definiti. Un'etichettatura logica si può utilizzare con informazioni come codici che collegano il dispositivo al suo proprietario, informazioni di contatto e scopo.
12.3.5 Usi accettabili della tecnologia	12.3.5 Verificare che le politiche che regolano l'uso definiscano usi accettabili della tecnologia.	Definendo l'uso aziendale accettabile e la posizione di dispositivi e tecnologie approvati dall'azienda, la società è in grado di gestire e controllare al meglio le lacune nelle configurazione e nei controlli operativi, per garantire che non venga aperta una "back door" tramite la quale un utente non autorizzato può accedere ai sistemi critici e ai dati dei titolari di carta.
12.3.6 Posizioni di rete accettabili per le tecnologie	12.3.6 Verificare che le politiche che regolano l'uso definiscano 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 includano 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.a 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.	Nelle tecnologie di accesso remoto vengono spesso inserite "back door" per le risorse critiche e i dati dei titolari di carta. Scollegando le tecnologie di accesso remoto quando non

Requisiti PCI DSS	Procedure di test	Istruzioni
	12.3.8.b Esaminare le configurazioni delle tecnologie di accesso remoto per verificare che le sessioni di accesso remoto vengano automaticamente scollegate dopo un determinato periodo di inattività.	sono in uso (per esempio quelle utilizzate per supportare i sistemi dal fornitore del POS, da altri rivenditori o da partner aziendali), l'accesso e i rischi per la rete vengono ridotti al minimo.
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	Istruzioni
<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>Laddove è presente un'esigenza aziendale autorizzata, le politiche che regolano l'uso devono richiedere la protezione dei dati in conformità a tutti i requisiti PCI DSS applicabili.</p>	<p>12.3.10.a Verificare che le politiche che regolano l'uso proibiscano la copia, lo spostamento o la memorizzazione dei dati dei titolari di carta su dischi rigidi locali e supporti elettronici rimovibili quando si accede ai dati tramite tecnologie di accesso remoto.</p>	<p>Per garantire che tutto il personale sia consapevole delle proprie responsabilità di non memorizzare o copiare i dati dei titolari di carta sul loro personal computer locale o su altri supporti, l'azienda dovrebbe disporre vietare chiaramente tali attività salvo nel caso di personale autorizzato esplicitamente. La memorizzazione o la copia dei dati dei titolari di carta su un disco rigido locale o altro supporto devono essere eseguite in conformità a tutti i requisiti PCI DSS applicabili.</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 Accertarsi che nelle procedure e nella politica di 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 sicurezza delle informazioni definiscano chiaramente le responsabilità in termini di protezione delle informazioni per tutto il personale.</p>	<p>Senza l'assegnazione di ruoli e responsabilità di protezione chiaramente definiti, potrebbero verificarsi interazioni incoerenti con il gruppo di protezione, che portano a un'implementazione non sicura delle tecnologie o l'uso di tecnologie non aggiornate e poco sicure.</p>
	<p>12.4.b Consultare un campione del personale responsabile per verificare che comprenda le politiche di sicurezza.</p>	
<p>12.4.1 <i>Requisito aggiuntivo solo per provider di servizi:</i> ai dirigenti verrà assegnata la responsabilità della protezione</p>	<p>12.4.1.a Esaminare la documentazione per verificare che ai dirigenti sia stata assegnata la responsabilità generale del rispetto della conformità PCI DSS dell'entità.</p>	<p>Nota: questo requisito si applica solo quando l'entità in corso di valutazione è un provider di</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>dei dati dei titolari di carta e di un programma di conformità PCI DSS per includere:</p> <ul style="list-style-type: none"> responsabilità generale del rispetto della conformità PCI DSS; definizione di un documento di dichiarazione di intenti per un programma di conformità PCI DSS e comunicazione tra di loro. <p>Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.</p>	<p>12.4.1.b Esaminare il documento di dichiarazione di intenti PCI DSS dell'azienda per verificare che descriva le condizioni in cui il programma di conformità PCI DSS è organizzato e comunicato ai dirigenti.</p>	<p>servizi.</p> <p>L'assegnazione ai dirigenti delle responsabilità della conformità PCI DSS garantisce visibilità a livello dirigenziale del programma di conformità PCI DSS e offre l'opportunità di porre domande appropriate per determinare l'efficacia del programma e influenzare le priorità strategiche. La responsabilità generale del programma di conformità PCI DSS può essere assegnata a singoli ruoli e/o business unit all'interno dell'organizzazione.</p> <p>I dirigenti possono includere posizioni di amministratore delegato, consigli di amministrazione o equivalente. I titoli specifici dipenderanno dalla determinata struttura organizzativa. Il livello di dettaglio fornito ai dirigenti deve essere appropriato per una determinazione organizzazione e i destinatari previsti.</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 Esaminare le politiche e le procedure di sicurezza delle informazioni per verificare:</p> <ul style="list-style-type: none"> l'assegnazione formale della responsabilità di sicurezza delle informazioni a un CSO (Chief Security Officer) o a un altro membro del management esperto in sicurezza; che le seguenti responsabilità di sicurezza delle informazioni vengano assegnate in modo specifico e formale. 	<p>Ogni persona o team con responsabilità di gestione della sicurezza delle informazioni deve essere chiaramente consapevole delle sue responsabilità e delle attività correlate tramite politiche specifiche. Senza questa responsabilità, le lacune nei processi possono aprire l'accesso a risorse critiche o dati dei titolari di carta.</p> <p>Le entità devono anche considerare piani di transizione e/o successione per il personale chiave per evitare potenziali lacune nelle assegnazioni in termini di sicurezza, che potrebbero determinare la mancata assegnazione e pertanto la mancata esecuzione delle responsabilità.</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 di definizione, documentazione e distribuzione delle politiche e delle procedure di sicurezza.</p>	
<p>12.5.2 Monitoraggio e analisi degli avvisi e delle informazioni sulla sicurezza e distribuzione 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 sicurezza delle informazioni appropriato e al management della business unit.</p>	

Requisiti PCI DSS	Procedure di test	Istruzioni
12.5.3 Definizione, documentazione e distribuzione di procedure di risposta ed escalation in caso di problemi di sicurezza per garantire una gestione tempestiva ed efficiente di tutte le situazioni.	12.5.3 Verificare che venga formalmente assegnata la responsabilità di definizione, documentazione e distribuzione delle politiche di risposta in caso di problemi e delle procedure di escalation.	
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 (aggiunta, eliminazione e modifica) 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 delle procedure e dei criteri di protezione dei dati dei titolari di carta.	12.6.a Esaminare il programma di consapevolezza della sicurezza per verificare che fornisca a tutto il personale la consapevolezza delle procedure e dei criteri di protezione dei dati dei titolari di carta.	Se il personale non viene istruito sulle proprie responsabilità di sicurezza, le misure di protezione e i processi implementati potrebbero divenire inefficaci a causa di errori o azioni intenzionali.
	12.6.b 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).	Se il programma di conoscenza della sicurezza non prevede sessioni di aggiornamento periodiche, i processi e le procedure di sicurezza potrebbero essere dimenticati o ignorati, provocando l'esposizione delle risorse critiche e dei dati dei titolari di carta.
	12.6.1.b Verificare che il personale partecipi alla formazione sulla consapevolezza al momento dell'assunzione e almeno una volta all'anno.	
	12.6.1.c Consultare un campione del personale per verificare che abbia completato la formazione sulla consapevolezza e siano consapevoli dell'importanza della sicurezza dei dati dei titolari di carta.	

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>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.</p>	<p>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.</p>	<p>La richiesta di un'attestazione da parte del personale in forma scritta o elettronica aiuta a garantire che abbiano letto e compreso le politiche e le procedure di sicurezza e che si siano impegnati e continuino ad impegnarsi a rispettarle.</p>
<p>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.</p> <p><i>Nota: per quel personale potenziale da assumere per determinate posizioni come cassieri di negozi, che hanno accesso a un solo numero di carta alla volta durante una transazione, questo requisito è solo consigliato.</i></p>	<p>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 dei titolari di carta o al relativo ambiente.</p>	<p>L'esecuzione di approfondite indagini di base prima dell'assunzione del personale potenziale che dovrà accedere ai dati dei titolari di carte riduce il rischio di uso non autorizzato dei PAN e di altri dati dei titolari di carta da parte di individui con precedenti penali o discutibili.</p>
<p>12.8 Implementare e gestire le politiche e le procedure per gestire i provider di servizi con cui vengono condivisi i dati dei titolari di carta o che potrebbero incidere sulla sicurezza dei dati dei titolari di carta, come segue.</p>	<p>12.8 Attraverso l'osservazione e l'analisi di politiche, procedure e documentazione di supporto, verificare che i processi siano implementati per gestire i provider di servizi con cui vengono condivisi i dati dei titolari di carta o che potrebbero incidere sulla sicurezza dei dati dei titolari di carta, come segue:</p>	<p>Se un esercente o un provider di servizi condivide i dati dei titolari di carta con un provider di servizi, tali provider dovranno applicare requisiti specifici per garantire la protezione continua di questi dati.</p> <p>Alcuni esempi dei differenti tipi di provider di servizi includono strutture di conservazione dei nastri di backup, provider di servizi gestiti come le società di hosting Web o provider di servizi di sicurezza, entità che ricevono dati a scopo di "fraud modeling", cioè per analizzare modelli di possibili truffe, ecc.</p>
<p>12.8.1 Conservare un elenco di provider di servizi inclusa una descrizione del servizio fornito.</p>	<p>12.8.1 Verificare che sia conservato un elenco di provider di servizi e che includa una descrizione del servizio fornito.</p>	<p>Tenere traccia di tutti i provider di servizi permette di identificare dove si estendono i rischi potenziali all'esterno dell'organizzazione.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>12.8.2 Conservare un accordo scritto in base al quale il provider di servizi si assume la responsabilità della protezione dei dati dei titolari di carta di cui entra in possesso oppure memorizzare, elaborare o trasmettere in altro modo per conto del cliente o nella misura in cui questi potrebbe avere un impatto sulla sicurezza dell'ambiente dei dati dei titolari di carta del cliente.</p> <p><i>Nota: la formulazione corretta di un riconoscimento dipende dall'accordo tra le due parti, dai dettagli del servizio fornito e dalle responsabilità assegnate a ciascuna delle parti. Il riconoscimento non deve includere la formulazione corretta fornita nel presente requisito.</i></p>	<p>12.8.2 Attenersi ai contratti scritti e confermare che includono un riconoscimento da parte dei provider di servizi che si assumono la responsabilità della protezione dei dati dei titolari di carta di cui entra in possesso oppure memorizzare, elaborare o trasmettere in altro modo per conto del cliente o nella misura in cui questi potrebbe avere un impatto sulla sicurezza dell'ambiente dei dati dei titolari di carta del cliente.</p>	<p>Il riconoscimento dei provider di servizi ne evidenzia l'impegno a mantenere la sicurezza dei dati dei titolari di carta che ottengono dai clienti. La misura in cui il provider di servizi è responsabile della sicurezza dei dati dei titolari di carta dipenderà dallo specifico servizio e dal contratto tra il provider e l'entità valutata.</p> <p>In abbinamento al Requisito 12.9, questo requisito ha lo scopo di promuovere un livello uniforme di comprensione tra le parti riguardo le proprie responsabilità PCI DSS pertinenti. Ad esempio, il contratto può includere i requisiti PCI DSS applicabili da conservare nell'ambito del servizio fornito.</p>
<p>12.8.3 Accertarsi che esista un processo definito per incaricare i provider di servizi, che includa tutte le attività di due diligence appropriate prima dell'incarico.</p>	<p>12.8.3 Verificare che le politiche e le procedure siano documentate e implementate, inclusa la corretta due diligence prima di assegnare l'incarico al provider di servizi.</p>	<p>Il processo garantisce che qualsiasi coinvolgimento di un provider di servizi sia attentamente esaminato da un'organizzazione a livello interno, comprendendo un'analisi dei rischi prima di stabilire una relazione formale con il provider.</p> <p>I processi e gli obiettivi di due diligence specifici variano per ciascuna organizzazione. Esempi di considerazioni possono includere le prassi di segnalazione del provider, procedure di notifica delle violazioni e di risposta in caso di problemi, dettagli sulle modalità di assegnazione delle responsabilità PCI DSS tra l'una e l'altra parte, modalità in cui il provider convalida la propria conformità PCI DSS e quali prove fornirà, ecc.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<p>12.8.4 Conservare un programma per monitorare lo stato di conformità allo 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 allo standard PCI DSS dei provider di servizi con cadenza almeno annuale.</p>	<p>La conoscenza dello stato di conformità PCI DSS di un provider di servizi garantisce certezza e consapevolezza sul loro rispetto degli stessi requisiti a cui è soggetta l'organizzazione. Se il provider di servizi offre vari servizi, questo requisito è valido solo per quei servizi erogati al cliente, e solo per quei servizi che rientrano nell'ambito per la valutazione PCI DSS per il cliente.</p> <p>Le informazioni specifiche che un'entità conserva dipenderanno dallo specifico contratto con i suoi provider, dal tipo di servizio, ecc. Lo scopo per l'entità valutata è comprendere quali requisiti PCI DSS i suoi provider hanno accettato di soddisfare.</p>
<p>12.8.5 Mantenere le informazioni su quali requisiti PCI DSS vengono gestiti da ogni provider di servizi e quali vengono gestiti dall'entità.</p>	<p>12.8.5 Verificare che l'entità mantenga le informazioni su quali requisiti PCI DSS vengono gestiti da ogni provider di servizi e quali vengono gestiti dall'entità.</p>	
<p>12.9 Requisito aggiuntivo solo per provider di servizi: i provider di servizi riconoscono per iscritto nei confronti dei clienti di essere responsabili della protezione dei dati dei titolari di carta di cui entrano in possesso oppure di memorizzare, elaborare o trasmettere in altro modo per conto del cliente o nella misura in cui questi potrebbe avere un impatto sulla sicurezza dell'ambiente dei dati dei titolari di carta del cliente.</p> <p>Nota: la formulazione corretta di un riconoscimento dipende dall'accordo tra le due parti, dai dettagli del servizio fornito e dalle responsabilità assegnate a ciascuna delle parti. Il riconoscimento non deve includere la formulazione corretta fornita nel presente requisito.</p>	<p>12.9 Ulteriore procedura di test solo per le valutazioni dei provider di servizi: rivedere le politiche e le procedure del provider di servizi e attenersi ai modelli utilizzati per i contratti scritti per confermare che il provider di servizi riconosce per iscritto ai clienti che soddisferà tutti i requisiti PCI DSS pertinenti nella misura in cui questi possiede o altrimenti memorizza, elabora o trasmette i dati dei titolari di carta per conto del cliente o nella misura in cui essi potrebbero avere un impatto sulla sicurezza dell'ambiente dei dati dei titolari di carta del cliente.</p>	<p>Nota: questo requisito si applica solo quando l'entità in corso di valutazione è un provider di servizi.</p> <p>In abbinamento al Requisito 12.8.2, questo requisito è da intendersi volto a promuovere un livello uniforme di comprensione tra i provider di servizi e i loro clienti in merito alle rispettive responsabilità PCI DSS pertinenti. Il riconoscimento dei provider di servizi ne evidenzia l'impegno a mantenere la sicurezza dei dati dei titolari di carta che ottengono dai clienti.</p> <p>Le procedure e le politiche interne del provider di servizi correlate al suo processo di coinvolgimento del cliente ed eventuali modelli utilizzati per i contratti scritti devono includere la garanzia di un riconoscimento PCI DSS valido ai loro clienti. Il metodo in base al quale il provider di servizi assicura un riconoscimento scritto deve essere concordato tra il provider e i suoi clienti.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
12.10 Implementare un piano di risposta agli incidenti. Prepararsi a rispondere immediatamente a una violazione del sistema.	12.10 Esaminare il piano di risposta agli incidenti e le relative procedure per accertarsi che l'entità sia pronta a rispondere immediatamente a una violazione di sistema eseguendo quanto segue.	Senza un piano di risposta agli incidenti di protezione correttamente divulgato, letto e compreso dalle parti responsabili, la confusione o la mancanza di una risposta unificata potrebbero causare ulteriori tempi di inattività del business, un'inutile esposizione ai mezzi di informazione e responsabilità legali.
12.10.1 Creare il piano di risposta agli incidenti da attuare in caso di violazione del sistema. Accertarsi che il piano includa almeno i seguenti elementi: <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. 	12.10.1.a Verificare che il piano di risposta agli incidenti includa i seguenti elementi: <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. 	Il piano di risposta agli incidenti dovrebbe essere completo e contenere tutti gli elementi importanti che consentono all'azienda di rispondere in modo efficace nel caso di una violazione che influisca sui dati dei titolari di carta.
	12.10.1.b Consultare il personale e rivedere la documentazione di un campione relativo ad un incidente o un allarme segnalato in precedenza per verificare che siano stati seguiti le procedure ed il piano di risposta agli incidenti documentati.	
12.10.2 Analizzare e testare il piano, inclusi tutti gli elementi elencati nel Requisito 12.10.1, almeno un volta all'anno.	12.10.2 Consultare il personale e analizzare la documentazione del test per verificare che il piano sia testato almeno un volta all'anno e che il test includa tutti gli elementi elencati nel Requisito 12.10.1.	Senza il test, è possibile che vengano trascurati passaggi chiave che potrebbero determinare una maggiore esposizione durante un incidente.

Requisiti PCI DSS	Procedure di test	Istruzioni
12.10.3 Nominare personale specifico disponibile 24 ore al giorno, 7 giorni su 7 in caso di emergenza.	12.10.3 Verificare attraverso l'osservazione, l'analisi delle politiche e le consultazioni con il personale responsabile 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.	Senza un team di risposta agli incidenti formato e prontamente disponibile, possono verificarsi danni estesi alla rete, e i dati e i sistemi critici potrebbero essere "inquinati" da una gestione inappropriata dei sistemi bersagliati. Questo può minare la riuscita di un'indagine successiva all'incidente.
12.10.4 Formare in modo appropriato il personale addetto al controllo delle violazioni della sicurezza.	12.10.4 Verificare attraverso l'osservazione, l'analisi delle politiche e le consultazioni con il personale responsabile che il personale addetto al controllo delle violazioni della sicurezza partecipi regolarmente a corsi di formazione.	
12.10.5 Includere allarmi provenienti dai sistemi di monitoraggio della sicurezza incluso, senza limitazioni, dai firewall di rilevamento e prevenzione delle intrusioni e dai sistemi di monitoraggio dell'integrità dei file.	12.10.5 Verificare attraverso l'osservazione e l'analisi dei processi che il monitoraggio e la risposta agli avvisi da parte dei sistemi di monitoraggio della sicurezza siano coperti nel piano di risposta agli incidenti.	Questi sistemi di monitoraggio sono pensati per porre l'attenzione sui potenziali rischi per i dati, sono fondamentali per intraprendere azioni rapide per impedire una violazione e devono essere inclusi nei processi di risposta agli incidenti.
12.10.6 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.	12.10.6 Verificare attraverso l'osservazione, l'analisi delle politiche e le consultazioni con il personale responsabile 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.	L'integrazione delle "lezioni apprese" nel piano di risposta agli incidenti dopo un incidente aiuta a mantenere aggiornato il piano e a reagire correttamente alle minacce emergenti e ai trend della sicurezza.
12.11 <i>Requisito aggiuntivo solo per provider di servizi:</i> eseguire analisi almeno una volta all'anno per confermare che il personale sta seguendo i criteri di protezione e le procedure operative. Le analisi devono coprire i seguenti processi: <ul style="list-style-type: none"> analisi dei log giornalieri; analisi dei set di regole dei firewall; applicazione di standard di configurazione a nuovi sistemi; risposta ad avvisi di sicurezza; 	12.11.a Esaminare politiche e procedure per verificare che siano definiti i processi per l'analisi e la conferma che il personale sta seguendo i criteri di protezione e le procedure operative e che le analisi coprano: <ul style="list-style-type: none"> analisi dei log giornalieri; analisi dei set di regole dei firewall; applicazione di standard di configurazione a nuovi sistemi; risposta ad avvisi di sicurezza; processi di gestione delle modifiche. 	<p>Nota: questo requisito si applica solo quando l'entità in corso di valutazione è un provider di servizi.</p> <p>Confermare regolarmente che i criteri di protezione e le procedure vengono seguiti garantisce che i controlli previsti sono attivi e funzionano come desiderato. L'obiettivo di queste analisi non è ri-eseguire altri requisiti PCI DSS, ma confermare se le procedure vengono seguite come previsto.</p>

Requisiti PCI DSS	Procedure di test	Istruzioni
<ul style="list-style-type: none"> processi di gestione delle modifiche. <p>Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.</p>	<p>12.11.b Consultare il personale responsabile ed esaminare i record delle analisi per verificare che le analisi vengano eseguite almeno una volta ogni tre mesi.</p>	
<p>12.11.1 Requisito aggiuntivo solo per provider di servizi: conservare la documentazione del processo di analisi trimestrale per includere:</p> <ul style="list-style-type: none"> documentazione dei risultati delle analisi; analisi e approvazione dei risultati da parte del personale a cui è stata assegnata la responsabilità del programma di conformità PCI DSS. <p>Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.</p>	<p>12.11.1 Esaminare la documentazione delle analisi trimestrali per verificare che includano:</p> <ul style="list-style-type: none"> documentazione dei risultati delle analisi; analisi e approvazione dei risultati da parte del personale a cui è stata assegnata la responsabilità del programma di conformità PCI DSS. 	<p>Nota: questo requisito si applica solo quando l'entità in corso di valutazione è un provider di servizi.</p> <p>Lo scopo di questi controlli indipendenti è confermare se le attività della sicurezza vengono eseguite in maniera costante. È possibile utilizzare queste analisi per verificare che sia stata conservata la prova corretta (ad esempio, log di audit, rapporti delle scansioni delle vulnerabilità, revisioni dei firewall, ecc.) per facilitare la preparazione dell'entità alla prossima valutazione PCI DSS.</p>

Appendice A - Requisiti PCI DSS aggiuntivi

Questa appendice contiene requisiti PCI DSS aggiuntivi per tipi di entità differenti. Le sezioni di questa Appendice includono:

- Appendice A1: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso
- Appendice A2: Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale
- Appendice A3: Convalida aggiuntiva delle entità designate

Istruzioni e informazioni sull'applicabilità vengono fornite in ciascuna sezione.

Appendice A1: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso

Come citato nei requisiti 12.8 e 12.9, tutti i provider di servizi con accesso ai dati dei titolari di carta (compresi i provider di hosting condiviso) devono aderire allo standard PCI DSS. Inoltre il Requisito 2.6 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 A1	Procedure di test	Istruzioni
<p>A.1 Proteggere l'ambiente e i dati ospitati di ogni entità (ossia, esercente, provider di servizi o altra entità), nei modi previsti dal punto A.1.1 al punto A.1.4:</p> <p>Il provider di hosting è tenuto a soddisfare questi requisiti, oltre a tutte le altre sezioni rilevanti dello standard PCI DSS.</p> <p><i>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 allo standard PCI DSS, come applicabile.</i></p>	<p>A.1 Specificamente per una valutazione PCI DSS di un provider di hosting condiviso, per verificare che i provider di hosting condivisi proteggano l'ambiente e i dati ospitati delle entità (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>L'Appendice A di PCI DSS è destinata ai provider di hosting condiviso che desiderano fornire ai clienti di esercenti e/o provider di servizi un ambiente di hosting compatibile con PCI DSS.</p>
<p>A.1.1 Garantire che ogni entità esegua solo processi con accesso esclusivo al proprio ambiente dei dati dei 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 le proprie applicazioni, verificare che i processi di queste applicazioni vengano eseguiti utilizzando l'ID univoco dell'entità. Ad esempio:</p> <ul style="list-style-type: none"> 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>Se un esercente o un provider di servizi può eseguire le sue applicazioni sul server condiviso, tali applicazioni devono essere eseguite con l'ID utente dell'esercente o del provider, anziché come utente privilegiato.</p>

Requisiti A1	Procedure di test	Istruzioni
A.1.2 Limitare l'accesso e i privilegi di ciascuna entità esclusivamente al relativo ambiente di dati dei titolari di carta.	A.1.2.a Verificare che l'ID utente di qualsiasi processo dell'applicazione non sia un utente con privilegi (root/amministratore).	Per garantire che l'accesso e i privilegi siano limitati, in modo tale che ogni esercente o provider di servizi abbia accesso solamente al proprio ambiente, prendere in considerazione quanto segue: <ol style="list-style-type: none"> 1. privilegi dell'ID utente sul server Web dell'esercente o del provider di servizi; 2. autorizzazioni di lettura, scrittura ed esecuzione file concesse; 3. autorizzazioni di scrittura nei file binari del sistema concesse; 4. autorizzazioni concesse per i file di registro dell'esercente o del provider di servizi; 5. controlli per garantire che un esercente o provider di servizi non possa monopolizzare le risorse di sistema.
	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 (limitazioni tramite autorizzazione su file system, elenchi di controllo dell'accesso, funzioni chroot o jailshell, ecc.). 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 log sia consentita solo all'entità proprietaria.	
	A.1.2.e Per impedire che ciascuna entità monopolizzi le risorse del server per sfruttarne le vulnerabilità (ad esempio, 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 log siano abilitate e siano univoche per l'ambiente dei dati dei 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 log per l'ambiente di ciascun esercente e provider di servizi: <ul style="list-style-type: none"> • i registri sono abilitati per applicazioni di terzi 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. 	I registri dovrebbero essere disponibili in un ambiente di hosting condiviso, in modo che gli esercenti e i provider di servizi possano accedere e rivedere i registri specifici per il loro ambiente dei dati dei titolari di carta.

Requisiti A1	Procedure di test	Istruzioni
A.1.4 Abilitare processi per fornire tutte le informazioni necessarie per un'indagine legale tempestiva in caso di una compromissione nei confronti 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 una compromissione.	I provider di hosting condiviso devono disporre di processi per garantire una risposta rapida nel caso sia necessaria un'indagine forense su una compromissione, fino al livello di dettagli appropriato, in modo che siano disponibili i dettagli del singolo esercente o provider di servizi.

Appendice A2: Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale

Le entità che utilizzano SSL e TLS iniziale devono provvedere all'aggiornamento a un protocollo di crittografia avanzata il prima possibile. Inoltre, SSL e/o TLS iniziale non devono essere introdotti in ambienti in cui tali protocolli non esistono già. Al momento della pubblicazione, le vulnerabilità note sono difficili da sfruttare negli ambienti di pagamento POI POS. Tuttavia, potrebbero emergere nuove vulnerabilità in qualsiasi momento e spetta all'organizzazione restare aggiornata in fatto di tendenze di vulnerabilità e determinare se è soggetta o meno a eventuali exploit noti.

I requisiti PCI DSS direttamente interessati sono:

- Requisito 2.2.3** Implementare funzioni di sicurezza aggiuntive per eventuali servizi, protocolli o daemon richiesti considerati non sicuri.
- Requisito 2.3** Eseguire la cifratura di tutto l'accesso amministrativo non da console tramite crittografia avanzata.
- Requisito 4.1** Utilizzare protocolli di sicurezza e crittografia avanzata per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche e aperte.

SSL e TLS iniziale non devono essere utilizzati come controllo di sicurezza per soddisfare questi requisiti. Per supportare le entità nell'eseguire la migrazione da SSL/TLS iniziale, sono incluse le seguenti disposizioni:

- le nuove implementazioni non devono utilizzare SSL o TLS iniziale come controllo di sicurezza;
- tutti i provider di servizi devono fornire un'offerta sicura entro il 30 giugno **2016**;
- dopo il 30 giugno **2018**, tutte le entità devono aver interrotto l'utilizzo di SSL/TLS iniziale come controllo di sicurezza e utilizzare solo versioni sicure del protocollo (una concessione per alcuni terminali POI POS è descritta nell'ultimo punto elenco riportato di seguito);
- prima del 30 giugno 2018, le implementazioni esistenti che utilizzano SSL e/o TLS iniziale devono avere adottato un piano formale di migrazione e riduzione dei rischi;
- i terminali POI POS (e i punti di terminazione SSL/TLS a cui si connettono) che possono essere verificati come non soggetti a eventuali exploit noti per SSL e TLS iniziale possono continuare a utilizzare questi protocolli come controllo di sicurezza dopo il 30 giugno 2018.

Questa appendice si applica alle entità che utilizzano SSL/TLS iniziale come controllo di sicurezza per proteggere il CDE e/o CHD (ad esempio, SSL/TLS iniziale utilizzato per soddisfare il Requisito 2.2.3, 2.3 o 4.1 PCI DSS). Fare riferimento al *Supplemento informativo PCI SSC sulla migrazione da SSL e TLS iniziale* corrente per ulteriori istruzioni sull'utilizzo di SSL/TLS iniziale.

Requisiti A2	Procedure di test	Istruzioni
<p>A2.1 Laddove i terminali POI POS (e i punti di terminazione SSL/TLS a cui si connettono) utilizzano SSL e/o TLS iniziale, l'entità deve:</p> <ul style="list-style-type: none"> • confermare che i dispositivi non sono soggetti a eventuali exploit noti per tali protocolli. <p>O:</p> <ul style="list-style-type: none"> • disporre di un piano formale di migrazione e di riduzione dei rischi. 	<p>A2.1 Per i terminali POI POS (e i punti di terminazione SSL/TLS a cui si connettono) che utilizzano SSL e/o TLS iniziale:</p> <ul style="list-style-type: none"> • confermare che l'entità dispone della documentazione (ad esempio, documentazione del fornitore, dettagli di configurazione del sistema/della rete, ecc.) che verifica che i dispositivi non siano soggetti a eventuali exploit noti per SSL/TLS iniziale; <p>O:</p> <ul style="list-style-type: none"> • completare A2.2 di seguito. 	<p>I POI possono continuare a utilizzare SSL/TLS iniziale quando si può dimostrare che il POI non è soggetto agli exploit attualmente noti. Tuttavia, SSL è una tecnologia obsoleta e può essere soggetta a vulnerabilità della sicurezza aggiuntive in futuro; si consiglia pertanto di aggiornare gli ambienti POI a un protocollo sicuro il prima possibile. Se SSL/TLS iniziale non è necessario nell'ambiente, si deve disabilitare l'utilizzo di e il fallback a queste versioni.</p> <p>Se l'ambiente POI POS è soggetto a exploit noti, la pianificazione della migrazione a un'alternativa sicura deve iniziare immediatamente.</p> <p>Nota: la concessione per i POI POS non attualmente soggetti agli exploit si basa sui rischi noti correnti. Se vengono introdotti nuovi exploit ai quali gli ambienti POI sono soggetti, gli ambienti POI dovranno essere aggiornati.</p>

Requisiti A2	Procedure di test	Istruzioni
<p>A2.2 Le entità con implementazioni esistenti (diverse da quelle consentite in A2.1) che utilizzano SSL e/o TLS iniziale devono avere adottato un piano formale di migrazione e riduzione dei rischi.</p>	<p>A2.2 Analizzare il piano documentato di migrazione e riduzione dei rischi per verificare che includa:</p> <ul style="list-style-type: none"> • descrizione dell'utilizzo, inclusi il tipo di dati trasmessi, i tipi e il numero di sistemi che utilizzano e/o supportano SSL/TLS iniziale come tipo di ambiente; • risultati della valutazione dei rischi e controlli per la riduzione dei rischi in atto; • descrizione dei processi per ricercare eventuali nuove vulnerabilità associate a SSL/TLS iniziale; • descrizione dei processi di controllo delle modifiche implementati per accertarsi che SSL/TLS iniziale non venga implementato nei nuovi ambienti; • panoramica del piano del progetto di migrazione inclusa la data di completamento della migrazione prevista non oltre il 30 giugno 2018. 	<p>Il piano di migrazione e riduzione dei rischi è un documento preparato dall'entità che illustra in maniera dettagliata i suoi piani per la migrazione a un protocollo sicuro e descrive anche i controlli che l'entità ha adottato per ridurre i rischi associati a SSL/TLS iniziale finché non viene completata la migrazione.</p> <p>Fare riferimento al Supplemento informativo PCI SSC sulla migrazione da SSL e TLS iniziale corrente per ulteriori istruzioni sui piani di migrazione e riduzione dei rischi.</p>
<p>A2.3 Requisito aggiuntivo solo per provider di servizi: tutti i provider di servizi devono fornire un'offerta sicura entro il 30 giugno 2016.</p> <p>Nota: prima del 30 giugno 2016, il provider di servizi deve disporre di un'opzione di protocollo sicuro inclusa nella sua offerta di servizi o di un piano documentato di migrazione e riduzione dei rischi (secondo A2.2) che includa una data di destinazione per la fornitura di un'opzione di protocollo sicuro entro il 30 giugno 2016. Dopo questa data, tutti i provider di servizi devono offrire un'opzione di protocollo sicuro per questo servizio.</p>	<p>A2.3 Esaminare le configurazioni di sistema e la documentazione di supporto per verificare che il provider di servizi offra un'opzione di protocollo sicuro per questo servizio.</p>	<p>Fare riferimento a "Provider di servizi" nel documento <i>Glossario, abbreviazioni e acronimi PCI DSS e PA-DSS</i> per ulteriori istruzioni.</p>

Appendice A3: Convalida aggiuntiva delle entità designate (DESV)

Questa appendice si applica solo alle entità designate da un acquirente o un marchio di pagamento che richiedono la convalida aggiuntiva di requisiti PCI DSS esistenti. Esempi di entità a cui questa Appendice **potrebbe** applicarsi includono:

- entità che memorizzano, elaborano e/o trasmettono grandi volumi di dati dei titolari di carta;
- entità che forniscono punti di aggregazione per i dati dei titolari di carta; o
- entità che hanno avuto violazioni significative o ripetute dei dati dei titolari di carta.

Questi passaggi aggiuntivi per la convalida sono destinati a fornire maggiore garanzia che i controlli PCI DSS vengano conservati in modo efficace e costante tramite la convalida dei processi business-as-usual (BAU) e maggiore considerazione della validità e della determinazione dell'ambito.

I passaggi aggiuntivi per la convalida presenti in questo documento sono organizzati nelle seguenti aree di controllo:

A3.1 Implementare un programma di conformità PCI DSS.

A3.2 Documentare e convalidare l'ambito PCI DSS.

A3.3 Convalidare che PCI DSS è incorporato nelle attività business-as-usual (BAU).

A3.4 Controllare e gestire l'accesso locale all'ambiente dei dati dei titolari di carta.

A3.5 Identificare e rispondere a eventi sospetti.

Nota: alcuni requisiti hanno tempi definiti (ad esempio, almeno una volta ogni tre mesi o ogni sei mesi) in cui devono essere eseguite determinate attività. Per la valutazione iniziale di questo documento, non è richiesto che un'attività sia stata eseguita per ogni periodo di tempo durante l'anno precedente, se il valutatore verifica che:

- 1) l'attività è stata eseguita in base al requisito applicabile nel periodo di tempo più recente (ossia, il periodo di tre mesi o sei mesi più recente); e
- 2) l'entità dispone di procedure e politiche documentate per continuare a eseguire l'attività nel periodo di tempo definito.

Per gli anni successivi dopo la valutazione iniziale, è stata eseguita un'attività per ogni periodo di tempo per cui è richiesta (ad esempio, un'attività trimestrale deve essere stata eseguita per ciascuno dei quattro trimestri dell'anno precedente).

Nota: un'entità deve essere sottoposta a una valutazione in base a questa Appendice **SOLO se richiesto** da un acquirente o un marchio di pagamento.

Requisiti A3	Procedure di test	Istruzioni
A3.1 Implementare un programma di conformità PCI DSS		
<p>A3.1.1 Ai dirigenti verrà assegnata la responsabilità della protezione dei dati dei titolari di carta e di un programma di conformità PCI DSS per includere:</p> <ul style="list-style-type: none"> responsabilità generale del rispetto della conformità PCI DSS; definizione di un documento di dichiarazione di intenti per un programma di conformità PCI DSS; fornitura di aggiornamenti a dirigenti e consiglio di amministrazione in merito alle iniziative e ai problemi relativi alla conformità PCI DSS, incluse attività di correzione, almeno una volta all'anno. <p>Riferimento PCI DSS: <i>Requisito 12</i></p>	<p>A3.1.1.a Esaminare la documentazione per verificare che ai dirigenti sia stata assegnata la responsabilità generale del rispetto della conformità PCI DSS dell'entità.</p> <p>A3.1.1.b Esaminare il documento di dichiarazione di intenti PCI DSS dell'azienda per verificare che descriva le condizioni in cui il programma di conformità PCI DSS è organizzato.</p> <p>A3.1.1.c Esaminare le presentazioni e/o i verbali delle riunioni di dirigenti e consiglio di amministrazione per accertarsi che le iniziative relative alla conformità PCI DSS e le attività di correzione vengano comunicate almeno una volta all'anno.</p>	<p>L'assegnazione ai dirigenti delle responsabilità della conformità PCI DSS garantisce visibilità a livello dirigenziale del programma di conformità PCI DSS e offre l'opportunità di porre domande appropriate per determinare l'efficacia del programma e influenzare le priorità strategiche. La responsabilità generale del programma di conformità PCI DSS può essere assegnata a singoli ruoli e/o business unit all'interno dell'organizzazione.</p>
<p>A3.1.2 Deve essere adottato un programma di conformità PCI DSS formale per includere:</p> <ul style="list-style-type: none"> definizione di attività per il rispetto e il monitoraggio della conformità PCI DSS globale, incluse attività business-as-usual; processi di valutazione PCI DSS annuale; processi per la convalida continua dei requisiti PCI DSS (ad esempio: giornaliera, settimanale, trimestrale, ecc. come applicabile secondo il requisito); un processo per l'esecuzione dell'analisi dell'impatto aziendale per determinare i potenziali impatti PCI DSS per le decisioni aziendali strategiche. <p>Riferimento PCI DSS: <i>Requisiti 1-12</i></p>	<p>A3.1.2.a Esaminare le politiche e le procedure di sicurezza delle informazioni per verificare che siano stati specificamente definiti i processi per quanto segue:</p> <ul style="list-style-type: none"> rispetto e monitoraggio della conformità PCI DSS globale, incluse le attività business-as-usual; valutazioni PCI DSS annuali; convalida continua dei requisiti PCI DSS; analisi dell'impatto aziendale per determinare i potenziali impatti PCI DSS per le decisioni aziendali strategiche. 	<p>Un programma di conformità formale consente a un'organizzazione di monitorare l'integrità dei suoi controlli di sicurezza, di essere proattiva nel caso in cui un controllo abbia esito negativo e di comunicare in modo efficace attività e stato della conformità a tutti i livelli.</p> <p>Il programma di conformità PCI DSS può essere un programma dedicato o parte di un programma di governance e/o conformità generale e deve includere una metodologia ben definita che dimostri una valutazione coerente ed efficace. Esempi di metodologie includono: ciclo di Deming di Plan-Do-Check-Act (PDCA), ISO 27001, COBIT, DMAIC e Six Sigma.</p> <p><i>(continua alla pagina successiva)</i></p>

Requisiti A3	Procedure di test	Istruzioni
	<p>A3.1.2.b Consultare il personale e osservare le attività di conformità per verificare che i processi definiti siano implementati per quanto segue:</p> <ul style="list-style-type: none"> rispetto e monitoraggio della conformità PCI DSS globale, incluse le attività business-as-usual; valutazioni PCI DSS annuali; convalida continua dei requisiti PCI DSS; analisi dell'impatto aziendale per determinare i potenziali impatti PCI DSS per le decisioni aziendali strategiche. 	<p>Il rispetto e il monitoraggio della conformità PCI DSS globale di un'organizzazione includono l'identificazione di attività da eseguire giornalmente, settimanalmente, mensilmente, trimestrale o annualmente e garantiscono che queste attività vengano eseguite di conseguenza (ad esempio, utilizzando una metodologia PDCA o un'autovalutazione della sicurezza).</p> <p>Esempi di decisioni aziendali strategiche che devono essere analizzate per potenziali impatti PCI DSS possono includere fusioni e acquisizioni, acquisti di nuove tecnologie o nuovi canali di pagamento-accettazione.</p>
<p>A3.1.3 Le responsabilità e i ruoli della conformità PCI DSS devono essere specificamente definiti e formalmente assegnati a uno o più membri del personale, incluso almeno quanto segue:</p> <ul style="list-style-type: none"> gestione delle attività business-as-usual; gestione delle valutazioni PCI DSS annuali; gestione della convalida continua dei requisiti PCI DSS (ad esempio: giornaliera, settimanale, trimestrale, ecc. come applicabile secondo il requisito); gestione dell'impatto aziendale per determinare i potenziali impatti PCI DSS per le decisioni aziendali strategiche. <p>Riferimento PCI DSS: Requisito 12</p>	<p>A3.1.3.a Esaminare le procedure e le politiche di sicurezza delle informazioni e consultare il personale per verificare che siano chiaramente definiti i ruoli e le responsabilità e che siano assegnati i doveri per includere almeno quanto segue:</p> <ul style="list-style-type: none"> gestione delle attività business-as-usual; gestione delle valutazioni PCI DSS annuali; gestione della convalida continua dei requisiti PCI DSS (ad esempio: giornaliera, settimanale, trimestrale, ecc. come applicabile secondo il requisito); gestione dell'impatto aziendale per determinare i potenziali impatti PCI DSS per le decisioni aziendali strategiche. <p>A3.1.3.b Consultare il personale responsabile e verificare che abbia familiarità con ed esegua le responsabilità della conformità PCI DSS designate.</p>	<p>La definizione formale di responsabilità e regole di conformità PCI DSS specifiche consente di garantire responsabilità e monitoraggio delle iniziative di conformità PCI DSS costanti. Queste regole possono essere assegnate a un unico proprietario o più proprietari per differenti aspetti. La proprietà deve essere assegnata a utenti con l'autorità per prendere decisioni basate su rischi e con la responsabilità per la funzione specifica. I doveri devono essere definiti formalmente e i proprietari devono essere in grado di dimostrare una comprensione delle loro responsabilità.</p>

Requisiti A3	Procedure di test	Istruzioni
<p>A3.1.4 Fornire una formazione aggiornata su PCI DSS e/o sicurezza delle informazioni almeno una volta all'anno al personale con responsabilità della conformità PCI DSS (come identificato in A3.1.3).</p> <p>Riferimento PCI DSS: <i>Requisito 12</i></p>	<p>A3.1.4.a Esaminare le politiche e le procedure di sicurezza delle informazioni per verificare che la formazione su PCI DSS e/o sicurezza delle informazioni sia richiesta almeno una volta all'anno per ciascun ruolo con responsabilità della conformità PCI DSS.</p>	<p>Il personale responsabile della conformità PCI DSS ha esigenze di formazione specifiche che superano ciò che è di solito fornito dalla formazione generale sulla consapevolezza della sicurezza. Utenti con responsabilità della conformità PCI DSS devono ricevere formazione specializzata che, oltre alla consapevolezza generale della sicurezza delle informazioni, sia incentrata su metodologie, processi, competenze e argomenti della sicurezza specifici che devono essere seguiti per consentire a tali utenti di eseguire le loro responsabilità della conformità in modo efficiente.</p> <p>La formazione deve essere offerta da terze parti, ad esempio SANS o PCI SSC (consapevolezza PCI, PCIP e ISA), marchi di pagamenti e acquirenti, oppure può essere interna. Il contenuto della formazione deve essere applicabile per la determinata mansione ed essere aggiornato in modo da includere la versione di PCI DSS e le minacce alla sicurezza più recenti.</p> <p>Per istruzioni aggiuntive sullo sviluppo del contenuto della formazione sulla sicurezza appropriato per ruoli specializzati, fare riferimento al Supplemento informativo di PCI SSC sulle <i>migliori pratiche per l'implementazione di un programma di consapevolezza della sicurezza</i>.</p>
	<p>A3.1.4.b Consultare il personale ed esaminare i certificati di partecipazione o altri record per verificare che il personale con responsabilità della conformità PCI DSS riceva formazione aggiornata su PCI DSS e/o sicurezza delle informazioni simile almeno una volta all'anno.</p>	

Requisiti A3	Procedure di test	Istruzioni
A3.2 Documentare e convalidare l'ambito PCI DSS		
<p>A3.2.1 Documentare e confermare l'accuratezza dell'ambito PCI DSS almeno ogni tre mesi e in caso di modifiche significative all'ambiente che rientra nell'ambito. La convalida della determinazione dell'ambito trimestrale deve includere almeno:</p> <ul style="list-style-type: none"> • identificazione di tutti i componenti di sistema e di tutte le reti che rientrano nell'ambito; • identificazione di tutte le reti che non rientrano nell'ambito e giustificazione per le reti che non rientrano nell'ambito, incluse descrizioni di tutti i controlli di segmentazione implementati; • identificazione di tutte le entità connesse, ad esempio entità di terzi con accesso all'ambiente dei dati dei titolari di carta (CDE). <p>Riferimento PCI DSS: Ambito dei requisiti PCI DSS</p>	<p>A3.2.1.a Esaminare i risultati documentati delle analisi dell'ambito e consultare il personale per verificare che le analisi vengano eseguite:</p> <ul style="list-style-type: none"> • almeno ogni tre mesi; • dopo ogni modifica significativa all'ambiente che rientra nell'ambito. <p>A3.2.1.b Esaminare i risultati documentati delle analisi dell'ambito trimestrali per verificare che venga eseguito quanto segue:</p> <ul style="list-style-type: none"> • identificazione di tutti i componenti di sistema e di tutte le reti che rientrano nell'ambito; • identificazione di tutte le reti che non rientrano nell'ambito e giustificazione per le reti che non rientrano nell'ambito, incluse descrizioni di tutti i controlli di segmentazione implementati; • identificazione di tutte le entità connesse, ad esempio entità di terzi con accesso al CDE. 	<p>La convalida dell'ambito PCI DSS deve essere eseguita il più frequentemente possibile per accertarsi che l'ambito PCI DSS sia aggiornato e allineato agli obiettivi aziendali mutevoli.</p>

Requisiti A3	Procedure di test	Istruzioni
<p>A3.2.2 Determinare l'impatto dell'ambito PCI DSS per tutte le modifiche a sistemi o reti, incluse aggiunte di nuovi sistemi e nuove connessioni di rete. I processi devono includere:</p> <ul style="list-style-type: none"> • esecuzione di una valutazione formale dell'impatto PCI DSS; • identificazione dei requisiti PCI DSS applicabili per il sistema o la rete; • aggiornamento dell'ambito PCI DSS come appropriato; • approvazione documentata dei risultati della valutazione dell'impatto da parte del personale responsabile (come definito in A3.1.3). <p>Riferimento PCI DSS: Ambito dei requisiti PCI DSS; Requisito 1-12</p>	<p>A3.2.2 Esaminare la documentazione delle modifiche e consultare il personale per verificare che per ciascuna modifica a sistemi o reti:</p> <ul style="list-style-type: none"> • sia stata eseguita una valutazione formale dell'impatto PCI DSS; • siano stati identificati i requisiti PCI DSS applicabili alle modifiche al sistema o alla rete; • sia stato aggiornato l'ambito PCI DSS come appropriato per la modifica; • sia stata ottenuta e documentata l'approvazione da parte del personale responsabile (come definito in A3.1.3). 	<p>Le modifiche a sistemi o reti possono avere un impatto significativo sull'ambito PCI DSS. Ad esempio, le modifiche alla regole del firewall possono inserire interi segmenti di rete nell'ambito o possono essere aggiunti al CDE nuovi sistemi che devono essere protetti in maniera appropriata.</p> <p>I processi per determinare il potenziale impatto che le modifiche a sistemi e reti possono avere sull'ambito PCI DSS di un'entità possono essere eseguiti come parte di un programma di conformità PCI DSS dedicato o possono rientrare nel programma di governance e/o conformità generale di un'entità.</p>

Requisiti A3	Procedure di test	Istruzioni
<p>A3.2.2.1 Al completamento di una modifica, tutti i requisiti PCI DSS pertinenti devono essere verificati su tutte le reti e tutti i sistemi nuovi o modificati e la documentazione deve essere aggiornata come applicabile. Esempi di requisiti PCI DSS che devono essere verificati includono, ma non sono limitati a, quanto segue:</p> <ul style="list-style-type: none"> ▪ il diagramma di rete viene aggiornato in base alle modifiche; ▪ i sistemi vengono configurati in base agli standard di configurazione, con tutte le password predefinite modificate e i servizi non necessari disabilitati; ▪ i sistemi vengono protetti con i controlli richiesti, ad es. monitoraggio dell'integrità dei file (FIM), antivirus, patch, log di audit; ▪ verificare che i dati sensibili di autenticazione (SAD) non siano memorizzati e che la memorizzazione di tutti i dati dei titolari di carta (CHD) sia documentata e incorporata nelle procedure e nella politica di conservazione dei dati; ▪ vengono inclusi nuovi sistemi nel processo di scansione delle vulnerabilità trimestrale. <p>Riferimento PCI DSS: Ambito dei requisiti PCI DSS; Requisiti 1-12</p>	<p>A3.2.2.1 Per un campione di modifiche a sistemi e rete, esaminare i record delle modifiche, consultare il personale e osservare le reti/i sistemi interessati per verificare che i requisiti PCI DSS applicabili siano stati implementati e la documentazione aggiornata in base alle modifiche.</p>	<p>È importante disporre di processi per analizzare tutte le modifiche apportate per accertarsi che tutti i controlli PCI DSS appropriati siano applicati a eventuali sistemi o reti aggiunti all'ambiente che rientra nell'ambito a causa di una modifica.</p> <p>Introdurre questa convalida nei processi di gestione delle modifiche garantisce che gli inventari di dispositivi e gli standard di configurazione siano aggiornati e che i controlli di sicurezza siano applicati laddove necessario.</p> <p>Un processo di gestione delle modifiche deve includere la prova che i requisiti PCI DSS vengano implementati o preservati nell'intero processo iterativo.</p>

Requisiti A3	Procedure di test	Istruzioni
<p>A3.2.3 Le modifiche alla struttura organizzativa, ad esempio, fusione o acquisizione aziendale, cambio o riassegnazione del personale con responsabilità dei controlli di sicurezza, comportano un'analisi formale (interna) dell'impatto sull'ambito PCI DSS e sull'applicabilità dei controlli.</p> <p>Riferimento PCI DSS: Requisito 12</p>	<p>A3.2.3 Esaminare politiche e procedure per verificare che una modifica alla struttura organizzativa comporti un'analisi formale dell'impatto sull'ambito PCI DSS e sull'applicabilità dei controlli.</p>	<p>La struttura e la gestione di un'organizzazione definiscono i requisiti e il protocollo per operazioni efficaci e sicure. Le modifiche a questa struttura potrebbero avere effetti negativi sui framework e sui controlli esistenti riallocando o rimuovendo risorse che una volta supportavano controlli PCI DSS o ereditando nuove responsabilità che potrebbero non aver applicato controlli. Pertanto, è importante rivedere i controlli e l'ambito PCI DSS quando si verificano modifiche per accertarsi che i controlli siano in atto e attivi.</p>
<p>A3.2.4 Se si utilizza la segmentazione, confermare l'ambito PCI DSS eseguendo test di penetrazione nei controlli di segmentazione almeno ogni sei mesi e dopo eventuali modifiche ai controlli/metodi di segmentazione.</p> <p>Riferimento PCI DSS: Requisito 11</p>	<p>A3.2.4 Esaminare i risultati dei test di penetrazione più recenti per verificare che:</p> <ul style="list-style-type: none"> • il test di penetrazione venga eseguito per verificare i controlli di segmentazione almeno ogni sei mesi e dopo eventuali modifiche ai controlli/metodi di segmentazione; • il test di penetrazione copra tutti i controlli/metodi di segmentazione in uso; • il test di penetrazione verifichi che i controlli/metodi di segmentazione siano funzionali ed efficaci e isolino tutti i sistemi che non rientrano nell'ambito dai sistemi che rientrano nel CDE. 	<p>Se la segmentazione viene utilizzata per isolare reti che rientrano nell'ambito da reti che non rientrano nell'ambito, tali controlli di segmentazione devono essere verificati utilizzando il test di penetrazione per verificare che continuino a operare come previsto e in maniera efficace. Le tecniche del test di penetrazione devono seguire la metodologia di penetrazione esistente come specificato nel Requisito 11 PCI DSS.</p> <p>Per informazioni aggiuntive sul test di penetrazione efficace, fare riferimento al Supplemento informativo di PCI SSC sulle <i>istruzioni per il test di penetrazione</i>.</p>

Requisiti A3	Procedure di test	Istruzioni
<p>A3.2.5 Implementare una metodologia di rilevamento dei dati per confermare l'ambito PCI DSS e per individuare tutte le origini e le posizioni del PAN in chiaro almeno ogni tre mesi e dopo modifiche significative ai processi o all'ambiente del titolare di carta.</p> <p>La metodologia di rilevamento dei dati deve prendere in considerazione la possibilità che il PAN in chiaro risieda su sistemi e reti al di fuori del CDE attualmente definito.</p> <p>Riferimento PCI DSS: Ambito dei requisiti PCI DSS</p>	<p>A3.2.5.a Esaminare la metodologia di rilevamento dei dati documentata per verificare quanto segue:</p> <ul style="list-style-type: none"> la metodologia di rilevamento dei dati includa processi per l'identificazione di tutte le origini e le posizioni del PAN in chiaro; la metodologia prenda in considerazione la possibilità che il PAN in chiaro risieda su sistemi e reti al di fuori del CDE attualmente definito. 	<p>PCI DSS richiede che, come parte dell'esercizio di determinazione dell'ambito, le entità valutate debbano identificare e documentare l'esistenza di tutto il PAN in chiaro nei loro ambienti. L'implementazione di una metodologia di rilevamento dei dati che identifica tutte le origini e le posizioni del PAN in chiaro e prende in considerazione la possibilità che il PAN in chiaro risieda su sistemi e reti al di fuori del CDE attualmente definito o in punti imprevisi all'interno del CDE definito, ad esempio in un log di errori o in un file di immagine della memoria, garantisce che le posizioni sconosciute in precedenza del PAN in chiaro vengano rilevate e protette in modo appropriato.</p> <p>Un processo di rilevamento dei dati può essere eseguito con diversi metodi, inclusi, senza limitazioni: (1) software di rilevamento dei dati disponibile in commercio, (2) un programma di rilevamento dei dati sviluppato internamente o (3) una ricerca manuale. Indipendentemente dal metodo utilizzato, l'obiettivo del processo è trovare tutte le origini e le posizioni del PAN in chiaro (non solo nel CDE definito).</p>
	<p>A3.2.5.b Esaminare i risultati dei processi di rilevamento dei dati recenti e consultare il personale responsabile per verificare che il rilevamento dei dati venga eseguito almeno ogni tre mesi e in caso di modifiche significative ai processi o all'ambiente del titolare di carta.</p>	
<p>A3.2.5.1 Accertarsi dell'efficienza dei metodi utilizzati per il rilevamento dei dati, ad es. i metodi devono essere in grado di rilevare il PAN in chiaro su tutti i tipi di componenti di sistema (ad esempio, su ciascun sistema operativo o piattaforma) e formati di file in uso.</p> <p>L'efficienza dei metodi di rilevamento dei dati deve essere confermata almeno una volta all'anno.</p> <p>Riferimento PCI DSS: Ambito dei requisiti</p>	<p>A3.2.5.1.a Consultare il personale e analizzare la documentazione per verificare che:</p> <ul style="list-style-type: none"> nell'entità sia in atto un processo per testare l'efficienza dei metodi utilizzati per il rilevamento dei dati; il processo includa la verifica che i metodi siano in grado di rilevare il PAN in chiaro su tutti i tipi di componenti di sistema e formati di file in uso. 	<p>Un processo per testare l'efficienza dei metodi utilizzati per il rilevamento dei dati garantisce la completezza e l'accuratezza del rilevamento dei dati dei titolari di carta. Per completezza, nel processo di rilevamento dei dati deve essere incluso almeno un campionamento dei componenti di sistema sia nelle reti che rientrano nell'ambito che quelle che non rientrano nell'ambito. L'accuratezza può essere testata inserendo i PAN dei test in un campione di componenti di sistema e formati di file in uso e confermando che il metodo di rilevamento dei dati ha rilevato i PAN.</p>
	<p>A3.2.5.1.b Esaminare i risultati dei test di efficienza recenti per verificare che l'efficienza dei metodi utilizzati per il rilevamento dei dati sia confermata almeno una volta all'anno.</p>	

Requisiti A3	Procedure di test	Istruzioni
<p><i>PCI DSS</i></p> <p>A3.2.5.2 Implementare le procedure di risposta in modo che vengano avviate al rilevamento del PAN in chiaro al di fuori del CDE per includere:</p> <ul style="list-style-type: none"> ▪ procedure per la determinazione delle operazioni da intraprendere nel caso in cui il PAN in chiaro venga rilevato al di fuori del CDE, inclusi il relativo recupero, eliminazione sicura e/o migrazione nel CDE attualmente definito, come applicabile; ▪ procedure per determinare come i dati sono finiti al di fuori del CDE; ▪ procedure per impedire perdite di dati o lacune di processi con conseguente presenza di dati al di fuori del CDE; ▪ procedure per l'identificazione dell'origine dei dati; ▪ procedure per l'identificazione di eventuali dati di traccia memorizzati con i PAN. 	<p>A3.2.5.2.a Esaminare le procedure di risposta documentate per verificare che le procedure per rispondere al rilevamento del PAN in chiaro al di fuori del CDE siano definite e includano:</p> <ul style="list-style-type: none"> ▪ procedure per la determinazione delle operazioni da intraprendere nel caso in cui il PAN in chiaro venga rilevato al di fuori del CDE, inclusi il relativo recupero, eliminazione sicura e/o migrazione nel CDE attualmente definito, come applicabile; ▪ procedure per determinare come i dati sono finiti al di fuori del CDE; ▪ procedure per impedire perdite di dati o lacune di processi con conseguente presenza di dati al di fuori del CDE; ▪ procedure per l'identificazione dell'origine dei dati; ▪ procedure per l'identificazione di eventuali dati di traccia memorizzati con i PAN. <p>A3.2.5.2.b Consultare il personale ed esaminare i record delle azioni di risposta per verificare che le attività di correzione vengano eseguite quando si rileva il PAN in chiaro al di fuori del CDE.</p>	<p>Disporre di procedure di risposta documentate seguite nel caso in cui venga rilevato il PAN in chiaro al di fuori del CDE consente di identificare le azioni di correzione e impedire perdite future. Ad esempio, se è stato rilevato il PAN al di fuori del CDE, deve essere eseguita l'analisi per (1) determinare se è stato salvato indipendentemente da altri dati (o faceva parte di una traccia completa?), (2) identificare l'origine dei dati e (3) identificare le lacune dei controlli che hanno determinato la presenza dei dati al di fuori del CDE.</p>

Requisiti A3	Procedure di test	Istruzioni
<p>A3.2.6 Implementare i meccanismi per rilevare il PAN in chiaro e impedire che esca dal CDE mediante un processo, un metodo o un canale non autorizzato, inclusa la generazione di avvisi e log di audit.</p> <p>Riferimento PCI DSS: <i>Ambito dei requisiti PCI DSS</i></p>	<p>A3.2.6.a Esaminare la documentazione e osservare i meccanismi implementati per verificare che i meccanismi siano/stiano:</p> <ul style="list-style-type: none"> • implementati e attivamente in esecuzione; • configurati per rilevare il PAN in chiaro e impedire che esca dal CDE mediante un processo, un metodo o un canale non autorizzato; • generando log e avvisi in caso di rilevamento del PAN in chiaro che esce dal CDE mediante un processo, un metodo o un canale non autorizzato. <p>A3.2.6.b Esaminare log di audit e avvisi e consultare il personale responsabile per verificare che gli avvisi vengano investigati.</p>	<p>I meccanismi per rilevare e impedire la perdita non autorizzata del PAN in chiaro possono includere strumenti appropriati, come soluzioni di prevenzione della perdita dei dati (DLP), e/o procedure e processi manuali. La copertura dei meccanismi deve includere, senza limitazioni, e-mail, download per supporti rimovibili e output su stampanti. L'utilizzo di questi meccanismi consente a un'organizzazione di rilevare e prevenire situazioni che possono portare a una perdita dei dati.</p>
<p>A3.2.6.1 Implementare le procedure di risposta in modo che vengano avviate al rilevamento di tentativi di rimozione del PAN in chiaro dal CDE mediante un processo, un metodo o un canale non autorizzato. Le procedure di risposta devono includere:</p> <ul style="list-style-type: none"> ▪ procedure per un'indagine tempestiva degli avvisi da parte del personale responsabile; ▪ procedure per impedire perdite di dati o lacune di processi, secondo necessità, al fine di proteggere i dati stessi. 	<p>A3.2.6.1.a Esaminare le procedure di risposta documentate per verificare che le procedure per rispondere alla tentata rimozione del PAN in chiaro dal CDE mediante un processo, un metodo o un canale non autorizzato includano:</p> <ul style="list-style-type: none"> ▪ procedure per un'indagine tempestiva degli avvisi da parte del personale responsabile; ▪ procedure per impedire perdite di dati o lacune di processi, secondo necessità, al fine di proteggere i dati stessi. <p>A3.2.6.1.b Consultare il personale ed esaminare i record delle azioni eseguite quando si rileva il PAN in chiaro al di fuori del CDE mediante un processo, un metodo o un canale non autorizzato e verificare che siano state eseguite le attività di correzione.</p>	<p>I tentativi di rimozione del PAN in chiaro mediante un processo, un metodo o un canale non autorizzato possono indicare l'intento doloso di rubare i dati o possono essere le azioni di un dipendente autorizzato che non è consapevole dei metodi appropriati o semplicemente non li sta seguendo. Un'indagine tempestiva di queste occorrenze può identificare il punto dove deve essere applicata la correzione e fornisce informazioni preziose per aiutare a comprendere da dove derivano le minacce.</p>

Requisiti A3	Procedure di test	Istruzioni
A3.3 Convalidare che PCI DSS è incorporato nelle attività business-as-usual (BAU)		
<p>A3.3.1 Implementare un processo per rilevare immediatamente e avvisare in caso di errori dei controlli di sicurezza critici. Esempi di controlli di sicurezza critici includono, senza limitazioni:</p> <ul style="list-style-type: none"> • Firewall • IDS/IPS • FIM • Antivirus • Controlli dell'accesso fisico • Controlli dell'accesso logico • Meccanismi di log di audit • Controlli di segmentazione (se utilizzati) <p>Riferimento PCI DSS: Requisiti 1-12</p>	<p>A3.3.1.a Esaminare le procedure e le politiche documentate per verificare che i processi siano definiti per rilevare e avvisare tempestivamente in caso di errori dei controlli di sicurezza critici.</p> <p>A3.3.1.b Esaminare i processi di rilevamento e generazione di avvisi e consultare il personale per verificare che siano implementati i processi per tutti i controlli di sicurezza critici e che l'errore di un controllo di sicurezza critico determini la generazione di un avviso.</p>	<p>Senza processi formali per il rilevamento e la generazione di avvisi tempestivi (il prima possibile) di errori dei controlli di sicurezza critici, gli errori possono risultare non rilevati per periodi prolungati e fornire agli aggressori molto tempo per compromettere sistemi e rubare dati sensibili dall'ambiente dei dati dei titolari di carta.</p>

Requisiti A3	Procedure di test	Istruzioni
<p>A3.3.1.1 Risolvere gli errori di eventuali controlli di sicurezza critici in maniera tempestiva. I processi di risoluzione degli errori presenti nei controlli di sicurezza devono includere:</p> <ul style="list-style-type: none"> ▪ ripristino delle funzioni di sicurezza; ▪ identificazione e documentazione della durata (data e ora dell'inizio e della fine) dell'errore della sicurezza; ▪ identificazione e documentazione delle cause dell'errore, inclusa la causa principale, e documentazione delle attività di correzione richieste per identificare ed eliminare la causa principale; ▪ identificazione e risoluzione di eventuali problemi di sicurezza che insorgono durante l'errore; ▪ esecuzione di una valutazione dei rischi per determinare se sono richieste ulteriori azioni come conseguenza dell'errore della sicurezza; ▪ implementazione di controlli per impedire il ripetersi della causa dell'errore; ▪ ripresa del monitoraggio dei controlli di sicurezza. <p>Riferimento PCI DSS: Requisiti 1-12</p>	<p>A3.3.1.1.a Esaminare le procedure e le politiche documentate per e consultare il personale per verificare che siano definiti e implementati i processi per risolvere un errore del controllo di sicurezza e includano:</p> <ul style="list-style-type: none"> ▪ ripristino delle funzioni di sicurezza; ▪ identificazione e documentazione della durata (data e ora dell'inizio e della fine) dell'errore della sicurezza; ▪ identificazione e documentazione delle cause dell'errore, inclusa la causa principale, e documentazione delle attività di correzione richieste per identificare ed eliminare la causa principale; ▪ identificazione e risoluzione di eventuali problemi di sicurezza che insorgono durante l'errore; ▪ esecuzione di una valutazione dei rischi per determinare se sono richieste ulteriori azioni come conseguenza dell'errore della sicurezza; ▪ implementazione di controlli per impedire il ripetersi della causa dell'errore; ▪ ripresa del monitoraggio dei controlli di sicurezza. <p>A3.3.1.1.b Esaminare i record per verificare che gli errori dei controlli di sicurezza siano documentati per includere:</p> <ul style="list-style-type: none"> ▪ identificazione delle cause dell'errore, inclusa la causa principale; ▪ durata (data e ora dell'inizio e della fine) dell'errore della sicurezza; ▪ dettagli delle attività di correzione richieste per identificare ed eliminare la causa principale. 	<p>La prova documentata (ad es. i record in un sistema di gestione dei problemi) deve supportare che sono in atto processi e procedure per risolvere gli errori della sicurezza. Inoltre, il personale deve essere a conoscenza delle sue responsabilità nel caso di un errore. Azioni e risoluzioni dell'errore devono essere acquisite nella prova documentata.</p>

Requisiti A3	Procedure di test	Istruzioni
<p>A3.3.2 Analizzare le tecnologie hardware e software almeno una volta all'anno per confermare se continuano a soddisfare i requisiti PCI DSS dell'organizzazione. Ad esempio, un'analisi delle tecnologie che non sono più supportate dal fornitore e/o non soddisfano più le esigenze di sicurezza dell'organizzazione.</p> <p>Il processo include un piano per aggiornare le tecnologie che non soddisfano più i requisiti PCI DSS dell'organizzazione, fino a e inclusa la sostituzione della tecnologia, come appropriato.</p> <p>Riferimento PCI DSS: Requisiti 2, 6</p>	<p>A3.3.2.a Esaminare le procedure e le politiche documentate e consultare il personale per verificare che siano definiti e implementati i processi per analizzare le tecnologie hardware e software al fine di confermare che continuano a soddisfare i requisiti PCI DSS dell'organizzazione.</p>	<p>Le tecnologie hardware e software sono in costante evoluzione e le organizzazioni devono essere consapevoli delle modifiche alle tecnologie che utilizzano, come pure delle minacce future a tali tecnologie. Le organizzazioni devono anche essere consapevoli delle modifiche apportate dai fornitori di tecnologia ai loro prodotti o processi di supporto, per comprendere come tali modifiche possono influire sull'utilizzo della tecnologia da parte dell'organizzazione.</p> <p>Analisi regolari delle tecnologie che incidono o influiscono sui controlli PCI DSS possono fornire assistenza con le strategie di acquisto, utilizzo e distribuzione e garantire che i controlli che si basano su tali tecnologie siano efficienti.</p>
	<p>A3.3.2.b Analizzare i risultati delle analisi recenti per verificare che le analisi vengano eseguite almeno una volta all'anno.</p>	
	<p>A3.3.2.c Per eventuali tecnologie che si ritiene non soddisfino più i requisiti PCI DSS dell'organizzazione, verificare che sia in atto un piano per aggiornare la tecnologia.</p>	

Requisiti A3	Procedure di test	Istruzioni
<p>A3.3.3 Eseguire analisi almeno ogni tre mesi per verificare che vengano seguite le attività BAU. Le analisi devono essere eseguite dal personale assegnato al programma di conformità PCI DSS (come identificato in A3.1.3) e includere quanto segue:</p> <ul style="list-style-type: none"> • conferma che tutte le attività BAU (ad es., A3.2.2, A3.2.6 e A3.3.1) sono eseguite; • conferma che il personale sta seguendo criteri di protezione e procedure operative (ad esempio, analisi dei log giornaliere, analisi dei set di regole dei firewall, standard di configurazione per nuovi sistemi, ecc.); • documentazione del completamento delle analisi, inclusa la verifica di tutte le attività BAU in atto; • raccolta della prova documentata come richiesto per la valutazione PCI DSS annuale; • analisi e approvazione dei risultati da parte del personale a cui è stata assegnata la responsabilità del programma di conformità PCI DSS (come identificato in A3.1.3); • conservazione dei record e documentazione per almeno 12 mesi, coprendo tutte le attività BAU. <p>Riferimento PCI DSS: Requisiti 1-12</p>	<p>A3.3.3.a Esaminare le politiche e le procedure per verificare che siano stati definiti i processi per l'analisi e la verifica delle attività BAU. Verificare che le procedure includano:</p> <ul style="list-style-type: none"> • conferma che tutte le attività BAU (ad es., A3.2.2, A3.2.6 e A3.3.1) sono eseguite; • conferma che il personale sta seguendo criteri di protezione e procedure operative (ad esempio, analisi dei log giornaliere, analisi dei set di regole dei firewall, standard di configurazione per nuovi sistemi, ecc.); • documentazione del completamento delle analisi, inclusa la verifica di tutte le attività BAU in atto; • raccolta della prova documentata come richiesto per la valutazione PCI DSS annuale; • analisi e approvazione dei risultati da parte dei dirigenti a cui è stata assegnata la responsabilità della governance PCI DSS; • conservazione dei record e documentazione per almeno 12 mesi, coprendo tutte le attività BAU. <p>A3.3.3.b Consultare il personale responsabile ed esaminare i record delle analisi per verificare che:</p> <ul style="list-style-type: none"> • le analisi vengano eseguite dal personale assegnato al programma di conformità PCI DSS; • le analisi vengano eseguite almeno ogni tre mesi. 	<p>L'implementazione dei controlli PCI DSS nelle attività business-as-usual è un metodo efficiente per accertarsi che la sicurezza sia inclusa come parte delle normali operazioni aziendali in maniera costante. Pertanto, è importante che vengano eseguite indagini indipendenti per accertarsi che i controlli BAU siano attivi e funzionino come previsto.</p> <p>Lo scopo di queste indagini indipendenti è analizzare la prova che conferma che vengono eseguite le attività business-as-usual.</p> <p>È possibile utilizzare queste analisi per verificare che sia stata conservata la prova corretta (ad esempio, log di audit, rapporti delle scansioni delle vulnerabilità, revisioni dei firewall, ecc.) per facilitare la preparazione dell'entità alla prossima valutazione PCI DSS.</p>

Requisiti A3	Procedure di test	Istruzioni
A3.4 Controllare e gestire l'accesso locale all'ambiente dei dati dei titolari di carta		
<p>A3.4.1 Analizzare gli account utente e i privilegi di accesso per i componenti di sistema che rientrano nell'ambito almeno ogni sei mesi per accertarsi che gli account utente e l'accesso siano appropriati in base alla mansione e autorizzati.</p> <p>Riferimento PCI DSS: Requisito 7</p>	<p>A3.4.1 Consultare il personale responsabile ed esaminare la documentazione di supporto per verificare che:</p> <ul style="list-style-type: none"> gli account utente e i privilegi di accesso siano analizzati almeno ogni sei mesi; le analisi confermino che l'accesso è appropriato in base alla mansione e che tutto l'accesso è autorizzato. 	<p>I requisiti di accesso evolvono nel corso del tempo poiché gli utenti cambiano ruoli o terminano il rapporto di lavoro e le mansioni cambiano. I dirigenti devono analizzare, riconvalidare e aggiornare regolarmente l'accesso utente, secondo necessità, per riflettere le modifiche al personale, inclusi terzi, e le mansioni degli utenti.</p>
A3.5 Identificare e rispondere a eventi sospetti		
<p>A3.5.1 Implementare una metodologia per l'identificazione tempestiva di schemi di attacchi e comportamento indesiderato nei sistemi, ad esempio utilizzando analisi manuali coordinate e/o strumenti di correlazione dei log automatici o gestiti a livello centrale, per includere almeno quanto segue:</p> <ul style="list-style-type: none"> identificazione di anomalie o attività sospette quando si verificano; invio di avvisi tempestivi dopo il rilevamento di anomalie o attività sospette al personale responsabile; risposta agli avvisi in conformità alle procedure di risposta documentate. <p>Riferimento PCI DSS: Requisiti 10, 12</p>	<p>A3.5.1.a Esaminare la documentazione e consultare il personale per verificare che sia definita e implementata una metodologia per identificare schemi di attacchi e comportamento indesiderato nei sistemi in maniera tempestiva e includa quanto segue:</p> <ul style="list-style-type: none"> identificazione di anomalie o attività sospette quando si verificano; invio di avvisi tempestivi al personale responsabile; risposta agli avvisi in conformità alle procedure di risposta documentate. <p>A3.5.1.b Esaminare le procedure di risposta agli incidenti e consultare il personale per verificare che:</p> <ul style="list-style-type: none"> solo il personale disponibile riceva avvisi tempestivi; si risponda agli avvisi secondo le procedure di risposta documentate. 	<p>La capacità di identificare schemi di attacchi e comportamento indesiderato nei sistemi è essenziale nel prevenire, rilevare o ridurre l'impatto di una compromissione dei dati. La presenza dei log in tutti gli ambienti consente di tenere traccia, generare avvisi ed eseguire un'analisi quando si verifica un problema. La determinazione della causa di una compromissione è molto difficile, se non impossibile, senza un processo per corroborare le informazioni provenienti dai sistemi e dai componenti di sistema critici che eseguono funzioni di sicurezza, come firewall, IDS/IPS e sistemi di monitoraggio dell'integrità dei file (FIM). Pertanto, devono essere raccolti, correlati e conservati i log per tutti i sistemi e componenti di sistema critici che eseguono funzioni di sicurezza. Ciò potrebbe includere l'utilizzo di prodotti software e di metodologie di servizio per fornire analisi in tempo reale, avvisi e report, come gestione di eventi e informazioni sulla sicurezza (SIEM), monitoraggio dell'integrità dei file (FIM) o rilevamento delle modifiche.</p>

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 più fattori è un requisito PCI DSS per l'accesso remoto. L'autenticazione a più 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 può essere supportata. L'autenticazione a più 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 dei 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 più 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 allo 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: 8.1.1 - Tutti gli utenti sono identificati con un ID utente univoco prima di consentire loro l'accesso a componenti del sistema o a dati dei 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 utilizzando i loro normali account utente e quindi di utilizzare il comando “sudo” per eseguire eventuali comandi amministrativi. Questo consente l'uso dei privilegi dell'account “root” per eseguire comandi predefiniti che sono registrati da sudo nel log della sicurezza. In questo modo, le azioni di ciascun utente possono essere registrate mediante un singolo account utente, senza la password “root” condivisa con gli utenti.</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 sudo è configurato correttamente utilizzando un file “sudoers”, che solo i comandi predefiniti possono essere eseguiti da utenti specificati e che tutte le attività eseguite da tali utenti utilizzando sudo sono registrate per identificare l'utente che eseguirà le azioni utilizzando i privilegi “root”.</i>
6. Manutenzione	Definire il processo e i controlli in atto per i controlli	<i>La società XYZ documenta i processi e le procedure per garantire che le configurazioni</i>

	compensativi.	<i>sudo non vengano modificate, alterate o rimosse per consentire ai singoli utenti di eseguire comandi root senza essere identificati, rilevati e registrati singolarmente.</i>
--	---------------	--

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

