Payment Card Industry (PCI)
Data Security Standard

Requisiti e procedure di valutazione della sicurezza

Versione 1.2

Ottobre 2008

Sommario

Introduzione e panoramica di PCI Data Security Standard 3
Informazioni sull'applicabilità degli standard PCI DSS 4
Ambito della valutazione per la conformità ai requisiti PCI DSS 5
Segmentazione di rete 5
Wireless 6
Terze parti/Outsourcing 6
Campionamento delle strutture aziendali e dei componenti di sistema 6
Controlli compensativi 7
Istruzioni e contenuto per il rapporto sulla conformità 8
Contenuto e formato del rapporto 8
Riconvalida dei problemi in attesa di soluzione 11
Conformità agli standard PCI DSS – Operazioni 11
Requisiti PCI DSS e procedure di valutazione della sicurezza dettagliate 12
Sviluppo e gestione di una rete sicura 13
Requisito 1: Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta 13
Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione 17
Protezione dei dati di titolari di carta 20
Requisito 3: Proteggere i dati di titolari di carta memorizzati 20
Requisito 4: Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche 26
Manutenzione di un programma per la gestione delle vulnerabilità 28
Requisito 5: Utilizzare e aggiornare regolarmente il software antivirus 28
Requisito 6: Sviluppare e gestire sistemi e applicazioni protette 29
Implementazione di rigide misure di controllo dell'accesso 35
Requisito 7: Limitare l'accesso ai dati di titolari di cartasolo se effettivamente necessario 35
Requisito 8: Assegnare un ID univoco a chiunque abbia accesso a un computer 37
Requisito 9: Limitare l'accesso fisico ai dati di titolari di carta. 42
Monitoraggio e test delle reti regolari 46
Requisito 10: Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta. 46
Requisito 11: Eseguire regolarmente test di sistemi e processi di protezione. 50
Gestione di una politica di sicurezza delle informazioni 53
Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori. 53
Appendice A: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso 60
Appendice B: Controlli compensativi 63
Appendice C: Foglio di lavoro - Controlli compensativi 64

Appendice D: Attestato di conformità – Esercenti 66
Appendice E: Attestato di conformità – Provider di servizi 70
Appendice F: Revisioni PCI DSS – Determinazione dell'ambito e scelta dei campioni 74

Introduzione e panoramica di PCI Data Security Standard

PCI (Payment Card Industry) DSS (Data Security Standard) è stato sviluppato per favorire e migliorare la protezione dei dati di titolari di carta nonché semplificare l'implementazione di misure di sicurezza dei dati coerenti a livello globale. Il presente documento, *PCI DSS - Requisiti e procedure di valutazione della sicurezza,* si basa sui 12 requisiti PCI DSS e li abbina alle corrispondenti procedure di test in uno strumento di valutazione della sicurezza. È destinato ai valutatori che conducono revisioni in sede per esercenti e provider di servizi che devono confermare la conformità agli standard PCI DSS. Di seguito, è riportata una panoramica di alto livello dei 12 requisiti PCI DSS. Nelle pagine seguenti vengono fornite informazioni sulla preparazione, l'esecuzione e il reporting di una valutazione PCI DSS; la descrizione dettagliata dei requisiti PCI DSS inizia a pagina 13.

PCI Data Security Standard – Panoramica di alto livello

Sviluppo e gestione di una rete sicura	
Requisito 1:	Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta
Requisito 2:	Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di sicurezza
Protezione dei dati di titolari di carta	
Requisito 3:	Proteggere i dati di titolari di carta memorizzati
Requisito 4:	Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche
Utilizzare un programma per la gestione delle vulnerabilità	
Requisito 5:	Utilizzare e aggiornare regolarmente il software antivirus
Requisito 6:	Sviluppare e gestire sistemi e applicazioni protette
Implementazione di rigide misure di controllo dell'accesso	
Requisito 7:	Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario
Requisito 8:	Assegnare un ID univoco a chiunque abbia accesso a un computer
Requisito 9:	Limitare l'accesso fisico ai dati di titolari di carta
Monitorare ed eseguire test delle reti regolari	
Requisito 10:	Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta
Requisito 11:	Eseguire regolarmente test dei sistemi e processi di protezione
Gestire una politica di sicurezza delle informazioni	
Requisito 12:	Gestire una politica che garantisca la sicurezza delle informazioni

Informazioni sull'applicabilità degli standard PCI DSS

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

	Elemento di dati	Memorizzazione consentita	Protezione richiesta	Req. 3.4 PCI DSS
Dati di titolari di carta	PAN (Primary Account Number)	Sì	Sì	Sì
	Nome titolare di carta [1]	Sì	Sì [1]	No
	Codice di servizio [1]	Sì	Sì [1]	No
	Data di scadenza [1]	Sì	Sì [1]	No
Dati sensibili di autenticazione [2]	Dati completi della striscia magnetica [3]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/Blocco PIN	No	N/A	N/A

[1] *Questi elementi di dati devono essere protetti se memorizzati insieme al PAN. Tale protezione rientra in base ai requisiti PCI DSS nella protezione generale dell'ambiente dei dati dei titolari di carta. Inoltre, altre leggi (ad esempio, correlate alla protezione dei dati personali, alla privacy, al furto di identità o alla sicurezza dei dati) possono richiedere una protezione specifica di questi dati o una divulgazione appropriata di pratiche di una società se i dati personali dei consumatori vengono raccolti durante lo svolgimento delle mansioni aziendali. Gli standard PCI DSS, tuttavia, non sono applicabili se i PAN non vengono memorizzati, elaborati o trasmessi.*

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

[3] *Dati della traccia completa della striscia magnetica, dell'immagine della striscia magnetica sul chip o in un altra posizione.*

Ambito della valutazione per la conformità ai requisiti PCI DSS

I requisiti di sicurezza PCI DSS si applicano a tutti i componenti di sistema. Per "componenti di sistema" si intende qualsiasi componente di rete, server o applicazione incluso o connesso all'ambiente dei dati dei titolari di carta. L'ambiente dei dati dei titolari di carta è la parte di rete che contiene dati dei titolari di carta o dati sensibili di autenticazione. I componenti di rete includono, senza limitazioni, firewall, switch, router, punti di accesso wireless, dispositivi di rete e altri dispositivi di sicurezza. I tipi di server possono essere: Web, applicazioni, database, autenticazione, e-mail, proxy, NTP (Network Time Protocol) e DNS (Domain Name Server). Le applicazioni includono tutte le applicazioni acquistate e personalizzate, comprese applicazioni interne ed esterne (Internet).

Segmentazione di rete

La segmentazione di rete o l'isolamento dell'ambiente dei dati dei titolari di carta dal resto della rete aziendale non è un requisito PCI DSS. Tuttavia, è un metodo 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 firewall di rete interni, router con elenchi di controllo dell'accesso avanzato o altre tecnologie che limitano l'accesso a un determinato segmento di una rete.

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

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

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

Appendice F: Revisioni PCI DSS– Determinazione dell'ambito e scelta dei campioni fornisce ulteriori informazioni sull'effetto della determinazione dell'ambito durante una valutazione PCI DSS.

Wireless

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

Terze parti/Outsourcing

Per i provider di servizi è necessario eseguire una valutazione annuale in sede e la convalida della conformità su tutti i componenti di sistema in cui i dati di titolari di carta vengono memorizzati, elaborati o trasmessi.

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

Per le entità che si avvalgono del supporto di provider di terze parti per la memorizzazione, l'elaborazione o la trasmissione dei dati di titolari di carta, il ROC (rapporto di conformità) deve documentare il ruolo di ogni provider, identificando chiaramente i requisiti che si applicano all'entità revisionata e quelli che si applicano al provider di servizi. I provider di servizi di terze parti possono convalidare la propria conformità ai requisiti PCI DSS nei due seguenti modi: 1) Eseguendo la valutazione PCI DSS personalmente e fornendo prova della propria conformità ai clienti oppure 2) Sottoponendo a revisione i propri servizi nell'ambito delle valutazioni PCI DSS di ciascuno dei loro clienti, se non possono eseguire personalmente la valutazione PCI DSS. Per ulteriori informazioni, vedere la sezione che inizia con "Per i provider di servizi gestiti (MSP)" nella Parte 3 della sezione "Istruzioni e contenuto per il rapporto sulla conformità" di seguito.

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

Campionamento delle strutture aziendali e dei componenti di sistema

Il valutatore può scegliere alcuni campioni rappresentativi delle strutture aziendali e dei componenti di sistema per valutare la conformità ai requisiti PCI DSS. Questi campioni devono includere sia le strutture aziendali che i componenti di sistema, devono essere una selezione rappresentativa di tutti i tipi e le posizioni delle strutture aziendali nonché dei componenti di sistema e devono essere sufficientemente grandi per fornire al valutatore la garanzia che i controlli vengano implementati nel modo previsto.

Esempi di strutture aziendali sono uffici, negozi, esercenti in franchising e strutture aziendali con diverse sedi. Il campionamento deve includere i componenti di sistema per ogni struttura aziendale. Ad esempio, per ogni struttura aziendale, includere diversi sistemi operativi, funzioni e applicazioni validi per l'area sottoposta a revisione. All'interno di ogni struttura aziendale, il responsabile della revisione può scegliere server Sun con Apache WWW, server Windows con Oracle, sistemi di mainframe che eseguono applicazioni per l'elaborazione dei dati delle carte precedenti, server di trasferimento dei dati con HP-UX e server Linux con MYSQL. Se tutte le applicazioni vengono eseguite da un singolo sistema operativo

(ad esempio, Windows o Sun), il campione deve includere comunque diverse applicazioni (ad esempio, database server, server Web, server di trasferimento dati). *Vedere l'Appendice F: Revisioni PCI DSS – Determinazione dell'ambito e scelta dei campioni*.

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

- Se esistono processi PCI DSS standard obbligatori che ogni struttura deve seguire, il campione può essere di dimensioni inferiori a quello necessario in assenza di processi standard, per fornire una ragionevole garanzia che ogni struttura sia configurata in base al processo standard.
- Se esistono più tipi di processo standard (ad esempio, per diversi tipi di componenti di sistema o strutture), il campione deve essere sufficientemente grande per includere i componenti di sistema o le strutture protette con ogni tipo di processo.
- Se non esistono processi PCI DSS standard e ogni struttura è responsabile dei propri processi, la dimensione del campione deve essere maggiore per garantire che ogni struttura comprenda e implementi i requisiti PCI DSS in modo corretto.

Fare riferimento all'Appendice F: Revisioni PCI DSS – Determinazione dell'ambito e scelta dei campioni.

Controlli compensativi

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

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

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

Istruzioni e contenuto per il rapporto sulla conformità

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

Contenuto e formato del rapporto

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

1. Riepilogo esecutivo

Includere quanto segue:

- Descrivere le attività relative alla carta di pagamento svolte dall'entità, includendo:
  - Il loro ruolo nella gestione delle carte di pagamento, ossia come e perché memorizzano, elaborano e/o trasmettono dati dei titolari di carta

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

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

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

- Ambiente sottoposto a valutazione (ad esempio, punti di accesso Internet del client, rete aziendale interna, connessioni per elaborazione)
- Se la segmentazione di rete è in atto ed è stata utilizzata per ridurre l'ambito della revisione PCI DSS, illustrare brevemente la segmentazione e il modo in cui il valutatore ha convalidato l'efficacia della segmentazione
- Documentare e giustificare il campionamento utilizzato sia per le entità (negozi, strutture, ecc.) che per i componenti di sistema selezionati, includendo:
  - Popolazione totale
  - Numero campionato
  - Motivo del campione selezionato
  - Perché la dimensione del campione è sufficiente per consentire al valutatore di garantire con una ragionevole certezza che i controlli revisionati rappresentano i controlli in atto nell'intera entità
  - Descrivere posizioni o ambienti che memorizzano, elaborano o trasmettono i dati di titolari di carta ESCLUSI dall'ambito della revisione e il motivo per cui tali posizioni/ambienti sono stati esclusi
- Elencare tutte le entità di completa proprietà che richiedono la conformità agli standard PCI DSS e indicare se sono state revisionate separatamente o nell'ambito di questa valutazione
- Elencare tutte le entità internazionali che richiedono la conformità agli standard PCI DSS e indicare se sono state revisionate separatamente o nell'ambito di questa valutazione
- Elencare le LAN wireless e/o le applicazioni di pagamento wireless (ad esempio, terminali POS) connesse o che potrebbero influire sulla sicurezza dell'ambiente dei dati di titolari di carta e descrivere le misure di sicurezza in atto per questi ambienti wireless
- La versione del documento Requisiti PCI DSS e procedure di valutazione della sicurezza utilizzata per eseguire la valutazione
- Tempi di valutazione

3. Dettagli sull'ambiente sottoposto a revisione

In questa sezione, includere i seguenti dettagli:

- Diagramma di ciascuna parte del link di comunicazione, incluse LAN, WAN o Internet
- Descrizione dell'ambiente dei dati dei titolari di carta, ad esempio:
  - Documentare la trasmissione e l'elaborazione dei dati dei titolari di carta, inclusi i flussi di autorizzazione, acquisizione, contabilizzazione, rettifica e di altro tipo, come applicabile

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

4. Informazioni di contatto e data del rapporto

Includere:

- Informazioni di contatto per l'esercente o il provider di servizi e il valutatore
- Data del rapporto

5. Risultati delle scansioni trimestrali

- Riepilogare i risultati delle quattro scansioni trimestrali più recenti nel Riepilogo esecutivo nonché nei commenti del Requisito 11.2

Nota: non è necessario completare quattro scansioni trimestrali con esito positivo per la conformità iniziale agli standard PCI DSS, se il valutatore verifica che 1) il risultato della scansione più recente era positivo, 2) l'entità dispone di politiche e procedure documentate che richiedono l'esecuzione di ulteriori scansioni trimestrali e 3) ogni vulnerabilità rilevata nella scansione iniziale è stata corretta come dimostrato da una nuova scansione. Per gli anni successivi alla revisione PCI DSS iniziale, è necessario eseguire quattro scansioni trimestrali con esito positivo.

- La scansione deve coprire tutti gli indirizzi IP (Internet) accessibili esternamente dell'entità, in base alle *Procedure di scansione della sicurezza PCI DSS*

6. Risultati e osservazioni

- Riepilogare nel Riepilogo esecutivo i risultati che potrebbero non rientrare nel formato del modello del Rapporto sulla conformità standard.
- Tutti i valutatori *devono* utilizzare il modello Requisiti PCI DSS e procedure di valutazione della sicurezza dettagliate per fornire descrizioni e risultati dettagliati su ogni requisito e sottorequisito.
- Il valutatore *deve* esaminare e documentare tutti i controlli compensativi presi in considerazione per verificare che vi sia un controllo in atto.

  Vedere la sezione sui controlli compensativi riportata sopra e le appendici B e C per ulteriori dettagli sui "controlli compensativi".

Riconvalida dei problemi in attesa di soluzione

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

Conformità agli standard PCI DSS – Operazioni

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

Requisiti PCI DSS e procedure di valutazione della sicurezza dettagliate

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

- **Requisiti PCI DSS**: questa colonna definisce lo standard DSS (Data Security Standard) ed elenca i requisiti per la conformità agli standard PCI DSS; la conformità verrà convalidata in base a tali requisiti.
- **Procedure di test**: questa colonna mostra i processi che il valutatore deve seguire per confermare che i requisiti PCI DSS sono "presenti"
- **Presenti**: questa colonna deve essere utilizzata dal valutatore per fornire una breve descrizione dei controlli presenti, includendo i controlli in atto identificati dai controlli compensativi. Nota: questa colonna *non* deve essere utilizzata per gli elementi non ancora presenti o per i problemi in attesa di soluzione che verranno risolti in un secondo momento.
- **Non presente**: questa colonna deve essere utilizzata dal valutatore per fornire una breve descrizione dei controlli non presenti. Tenere presente che un rapporto non conforme non deve essere inviato a un marchio di pagamento o a un acquirente se non specificamente richiesto. Vedere le appendici D ed E: Attestati di conformità per ulteriori istruzioni sui rapporti di non conformità.
- **Data di scadenza/Commenti**: per i controlli "non presenti", il valutatore può includere una data di scadenza entro la quale è previsto che l'esercente o il provider di servizi implementi tali controlli. È possibile includere eventuali note o commenti aggiuntivi.

Sviluppo e gestione di una rete sicura

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

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

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, connessione dedicata 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.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
1.1 Stabilire standard di configurazione del firewall e del router che includano:	**1.1** Richiedere ed esaminare gli standard di configurazione del firewall e del router e altra documentazione specificata di seguito per verificare che tali standard siano completi. Completare quanto segue:			
1.1.1 Un processo formale per l'approvazione e il test di tutte le connessioni di rete e le modifiche apportate alla configurazione del firewall e del router	**1.1.1** Verificare la presenza di un processo formale per il test e l'approvazione di tutte le connessioni di rete e le modifiche apportate alla configurazione del firewall e del router.			
1.1.2 Un diagramma aggiornato della rete con tutte le connessioni ai dati di titolari di carta, comprese eventuali reti wireless	**1.1.2.a** Verificare la presenza di un diagramma di rete aggiornato (ad esempio, un diagramma che illustra il flusso dei dati di titolari di carta attraverso la rete) che documenti tutte le connessioni ai dati di titolari di carta, compresa qualsiasi rete wireless.			
	1.1.2.b Verificare che il diagramma sia aggiornato.			
1.1.3 I requisiti per un firewall per ogni connessione Internet e tra tutte le zone demilitarizzate (DMZ) e la zona della rete interna	**1.1.3** Verificare che gli standard di configurazione del firewall includano i requisiti per un firewall per ogni connessione Internet e tra la zona DMZ e la zona della rete interna. Verificare che il diagramma di rete aggiornato sia coerente con gli standard di configurazione del firewall.			
1.1.4 Una descrizione di gruppi, ruoli e responsabilità per la gestione logica dei componenti della rete	**1.1.4** Verificare che gli standard di configurazione del firewall e del router includano una descrizione dei gruppi, dei ruoli e delle responsabilità per la gestione logica dei componenti della rete.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
1.1.5 La documentazione e la giustificazione aziendale per l'uso di tutti i servizi, i protocolli e le porte consentite, inclusa la documentazione delle funzioni di sicurezza implementate per i protocolli considerati non sicuri	**1.1.5.a** Verificare che gli standard di configurazione del firewall e del router includano un elenco documentato di servizi, protocolli e porte necessari per l'azienda, ad esempio i protocolli HTTP (Hypertext Transfer Protocol) e SSL (Secure Sockets Layer), SSH (Secure Shell) e VPN (Virtual Private Network).			
	1.1.5.b Identificare i servizi, i protocolli e le porte consentite non sicuri, verificare la loro necessità e che le funzioni di sicurezza siano documentate e implementate esaminando gli standard di configurazione del firewall e del router e le impostazioni per ogni servizio. Un esempio di servizio, protocollo o porta non sicuro è l'FTP, che trasferisce le credenziali dell'utente in testo in chiaro.			
1.1.6 Una revisione dei set di regole del firewall e del router almeno ogni sei mesi	**1.1.6.a** Verificare che gli standard di configurazione del firewall e del router richiedano una revisione dei set di regole del firewall e del router almeno ogni sei mesi.			
	1.1.6.b Richiedere ed esaminare la documentazione per verificare che i set di regole vengano revisionati almeno ogni sei mesi.			
1.2 Creare una configurazione del firewall che limiti le connessioni tra le reti non attendibili e qualsiasi componente di sistema nell'ambiente dei dati di titolari di carta.	**1.2** Esaminare la configurazione del firewall e del router per verificare che le connessioni tra le reti non attendibili e i componenti di sistema nell'ambiente dei dati di titolari di carta siano limitate, nel modo illustrato di seguito:			
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.				
1.2.1 Limitare il traffico in entrata e in uscita a quello indispensabile per l'ambiente dei dati dei titolari di carta.	**1.2.1.a** Verificare che il traffico in entrata e in uscita sia limitato a quello necessario per l'ambiente dei dati di titolari di carta e che le restrizioni siano documentate.			
	1.2.1.b Verificare che il resto del traffico in entrata e in uscita venga negato in modo specifico, ad esempio utilizzando un comando esplicito "deny all" o un comando implicito di negazione dopo un'istruzione "allow".			

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

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
1.3.6 Implementare un controllo efficiente, anche noto come "dynamic packet filtering" (ossia che consente solo alle connessioni già "stabilite" di accedere alla rete).	**1.3.6** Verificare che il firewall esegua un controllo efficiente (dynamic packet filtering). [Solo le connessioni stabilite sono autorizzate e solo se associate a una sessione stabilita precedentemente (eseguire una scansione su tutte le porte TCP con il set di bit "syn reset" o "syn ack"; una risposta implica che i pacchetti sono autorizzati anche se non fanno parte di una sessione stabilita precedentemente).]			
1.3.7 Posizionare il database in una zona di rete interna, separata dalla zona DMZ.	**1.3.7** Verificare che il database sia posizionato in una zona di rete interna, separata dalla zona DMZ.			
1.3.8 Implementare un IP-masquerading per evitare che gli indirizzi interni vengano tradotti e resi noti su Internet, tramite lo spazio indirizzi RFC 1918. Utilizzare tecnologie NAT (Network Address Translation), ad esempio PAT (Port Address Ttranslation).	**1.3.8** Per il campione di componenti firewall e router, verificare che la tecnologia NAT o altre tecnologie che utilizzano lo spazio indirizzi RFC 1918 siano utilizzate per limitare la trasmissione degli indirizzi IP dalla rete interna a Internet (IP-masquerading).			
1.4 Installare firewall personali (software) su tutti i computer portatili e i computer di proprietà dei dipendenti con connettività diretta a Internet (ad esempio, laptop utilizzati dai dipendenti), che vengono utilizzati per accedere alla rete aziendale.	**1.4.a** Verificare l'installazione e l'attivazione di firewall personali (software) su tutti i computer portatili e i computer di proprietà dei dipendenti con connettività diretta a Internet (ad esempio, laptop utilizzati dai dipendenti), che vengono utilizzati per accedere alla rete aziendale.			
	1.4.b Verificare che il firewall personale (software) sia configurato dall'organizzazione in base a standard specifici e che gli utenti di computer portatili non possano modificarlo.			

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'azienda) utilizzano spesso password e altre impostazioni predefinite dei fornitori per accedere in modo improprio ai sistemi. Queste password e impostazioni sono ben note alle comunità di hacker e vengono determinate facilmente tramite informazioni pubbliche.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
2.1 Modificare sempre le impostazioni predefinite del fornitore **prima** di installare un sistema su una rete, ad esempio, password, stringhe di comunità SNMP (Simple Network Management Protocol) ed eliminazione di account non necessari.	**2.1** Scegliere un campione di componenti di sistema, server critici e punti di accesso wireless, quindi tentare l'accesso (con l'aiuto dell'amministratore di sistema) ai dispositivi utilizzando account e password predefiniti del fornitore per verificare che siano stati modificati. Per trovare account/password del fornitore, consultare i manuali e le fonti su Internet.			
2.1.1 Per gli ambienti wireless connessi all'ambiente dei dati di titolari di carta o che trasmettono tali dati, modificare le impostazioni predefinite del fornitore wireless, incluse, senza limitazione, chiavi di cifratura wireless predefinite, password e stringhe di comunità SNMP. Accertarsi che le impostazioni di sicurezza dei dispositivi wireless consentano l'uso della tecnologia di cifratura avanzata per l'autenticazione e la trasmissione.	**2.1.1** Verificare quanto segue relativamente alle impostazioni predefinite del fornitore per gli ambienti wireless e garantire che tutte le reti wireless implementino meccanismi di cifratura avanzata (ad esempio, AES): ▪ Le chiavi di cifratura predefinite sono state modificate al momento dell'installazione e vengono modificate ogni volta che un utente a conoscenza delle chiavi lascia l'azienda o cambia sede. ▪ Le stringhe di comunità SNMP predefinite sui dispositivi wireless sono state modificate. ▪ Le password/passphrase predefinite sui punti di accesso sono state modificate. ▪ Il firmware sui dispositivi wireless è aggiornato per supportare la cifratura avanzata per l'autenticazione e la trasmissione su reti wireless (ad esempio, WPA/WPA2). ▪ Altre impostazioni predefinite del fornitore wireless relative alla sicurezza, se applicabili.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
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.	**2.2.a** Esaminare gli standard di configurazione del sistema dell'organizzazione per tutti i tipi di componente di sistema e verificare che tali standard siano coerenti con gli standard di hardening accettati dal settore, ad esempio da SANS (SysAdmin Audit Network Security), NIST (National Institute of Standards Technology) e CIS (Center for Internet Security).			
	2.2.b Verificare che gli standard di configurazione del sistema includano ogni elemento riportato di seguito (nelle sezioni 2.2.1 – 2.2.4).			
	2.2.c Verificare che gli standard di configurazione del sistema vengano applicati quando si configurano nuovi sistemi.			
2.2.1 Implementare una sola funzione principale per server.	**2.2.1** Per un campione di componenti di sistema, verificare che sia stata implementata una sola funzione principale per server. Ad esempio, server Web, database server e DNS devono essere implementati su server separati.			
2.2.2 Disattivare tutti i servizi e i protocolli non necessari e non protetti (che non sono strettamente necessari per eseguire la funzione specifica del dispositivo).	**2.2.2** Per un campione di componenti di sistema, ispezionare servizi di sistema, daemon e protocolli attivati. Verificare che i servizi o i protocolli non necessari o non protetti non siano attivati o che siano giustificati e documentati per un uso appropriato del servizio. Ad esempio, il servizio FTP non è utilizzato o è cifrato tramite SSH o altra tecnologia.			
2.2.3 Configurare i parametri di sicurezza del sistema per evitare un uso improprio.	**2.2.3.a** Consultare gli amministratori del sistema e/o i responsabili della sicurezza per verificare che conoscano le impostazioni dei parametri della sicurezza comuni per i componenti di sistema.			
	2.2.3.b Verificare che le impostazioni dei parametri di sicurezza comuni siano incluse negli standard di configurazione del sistema.			
	2.2.3.c Per un campione di componenti di sistema, verificare che i parametri di sicurezza comuni siano impostati correttamente.			
2.2.4 Rimuovere tutta la funzionalità non necessaria, ad esempio script, driver, funzioni, sottosistemi, file system e server Web non utilizzati.	**2.2.4** Per un campione di componenti del sistema, verificare che tutta la funzionalità non necessaria (ad esempio, script, driver, funzioni, sottosistemi, file system, eccetera) sia rimossa. Verificare che le funzioni attivate siano documentate e supportino la configurazione sicura e che solo le funzionalità documentate siano presenti sui computer appartenenti al campione.			

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

Protezione dei dati di titolari di carta

Requisito 3: Proteggere i dati di titolari di carta memorizzati

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

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

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
3.1 Limitare il più possibile la memorizzazione dei dati di titolari di carta. Sviluppare una politica per la conservazione e l'eliminazione dei dati. Limitare la quantità di dati memorizzati e il tempo di conservazione in base alle esigenze aziendali, legali e/o legislative, come documentato nella politica per la conservazione dei dati.	**3.1** Richiedere ed esaminare le politiche e le procedure aziendali per la conservazione e l'eliminazione dei dati ed effettuare quanto segue: ▪ Verificare che le politiche e le procedure includano requisiti legali, legislativi e aziendali per la conservazione dei dati, inclusi requisiti specifici per la conservazione dei dati di titolari di carta (ad esempio, è necessario conservare i dati di titolari di carta per un periodo X per scopi aziendali Y). ▪ Verificare che le politiche e le procedure includano disposizioni per l'eliminazione dei dati non più necessari per scopi legali, legislativi o aziendali, inclusa l'eliminazione dei dati di titolari di carta. ▪ Verificare che le politiche e le procedure includano disposizioni per ogni tipo di memorizzazione dei dati di titolari di carta. ▪ Verificare che le politiche e le procedure includano un processo programmatico (automatico) per rimuovere, almeno su base trimestrale, i dati di titolari di carta memorizzati che superano i requisiti di conservazione aziendali o, in alternativa, i requisiti per una revisione, condotta almeno su base trimestrale, per verificare che i dati di titolari di carta non superano i requisiti aziendali per la conservazione.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
3.2 Non memorizzare dati sensibili di autenticazione dopo l'autorizzazione (anche se crittografati). I dati sensibili di autenticazione includono i dati citati nei seguenti Requisiti da 3.2.1 a 3.2.3:	**3.2** Se sono stati ricevuti ed eliminati dati sensibili di autenticazione, richiedere ed esaminare i processi per l'eliminazione dei dati per verificare che i dati non siano recuperabili. Per ogni elemento di dati sensibili di autenticazione di seguito, effettuare la seguente procedura:			
3.2.1 Non memorizzare l'intero contenuto delle tracce della striscia magnetica (presente sul retro della carta, contenuto in un chip o in altro luogo). Questi dati sono denominati anche traccia completa, traccia, traccia 1, traccia 2 e dati di striscia magnetica. *Nota: nel normale svolgimento delle attività, è possibile che sia necessario conservare i seguenti elementi di dati della striscia magnetica:* ▪ *Nome del titolare della carta* ▪ *PAN (Primary Account Number)* ▪ *Data di scadenza* ▪ *Codice di servizio* *Per ridurre al minimo il rischio, memorizzare solo gli elementi di dati necessari.* *Nota: vedere il documento* PCI DSS Glossario, abbreviazioni e acronimi *per ulteriori informazioni.*	**3.2.1** Per un campione di componenti di sistema, esaminare quanto riportato di seguito e verificare che l'intero contenuto delle tracce della striscia magnetica sul retro della carta non venga memorizzato in nessun caso: ▪ 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			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
3.2.2 Non memorizzare il codice o il valore di validazione della carta (numero di tre o quattro cifre stampato sulla parte anteriore o posteriore della carta di pagamento) utilizzato per verificare le transazioni con carta non presente. *Nota: vedere il documento* PCI DSS Glossario, abbreviazioni e acronimi *per ulteriori informazioni.*	**3.2.2** Per un campione di componenti di sistema, verificare che il codice o il valore di verifica della carta a tre o quattro cifre impresso sulla parte anteriore della carta o nel riquadro della firma (dati CVV2, CVC2, CID, CAV2) non venga memorizzato in nessun caso: ▪ 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			
3.2.3 Non memorizzare il numero di identificazione personale (PIN) o il blocco PIN cifrato.	**3.2.3** Per un campione di componenti di sistema, esaminare quanto riportato di seguito e verificare che i PIN e i blocchi PIN cifrati non vengano memorizzati in nessun caso: ▪ 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			
3.3 Mascherare il PAN quando visualizzato (non devono essere visibili più di sei cifre all'inizio e quattro cifre alla fine) *Note:* ▪ *Questo requisito non si applica ai dipendenti e ad altre parti che hanno l'esigenza aziendale legittima di visualizzare il numero PAN intero.* ▪ *Questo requisito non sostituisce i requisiti più rigorosi per la visualizzazione dei dati di titolari di carta, ad esempio per ricevute di punti di vendita (POS).*	**3.3** Richiedere ed esaminare le politiche scritte e le visualizzazioni del numero PAN (ad esempio, su schermo e in ricevute cartacee) per verificare che i numeri PAN (Primary Account Number) siano mascherati durante la visualizzazione dai dati di titolari di carta, ad eccezione dei casi in cui occorre visualizzare il numero PAN completo per un'esigenza aziendale legittima.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
3.4 Rendere illeggibile almeno il numero PAN ovunque sia memorizzato (inclusi i dati su supporti digitali portatili, supporti di backup, registri) utilizzando uno dei seguenti approcci: ▪ Hash one-way basati su crittografia avanzata ▪ Troncatura ▪ Token e pad indicizzati (i pad devono essere custoditi in un luogo sicuro) ▪ Crittografia avanzata con relativi processi e procedure di gestione delle chiavi Il PAN è l'informazione MINIMA sull'account che deve essere resa illeggibile. *Note:* ▪ *In caso di problemi nel rendere illeggibile il numero PAN, consultare l'*Appendice B: Controlli compensativi. ▪ *La "crittografia avanzata" viene definita nel documento* PCI DSS Glossario, abbreviazioni e acronimi.	**3.4.a** Richiedere ed 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). Verificare che il numero PAN sia stato reso illeggibile tramite uno dei seguenti metodi: ▪ 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			
	3.4.b Esaminare diverse tabelle o file del campione di repository dei dati per verificare che il numero PAN sia illeggibile (cioè, non memorizzato come testo semplice).			
	3.4.c Esaminare un campione dei supporti rimovibili (ad esempio, nastri di backup) per confermare che il numero PAN sia illeggibile.			
	3.4.d Esaminare un campione di log di audit per confermare che il PAN è stato modificato o rimosso dai registri.			
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 indipendente dai meccanismi di controllo dell'accesso al sistema operativo nativo (ad esempio, non utilizzando database di account	**3.4.1.a** Se viene utilizzata la cifratura del disco, verificare che l'accesso logico a file system cifrati venga implementato tramite un meccanismo separato dal meccanismo dei sistemi operativi nativi (ad esempio, non utilizzando i database di account utente locali).			
	3.4.1.b 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	Presente	Non presente	Data di scadenza/ Commenti
utente locali). Le chiavi di decifratura non devono essere associate agli account utente.	**3.4.1.c** Verificare che i dati di titolari di carta su supporti rimovibili siano cifrati in ogni posizione di memorizzazione. *Nota: spesso, la cifratura del disco non può cifrare i dati su supporti rimovibili, pertanto, i dati memorizzati su tali supporti devono essere cifrati separatamente.*			
3.5 Proteggere le chiavi di crittografia utilizzate per la cifratura dei dati di titolari di carta da divulgazione e uso improprio:	**3.5** Verificare i processi per proteggere le chiavi utilizzati per la cifratura dei dati di titolari di carta da divulgazione e uso improprio effettuando quanto segue:			
3.5.1 Limitare l'accesso alle chiavi di crittografia al minor numero possibile di persone necessarie.	**3.5.1** Esaminare gli elenchi di accesso utente per verificare che l'accesso alle chiavi sia consentito a un numero limitato di persone.			
3.5.2 Memorizzare le chiavi di crittografia in modo sicuro nel minor numero possibile di posizioni e moduli.	**3.5.2** Esaminare i file di configurazione dei sistemi per verificare che le chiavi siano memorizzate in un formato cifrato e che le chiavi di crittografia principali siano memorizzate separatamente dalle chiavi di crittografia dei dati.			
3.6 Documentare e implementare completamente tutti i processi e le procedure di gestione delle chiavi di crittografia utilizzate per la cifratura dei dati di titolari di carta, incluso quanto segue:	**3.6.a** Verificare l'esistenza delle procedure di gestione delle chiavi per le chiavi utilizzate per la cifratura dei dati di titolari di carta. *Nota: sono disponibili numerosi standard di settore per la gestione delle chiavi, tra cui il sito del NIST all'indirizzo http://csrc.nist.gov.*			
	3.6.b Solo per provider di servizi: se il provider di servizi condivide le chiavi con i propri clienti per la trasmissione dei dati di titolari di carta, verificare che il provider fornisca ai clienti istruzioni dettagliate per la memorizzazione e la modifica sicura delle chiavi dei clienti (utilizzate per trasmettere i dati tra i clienti e il provider di servizi).			
	3.6.c Esaminare le procedure di gestione delle chiavi ed effettuare quanto segue:			
3.6.1 Generazione di chiavi di crittografia avanzata	**3.6.1** Verificare che siano implementate procedure di gestione delle chiavi per richiedere la generazione di chiavi avanzate.			
3.6.2 Distribuzione di chiavi di crittografia sicure	**3.6.2** Verificare che siano implementate procedure di gestione delle chiavi per richiedere la distribuzione di chiavi sicure.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
3.6.3 Memorizzazione di chiavi di crittografia sicure	**3.6.3** Verificare che siano implementate procedure di gestione delle chiavi per richiedere la memorizzazione di chiavi sicure.			
3.6.4 Modifica periodica di chiavi di crittografia ▪ In base a quanto richiesto e consigliato dall'applicazione associata (ad esempio, re-keying), preferibilmente in modo automatico ▪ Almeno una volta all'anno	**3.6.4** Verificare che siano implementate procedure di gestione delle chiavi per richiedere la modifica periodica delle chiavi almeno una volta all'anno.			
3.6.5 Ritiro o sostituzione di chiavi di crittografia precedentemente o potenzialmente compromesse	**3.6.5.a** Verificare che siano implementate procedure di gestione delle chiavi per richiedere il ritiro delle chiavi obsolete (ad esempio: archiviazione, distruzione e revoca, come applicabile).			
	3.6.5.b Verificare che siano implementate procedure di gestione delle chiavi per richiedere la sostituzione delle chiavi potenzialmente o effettivamente compromesse.			
3.6.6 Uso della procedura "split knowledge" e definizione del controllo duale delle chiavi	**3.6.6** Verificare che siano implementate procedure di gestione delle chiavi per richiedere l'uso della procedura "split knowledge" e della definizione del controllo duale delle chiavi (ad esempio, in modo che per ricostruire l'intera chiave siano necessarie due o più persone, ciascuna a conoscenza di una sola parte della chiave).			
3.6.7 Prevenzione di tentativi di sostituzione non autorizzata delle chiavi di crittografia	**3.6.7** Verificare che siano implementate procedure di gestione delle chiavi per richiedere la prevenzione dai tentavi di sostituzione non autorizzata delle chiavi.			
3.6.8 Obbligo per i custodi delle chiavi di crittografia di firmare una dichiarazione in cui accettano e confermano di conoscere le proprie responsabilità.	**3.6.8** Verificare che siano implementate procedure di gestione delle chiavi per richiedere ai custodi delle chiavi di firmare un modulo in cui accettano e confermano la conoscenza delle proprie responsabilità.			

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

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

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
4.1 Utilizzare protocolli di crittografia e sicurezza avanzati, quali SSL/TLS o IPSEC, per proteggere i dati sensibili di titolari di carta durante la trasmissione su reti pubbliche e aperte. *Esempi di rete pubbliche e aperte nell'ambito della valutazione PCI DSS sono:* ▪ *Internet* ▪ *Tecnologie wireless* ▪ *Comunicazioni GSM (Global System for Mobile)* ▪ *GPRS (General Packet Radio Service)*	**4.1.a** Verificare l'uso della cifratura (ad esempio, SSL/TLS o IPSEC) ogni volta che i dati di titolari di carta vengono trasmessi o ricevuti su reti pubbliche e aperte. ▪ Verificare che la cifratura avanzata venga utilizzata durante la trasmissione dei dati. ▪ Per le implementazioni SSL: – Verificare che il server supporti le versioni con patch più recenti. – Verificare che HTTPS venga visualizzato come parte dell'URL del browser. – Verificare che nessuno dei dati di titolari di carta sia richiesto quando HTTPS non viene visualizzato nell'URL. ▪ Selezionare un campione di transazioni al momento della ricezione e osservare l'esecuzione delle transazioni per accertarsi che i dati di titolari di carta siano cifrati durante la transazione. ▪ Verificare che vengano accettati solo certificati/chiavi SSL/TLS affidabili. ▪ Verificare che sia implementato il livello di cifratura corretto per la metodologia di cifratura in uso. Controllare suggerimenti/pratiche consigliate del fornitore.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
4.1.1 Garantire che le reti wireless che trasmettono i dati di titolari di carta o connesse all'ambiente dei dati di titolari di carta utilizzano le pratiche di settore consigliate (ad esempio, IEEE 802.11i) per implementare la cifratura avanzata per l'autenticazione e la trasmissione. ▪ *Per le nuove implementazioni wireless, non è consentito implementare la tecnologia WEP dopo il 31 marzo 2009.* ▪ *Per le implementazioni wireless correnti, non è consentito utilizzare la tecnologia WEP dopo il 30 giugno 2010.*	**4.1.1** Per le reti wireless che trasmettono i dati di titolari di carta o connesse all'ambiente dei dati di titolari di carta, verificare che vengano utilizzate le pratiche di settore consigliate (ad esempio, IEEE 802.11i) per implementare la cifratura avanzata per l'autenticazione e la trasmissione.			
4.2 Non inviare mai i numeri PAN non cifrati mediante tecnologie di messaggistica degli utenti finali (ad esempio, e-mail, messaggistica istantanea, chat).	**4.2.a** Verificare che venga eseguita la crittografia avanzata sui dati di titolari di carta quando inviati tramite tecnologie di messaggistica dell'utente finale.			
	4.2.b Verificare l'esistenza di una politica in cui viene stabilito che i numeri PAN non cifrati non devono essere inviati tramite tecnologie di messaggistica dell'utente finale.			

Manutenzione di un programma per la gestione delle vulnerabilità

Requisito 5: Utilizzare e aggiornare regolarmente 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.

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

Requisito 6: Sviluppare e gestire sistemi e applicazioni protette

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

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

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
6.1 Garantire che su tutti i componenti di sistema e il software siano installate le patch di sicurezza più recenti. Installare patch di sicurezza critiche entro un mese dal rilascio.	**6.1.a** Per un campione di componenti di sistema e il software correlato, confrontare l'elenco delle patch di sicurezza installate su ogni sistema con l'elenco delle patch di sicurezza del fornitore più recenti, per verificare che siano installate le patch del fornitore correnti.			
Nota: è possibile adottare un approccio basato su rischio per dare priorità alle installazioni delle patch. Ad esempio, dare la massima priorità all'infrastruttura critica (dispositivi e sistemi rivolti al pubblico e database), rispetto ai dispositivi interni meno importanti, per garantire che le patch necessarie vengano installate sui sistemi e sui dispositivi ad alta priorità entro un mese e su altri dispositivi e sistemi meno importanti entro tre mesi.	**6.1.b** Esaminare la politica per l'installazione della patch di sicurezza per verificare che venga richiesta l'installazione di tutte le nuove patch di sicurezza critiche entro un mese.			
6.2 Stabilire un processo per identificare le vulnerabilità della sicurezza recentemente rilevate (ad esempio, attraverso un abbonamento a servizi di notifica gratuiti disponibili in Internet). Aggiornare gli standard di configurazione secondo il Requisito 2.2 PCI DSS per risolvere nuovi problemi di vulnerabilità.	**6.2.a** Consultare il personale responsabile per verificare che i processi per identificare le nuove vulnerabilità della sicurezza siano stati implementati.			
	6.2.b Verificare che i processi per identificare le nuove vulnerabilità della sicurezza includano l'uso di risorse esterne per la vulnerabilità della sicurezza e l'aggiornamento degli standard di configurazione del sistema esaminati nel Requisito 2.2 nel momento in cui vengono rilevati problemi di vulnerabilità.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
6.3 Sviluppare applicazioni software in base agli standard PCI DSS (ad esempio, autenticazione e registrazione sicure) e alle pratiche di settore consigliate, quindi incorporare la protezione delle informazioni nell'intero ciclo di sviluppo del software. Questi processi devono includere quanto segue:	**6.3.a** Richiedere ed esaminare i processi di sviluppo del software scritti per verificare che i processi siano basati sugli standard del settore, che la protezione sia inclusa nell'intero ciclo e che le applicazioni software siano sviluppate secondo gli standard PCI DSS.			
	6.3.b Sulla base dell'analisi dei processi di sviluppo del software scritti, dei colloqui con gli sviluppatori del software e dell'esame dei dati rilevanti (documentazione della configurazione di rete, dati di produzione e test, eccetera), verificare che:			
6.3.1 Tutte le patch di sicurezza e le modifiche di configurazione del sistema e del software vengono sottoposte a test prima di essere distribuite, incluso, senza limitazione, quanto segue:	**6.3.1** Tutte le modifiche (incluse le patch) vengano sottoposte a test prima del rilascio in produzione.			
6.3.1.1 Convalida di tutto l'input (per prevenire cross-site scripting, injection flaw, esecuzione di file pericolosi, eccetera)	**6.3.1.1** Convalida di tutto l'input (per prevenire cross-site scripting, injection flaw, esecuzione di file pericolosi, ecc.)			
6.3.1.2 Convalida del processo di gestione degli errori appropriato	**6.3.1.2** Convalida del processo di gestione degli errori appropriato			
6.3.1.3 Convalida del processo di memorizzazione di dati crittografici sicuro	**6.3.1.3** Convalida del processo di memorizzazione di dati crittografici sicuro			
6.3.1.4 Convalida di comunicazioni sicure	**6.3.1.4** Convalida di comunicazioni sicure			
6.3.1.5 Convalida di un processo di controllo dell'accesso basato su ruolo (RBAC, Role-Based Access Control) appropriato	**6.3.1.5** Convalida di un processo di controllo dell'accesso basato su ruoli (RBAC, Role-Based Access Control) appropriato			
6.3.2 Separazione degli ambienti di sviluppo/test dagli ambienti di produzione.	**6.3.2** Gli ambienti di sviluppo/test sono separati dagli ambienti di produzione; sono in atto metodi di controllo dell'accesso per garantire la separazione di tali ambienti.			
6.3.3 Separazione delle responsabilità tra ambienti di sviluppo/test e ambienti di produzione.	**6.3.3** Esiste una separazione di responsabilità tra il personale assegnato agli ambienti di sviluppo/test e il personale assegnato all'ambiente di produzione.			
6.3.4 I dati di produzione (PAN attivi) sono esclusi dalle attività di test o sviluppo	**6.3.4** I dati di produzione (PAN attivi) sono esclusi dalle attività di test e sviluppo oppure vengono modificati prima dell'uso.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
6.3.5 Dati e account di test vengono rimossi prima dell'attivazione dei sistemi di produzione	**6.3.5** I dati e gli account di test vengono rimossi prima dell'attivazione di un sistema di produzione.			
6.3.6 Account, ID utente e password di applicazioni personalizzate vengono rimossi prima dell'attivazione o della distribuzione di tali applicazioni ai clienti	**6.3.6** Gli account, gli ID utente e/o le password delle applicazioni personalizzate vengono rimossi prima della produzione o della distribuzione di tali applicazioni ai clienti.			
6.3.7 Il codice personalizzato viene analizzato prima del rilascio in produzione o della distribuzione ai clienti per identificare eventuali vulnerabilità della codifica. *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 richiesto nel Requisito 6.3 PCI DSS. Le analisi del codice possono essere condotte da personale interno preparato o da terze parti. Le applicazioni Web sono anche soggette a controlli aggiuntivi, se sono pubbliche, per risolvere le minacce costanti e le vulnerabilità dopo l'implementazione, secondo quanto definito nel Requisito 6.6 PCI DSS.*	**6.3.7.a** Ottenere ed esaminare le politiche per confermare che tutte le modifiche del codice di applicazioni personalizzate per le *applicazioni interne* devono essere analizzate (tramite processi manuali o automatici), come segue: ▪ Le modifiche del codice vengono esaminate da singoli utenti diversi dall'autore del codice originario e da utenti esperti di tecniche di analisi del codice e pratiche di codifica sicure. ▪ Le correzioni appropriate vengono implementate prima del rilascio. ▪ I risultati dell'analisi del codice vengono esaminati e approvati dal management prima del rilascio.			
	6.3.7.b Richiedere ed esaminare le politiche per confermare che tutte le modifiche del codice di applicazioni personalizzate per le *applicazioni Web* devono essere analizzate (tramite processi manuali o automatici), come segue: ▪ 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 come *Open Web Security Project Guide* (vedere il Requisito 6.5 PCI DSS). ▪ Le correzioni appropriate vengono implementate prima del rilascio. ▪ I risultati dell'analisi del codice vengono esaminati e approvati dal management prima del rilascio.			
	6.3.7.c Selezionare un campione di modifiche di applicazioni personalizzate recenti e verificare che il codice dell'applicazione venga analizzato in base ai punti 6.3.7a e 6.3.7.b precedenti.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
6.4 Seguire le procedure di controllo delle modifiche per tutte le modifiche da apportare ai componenti di sistema. Le procedure devono includere quanto segue:	**6.4.a** Richiedere ed esaminare le procedure di controllo delle modifiche aziendali correlate all'implementazione di patch di sicurezza e di modifiche del software, quindi verificare che le procedure richiedano quanto previsto ai punti 6.4.1 – 6.4.4 riportati di seguito.			
	6.4.b Per un campione di componenti di sistema e recenti modifiche/patch di sicurezza, tenere traccia delle modifiche in base alla documentazione correlata. Per ogni modifica esaminata, effettuare quanto segue:			
6.4.1 Documentazione dell'impatto	**6.4.1** Verificare che la documentazione dell'impatto sul cliente sia inclusa nella documentazione di controllo delle modifiche per ciascuna modifica inserita nel campione.			
6.4.2 Approvazione del management delle parti interessate	**6.4.2** Verificare che il management delle parti appropriate abbia approvato ogni modifica inserita nel campione.			
6.4.3 Test della funzionalità operativa	**6.4.3** Verificare che venga eseguito il test della funzionalità operativa per ciascuna modifica inserita nel campione.			
6.4.4 Procedure di back-out	**6.4.4** Verificare che siano pronte procedure di back-out per ogni modifica inserita nel campione.			
6.5 Sviluppare tutte le applicazioni Web (interne, esterne e con accesso amministrativo all'applicazione tramite Web) in base alle linee guida di codifica sicura, quali *Open Web Application Security Project Guide.* Prevenire possibili vulnerabilità del codice comuni nei processi di sviluppo del software, incluso quanto segue: *Nota: le vulnerabilità elencate dal punto 6.5.1 al punto 6.5.10 erano presenti nella guida OWASP al momento della pubblicazione degli standard PCI DSS v1.2. Tuttavia, in caso di aggiornamento della guida OWASP, è necessario utilizzare la versione più recente per questi requisiti.*	**6.5.a** Richiedere ed esaminare i processi di sviluppo del software per ogni applicazione basata sul Web. Verificare che i processi richiedano la formazione su tecniche di codifica sicure per gli sviluppatori e siano basati sulle istruzioni fornite nella guida OWASP (http://www.owasp.org).			
	6.5.b Consultare alcuni sviluppatori e verificarne la preparazione relativamente alle tecniche di codifica sicura.			
	6.5.c Verificare che siano in atto processi per garantire che le applicazioni Web non siano vulnerabili alle seguenti minacce:			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
6.5.1 XSS (Cross-Site Scripting)	**6.5.1** Cross-site scripting (XSS) (convalidare tutti i parametri prima dell'inclusione).			
6.5.2 Injection flaw, in particolare SQL injection. Considerare, inoltre, LDAP e Xpath injection flaw, nonché altri tipi di injection flaw.	**6.5.2** Injection flaw, in particolare SQL injection (convalidare l'input per verificare che i dati dell'utente non possono modificare il significato di comandi e query).			
6.5.3 Esecuzione di file pericolosi	**6.5.3** Esecuzione di file pericolosi (convalidare l'input per verificare che l'applicazione non accetta nomi file o file di utenti).			
6.5.4 Riferimenti a oggetti diretti non sicuri	**6.5.4** Riferimenti a oggetti diretti non sicuri (non fornire riferimenti a oggetti interni a utenti).			
6.5.5 Cross-site request forgery (CSRF)	**6.5.5** Cross-site request forgery (CSRF) (non considerare sicure credenziali di autorizzazione e token inviati automaticamente dai browser).			
6.5.6 Perdita di informazioni e gestione degli errori non appropriata	**6.5.6** Perdita di informazioni e gestione degli errori non appropriata (non perdere informazioni mediante messaggi di errore o altri mezzi).			
6.5.7 Violazione dell'autenticazione e gestione delle sessioni	**6.5.7** Violazione della gestione delle autenticazioni e delle sessioni (autenticare in modo corretto gli utenti e proteggere le credenziali degli account e i token di sessione).			
6.5.8 Memorizzazione crittografica non sicura	**6.5.8** Memorizzazione crittografica non sicura (evitare errori di crittografia).			
6.5.9 Comunicazioni non sicure	**6.5.9** Comunicazioni non sicure (cifrare in modo appropriato tutte le comunicazioni autenticate e riservate).			
6.5.10 Mancata limitazione dell'accesso URL	**6.5.10** Mancata limitazione dell'accesso URL (applicare in modo coerente il controllo dell'accesso a livello di presentazione e business logic per tutti gli URL).			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
6.6 Per le applicazioni Web rivolte al pubblico, assicurare una protezione costante da nuove minacce e vulnerabilità e garantire che queste applicazioni siano protette da attacchi noti mediante *uno* dei seguenti metodi: ▪ Analisi delle applicazioni Web rivolte al pubblico tramite strumenti o metodi di valutazione della sicurezza delle applicazioni manuali o automatici, almeno una volta all'anno e dopo ogni modifica ▪ Installazione di un firewall per applicazioni Web davanti alle applicazioni Web rivolte al pubblico	**6.6** Per le applicazioni Web *rivolte al pubblico* , garantire che *una* delle seguenti misure di protezione sia in atto: ▪ Verificare che le applicazioni Web rivolte al pubblico vengano analizzate (tramite strumenti o metodi di valutazione della sicurezza manuali o automatici), come descritto di seguito: – Almeno una volta all'anno – Dopo ogni modifica – Da un'organizzazione specializzata in sicurezza delle applicazioni – Che tutte le vulnerabilità vengano corrette – Che l'applicazione venga nuovamente valutata dopo le correzioni ▪ Verificare che un firewall per applicazioni Web sia presente davanti alle applicazioni Web rivolte al pubblico per rilevare ed evitare attacchi basati su Web. *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.*			

Implementazione di rigide misure di controllo dell'accesso

Requisito 7: Limitare l'accesso ai dati di titolari di cartasolo 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 intende situazioni in cui vengono concessi diritti di accesso solo alla quantità minima di dati e privilegi necessari per svolgere una mansione.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
7.1 Limitare l'accesso ai componenti di sistema e ai dati di titolari di carta solo alle persone per le cui mansioni è realmente necessario. Le limitazioni di accesso devono includere quanto segue:	**7.1** Richiedere ed esaminare la politica scritta per il controllo dei dati e verificare che tale politica comprenda quanto segue:			
7.1.1 Limitazione dei diritti di accesso a ID utente privilegiati alla quantità minima necessaria per le responsabilità di ruolo	**7.1.1** Confermare che i diritti di accesso per gli ID utente privilegiati siano limitati alla quantità minima necessaria per svolgere le responsabilità del ruolo.			
7.1.2 Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale	**7.1.2** Confermare che i privilegi vengono assegnati a utenti singoli in base alla classificazione e alla funzione del relativo ruolo (anche noto come controllo dell'accesso basato su ruolo).			
7.1.3 Richiesta di un modulo di autorizzazione firmato dal management che specifica i privilegi necessari	**7.1.3** Confermare che venga richiesto un modulo di autorizzazione per tutti gli accessi, che specifica i privilegi necessari e che deve essere firmato dal management.			
7.1.4 Implementazione di un sistema di controllo dell'accesso automatico	**7.1.4** Confermare che siano stati implementati controlli dell'accesso tramite un sistema di controllo dell'accesso automatico.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
7.2 Stabilire un sistema di controllo dell'accesso per i componenti di sistema con utenti multipli che limiti l'accesso in base all'effettiva esigenza di un utente e che sia impostato su "deny all" a meno che non sia specificatamente consentito. Il sistema di controllo dell'accesso deve includere quanto segue:	**7.2** Esaminare le impostazioni del sistema e la documentazione del fornitore per verificare che un sistema di controllo dell'accesso sia implementato come segue:			
7.2.1 Copertura di tutti i componenti di sistema	**7.2.1** Confermare che siano in atto sistemi di controllo dell'accesso su tutti i componenti di sistema.			
7.2.2 Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale	**7.2.2** Confermare che i sistemi di controllo dell'accesso siano configurati in modo che i privilegi vengano assegnati agli utenti in base alla classificazione e alla funzione del ruolo.			
7.2.3 Impostazione predefinita "deny-all"	**7.2.3** Confermare che i sistemi di controllo dell'accesso siano impostati in modo predefinito su "deny-all". *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.*			

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

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

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
8.1 Assegnare a tutti gli utenti un ID univoco prima di consentire l'accesso ai componenti di sistema o ai dati di titolari di carta.	**8.1** Verificare che tutti gli utenti dispongano di un ID univoco per l'accesso ai componenti di sistema o ai dati di titolari di carta.			
8.2 Oltre ad assegnare un ID univoco utilizzare almeno uno dei seguenti metodi per l'autenticazione di tutti gli utenti: ▪ Password o passphrase ▪ Autenticazione a due fattori (ad esempio, dispositivi token, smart card, biometrica o chiavi pubbliche)	**8.2** Per verificare che gli utenti vengano autenticati tramite un ID univoco e un altro elemento di autenticazione (ad esempio, una password) per l'accesso all'ambiente dei dati di titolari di carta, effettuare quanto segue: ▪ Richiedere ed esaminare la documentazione che descrive i metodi di autenticazione utilizzati. ▪ Per ogni tipo di metodo di autenticazione utilizzato e per ogni tipo di componente di sistema, osservare un'autenticazione per verificare venga eseguita nel modo documentato.			
8.3 Incorporare l'autenticazione a due fattori per l'accesso remoto alla rete (accesso a livello di rete dall'esterno) da parte di dipendenti, amministratori e terze parti. Utilizzare tecnologie, quali RADIUS (Remote Authentication and Dial-In Service) o TACACS (Terminal Access Controller Access Control System) con token oppure VPN (basata su SSL/TLS o IPSEC) con certificati singoli.	**8.3** Per verificare che l'autenticazione a due fattori sia implementata per tutti gli accessi di rete remoti, osservare la connessione remota di un dipendente (ad esempio, un amministratore) alla rete e verificare che sia la password che l'elemento di autenticazione aggiuntivo (ad esempio, smart card, token o PIN) vengano richiesti.			
8.4 Rendere tutte le password illeggibili durante la trasmissione e la memorizzazione su tutti i componenti di sistema tramite la crittografia avanzata (definita nel documento *PCI DSS Glossario, abbreviazioni e acronimi*).	**8.4.a** Per un campione di componenti di sistema, esaminare i file di password per verificare che le password siano illeggibili durante la trasmissione e la memorizzazione.			
	8.4.b Solo per i provider di servizi, osservare i file di password per verificare che le password dei clienti siano cifrate.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
8.5 Garantire una corretta autenticazione utente e gestione delle password per amministratori e utenti non consumatori su tutti i componenti di sistema nel seguente modo:	**8.5** Rivedere le procedure e consultare il personale per verificare che siano implementate procedure per l'autenticazione utente e la gestione delle password, effettuando quanto segue:			
8.5.1 Controllare le operazioni di aggiunta, eliminazione e modifica di ID utente, credenziali e altri oggetti identificativi.	**8.5.1.a** Selezionare un campione di ID utente, che includa amministratori e utenti generici. Verificare che ogni utente sia autorizzato a utilizzare il sistema in base alla politica aziendale, effettuando quanto segue: ▪ Richiedere ed esaminare un modulo di autorizzazione per ogni ID. ▪ Verificare che gli ID utente inseriti nel campione siano implementati secondo il modulo di autorizzazione (inclusi i privilegi specificati e tutte le firme ottenute) tenendo traccia delle informazioni per l'intero percorso dal modulo al sistema.			
8.5.2 Verificare l'identità dell'utente prima di eseguire il ripristino delle password.	**8.5.2** Esaminare le procedure delle password e osservare il personale responsabile della sicurezza per verificare che, se l'utente richiede il ripristino di una password per telefono, e-mail, Web o in altra forma non diretta, l'identità di tale utente venga controllata prima di ripristinare la password.			
8.5.3 Impostare la password per il primo accesso su un valore univoco per ogni utente e modificarla immediatamente dopo il primo uso.	**8.5.3** Esaminare le procedure delle password e osservare il personale responsabile della sicurezza per verificare che le password per il primo accesso per i nuovi utenti siano impostate su un valore univoco per ogni utente e modificate dopo il primo uso.			
8.5.4 Revocare immediatamente l'accesso per gli utenti non attivi.	**8.5.4** Selezionare un campione di dipendenti che hanno lasciato l'azienda negli ultimi sei mesi e analizzare gli elenchi di accesso utente correnti per verificare che gli ID relativi a tali utenti siano stati disattivati o rimossi.			
8.5.5 Rimuovere/disabilitare gli account utente non attivi almeno ogni 90 giorni.	**8.5.5** Verificare che gli account non attivi da oltre 90 giorni siano stati rimossi o disabilitati.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
8.5.6 Abilitare gli account utilizzati dai fornitori per la gestione in remoto solo durante il periodo di tempo necessario.	**8.5.6** Verificare che gli account utilizzati dai fornitori per supportare e gestire i componenti di sistema siano disabilitati e vengano abilitati solo quando necessario e monitorati durante l'uso.			
8.5.7 Comunicare le procedure e le politiche relative alle password a tutti gli utenti con accesso ai dati di titolari di carta.	**8.5.7** Consultare gli utenti appartenenti a un campione di ID utente per verificare che siano a conoscenza delle procedure e delle politiche relative alle password.			
8.5.8 Non utilizzare account e password di gruppo, condivisi o generici.	**8.5.8.a** Per un campione di componenti di sistema, esaminare gli elenchi di ID utente per verificare quanto segue: ▪ Gli ID e gli account utente generici sono disabilitati o rimossi. ▪ Non esistono ID utente condivisi per le attività di amministrazione del sistema e altre funzioni critiche. ▪ Gli ID utente condivisi e generici non vengono utilizzati per gestire i componenti di sistema.			
	8.5.8.b Esaminare le politiche/procedure relative alla password per verificare che siano esplicitamente proibite password di gruppo e condivise.			
	8.5.8.c Consultare gli amministratori di sistema per verificare che non vengano distribuite, anche se richiesto, password di gruppo o condivise.			
8.5.9 Modificare le password utente almeno ogni 90 giorni.	**8.5.9** Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password utente siano impostati in modo che ne venga richiesta la modifica almeno ogni 90 giorni. Per i provider di servizi, esaminare i processi interni e la documentazione per clienti/utenti per verificare che venga richiesta la modifica periodica delle password dei clienti e che vengano fornite ai clienti tutte le informazioni necessarie relativamente a quando e in quali circostanze occorre modificare la password.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
8.5.10 Richiedere una lunghezza minima della password di 7 caratteri.	**8.5.10** Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password utente siano impostati in modo che la lunghezza minima sia di 7 caratteri. Solo per i provider di servizi, esaminare i processi interni e la documentazione per clienti/utenti per verificare che venga richiesta una lunghezza minima per le password dei clienti.			
8.5.11 Utilizzare password contenenti valori numerici e alfabetici.	**8.5.11** Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password siano impostati in modo che vengano richieste password composte da valori numerici e alfabetici. Solo per i provider di servizi, esaminare i processi interni e la documentazione per clienti/utenti per verificare che venga richiesto l'uso di valori numerici e alfabetici per le password dei clienti.			
8.5.12 Non consentire l'invio di una nuova password uguale a una delle ultime quattro password utilizzate.	**8.5.12** Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password siano impostati in modo che vengano richieste nuove password diverse dalle ultime quattro password utilizzate. Solo per i provider di servizi, esaminare i processi interni e la documentazione per clienti/utenti per verificare che un cliente non possa specificare una nuova password uguale a una delle ultime quattro utilizzate.			
8.5.13 Limitare i tentativi di accesso ripetuti bloccando l'ID utente dopo un massimo di sei tentativi.	**8.5.13** Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password siano impostati in modo che venga richiesto il blocco dell'account utente dopo sei tentativi di accesso non validi. Solo per i provider di servizi, esaminare i processi interni e la documentazione per clienti/utenti per verificare che gli account utente vengano temporaneamente bloccati dopo sei tentativi di accesso non validi.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
8.5.14 Impostare la durata del blocco a un minimo di 30 minuti o finché l'amministratore non abilita l'ID utente.	**8.5.14** Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che i parametri delle password siano impostati in modo che venga richiesto il blocco dell'account utente per almeno 30 minuti o finché l'amministratore non ripristina l'account.			
8.5.15 Se una sessione è inattiva per oltre 15 minuti, l'utente deve immettere nuovamente la password per riattivare il terminale.	**8.5.15** Per un campione di componenti di sistema, richiedere e ispezionare le impostazioni di configurazione del sistema per verificare che la funzione del periodo di inattività del sistema/sessione sia stata impostata al massimo su 15 minuti.			
8.5.16 Autenticare tutti gli accessi al database contenente i dati di titolari di carta. Sono compresi gli accessi da applicazioni, amministratori e tutti gli altri utenti.	**8.5.16.a** Esaminare le impostazioni di configurazione del database e dell'applicazione e verificare che l'autenticazione utente e l'accesso ai database includano quanto segue: ▪ Tutti gli utenti vengono autenticati prima dell'accesso. ▪ 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). ▪ L'accesso diretto o le query ai database sono consentiti solo agli amministratori del database.			
	8.5.16.b Esaminare le applicazioni del database e gli ID di applicazione correlati per verificare che tali ID possano essere utilizzati solo dalle applicazioni e non da utenti singoli o altri processi.			

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

Gli accessi fisici ai dati o ai sistemi che ospitano i dati di titolari di carta offrono la possibilità di accedere ai dispositivi o ai dati e di rimuovere i sistemi o le copie cartacee; pertanto dovrebbero essere limitati in modo appropriato.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
9.1 Utilizzare i controlli dell'accesso alle strutture appropriati per limitare e monitorare gli accessi fisici ai sistemi nell'ambiente dei dati di titolari di carta.	**9.1** Verificare la presenza di controlli di sicurezza fisica per ogni area computer, centro dati e altre aree fisiche con sistemi nell'ambiente dei dati di titolari di carta. ▪ Verificare che l'accesso sia controllato da lettori di tessere magnetiche o altri dispositivi, incluse tessere magnetiche autorizzate e lucchetti con chiavi. ▪ Osservare un tentativo di accesso dell'amministratore del sistema a console per sistemi selezionati casualmente nell'ambiente dei dati di titolari di carta e verificare che siano "sotto chiave" per impedire l'uso non autorizzato.			
9.1.1 Utilizzare videocamere o altri meccanismi di controllo dell'accesso per monitorare gli accessi fisici ad aree sensibili. Esaminare i dati raccolti e correlarli con altri. Conservare i dati per almeno tre mesi, se non diversamente richiesto dalle leggi in vigore. *Nota: per "aree sensibili" si intende centri dati, aree server e aree che ospitano sistemi di memorizzazione, elaborazione o trasmissione dei dati di titolari di carta. Ciò esclude le aree in cui vi sono i terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio.*	**9.1.1** Verificare che siano attive videocamere o altri meccanismi di controllo dell'accesso per monitorare i punti di entrata/uscita delle aree sensibili. Le videocamere e gli altri meccanismi di controllo devono essere protetti da manomissione o disattivazione. Verificare che le videocamere o gli altri meccanismi di controllo siano monitorati e che i dati derivanti da tali meccanismi vengano conservati per almeno tre mesi.			
9.1.2 Limitare l'accesso fisico a connettori di rete accessibili pubblicamente.	**9.1.2** Verificare, tramite consultazione con gli amministratori di rete e osservazione, che i connettori di rete vengano attivati solo se necessario da parte di dipendenti autorizzati. Ad esempio, le sale conferenza utilizzate dai visitatori non devono disporre di porte di rete con DHCP. In alternativa, verificare che i visitatori siano scortati costantemente nelle aree con connettori di rete attivi.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
9.1.3 Limitare l'accesso fisico a punti di accesso wireless, gateway e dispositivi portatili.	**9.1.3** Verificare che l'accesso fisico a punti di accesso wireless, gateway e dispositivi portatili sia limitato in modo corretto.			
9.2 Sviluppare procedure che consentono a tutto il personale di distinguere facilmente tra dipendenti e visitatori, in particolare in aree che permettono l'accesso ai dati di titolari di carta. *Ai fini del presente requisito, per "dipendente" 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. Per "visitatore" si intende un fornitore, un ospite di un dipendente, un tecnico dell'assistenza o chiunque abbia necessità di accedere alla struttura per un breve periodo di tempo, solitamente non più di un giorno.*	**9.2.a** Esaminare i processi e le procedure per l'assegnazione delle tessere magnetiche a dipendenti e visitatori e verificare che tali processi includano quanto segue: ▪ Concessione di nuove tessere magnetiche, modifica dei requisiti di accesso e revoca per i dipendenti che hanno lasciato l'azienda e tessere magnetiche per visitatori scadute ▪ Accesso limitato al sistema delle tessere magnetiche			
	9.2.b Osservare le persone all'interno della struttura e verificare che sia possibile distinguere facilmente dipendenti e visitatori.			
9.3 Accertarsi che tutti i visitatori vengano gestiti nel modo seguente:	**9.3** Verificare che siano in atto controlli di dipendenti/visitatori come segue:			
9.3.1 Siano autorizzati prima di accedere ad aree in cui vengono elaborati o gestiti dati di titolari di carta.	**9.3.1** Osservare i visitatori per verificare che utilizzino le tessere magnetiche di identificazione. Tentare di accedere al centro dati per verificare che la tessera magnetica di un visitatore non consenta l'accesso senza scorta ad aree fisiche in cui sono conservati dati di titolari di carta.			
9.3.2 Ricevano un token fisico (ad esempio, una tessera magnetica o un dispositivo di accesso) con scadenza, che identifica i visitatori come non dipendenti.	**9.3.2** Esaminare le tessere magnetiche per dipendenti e per visitatori per verificare che distinguano in modo chiaro i dipendenti dai visitatori/collaboratori esterni e che abbiano una scadenza.			
9.3.3 Restituiscano il token fisico prima di lasciare la struttura o in corrispondenza della data di scadenza.	**9.3.3** Osservare i visitatori che lasciano la struttura per verificare che venga loro richiesta la restituzione della tessera magnetica di identificazione all'uscita o al momento della scadenza.			

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

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

Monitoraggio e test delle reti regolari

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

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

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
10.1 Stabilire un processo per collegare tutti gli accessi ai componenti di sistema (in particolare l'accesso eseguito con privilegi di amministratore, ad esempio come utente root) a ciascun utente.	**10.1** Verificare tramite osservazione e consultazione dell'amministratore di sistema che gli audit trail siano attivi e funzionanti per i componenti di sistema.			
10.2 Implementare audit trail automatici per tutti i componenti di sistema per ricostruire i seguenti eventi:	**10.2** Tramite consultazioni ed esami dei registri di audit e delle relative impostazioni, effettuare quanto segue:			
10.2.1 Tutti gli accessi utente ai dati di titolari di carta	**10.2.1** Verificare che tutti gli accessi utente ai dati di titolari di carta siano registrati.			
10.2.2 Tutte le azioni intraprese da un utente con privilegi di utente root o amministratore	**10.2.2** Verificare che tutte le azioni intraprese da un utente con privilegi di utente root o amministratore siano registrate.			
10.2.3 Accesso a tutti gli audit trail	**10.2.3** Verificare che l'accesso a tutti gli audit trail sia registrato.			
10.2.4 Tentativi di accesso logico non validi	**10.2.4** Verificare che i tentativi di accesso logico non validi siano registrati.			
10.2 5 Uso dei meccanismi di identificazione e autenticazione	**10.2.5** Verificare che l'uso dei meccanismi di identificazione e autenticazione sia registrato.			
10.2.6 Inizializzazione dei registri di audit	**10.2.6** Verificare che l'inizializzazione dei registri di audit sia registrata.			
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.			
10.3 Registrare almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento:	**10.3** Eseguire quanto indicato di seguito, tramite consultazioni e osservazione, per ogni evento inseribile nell'audit (da 10.2):			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
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	**10.3.2** Verificare che data e ora siano incluse nelle voci di registro.			
10.3.4 Indicazione di successo o fallimento	**10.3.2** Verificare che l'indicazione di successo o fallimento sia inclusa nelle voci di registro.			
10.3.5 Origine dell'evento	**10.3.5** Verificare che l'origine dell'evento sia inclusa nelle voci di registro.			
10.3.6 Identità o nome dell'elemento interessato (dati, componente di sistema o risorsa)	**10.3.6** Verificare che l'identità o il nome dell'elemento interessato (dati, componente di sistema o risorsa) sia inclusa nelle voci di registro.			
10.4 Sincronizzare tutti gli orologi e gli orari critici del sistema.	**10.4** Richiedere ed esaminare il processo per acquisire e distribuire l'ora corretta all'interno dell'organizzazione, nonché le impostazioni di parametri del sistema correlate all'orario per un campione di componenti di sistema. Verificare che quanto indicato di seguito sia incluso nel processo e implementato:			
	10.4.a Verificare che una versione nota e stabile di NTP (Network Time Protocol) o tecnologia simile, aggiornata per i Requisiti 6.1 e 6.2 PCI DSS, venga utilizzata per la sincronizzazione dell'ora.			
	10.4.b Verificare che non tutti i server interni ricevano segnali orari da sorgenti esterne. [Due o tre server di rilevamento dell'orario centrali all'interno dell'organizzazione ricevono segnali orari esterni [direttamente da radio speciale, satelliti GPS o altre sorgenti esterne basate su International Atomic Time e UTC (ex GMT)], comunicano tra loro per mantenere un orario esatto e condividono l'orario con altri server interni.]			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
	10.4.c Verificare da quali host esterni specifici i server di rilevamento dell'orario accettano gli aggiornamenti di ora NTP (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 forniti dal servizio NTP (per evitare un uso non autorizzato dei server di rilevamento dell'ora esterni). Per ulteriori informazioni, visitare il sito www.ntp.org			
10.5 Proteggere gli audit trail in modo che non possano essere modificati.	**10.5** Consultare l'amministratore di sistema ed esaminare le autorizzazioni per verificare che gli audit trail siano protetti e non possano essere modificati, come segue:			
10.5.1 Limitare la visualizzazione degli audit trail a coloro che realmente necessitano di tali informazioni per scopi aziendali.	**10.5.1** Verificare che solo coloro che necessitano di tali informazioni per scopi aziendali possano visualizzare i file di audit trail.			
10.5.2 Proteggere i file di audit trail da modifiche non autorizzate.	**10.5.2** Verificare che i file di audit trail correnti siano protetti da modifiche non autorizzate tramite meccanismi di controllo dell'accesso, separazione fisica e/o di rete.			
10.5.3 Eseguire immediatamente il backup dei file di audit trail su un server di registro centralizzato o un supporto difficile da modificare.	**10.5.3** Verificare che venga eseguito immediatamente il backup dei file di audit trail su un server di registro centralizzato o un supporto difficile da modificare.			
10.5.4 Scrivere registri per tecnologie rivolte al pubblico su un server di registro sulla LAN interna.	**10.5.4** Verificare che i registri per le tecnologie rivolte al pubblico (ad esempio, wireless, firewall, DNS, e-mail) vengano scaricati o copiati su un server di registro interno centralizzato o un supporto sicuro.			
10.5.5 Utilizzare un meccanismo di monitoraggio dell'integrità dei file o un software di rilevamento delle modifiche sui registri per accertarsi che i dati di registro esistenti non possano essere modificati senza generare avvisi (sebbene l'aggiunta di nuovi dati non dovrebbe generare avvisi).	**10.5.5** Verificare l'uso di un software di monitoraggio dell'integrità dei file o di rilevamento delle modifiche per i registri esaminando le impostazioni di sistema, i file monitorati e i risultati delle attività di monitoraggio.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
10.6 Esaminare i registri per tutti i componenti di sistema almeno una volta al giorno. Le revisioni dei registri devono includere i server che eseguono funzioni di sicurezza, quali i servizi antintrusione IDS (Intrusion Detection System), i server AAA (Autenticazione, Autorizzazione e Accounting), ad esempio RADIUS. *Nota: strumenti di raccolta, analisi e generazione di avvisi per i registri possono essere utilizzati ai fini della conformità al Requisito 10.6.*	**10.6.a** Richiedere ed esaminare le politiche e le procedure di sicurezza per verificare che includano l'analisi dei registri di sicurezza su base giornaliera e che venga richiesto un intervento per le eccezioni.			
	10.6.b Verificare che vengano eseguite revisioni dei registri regolari per tutti i componenti di sistema, tramite osservazione e consultazioni.			
10.7 Conservare la cronologia dell'audit trail per almeno un anno, con un minimo di tre mesi di disponibilità immediata per l'analisi (ad esempio, online, archiviazione o recuperabile da backup).	**10.7.a** Richiedere ed esaminare le politiche e le procedure di sicurezza e verificare che includano politiche per la conservazione del registro di audit per almeno un anno.			
	10.7.b Verificare che i registri di audit siano disponibili per almeno un anno e che siano in atto processi di recupero dei registri degli ultimi tre mesi per un'analisi immediata.			

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

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

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
11.1 Verificare la presenza di punti di accesso wireless utilizzando un analizzatore wireless almeno una volta ogni tre mesi oppure distribuendo un IDS/IPS wireless per identificare tutti i dispositivi wireless in uso.	**11.1.a** Verificare che venga utilizzato un analizzatore wireless almeno su base trimestrale o che venga implementato e configurato un IDS/IPS wireless per identificare tutti i dispositivi wireless.			
	11.1.b Se viene implementato un IDS/IPS wireless, verificare che la configurazione generi avvisi per il personale.			
	11.1 c Verificare che il piano di risposta agli incidenti aziendale (Requisito 12.9) includa una risposta in caso di rilevamento di dispositivi wireless non autorizzati.			
11.2 Eseguire scansioni di vulnerabilità della rete interne ed esterne almeno una volta ogni tre mesi e dopo ogni cambiamento significativo apportato alla rete (ad esempio, installazione di nuovi componenti di sistema, modifica della topologia della rete, modifica delle regole del firewall o aggiornamento di un prodotto). *Nota: le scansioni esterne delle vulnerabilità trimestrali devono essere eseguite da un fornitore di scansioni approvato (ASV) e qualificato da PCI SSC. Le scansioni dopo le modifiche della rete possono essere eseguite dal personale interno della società.*	**11.2.a** Ispezionare l'output delle ultime quattro scansioni delle vulnerabilità trimestrali della rete interna, dell'host e delle applicazioni per verificare l'esecuzione di un test della sicurezza periodico dei dispositivi all'interno dell'ambiente dei dati di titolari di carta. Verificare che il processo di scansione preveda l'esecuzione di ulteriori scansioni finché non vengono ottenuti risultati positivi. *Nota: le scansioni esterne condotte dopo le modifiche di rete e le scansioni interne possono essere eseguite da personale aziendale interno qualificato o da terze parti.*			
	11.2.b Verificare che la scansione esterna venga eseguita su base trimestrale secondo quanto specificato nelle procedure di scansione della sicurezza PCI, esaminando l'output delle ultime quattro scansioni della vulnerabilità trimestrali per verificare che: ▪ Siano state eseguite quattro scansioni trimestrali negli ultimi 12 mesi; ▪ I risultati di ogni scansione soddisfano le procedure di scansione della sicurezza PCI (ad esempio, assenza di vulnerabilità urgenti, critiche o di livello elevato);			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
	▪ Le scansioni sono state portate a termine da un fornitore di scansioni approvato (ASV), qualificato da PCI SSC. *Nota: non è necessario completare quattro scansioni trimestrali per la conformità iniziale a PCI DSS, se il valutatore verifica che 1) il risultato della scansione più recente era positivo, 2) l'entità dispone di politiche e procedure documentate che richiedono l'esecuzione di scansioni trimestrali e 3) ogni vulnerabilità rilevata dalla scansione è stata corretta nel modo dimostrato da una nuova scansione. Per gli anni successivi alla scansione PCI DSS iniziale, è necessario eseguire quattro scansioni trimestrali con esito positivo.*			
	11.2.c Verificare che la scansione interna e/o esterna venga eseguita dopo ogni modifica significativa nella rete, esaminando i risultati della scansione dell'ultimo anno. Verificare che il processo di scansione preveda l'esecuzione di ulteriori scansioni finché non vengono ottenuti risultati positivi.			
11.3 Eseguire test di penetrazione esterna ed interna almeno una volta all'anno e dopo ogni aggiornamento o modifica significativa dell'infrastruttura o dell'applicazione (quale un aggiornamento del sistema operativo, l'aggiunta all'ambiente di una subnet o di un server Web). Questi test di penetrazione devono includere quanto segue:	**11.3.a** Richiedere ed esaminare i risultati dell'ultimo test di penetrazione per verificare che tali test vengano eseguiti almeno una volta all'anno e dopo ogni modifica significativa dell'ambiente. Verificare che le vulnerabilità rilevate siano state corrette e il test ripetuto.			
	11.3.b Verificare che il test sia stato eseguito da una risorsa interna o da una terza parte qualificata e che chi esegue il test sia indipendente dall'organizzazione, ove possibile (non necessariamente un QSA o un ASV).			
11.3.1 Test di penetrazione a livello di rete	**11.3.1** Verificare che il test di penetrazione includa anche i test di penetrazione a livello di rete. Tali test devono includere i componenti che supportano le funzioni di rete nonché i sistemi operativi.			
11.3.2 Test di penetrazione a livello di applicazione	**11.3.2** Verificare che il test di penetrazione includa anche i test di penetrazione a livello di applicazione. Per le applicazioni Web, i test devono includere almeno le vulnerabilità elencate nel Requisito 6.5.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
11.4 Utilizzare sistemi di rilevamento e/o di prevenzione delle intrusioni per monitorare tutto il traffico nell'ambiente dei dati di titolari di carta e segnalare possibili rischi al personale addetto. Mantenere tutti i sistemi di rilevamento e prevenzione delle intrusioni aggiornati.	**11.4.a** Verificare l'uso di sistemi di rilevamento e/o prevenzione delle intrusioni e che tutto il traffico dell'ambiente dei dati di titolari di carta venga monitorato.			
	11.4.b Confermare che i dispositivi IDS e/o IPS siano configurati per segnalare possibili compromissioni al personale.			
	11.4.c Esaminare le configurazioni IDS/IPS e confermare che i dispositivi IDS/IPS vengano configurati, conservati e aggiornati secondo le istruzioni del fornitore per garantire una protezione ottimale.			
11.5 Distribuire il software di monitoraggio dell'integrità dei file per segnalare al personale modifiche non autorizzate di file system, file di configurazione o file di contenuto critici; inoltre, configurare il software in modo che esegua confronti di file critici almeno una volta alla settimana. *Nota: ai fini del monitoraggio dell'integrità dei file, i file critici sono solitamente file che non cambiano frequentemente, ma la cui modifica può indicare la compromissione, effettiva o potenziale, del sistema. In genere, i prodotti per il monitoraggio dell'integrità dei file sono preconfigurati con file critici per il sistema operativo in uso. Altri file critici, ad esempio quelli per applicazioni personalizzate, devono essere valutati e definiti dall'entità (ossia dall'esercente o dal provider di servizi).*	**11.5** Verificare l'uso dei prodotti di monitoraggio dell'integrità dei file all'interno dell'ambiente dei dati di titolari di carta osservando le impostazioni del sistema e i file monitorati ed esaminando i risultati delle attività di monitoraggio. Esempi di file che devono essere monitorati: ▪ Eseguibili di sistema ▪ Eseguibili di applicazioni ▪ File di configurazione e parametri ▪ File memorizzati centralmente, di cronologia o archiviazione, di registro e audit			

Gestione di una politica di sicurezza delle informazioni

Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori.

Una politica di sicurezza rigida definisce il livello di sicurezza per l'intera società e spiega ai dipendenti quali sono le aspettative nei loro confronti in termini di sicurezza. Tutti i dipendenti devono essere a conoscenza della sensibilità dei dati e delle proprie responsabilità in termini di protezione. Ai fini del presente requisito, per "dipendente" 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.

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
12.1 Stabilire, pubblicare, conservare e rendere disponibile una politica di sicurezza conforme a quanto indicato di seguito:	**12.1** Esaminare la politica di sicurezza delle informazioni e verificare che venga pubblicata e resa disponibile a tutti gli utenti di sistema interessati (inclusi fornitori, collaboratori esterni e partner aziendali).			
12.1.1 Risponde a tutti i requisiti PCI DSS.	**12.1.1** Verificare che la politica risponda a tutti i requisiti PCI DSS.			
12.1.2 Include un processo annuale che identifica minacce e vulnerabilità e che consente di ottenere una valutazione dei rischi formale.	**12.1.2** Verificare che la politica di sicurezza delle informazioni includa una valutazione dei rischi annuale che identifichi minacce, vulnerabilità e che consenta di ottenere una valutazione dei rischi formale.			
12.1.3 Include una revisione almeno una volta all'anno e aggiornamenti in caso di cambiamenti dell'ambiente.	**12.1.3** Verificare che la politica di sicurezza delle informazioni venga analizzata almeno una volta all'anno e venga aggiornata per riflettere i cambiamenti negli obiettivi aziendali o nell'ambiente a rischio.			
12.2 Sviluppare procedure di sicurezza operativa giornaliere coerenti con i requisiti di questa specifica (ad esempio, procedure per la manutenzione degli account utente e procedure di revisione dei registri).	**12.2.a** Esaminare le procedure di sicurezza operative giornaliere. Verificare che siano coerenti con la presente specifica e che includano procedure tecniche e amministrative per ogni requisito.			

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

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
12.3.10 Durante l'accesso ai dati di titolari di carta tramite tecnologie di accesso remoto, vietare la copia, lo spostamento e la memorizzazione dei dati di titolari di carta su dischi rigidi locali e supporti elettronici rimovibili.	**12.3.10** Verificare che le politiche che regolano l'uso proibiscano la copia, lo spostamento o la memorizzazione dei dati di titolari di carta su dischi rigidi locali e supporti elettronici rimovibili quando si accede ai dati tramite tecnologie di accesso remoto.			
12.4 Accertarsi che la politica e le procedure di sicurezza definiscano chiaramente le responsabilità in termini di protezione delle informazioni per tutti i dipendenti e i collaboratori.	**12.4** Verificare che le politiche di protezione delle informazioni definiscano chiaramente le responsabilità in termini di protezione delle informazioni per dipendenti e collaboratori.			
12.5 Assegnare a un utente singolo o a un team le seguenti responsabilità di gestione della sicurezza delle informazioni:	**12.5** Verificare l'assegnazione formale della responsabilità di protezione delle informazioni a un CSO (Chief Security Officer) o a un altro membro del management esperto in sicurezza. Richiedere ed esaminare le politiche e le procedure di protezione delle informazioni per verificare che le responsabilità di protezione delle informazioni vengano assegnate in modo specifico e formale:			
12.5.1 Stabilire, documentare e distribuire le politiche e le procedure di sicurezza.	**12.5.1** Verificare che venga formalmente assegnata la responsabilità per la creazione e la distribuzione delle politiche e delle procedure di sicurezza.			
12.5.2 Monitorare ed esaminare avvisi e informazioni sulla sicurezza e distribuirli al personale appropriato.	**12.5.2** Verificare che venga formalmente assegnata la responsabilità del monitoraggio e dell'analisi degli avvisi di sicurezza e della distribuzione delle informazioni al personale addetto alla protezione delle informazioni appropriato e al management della business unit.			
12.5.3 Stabilire, documentare e distribuire le procedure di risposta ed escalation in caso di problemi di sicurezza per garantire una gestione tempestiva ed efficiente di tutte le situazioni.	**12.5.3** Verificare che venga formalmente assegnata la responsabilità di creazione e distribuzione delle politiche di risposta in caso di problemi e le procedure di escalation.			
12.5.4 Amministrare gli account utente, incluse aggiunte, eliminazioni e modifiche	**12.5.4** Verificare che venga formalmente assegnata la responsabilità per l'amministrazione degli account utente e la gestione delle autenticazioni.			
12.5.5 Monitorare e controllare tutti gli accessi ai dati.	**12.5.5** Verificare che venga formalmente assegnata la responsabilità per il monitoraggio e il controllo di tutti gli accessi ai dati.			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
12.6 Implementare un programma formale di consapevolezza della sicurezza per rendere tutti i dipendenti consapevoli dell'importanza della sicurezza dei dati di titolari di carta.	**12.6.a** Verificare l'esistenza di un programma formale di consapevolezza della sicurezza per tutti i dipendenti.			
	12.6.b Richiedere ed esaminare le procedure e la documentazione del programma di consapevolezza della sicurezza ed effettuare quanto segue:			
12.6.1 Formare i dipendenti al momento dell'assunzione e almeno una volta all'anno.	**12.6.1.a** Verificare che il programma di consapevolezza della sicurezza utilizzi diversi strumenti di comunicazione e formazione dei dipendenti (ad esempio, poster, lettere, promemoria, formazione basata su Web, riunioni e promozioni).			
	12.6.1.b Verificare che i dipendenti partecipino alla formazione sulla consapevolezza al momento dell'assunzione e almeno una volta all'anno.			
12.6.2 Richiedere ai dipendenti di certificare almeno una volta all'anno che hanno letto e compreso la politica e le procedure di sicurezza della società.	**12.6.2** Verificare che il programma di consapevolezza della sicurezza richieda ai dipendenti di certificare (ad esempio, per iscritto o elettronicamente) almeno una volta all'anno che hanno letto e compreso la politica di protezione delle informazioni della società.			
12.7 Sottoporre i potenziali dipendenti a screening (vedere la definizione di "dipendente" al punto 9.2 riportato sopra) prima di assumerli per ridurre al minimo il rischio di attacchi da fonti interne. *Per i dipendenti, quali i cassieri di un negozio, che hanno accesso a un solo numero di carta alla volta durante una transazione, questo requisito è solo consigliato.*	**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) dei dipendenti prima di assumere quelli che avranno accesso ai dati di titolari di carta o al relativo ambiente. Esempi di indagini sulla storia personale sono informazioni su impieghi precedenti, precedenti penali, storico del credito e controlli delle referenze.			
12.8 Se i dati di titolari di carta sono condivisi con provider di servizi, gestire e implementare politiche e procedure per i provider di servizi per includere quanto segue:	**12.8** Se l'entità valutata condivide i dati di titolari di carta con provider di servizi (ad esempio, strutture di conservazione dei nastri di backup, provider di servizi gestiti come le società di hosting Web, provider di servizi di sicurezza oppure soggetti che ricevono i dati a scopo di "fraud modeling", cioè per analizzare modelli di possibili truffe), effettuare quanto indicato di seguito, tramite osservazione, revisione delle politiche e delle procedure e analisi della documentazione di supporto:			

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
12.8.1 Conservare un elenco dei provider di servizi.	**12.8.1** Verificare che venga conservato un elenco di provider di servizi.			
12.8.2 Conservare un accordo scritto in base al quale il provider di servizi si assume la responsabilità della protezione dei dati di titolari di carta di cui entra in possesso.	**12.8.2** Verificare che nell'accordo scritto il provider di servizi si assuma la responsabilità della protezione di dati di titolari di carta.			
12.8.3 Accertarsi che esista un processo definito per incaricare i provider di servizi, che includa tutte le attività di dovuta diligenza appropriate prima dell'incarico.	**12.8.3** Verificare che le politiche e le procedure siano documentate e rispettate, inclusa la dovuta diligenza appropriata prima di assegnare l'incarico al provider di servizi.			
12.8.4 Conservare un programma per monitorare lo stato di conformità agli standard PCI DSS dei provider di servizi.	**12.8.4** Verificare che l'entità valutata conservi un programma per monitorare lo stato di conformità agli standard PCI DSS dei provider di servizi.			
12.9 Implementare un piano di risposta agli incidenti. Prepararsi a rispondere immediatamente a una violazione del sistema.	**12.9** Richiedere ed esaminare il piano di risposta agli incidenti e le procedure correlate ed effettuare quanto segue:			

(12.9 continua alla pagina successiva)

Requisiti PCI DSS	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
12.9.1 Creare il piano di risposta agli incidenti da attuare in caso di violazione del sistema. Accertarsi che il piano includa almeno i seguenti elementi: ▪ 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	**12.9.1** Verificare che il piano di risposta agli incidenti includa i seguenti elementi: ▪ 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			
12.9.2 Eseguire un test del piano almeno una volta all'anno.	**12.9.2** Verificare che il piano venga testato almeno una volta all'anno.			
12.9.3 Nominare personale specifico disponibile 24 ore al giorno, 7 giorni su 7 in caso di emergenza.	**12.9.3** Attraverso l'osservazione e l'analisi delle politiche, verificare che il monitoraggio e la capacità di risposta siano disponibili 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.			
12.9.4 Formare in modo appropriato il personale addetto al controllo delle violazioni della sicurezza.	**12.9.4** Attraverso l'osservazione e l'analisi delle politiche, verificare che il personale addetto al controllo delle violazioni della sicurezza partecipi regolarmente a corsi di formazione.			

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

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

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

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

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

Requisiti	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
A.1.2 Limitare l'accesso e i privilegi di ciascuna entità esclusivamente al relativo ambiente di dati di titolari di carta.	**A.1.2.a** Verificare che l'ID utente di tutti i processi dell'applicazione non sia un utente privilegiato (root/amministratore).			
	A.1.2.b Verificare che ogni entità (esercente, provider di servizi) disponga dei diritti di lettura, scrittura o esecuzione solo per i propri file e directory o per i system file necessari (tramite autorizzazione su file system, elenchi di controllo degli accessi, funzioni chroot o jailshell, eccetera). IMPORTANTE: i file di un'entità non possono essere condivisi per gruppi.			
	A.1.2.c Verificare che gli utenti di un'entità non abbiano accesso in scrittura a file di sistema binari condivisi.			
	A.1.2.d Verificare che la visualizzazione delle voci del registro sia consentita solo all'entità proprietaria.			
	A.1.2.e Per impedire che un'entità monopolizzi le risorse del server per sfruttarne le vulnerabilità (condizioni di errore, "race" e riavvio che generano, ad esempio, buffer overflow), verificare che siano applicate limitazioni all'uso di queste risorse del sistema: ▪ Spazio sul disco ▪ Larghezza di banda ▪ Memoria ▪ CPU			
A.1.3 Accertarsi che le funzioni di audit trail e di generazione dei registri siano abilitate e siano univoche per l'ambiente dei dati di titolari di carta di ciascuna entità e che siano coerenti con il Requisito 10 PCI DSS.	**A.1.3.a** Verificare che il provider di hosting condiviso abbia abilitato la generazione dei registri per l'ambiente di esercenti e provider di servizi nel modo descritto di seguito: ▪ I registri sono abilitati per applicazioni di terze parti comuni. ▪ I registri sono attivi per impostazione predefinita. ▪ I registri sono disponibili per la revisione da parte dell'entità proprietaria. ▪ Le posizioni dei registri sono comunicate in modo chiaro all'entità proprietaria.			

Requisiti	Procedure di test	Presente	Non presente	Data di scadenza/ Commenti
A.1.4 Abilitare processi in grado di fornire tutte le informazioni necessarie per un'indagine legale tempestiva in caso di violazione di dati di un esercente o un provider di servizi ospitato.	**A.1.4** Verificare che il provider di hosting condiviso disponga di politiche scritte che forniscono tutte le informazioni necessarie per un'indagine legale tempestiva dei server correlati in caso di violazione.			

Appendice B: Controlli compensativi

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

I controlli compensativi devono soddisfare i seguenti criteri:

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

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

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

   a) I requisiti PCI DSS esistenti NON POSSONO essere considerati controlli compensativi se sono già richiesti per l'elemento sottoposto a revisione. Ad esempio, le password per l'accesso amministrativo non da console devono essere inviate già cifrate per ridurre il rischio di intercettazione delle password amministrative con testo in chiaro. Un'entità non può utilizzare altri requisiti di password PCI DSS (blocco intrusioni, password complesse, ecc.) per compensare la mancanza di password cifrate, poiché tali altri requisiti di password non riducono il rischio di intercettazione delle password con testo in chiaro. Inoltre, gli altri controlli delle password rappresentano già requisiti PCI DSS per l'elemento sottoposto a revisione (password).

   b) I requisiti PCI DSS esistenti POSSONO essere considerati controlli compensativi se sono richiesti per un'altra area, ma non sono richiesti per l'elemento sottoposto a revisione. Ad esempio, l'autenticazione a due fattori è un requisito PCI DSS per l'accesso remoto. L'autenticazione a due fattori *dalla rete interna* può anche essere considerata un controllo compensativo per l'accesso amministrativo non da console se la trasmissione di password cifrate non è supportata. L'autenticazione a due fattori può essere considerata un controllo compensativo accettabile se: (1) risponde alle intenzioni del requisito originale riducendo il rischio di intercettazione delle password amministrative con testo in chiaro e (2) è configurata correttamente e in un ambiente protetto.

   c) I requisiti PCI DSS esistenti possono essere combinati con nuovi controlli per diventare un controllo compensativo. Ad esempio, se una società non è in grado di rendere illeggibili i dati di titolari di carta secondo il Requisito 3.4 (ad esempio, tramite cifratura), un controllo compensativo potrebbe essere composto da un dispositivo o da una combinazione di dispositivi, applicazioni e controlli che rispondano a tutte le seguenti condizioni: (1) segmentazione di rete interna; (2) filtro degli indirizzi IP o MAC; (3) autenticazione a due fattori dalla rete interna.
4. Essere adeguato al rischio ulteriore provocato dalla mancata adesione al requisito PCI DSS

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

Appendice C: Foglio di lavoro - Controlli compensativi

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

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

Numero e definizione del requisito:

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

Foglio di lavoro Controlli compensativi - Esempio

Utilizzare questo foglio di lavoro per definire i controlli compensativi per qualsiasi requisito per il quale è stata selezionata la risposta "SÌ" e sono stati specificati nella colonna "Speciale" altri controlli compensativi.

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

	Informazioni richieste	Spiegazione
1. Vincoli	Elencare i vincoli che impediscono di soddisfare il requisito originale.	*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.*
2. Obiettivo	Definire l'obiettivo del controllo originale; identificare l'obiettivo soddisfatto mediante il controllo compensativo.	*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.*
3. Rischio identificato	Identificare eventuali rischi aggiuntivi dovuti alla non applicazione del controllo originale.	*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.*
4. Definizione di controlli compensativi	Definire i controlli compensativi e spiegare come soddisfano gli obiettivi del controllo originale e il rischio maggiore, se presente.	*La società XYZ richiederà a tutti gli utenti di accedere ai server dai propri desktop utilizzando il comando SU. Tale comando consente a un utente di accedere all'account "root" ed eseguire le azioni come utente "root", ma essere registrato nella directory di log SU. In questo modo, le azioni di ciascun utente possono essere registrate mediante l'account SU.*
5. Convalida dei controlli compensativi	Definire la modalità di convalida e test dei controlli compensativi.	*La società XYZ dimostra al valutatore che il comando SU è in esecuzione e che gli utenti che utilizzano tale comando sono registrati per identificare l'utente che esegue le azioni con i privilegi root*
6. Manutenzione	Definire il processo e i controlli in atto per i controlli compensativi.	*La società XYZ documenta i processi e le procedure per garantire che le configurazioni SU non vengano modificate, alterate o rimosse per consentire ai singoli utenti di eseguire comandi root senza essere identificati e registrati singolarmente*

Appendice D: Attestato di conformità – Esercenti

Payment Card Industry (PCI)
Data Security Standard

Attestato di conformità per valutazione in sede – Esercenti

Versione 1.2

Ottobre 2008

Istruzioni per l'invio

Questo documento deve essere completato da un QSA (Qualified Security Assessor) o esercente (se l'audit interno dell'esercente esegue la convalida) come dichiarazione dello stato di conformità dell'esercente agli standard PCI DSS. Completare tutte le sezioni applicabili e inviare all'acquirente o al marchio di pagamento richiedente.

Parte 1. Informazioni su società Qualified Security Assessor (QSA)						
Nome società:						
Nome contatto QSA principale:			Mansione:			
Telefono:			E-mail:			
Indirizzo ufficio:			Città:			
Stato/Provincia:		Paese:		CAP:		
URL:						

Parte 2. Informazioni su società esercente						
Nome società:			DBA:			
Nome contatto:			Mansione:			
Telefono:			E-mail:			
Indirizzo ufficio:			Città:			
Stato/Provincia:		Paese:		CAP:		
URL:						

Parte 2a. Tipo di settore di attività dell'esercente (selezionare tutte le risposte applicabili)

☐ Rivenditore ☐ Telecomunicazioni ☐ Minimarket e supermarket

☐ Distributori di benzina ☐ E-Commerce ☐ Ordini via posta/telefono

☐ Viaggi e divertimento ☐ Altro (specificare):

Elencare le strutture e le posizioni incluse nella valutazione della conformità agli standard PCI DSS:

Parte 2b. Rapporti

La società ha rapporti con uno o più agenti di terze parti (ad esempio gateway, società di hosting Web, addetti alle prenotazioni aeree, agenti di programmi di fedeltà, eccetera)? ☐ Sì ☐ No

La società ha rapporti con più di un acquirente? ☐ Sì ☐ No

Parte 2c. Elaborazione delle transazioni

Applicazione di pagamento in uso: Versione applicazione di pagamento:

Parte 3. Convalida PCI DSS

In base ai risultati inseriti nel Rapporto sulla conformità datato *(date of ROC)*, *(QSA Name/Merchant Name)* dichiara lo stato di conformità riportato di seguito per l'entità identificata nella Parte 2 del presente documento in data *(date)* (selezionare una risposta):

☐ **Conforme:** Tutti i requisiti nel Rapporto sulla conformità sono contrassegnati come presenti[4], è stata completata una scansione con esito positivo dal fornitore di scansioni approvato PCI SSC*(ASV Name)*; pertanto, *(Merchant Company Name)* ha dimostrato la completa conformità agli standard PCI DSS *(insert version number)*.

☐ **Non conforme:** Alcuni requisiti nel Rapporto sulla conformità sono contrassegnati come non presenti, determinando una valutazione di **NON CONFORMITÀ** generale **oppure** non è stata completata una scansione con esito positivo da un fornitore di scansioni approvato PCI SSC, pertanto *(Merchant Company Name)* non ha dimostrato la completa conformità agli standard PCI DSS.

Data di scadenza per conformità:

È possibile che a un'entità che invia questo modulo con lo stato 'Non conforme' venga richiesto di completare il Piano d'azione presente nella Parte 4 del presente documento. *Consultare il proprio acquirente o il marchio di pagamento prima di completare la Parte 4, perché non tutti i marchi di pagamento richiedono questa sezione.*

Parte 3a. Conferma dello stato di conformità

L'esercente/QSA conferma che:

☐	Il Rapporto sulla conformità è stato completato in base al documento *Requisiti PCI DSS e procedure di valutazione della sicurezza*, versione *(insert version number)* e alle istruzioni ivi fornite.
☐	Tutte le informazioni contenute nel Rapporto sulla conformità sopra menzionato e in questo attestato rappresentano in modo onesto i risultati della valutazione sotto tutti gli aspetti.
☐	L'esercente ha confermato insieme al fornitore dell'applicazione di pagamento che l'applicazione di pagamento non memorizza dati sensibili di autenticazione dopo l'autorizzazione.
☐	L'esercente ha letto gli standard PCI DSS e accetta di garantire sempre la massima conformità a tali standard.
☐	Nessuna prova di memorizzazione dei dati della striscia magnetica (traccia)[5], CAV2, CVC2, CID o CVV2[6], oppure dei dati PIN [7] dopo l'autorizzazione della transazione è stata trovata sui sistemi controllati durante questa valutazione.

Parte 3b. Accettazione QSA ed esercente

Firma QSA principale ↑	***Data:***
Nome QSA principale:	***Mansione:***

Firma del funzionario esecutivo dell'esercente ↑	***Data:***
Nome funzionario esecutivo dell'esercente:	***Mansione:***

[4] Nei risultati contrassegnati come "presenti" devono essere inclusi i controlli compensativi esaminati dall'audit interno del QSA/esercente. Se si rilevano controlli compensativi sufficienti per ridurre il rischio associato a un requisito, il QSA deve contrassegnare tale requisito come "presente".

[5] Dati codificati nella striscia magnetica utilizzati per l'autorizzazione durante una transazione con carta presente. Le entità non possono conservare tutti i dati completi della striscia magnetica dopo l'autorizzazione della transazione. I soli elementi dei dati di traccia che possono essere conservati sono il numero cliente, la data di scadenza e il nome.

[6] Il valore di tre o quattro cifre stampato nel riquadro della firma o nella parte anteriore di una carta di pagamento utilizzato per verificare le transazioni con carta non presente.

[7] 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.

Parte 4. Piano d'azione per lo stato di non conformità

Selezionare lo "Stato di conformità" appropriato per ciascun requisito. In caso di risposta negativa a uno dei requisiti, è necessario fornire la data in cui la Società sarà conforme al requisito e una breve descrizione delle azioni che verranno intraprese per soddisfare il requisito. *Consultare il proprio acquirente o il marchio di pagamento prima di completare la Parte 4, perché non tutti i marchi di pagamento richiedono questa sezione.*

Requisito PCI	Descrizione	Stato di conformità (selezionare una risposta)	Data e azioni di correzione (in caso di non conformità)
1	Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta.	☐ Sì ☐ No	
2	Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di sicurezza.	☐ Sì ☐ No	
3	Proteggere i dati di titolari di carta memorizzati.	☐ Sì ☐ No	
4	Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche.	☐ Sì ☐ No	
5	Utilizzare e aggiornare regolarmente il software antivirus.	☐ Sì ☐ No	
6	Sviluppare e gestire sistemi e applicazioni protette.	☐ Sì ☐ No	
7	Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario.	☐ Sì ☐ No	
8	Assegnare un ID univoco a chiunque abbia accesso a un computer.	☐ Sì ☐ No	
9	Limitare l'accesso fisico ai dati di titolari di carta.	☐ Sì ☐ No	
10	Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta.	☐ Sì ☐ No	
11	Eseguire regolarmente test dei sistemi e processi di protezione.	☐ Sì ☐ No	
12	Gestire una politica che garantisca la sicurezza delle informazioni	☐ Sì ☐ No	

Appendice E: Attestato di conformità – Provider di servizi

Payment Card Industry (PCI)
Data Security Standard

Attestato di conformità per valutazione in sede – Provider di servizi

Versione 1.2

Ottobre 2008

Istruzioni per l'invio

Il QSA e il provider di servizi devono completare questo documento come dichiarazione dello stato di conformità del provider di servizi agli standard PCI DSS. Completare tutte le sezioni applicabili e inviare al marchio di pagamento richiedente.

Parte 1. Informazioni su società Qualified Security Assessor					
Nome società:					
Nome contatto QSA principale:			Mansione:		
Telefono:			E-mail:		
Indirizzo ufficio:			Città:		
Stato/Provincia:		Paese:		CAP:	
URL:					

Parte 2. Informazioni su società provider di servizi					
Nome società:			DBA:		
Nome contatto:			Mansione:		
Telefono:			E-mail:		
Indirizzo ufficio:			Città:		
Stato/Provincia:		Paese:		CAP:	
URL:					

Parte 2a. Servizi forniti (selezionare tutte le risposte appropriate)

☐ Autorizzazione	☐ Programmi di fedeltà	☐ 3-D Secure Access Control Server (ACS)
☐ Switching	☐ IPSP (E-commerce)	☐ Elaborazione transazioni striscia magnetica
☐ Gateway pagamenti	☐ Clearing & Settlement	☐ Elaborazione transazioni MO/TO
☐ Hosting	☐ Elaborazione emissioni	☐ Altro (specificare):

Elencare le strutture e le posizioni incluse nella valutazione della conformità agli standard PCI DSS:

Parte 2b. Rapporti

La società ha rapporti con uno o più provider di servizi di terze parti (ad esempio, gateway, società di hosting Web, addetti alle prenotazioni aeree, agenti di programmi di fedeltà, eccetera)? ☐ Sì ☐ No

Parte 2c. Elaborazione delle transazioni

In che modo e con quale titolo la società memorizza, elabora e/o trasmette dati di titolari di carta?

Applicazione di pagamento in uso: *Versione applicazione di pagamento:*

Parte 3. Convalida PCI DSS

In base ai risultati annotati nel Rapporto sulla conformità datato *(date of ROC)*, *(QSA Name)* dichiara lo stato di conformità riportato di seguito per l'entità identificata nella Parte 2 del presente documento in data *(date)* (selezionare una risposta):

☐ **Conforme:** Tutti i requisiti nel Rapporto sulla conformità sono contrassegnati come presenti[8], è stata completata una scansione con esito positivo dal fornitore di scansioni approvato PCI SSC*(ASV Name)*; pertanto, *(Service Provider Name)*ha dimostrato la completa conformità agli standard PCI DSS*(insert version number).*

☐ **Non conforme:** alcuni requisiti nel Rapporto sulla conformità sono contrassegnati come non presenti, determinando una valutazione di **NON CONFORMITÀ** generale **oppure** non è stata completata una scansione con esito positivo da un fornitore di scansioni approvato PCI SSC, pertanto *(Service Provider Name)*non ha dimostrato la completa conformità agli standard PCI DSS.

Data di scadenza per conformità:

È possibile che a un'entità che invia questo modulo con lo stato 'Non conforme' venga richiesto di completare il Piano d'azione presente nella Parte 4 del presente documento. *Consultare il marchio di pagamento prima di completare la Parte 4, perché non tutti i marchi di pagamento richiedono questa sezione.*

Parte 3a. Conferma dello stato di conformità

Il QSA e il provider di servizi confermano che:

☐	Il Rapporto sulla conformità è stato completato in base al documento *Requisiti PCI DSS e procedure di valutazione della sicurezza*, versione *(insert version number)* e alle istruzioni ivi fornite.
☐	Tutte le informazioni contenute nel Rapporto sulla conformità sopra menzionato e in questo attestato rappresentano in modo onesto i risultati della valutazione sotto tutti gli aspetti.
☐	Il provider di servizi ha letto gli standard PCI DSS e accetta di garantire sempre la massima conformità a tali standard.
☐	Nessuna prova di memorizzazione dei dati della striscia magnetica (traccia)[9], CAV2, CVC2, CID o CVV2[10], oppure dei dati PIN [11] dopo l'autorizzazione della transazione è stata trovata sui sistemi controllati durante questa valutazione.

Parte 3b. Accettazione QSA e provider di servizi

Firma QSA principale ↑	***Data:***
Nome QSA principale:	***Mansione:***

Firma del funzionario esecutivo del provider di servizi ↑	***Data:***
Nome funzionario esecutivo del provider di servizi:	***Mansione:***

[8] Nei risultati contrassegnati come "presenti" devono essere inclusi i controlli compensativi esaminati da dal QSA. Se si rilevano controlli compensativi sufficienti per ridurre il rischio associato a un requisito, il QSA deve contrassegnare tale requisito come "presente".

[9] Dati codificati nella striscia magnetica utilizzati per l'autorizzazione durante una transazione con carta presente. Le entità non possono conservare tutti i dati completi della striscia magnetica dopo l'autorizzazione della transazione. I soli elementi dei dati di traccia che possono essere conservati sono il numero cliente, la data di scadenza e il nome.

[10] Il valore di tre o quattro cifre stampato nel riquadro della firma o nella parte anteriore di una carta di pagamento utilizzato per verificare le transazioni con carta non presente.

[11] 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.

Parte 4. Piano d'azione per lo stato di non conformità

Selezionare lo "Stato di conformità" appropriato per ciascun requisito. In caso di risposta negativa a uno dei requisiti, è necessario fornire la data in cui la Società sarà conforme al requisito e una breve descrizione delle azioni che verranno intraprese per soddisfare il requisito. *Consultare il marchio di pagamento prima di completare la Parte 4, perché non tutti i marchi di pagamento richiedono questa sezione.*

Requisito PCI	Descrizione	Stato di conformità (selezionare una risposta)	Data e azioni di correzione (in caso di non conformità)
1	Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta.	☐ Sì ☐ No	
2	Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di sicurezza.	☐ Sì ☐ No	
3	Proteggere i dati di titolari di carta memorizzati.	☐ Sì ☐ No	
4	Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche.	☐ Sì ☐ No	
5	Utilizzare e aggiornare regolarmente il software antivirus.	☐ Sì ☐ No	
6	Sviluppare e gestire sistemi e applicazioni protette.	☐ Sì ☐ No	
7	Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario.	☐ Sì ☐ No	
8	Assegnare un ID univoco a chiunque abbia accesso a un computer.	☐ Sì ☐ No	
9	Limitare l'accesso fisico ai dati di titolari di carta.	☐ Sì ☐ No	
10	Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta.	☐ Sì ☐ No	
11	Eseguire regolarmente test dei sistemi e processi di protezione.	☐ Sì ☐ No	
12	Gestire una politica che garantisca la sicurezza delle informazioni	☐ Sì ☐ No	

Appendice F: Revisioni PCI DSS – Determinazione dell'ambito e scelta dei campioni