



**Payment Card Industry (PCI)  
Data Security Standard  
Navigazione in PCI DSS**

---

**Comprensione dello scopo dei requisiti**

**Versione 2.0**

ottobre 2010

## Modifiche del documento

<i>Data</i>	<i>Versione</i>	<i>Descrizione</i>
<i>1 ottobre 2008</i>	<i>1.2</i>	<i>Allineare il contenuto con i nuovi standard PCI DSS v1.2 e implementare modifiche minori apportate dopo la versione originale v1.1.</i>
<i>28 ottobre 2010</i>	<i>2.0</i>	<i>Allineare il contenuto con il nuovo PCI DSS v2.0.</i>

## Sommario

---

<b>Modifiche del documento .....</b>	<b>2</b>
<b>Prefazione .....</b>	<b>4</b>
<i>Virtualizzazione.....</i>	<i>5</i>
<b>Dati dei titolari di carta e dati sensibili di autenticazione .....</b>	<b>6</b>
<i>Posizione dei dati dei titolari di carta e dei dati sensibili di autenticazione .....</i>	<i>8</i>
<i>Dati della traccia 1 e dati della traccia 2 .....</i>	<i>9</i>
<b>Istruzioni correlate per lo standard di sicurezza dei dati PCI.....</b>	<b>10</b>
<b>Istruzioni per i requisiti 1 e 2: Sviluppo e gestione di una rete sicura .....</b>	<b>11</b>
<i>Requisito 1: Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta .....</i>	<i>11</i>
<i>Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione .....</i>	<i>17</i>
<b>Istruzioni per i requisiti 3 e 4: Protezione dei dati di titolari di carta .....</b>	<b>20</b>
<i>Requisito 3: Proteggere i dati di titolari di carta memorizzati .....</i>	<i>20</i>
<i>Requisito 4: Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche.....</i>	<i>27</i>
<b>Istruzioni per i requisiti 5 e 6: Utilizzare un programma per la gestione delle vulnerabilità.....</b>	<b>29</b>
<i>Requisito 5: Utilizzare e aggiornare regolarmente il software o i programmi antivirus .....</i>	<i>29</i>
<i>Requisito 6: Sviluppare e gestire sistemi e applicazioni protette .....</i>	<i>31</i>
<b>Istruzioni per i requisiti 7, 8 e 9: Implementazione di rigide misure di controllo dell'accesso.....</b>	<b>39</b>
<i>Requisito 7: Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario .....</i>	<i>39</i>
<i>Requisito 8: Assegnare un ID univoco a chiunque abbia accesso a un computer .....</i>	<i>41</i>
<i>Requisito 9: Limitare l'accesso fisico ai dati dei titolari di carta.....</i>	<i>46</i>
<b>Istruzioni per i requisiti 10 e 11: Monitoraggio e test delle reti regolari .....</b>	<b>50</b>
<i>Requisito 10: Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta .....</i>	<i>50</i>
<i>Requisito 11: Eseguire regolarmente test dei sistemi e processi di protezione .....</i>	<i>54</i>
<b>Istruzioni per il requisito 12: Gestire una politica di sicurezza delle informazioni.....</b>	<b>60</b>
<i>Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale .....</i>	<i>60</i>
<b>Istruzioni per il requisito A.1: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso .....</b>	<b>66</b>
<b>Appendice A: PCI DSS: Documenti correlati .....</b>	<b>68</b>

## Prefazione

In questo documento sono descritti i 12 requisiti di Payment Card Industry Data Security Standard (PCI DSS) con una spiegazione dello scopo di ciascun requisito. Il presente documento è pensato per assistere gli esercenti, i provider di servizi e le istituzioni finanziarie che desiderano comprendere più chiaramente Payment Card Industry Data Security Standard e lo scopo e il significato specifici alla base dei requisiti dettagliati per i componenti di sistema sicuri (server, rete, applicazioni, ecc.) che supportano gli ambienti dei dati dei titolari di carta.

**NOTA: Navigazione in PCI DSS: Comprensione dello scopo dei requisiti è fornito solo a scopo informativo. Al completamento di una valutazione PCI DSS in sede o di un questionario di autovalutazione (SAQ), i documenti per la registrazione sono *Requisiti PCI DSS e procedure di valutazione della sicurezza e Questionari di autovalutazione PCI DSS v.2.0*.**

I requisiti di sicurezza PCI DSS si applicano a tutti i componenti di sistema. In ambito PCI DSS, per "componenti di sistema" si intende qualsiasi componente di rete, server o applicazione incluso o connesso all'ambiente dei dati dei titolari di carta. I "componenti di sistema" comprendono anche ogni componente di virtualizzazione come computer, switch/router, dispositivi, applicazioni/desktop virtuali e hypervisor. L'ambiente dei dati dei titolari di carta è composto da persone, processi e tecnologia che gestiscono 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 possono comprendere, senza limitazioni, tutte le applicazioni acquistate e personalizzate, comprese applicazioni interne ed esterne (ad esempio, Internet).

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

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

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

società Qualified Security Assessor (QSA) può offrire assistenza nella determinazione dell'ambito all'interno dell'ambiente dei dati dei titolari di carta di un'entità, mettendo a disposizione le istruzioni su come circoscrivere l'ambito di una valutazione PCI DSS mediante implementazione della segmentazione di rete adeguata.

Per le domande che riguardano la coerenza di una specifica implementazione con lo standard o con uno specifico requisito, PCI SSC consiglia di consultare una società Qualified Security Assessor (QSA) che si occuperà della convalida dell'implementazione di tecnologie e processi e della conformità allo standard di sicurezza dei dati PCI. L'esperienza delle società QSA nella gestione di ambienti di rete ben si presta a fornire le migliori pratiche e le indicazioni all'esercente o al provider di servizi che tenta di ottenere la conformità. L'elenco di QSA di PCI SSC è disponibile sul sito Web all'indirizzo: <https://www.pcisecuritystandards.org>.

## **Virtualizzazione**

In caso di implementazione della virtualizzazione, tutti i componenti all'interno dell'ambiente virtuale dovranno essere identificati e considerati nell'ambito della revisione, compresi i singoli host o dispositivi virtuali, computer guest, applicazioni, interfacce di gestione, console di gestione centrale, hypervisor, ecc. Tutte le comunicazioni intra-host e i flussi di dati devono essere identificati e documentati, così come quelli tra il componente virtuale ed altri componenti di sistema.

L'implementazione di un ambiente virtualizzato deve soddisfare lo scopo di tutti i requisiti, in modo che i sistemi virtualizzati possano essere considerati effettivamente come hardware separato. Ad esempio, ci deve essere una chiara segmentazione delle funzioni e la separazione delle reti con diversi livelli di sicurezza; la segmentazione dovrebbe impedire la condivisione ambienti di sviluppo/test e produzione; la configurazione virtuale deve essere protetta in modo che le vulnerabilità per una funzione non possano influire sulla sicurezza delle altre funzioni; ed i dispositivi, come dispositivi seriali/USB, non dovrebbero essere accessibili da tutte le istanze virtuali.

Inoltre, si dovrebbero inserire nella documentazione di sistema tutti i protocolli di interfaccia di gestione virtuale, e si dovrebbero definire ruoli e permessi per la gestione di reti e di componenti di sistema virtuali. Le piattaforme di virtualizzazione devono essere in grado di imporre una separazione di doveri e privilegi limitati, per separare la gestione della rete virtuale da quella del server virtuale.

É necessario prestare un'attenzione particolare in sede di implementazione di controlli di autenticazione per garantire che gli utenti effettuino l'autenticazione ai componenti di sistema virtuali corretti, e si operi una distinzione tra macchine virtuali (VM) guest ed hypervisor.

## Dati dei titolari di carta e dati sensibili di autenticazione

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

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

**Il PAN costituisce il fattore determinante nell'applicabilità dei requisiti PCI DSS.** Gli standard PCI DSS sono applicabili in caso di memorizzazione, elaborazione o trasmissione di un PAN (Primary Account Number, numero account primario). Se il PAN non viene memorizzato, elaborato o trasmesso, gli standard PCI DSS non sono validi.

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

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

La tabella riportata di seguito illustra gli elementi dei dati dei titolari di carta e dei dati di autenticazione sensibili 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 intende essere completa, ma illustra i diversi tipi di requisiti che si applicano a ciascun elemento di dati.

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

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

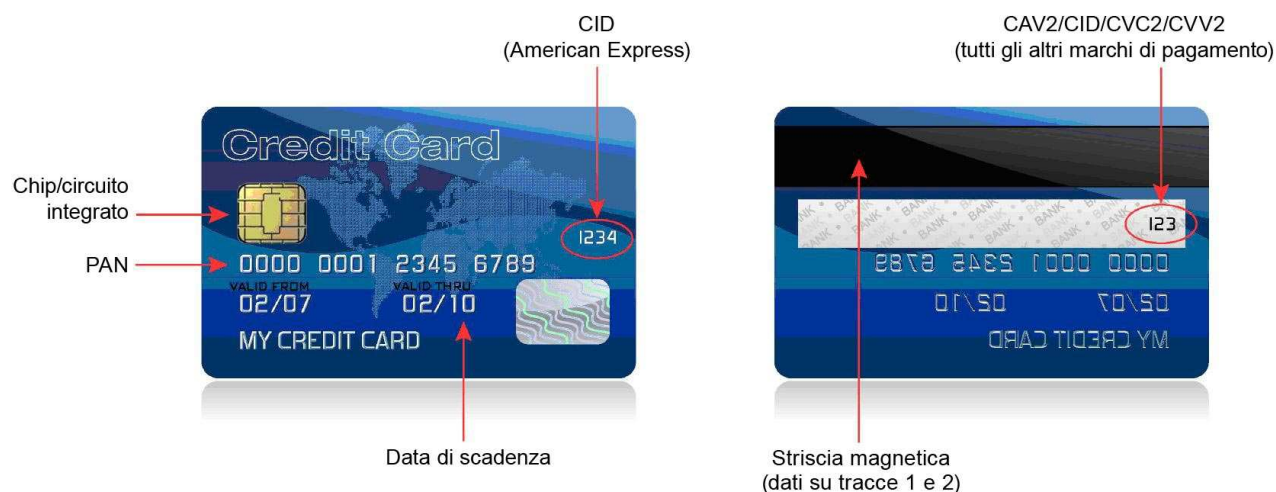
Gli standard PCI DSS **si applicano solo** in caso di memorizzazione, elaborazione e/o trasmissione dei PAN.

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

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

## Posizione dei dati dei titolari di carta e dei dati sensibili di autenticazione

I dati sensibili di autenticazione sono composti da dati della striscia magnetica (o traccia)<sup>3</sup>, valore o codice di validazione della carta<sup>4</sup>, e dati PIN<sup>5</sup>. **La memorizzazione dei dati sensibili di autenticazione è vietata.** Questi dati sono particolarmente preziosi per gli utenti non autorizzati, in quanto consentono loro di generare carte di pagamento false e conseguenti transazioni fraudolente. Fare riferimento al *PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi* per una definizione completa di "dati sensibili di autenticazione". Le immagini della parte anteriore e posteriore di una carta di credito, riportate sotto, mostrano la posizione dei dati del titolare della carta e dei dati di autenticazione sensibili.



**Nota:** Il chip contiene dati di traccia equivalenti ed altri dati sensibili, compreso il valore di verifica della carta con chip IC (Integrated Circuit) (definito anche Chip CVC, iCVV, CAV3 o iCSC).

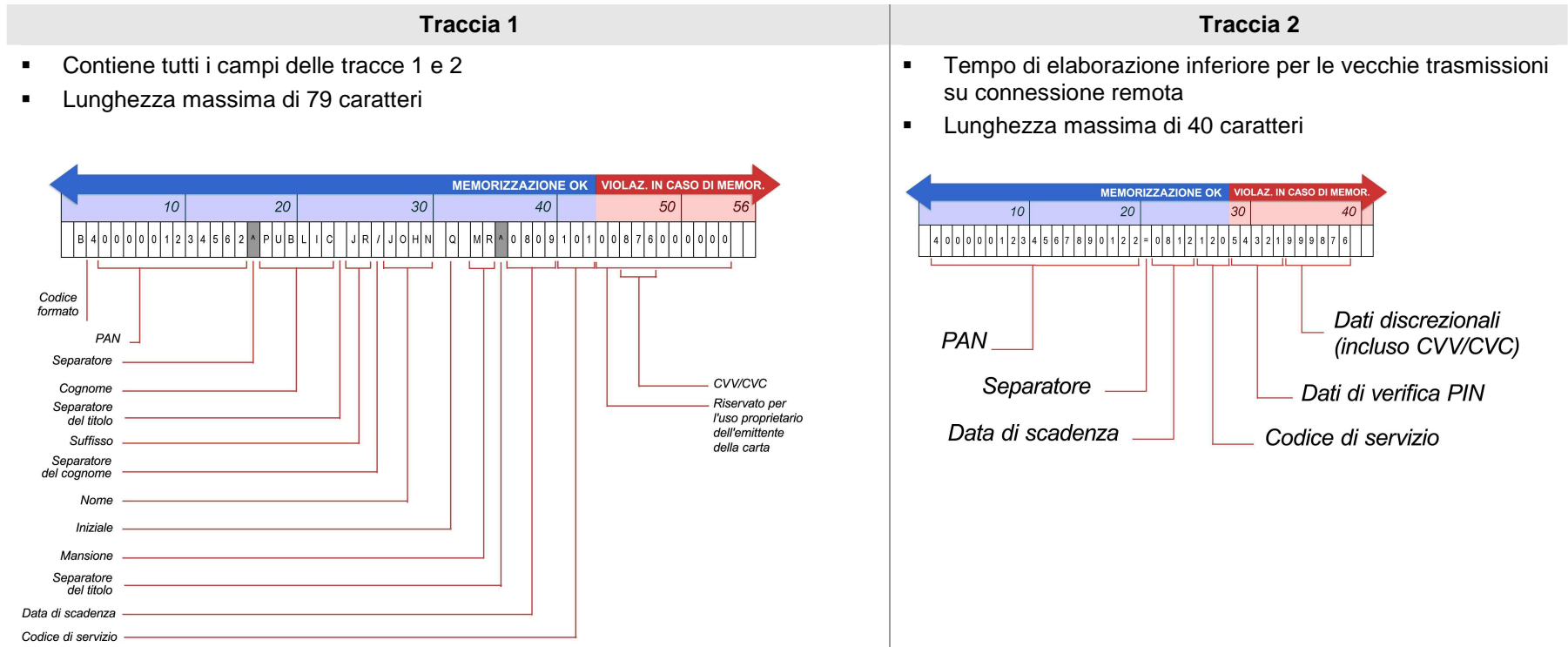
<sup>3</sup> Dati codificati nella striscia magnetica utilizzati per l'autorizzazione durante una transazione con carta presente. Questi dati possono essere anche in un chip o in un'altra posizione nella carta. Le entità non possono conservare i dati completi della striscia magnetica dopo l'autorizzazione della transazione. I soli elementi dei dati di traccia che possono essere conservati sono il PAN, il nome del titolare della carta, la data di scadenza e il codice di servizio.

<sup>4</sup> Il valore di tre o quattro cifre stampato nel riquadro della firma o a destra di questo riquadro oppure nella parte anteriore di una carta di pagamento utilizzato per verificare le transazioni con carta non presente.

<sup>5</sup> 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.

## Dati della traccia 1 e dati della traccia 2

Se vengono memorizzati dati a traccia completa (traccia 1 o traccia 2, dalla striscia magnetica, dall'immagine della striscia magnetica in un chip o in un'altra posizione), gli utenti non autorizzati che otterranno tali dati potranno riprodurre e vendere carte di pagamento nel mondo. La memorizzazione di dati a traccia completa, inoltre, viola le regolamentazioni operative dei marchi di pagamento e può comportare l'applicazione di multe e penali. L'illustrazione di seguito fornisce informazioni sui dati della traccia 1 e della traccia 2, descrivendo le differenze e presentando il layout dei dati memorizzati nella striscia magnetica.



**Nota:** I campi per i dati discrezionali sono definiti dall'emittente della carta e/o dal marchio di carte di pagamento. I campi definiti dall'emittente che contengono dati che l'emittente/marchio di carte di pagamento non considera dati sensibili di autenticazione possono essere inclusi all'interno della parte di dati discrezionali della traccia e, in determinate circostanze e condizioni, può essere consentita la memorizzazione di questi dati specifici come definito dall'emittente e/o marchio di carte di pagamento.

Ad ogni modo, eventuali dati considerati dati sensibili di autenticazione, contenuti in un campo per i dati discrezionali o in altra posizione, non possono essere memorizzati dopo l'autorizzazione.

## Istruzioni correlate per lo standard di sicurezza dei dati PCI

### 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 protezione

### 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 dei titolari di carta

### Monitoraggio e 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 per tutto il personale

## Istruzioni per i requisiti 1 e 2: Sviluppo e gestione di una rete sicura

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

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

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

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

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

Requisito	Istruzioni
<p><b>1.1</b> Stabilire standard di configurazione del firewall e del router che includano:</p>	<p>Firewall e router sono i componenti principali dell'architettura che controlla l'accesso e l'uscita dalla rete. Questi dispositivi di tipo software o hardware bloccano l'accesso indesiderato e gestiscono l'accesso autorizzato alla rete e l'uscita dalla stessa. Senza criteri e procedure in vigore per documentare la configurazione di router e firewall da parte del personale, un'azienda potrebbe facilmente perdere la sua prima linea di difesa per la protezione dei dati. I criteri e le procedure aiuteranno a garantire che la prima linea di difesa dell'organizzazione per la protezione dei suoi dati sia sempre solida.</p> <p>Gli ambienti virtuali in cui i flussi di dati non passano per una rete fisica dovrebbero essere sottoposti a valutazione per verificare la corretta esecuzione della segmentazione di rete.</p>
<p><b>1.1.1</b> 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</p>	<p>Un criterio e un processo per approvare e testare tutte le connessioni e le modifiche ai firewall e a i router aiuteranno a prevenire i problemi di protezione causati dall'errata configurazione della rete, del router o del firewall.</p> <p>I flussi di dati tra macchine virtuali dovrebbero essere inseriti in un criterio ed in un processo.</p>

Requisito	Istruzioni
<p><b>1.1.2</b> Un diagramma aggiornato della rete con tutte le connessioni ai dati di titolari di carta, comprese eventuali reti wireless</p>	<p>I diagrammi di rete consentono all'organizzazione di identificare la posizione di tutti i suoi dispositivi di rete. Inoltre, il diagramma di rete può essere utilizzato per rilevare il flusso dei dati dei titolari di carta all'interno della rete e tra i singoli dispositivi, in modo da comprendere a fondo l'ambito dell'ambiente dei dati dei titolari di carta. In assenza dei diagrammi della rete corrente e del flusso di dati, i dispositivi che contengono dati dei titolari di carta possono essere trascurati e privati inconsapevolmente dei controlli di protezione a strati implementati per PCI DSS, rimanendo così vulnerabili in caso di compromissione.</p> <p>I diagrammi della rete e del flusso di dati dovrebbero comprendere componenti di sistema virtuali e documentare i flussi di dati Intra-host.</p>
<p><b>1.1.3</b> Requisiti per un firewall per ogni connessione Internet e tra tutte le zone demilitarizzate (DMZ) e la zona della rete interna</p>	<p>L'uso di un firewall su ogni connessione in ingresso (e in uscita) nella rete consente all'organizzazione di controllare l'accesso e l'uscita, nonché di ridurre al minimo le possibilità che un utente non autorizzato ottenga l'accesso alla rete interna.</p>
<p><b>1.1.4</b> Descrizione di gruppi, ruoli e responsabilità per la gestione logica dei componenti della rete</p>	<p>Questa descrizione dei ruoli e dell'assegnazione di responsabilità garantisce la disponibilità di un responsabile della sicurezza di tutti i componenti e la sua consapevolezza di tale responsabilità, evitando che alcuni dispositivi rimangano ingestiti.</p>
<p><b>1.1.5</b> 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.</p> <p>Esempi di servizi, protocolli o porte non sicuri includono, senza limitazioni, FTP, Telnet, POP3, IMAP e SNMP.</p>	<p>Le compromissioni spesso avvengono a causa di servizi e porte inutilizzati o non protetti, in quanto spesso essi presentano delle vulnerabilità note. Molte organizzazioni sono vulnerabili a questi tipi di compromissioni, perché non applicano le patch di protezione per la correzione delle vulnerabilità di servizi, protocolli e porte non in uso (anche se le vulnerabilità sono tuttora presenti). Ogni organizzazione dovrebbe chiaramente decidere quali servizi, protocolli e porte sono necessari per il relativo business, documentarli a fini di registrazione e garantire che tutti gli altri servizi, protocolli e porte vengano disabilitati o rimossi. Inoltre, le organizzazioni dovrebbero valutare la possibilità di bloccare tutto il traffico, riaprendo le porte solo dopo aver determinato e documentato un'esigenza.</p> <p>Inoltre, esistono molti servizi, protocolli o porte di cui un'azienda potrebbe avere bisogno (o che sono attivate per impostazione predefinita), e che sono comunemente utilizzate da utenti non autorizzati per compromettere una rete. Se questi servizi, protocolli o porte non sicuri sono indispensabili per l'azienda, è necessario comprendere pienamente il rischio posto dall'uso di questi protocolli e accettarlo; occorre inoltre giustificare l'uso del protocollo e documentare e implementare le funzionalità di protezione che consentono l'uso sicuro di tali protocolli. Se questi servizi, protocolli o porte non sicuri non sono indispensabili per l'azienda, è opportuno disabilitarli o rimuoverli.</p>

Requisito	Istruzioni
<p><b>1.1.6</b> Una revisione dei set di regole del firewall e del router almeno ogni sei mesi</p>	<p>Questa revisione consente all'organizzazione di cancellare ogni sei mesi eventuali regole inutili, obsolete o errate, garantendo che tutti i set di regole consentano solamente le porte e i servizi autorizzati corrispondenti alle giustificazioni aziendali.</p> <p>È consigliabile svolgere tali revisioni con maggiore frequenza, ad esempio ogni mese, per garantire che i set di regole siano aggiornati e corrispondano alle esigenze dell'azienda, senza aprire falle nella protezione e correre rischi inutili.</p>
<p><b>1.2</b> Creare la configurazione del firewall e del router che limiti le connessioni tra le reti non attendibili e qualsiasi componente di sistema nell'ambiente dei dati dei titolari di carta.</p> <p><b>Nota:</b> una "rete non attendibile" è una qualsiasi rete esterna alle reti che appartengono all'entità sottoposta a revisione e/o che l'entità non è in grado di controllare o gestire.</p>	<p>È fondamentale installare una protezione di rete, nello specifico un componente di sistema con (come minimo) una capacità di firewall di controllo efficiente, tra la rete interna attendibile e qualsiasi altra rete non attendibile che sia esterna e/o non compresa nella capacità di controllo o gestione dell'entità. La mancata implementazione di questa misura comporta la vulnerabilità dell'entità all'accesso non autorizzato da parte di utenti o software dannosi.</p> <p>Se il firewall è installato ma non dispone di regole che controllano o limitano determinati tipi di traffico, gli utenti non autorizzati possono ancora sfruttare protocolli e porte vulnerabili per attaccare la rete.</p>
<p><b>1.2.1</b> Limitazione del traffico in entrata e in uscita a quello indispensabile per l'ambiente dati dei titolari di carta.</p>	<p>Questo requisito intende impedire agli utenti non autorizzati di accedere alla rete dell'organizzazione tramite indirizzi IP non autorizzati o mediante l'uso di servizi, protocolli o porte in maniera non autorizzata (ad esempio per inviare i dati ottenuti all'interno della rete verso un server non attendibile).</p> <p>Tutti i firewall dovrebbero includere una regola che nega il traffico in entrata e in uscita che non è specificamente necessario. Questa scelta può impedire l'apertura involontaria di falle che consentirebbero l'entrata o l'uscita di altro traffico non previsto e potenzialmente dannoso.</p>
<p><b>1.2.2</b> Protezione e sincronizzazione dei file di configurazione del router.</p>	<p>Se i file di configurazione in esecuzione sono generalmente implementati con impostazioni sicure, i file di avvio (i router eseguono questi file solo al riavvio) potrebbero non essere implementati con le stesse impostazioni sicure a causa dell'esecuzione occasionale. Quando un router esegue il riavvio con le stesse impostazioni sicure utilizzate nei file di configurazione in esecuzione, le regole potrebbero indebolirsi e consentire la presenza sulla rete di individui non autorizzati, perché i file di avvio potrebbero non essere implementati con le stesse impostazioni sicure dei file di configurazione in esecuzione.</p>

Requisito	Istruzioni
<p><b>1.2.3</b> 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.</p>	<p>L'implementazione e lo sfruttamento noti (o sconosciuti) della tecnologia wireless all'interno di una rete rappresentano un percorso noto agli utenti non autorizzati per ottenere l'accesso alla rete e ai dati dei titolari di carte. Se viene installato un dispositivo o una rete wireless senza che l'azienda ne sia a conoscenza, un utente non autorizzato potrebbe accedere alla rete con facilità e in modo "invisibile". Se i firewall non limitano l'accesso dalle reti wireless all'ambiente delle carte di pagamento, gli utenti che ottengono accesso non autorizzato alla rete wireless possono facilmente connettersi all'ambiente delle carte di pagamento e compromettere le informazioni dei conti.</p> <p>Si devono installare i firewall tra tutte le reti wireless ed l'ambiente dei dati dei titolari di carta (CDE), indipendentemente dallo scopo dell'ambiente al quale la rete wireless network è collegata. Ciò può comprendere, tra l'altro, reti aziendali, negozi di vendita al dettaglio, ambienti magazzino, ecc.</p>
<p><b>1.3</b> Vietare l'accesso pubblico diretto tra Internet e i componenti di sistema nell'ambiente dei dati di titolari di carta.</p>	<p>Lo scopo di un firewall è gestire e controllare tutte le connessioni tra sistemi pubblici e sistemi interni (in particolare quelli che memorizzano, elaborano o trasmettono i dati dei titolari di carta). Se è consentito l'accesso diretto tra sistemi pubblici e gli ambienti dei dati dei titolari di carta, la protezione offerta dal firewall viene superata e i componenti di sistema che memorizzano i dati dei titolari di carta sono esposti alla compromissione.</p>
<p><b>1.3.1</b> Implementare una zona demilitarizzata (DMZ) per limitare il traffico in entrata ai soli componenti di sistema che forniscono servizi, protocolli e porte autorizzati accessibili pubblicamente.</p>	<p>La zona DMZ è la parte del firewall che gestisce le connessioni tra Internet (o altre reti non attendibili) e i servizi interni che un'organizzazione deve mettere a disposizione del pubblico (ad esempio un server Web). È la prima linea di difesa per l'isolamento e la separazione del traffico che necessita di comunicare con la rete interna dal traffico che non ha tale esigenza.</p> <p>Questa funzionalità intende impedire agli utenti non autorizzati di accedere alla rete dell'organizzazione tramite indirizzi IP non autorizzati o mediante l'uso di servizi, protocolli o porte in maniera non autorizzata.</p>
<p><b>1.3.2</b> Limitare il traffico Internet in entrata agli indirizzi IP all'interno della zona DMZ.</p>	<p>La terminazione delle connessioni IP alla zona DMZ fornisce l'opportunità per controllare e limitare fonte/destinazione e/o per controllare e bloccare i contenuti, in modo da evitare accesso non filtrato tra ambienti attendibili e non attendibili.</p>
<p><b>1.3.3</b> Non consentire alcun percorso diretto per il traffico in entrata o in uscita tra Internet e l'ambiente dei dati di titolari di carta.</p>	<p>La terminazione delle connessioni IP sia in entrata che in uscita fornisce l'opportunità per controllare e limitare fonte/destinazione e/o per controllare e bloccare i contenuti, in modo da evitare accesso non filtrato tra ambienti attendibili e non attendibili. Ciò contribuisce ad impedire, ad esempio, l'invio, da parte di utenti non autorizzati, di dati che hanno ottenuto all'interno della rete ad un server esterno non attendibile in una rete non attendibile.</p>

Requisito	Istruzioni
<p><b>1.3.4</b> Non consentire agli indirizzi interni di passare da Internet alla zona DMZ.</p>	<p>Di solito un pacchetto contiene l'indirizzo IP del computer che lo ha inviato: in questo modo gli altri computer della rete sanno da dove proviene. In alcuni casi, questo indirizzo IP di invio viene sottoposto a spoofing da parte di utenti non autorizzati.</p> <p>Ad esempio, gli individui non autorizzati inviano un pacchetto con un indirizzo sottoposto a spoofing, in modo che il pacchetto sia in grado di raggiungere la rete da Internet (se il firewall non lo proibisce) fingendo di essere un traffico interno e quindi legittimo. Una volta ottenuto l'accesso alla rete, l'utente non autorizzato può iniziare a compromettere i sistemi.</p> <p>L'uso di filtri in ingresso è una tecnica adottabile sul firewall per filtrare i pacchetti in arrivo nella rete al fine di, tra le altre cose, garantire che i pacchetti non abbiano subito un spoofing per far sì che sembrino provenire dalla rete interna.</p> <p>Per ulteriori informazioni sui filtri dei pacchetti, è possibile cercare informazioni su una tecnica corollario chiamata "uso di filtri in uscita".</p>
<p><b>1.3.5</b> Non consentire il traffico in uscita non autorizzato dall'ambiente dei dati dei titolari di carta ad Internet.</p>	<p>Tutto il traffico in uscita dall'interno dell'ambiente dei dati dei titolari di carta dovrebbe essere valutato per assicurare che segua norme autorizzate e definite. Si dovrebbero controllare le connessioni per limitare il traffico solo alle comunicazioni autorizzate (ad esempio limitando indirizzi/porte fonte/destinazione e/o bloccando i contenuti).</p> <p>Nei casi in cui negli ambienti non è consentita la connettività in entrata, le connessioni in uscita possono essere ottenute mediante architetture o componenti di sistema che interrompono e controllano la connettività IP.</p>
<p><b>1.3.6</b> Implementare un controllo efficiente, anche noto come "dynamic packet filtering" (ossia che consente solo alle connessioni già "stabilite" di accedere alla rete).</p>	<p>Un firewall che esegue l'ispezione dei pacchetti "stateful" mantiene lo stato di ogni connessione al firewall. Grazie alla conservazione dello stato, il firewall sa se quella che sembra essere la risposta a una connessione precedente è realmente una risposta (in quanto "ricorda" la connessione precedente) o se si tratta di un utente o software non autorizzato che cerca di indurre il firewall a consentire la connessione.</p>
<p><b>1.3.7</b> Posizionare i componenti di sistema che memorizzano dati dei titolari di carta (come un database) in una zona di rete interna, separata dalla zona DMZ e da altre reti non attendibili.</p>	<p>I dati dei titolari di carte richiedono il massimo livello di protezione delle informazioni. Se i dati dei titolari di carte sono all'esterno della zona DMZ, un aggressore può accedere più facilmente a queste informazioni, in quanto esistono meno strati da penetrare.</p> <p><b>Nota:</b> lo scopo di questo requisito non comprende la memorizzazione nella memoria volatile.</p>

Requisito	Istruzioni
<p><b>1.3.8</b> Non divulgare indirizzi IP privati ed informazioni di routing a parti non autorizzate.</p> <p><b>Nota:</b> <i>i metodi per oscurare l'indirizzamento IP possono includere, senza limitazioni:</i></p> <ul style="list-style-type: none"> <li>▪ NAT (Network Address Translation)</li> <li>▪ Posizionamento di server contenenti dati dei titolari di carta dietro server/firewall proxy o cache contenuti,</li> <li>▪ Rimozione o filtraggio di annunci di instradamento per reti private che utilizzano indirizzamento registrato,</li> <li>▪ Uso interno di spazio indirizzi RFC1918 invece degli indirizzi registrati.</li> </ul>	<p>Limitare la trasmissione degli indirizzi IP è fondamentale per evitare che un hacker si "impossessi" degli indirizzi IP della rete interna, e utilizzi tali informazioni per accedere alla rete.</p> <p>I metodi efficaci per soddisfare lo scopo di questo requisiti possono variare in funzione della tecnologia di rete specifica in uso nell'ambiente. Ad esempio, i controlli adottati per soddisfare questo requisito possono essere diversi per reti IPv4 rispetto a quelli in uso per le reti IPv6.</p> <p>Una tecnica per impedire che le informazioni degli indirizzi IP vengano scoperte su una rete IPv4 prevede l'implementazione di NAT (Network Address translation). Il NAT, generalmente gestito dal firewall, consente a un'organizzazione di disporre di indirizzi interni visibili solo all'interno della rete e di indirizzi esterni visibili esternamente. Se un firewall non "nasconde" o maschera gli indirizzi IP della rete interna, un utente non autorizzato potrebbe scoprire gli indirizzi IP interni e tentare di accedere alla rete con un indirizzo IP falsificato.</p> <p>Per le reti IPv4, lo spazio indirizzi RFC1918 è riservato all'indirizzamento interno e non dovrebbe essere instradabile su Internet. In quanto tale, viene preferito per l'indirizzamento IP di reti interne. Tuttavia, le organizzazioni possono avere dei motivi per usare spazio indirizzi non-RFC1918 sulla rete interna. In tali circostanze, si dovrebbero impedire annunci di instradamento oppure usare altre tecniche per evitare la trasmissione dello spazio indirizzi interno su Internet o la sua divulgazione a parti non autorizzate.</p>
<p><b>1.4</b> Installare firewall personali (software) su tutti i computer portatili e i computer di proprietà dei dipendenti con connettività diretta a Internet (ad esempio, laptop utilizzati dai dipendenti), che vengono utilizzati per accedere alla rete aziendale.</p>	<p>Se un computer non dispone di un firewall o di un programma antivirus installato, spyware, cavalli di Troia, virus, worm e rootkit (malware) possono essere scaricati e/o installati inconsapevolmente. Il computer è ancora più vulnerabile se è connesso direttamente a Internet e non è dietro il firewall aziendale. Il malware caricato su un computer quando non si trova dietro il firewall aziendale può quindi scegliere come bersaglio le informazioni all'interno della rete nel momento in cui il computer viene ricollegato alla rete aziendale.</p> <p><b>Nota:</b> <i>Lo scopo di questo requisito riguarda i computer per l'accesso remoto indipendentemente dal fatto che siano di proprietà dei dipendenti o della società. I sistemi che non possono essere gestiti dalla politica aziendale introducono dei punti deboli al perimetro e offrono opportunità di cui gli utenti non autorizzati possono approfittare.</i></p>

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

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

Requisito	Istruzioni
<p><b>2.1</b> Modificare sempre le impostazioni predefinite dei fornitori <b>prima</b> di procedere all'installazione di un sistema sulla rete, incluso, senza limitazione, password, stringhe di comunità SNMP (simple network management protocol) ed eliminazione di account non necessari.</p>	<p>Gli utenti non autorizzati (all'interno o all'esterno dell'azienda) utilizzano spesso le impostazioni predefinite, i nomi degli account e le password dei fornitori per accedere in modo improprio ai sistemi. Queste impostazioni sono note nelle comunità degli hacker e aumentano la vulnerabilità agli attacchi del sistema.</p>
<p><b>2.1.1</b> 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.</p>	<p>Molti utenti installano questi dispositivi senza l'approvazione del management e non cambiano le impostazioni predefinite né configurano le impostazioni di protezione. Se le reti wireless non vengono implementate con configurazioni di sicurezza sufficienti (che comprendono la modifica delle impostazioni predefinite), gli sniffer wireless possono ascoltare di nascosto il traffico, acquisire facilmente i dati e accedere alla rete per l'attacco. Inoltre, il protocollo di scambio delle chiavi per la precedente versione della cifratura 802.11x (WEP) è stato violato e può rendere inutile la crittografia. Verificare che il firmware dei dispositivi sia aggiornato per supportare protocolli più sicuri (ad esempio, WPA2).</p>
<p><b>2.2.</b> Sviluppare standard di configurazione per tutti i componenti di sistema. Accertarsi che questi standard risolvano tutte le vulnerabilità della sicurezza note e siano coerenti con gli standard di hardening accettati dal settore.</p> <p>Le fonti di standard di hardening accettati dal settore possono includere, senza limitazione:</p> <ul style="list-style-type: none"> <li>▪ CIS (Center for Internet Security)</li> <li>▪ ISO (International Organization for Standardization)</li> <li>▪ SANS (SysAdmin Audit Network Security)</li> <li>▪ NIST (National Institute of Standards Technology)</li> </ul>	<p>Esistono punti deboli noti in molti sistemi operativi, database e applicazioni aziendali, ma esistono anche metodi noti per configurare questi sistemi e risolvere le vulnerabilità di protezione. Per aiutare i meno esperti nel campo della sicurezza, le organizzazioni che si occupano di sicurezza hanno stabilito alcune raccomandazioni per il rafforzamento dei sistemi che spiegano anche come gestire questi punti deboli. Se i punti deboli dei sistemi (ad esempio impostazioni deboli per i file, oppure servizi e protocolli predefiniti che spesso non sono necessari) non vengono risolti, un aggressore può utilizzare più sfruttamenti noti per attaccare servizi e protocolli vulnerabili, ottenendo così l'accesso alla rete dell'organizzazione. Siti Web di base dove è possibile ottenere ulteriori informazioni sulle pratiche migliori che possono fornire assistenza per l'implementazione degli standard di configurazione, comprendono, senza limitazione: <a href="http://www.nist.gov">www.nist.gov</a>, <a href="http://www.sans.org">www.sans.org</a>, <a href="http://www.cisecurity.org">www.cisecurity.org</a>, <a href="http://www.iso.org">www.iso.org</a>.</p> <p>É necessario anche tenere aggiornati gli standard di configurazione del sistema per assicurare che i punti deboli rilevati di recente vengano corretti prima dell'installazione del sistema nella rete.</p>

Requisito	Istruzioni
<p><b>2.2.1</b> Implementare solo una funzione principale per server per impedire la coesistenza sullo stesso server di funzioni che richiedono livelli di sicurezza diversi. Ad esempio, server Web, database server e DNS devono essere implementati su server separati.</p> <p><i>Nota: Dove si utilizzano tecnologie di virtualizzazione, implementare solo una funzione principale per componente di sistema virtuale.</i></p>	<p>Questo requisito consente di garantire che gli standard di configurazione dei sistemi e i processi correlati dell'organizzazione gestiscano le funzioni server che necessitano di diversi livelli di protezione o che possono introdurre punti deboli a livello di sicurezza nelle altre funzioni dello stesso server. Ad esempio:</p> <ol style="list-style-type: none"> <li>1. Un database, che necessita di solide misure di protezione attive, sarebbe a rischio se il server fosse condiviso con un'applicazione Web, che deve essere aperta e affacciarsi direttamente su Internet.</li> <li>2. La mancata applicazione di una patch per una funzione all'apparenza minore potrebbe generare una compromissione che influisce su altre funzioni più importanti (ad esempio un database) sullo stesso server.</li> </ol> <p>Questo requisito è pensato per tutti i server all'interno dell'ambiente dei dati dei titolari di carta (in genere basati su Unix, Linux o Windows). Questo requisito non si può applicare ai sistemi che hanno la capacità di implementare in modo nativo i livelli di sicurezza su un singolo server (ad es. mainframe).</p> <p>Nei casi in cui si utilizzano tecnologie di virtualizzazione, ogni componente virtuale (ad es. macchina virtuale, switch virtuale, dispositivi di sicurezza virtuale, ecc.) dovrebbe essere considerato un limite di "server". Singoli hypervisor possono supportare funzioni diverse, ma una singola macchina virtuale dovrebbe attenersi alla regola di "una funzione primaria". In questo scenario, la compromissione dell'hypervisor potrebbe determinare la compromissione di tutte le funzioni di sistema. Di conseguenza, si dovrebbe tener conto anche del livello di rischio quando si collocano funzioni o componenti multipli su un singolo sistema fisico.</p>
<p><b>2.2.2</b> Abilitare solo servizi, protocolli, daemon ecc. necessari e sicuri, come richiesto per la funzione del sistema.</p> <p>Implementare funzioni di sicurezza per ogni servizio, protocollo o daemon necessario considerato non sicuro. Ad esempio, usare tecnologie sicure come SSH, S-FTP, SSL, o IPsec VPN per proteggere servizi non sicuri come NetBIOS, file-sharing, Telnet, FTP, ecc.</p>	<p>Come affermato al requisito 1.1.5, esistono molti protocolli di cui un'azienda potrebbe avere bisogno (o che sono attivati per impostazione predefinita), e che sono comunemente utilizzati da utenti non autorizzati per compromettere una rete. Per garantire che solo i servizi e i protocolli necessari siano attivati e che tutti i servizi o protocolli non sicuri siano protetti in modo adeguato prima dell'implementazione di nuovi server, questo requisito deve essere parte degli standard di configurazione dell'organizzazione e dei processi correlati.</p>
<p><b>2.2.3</b> Configurare i parametri di sicurezza del sistema per evitare un uso improprio.</p>	<p>Questo requisito intende garantire che gli standard di configurazione dei sistemi dell'organizzazione e i processi correlati gestiscano nello specifico le impostazioni di protezione e i parametri che presentano implicazioni note per la sicurezza.</p>
<p><b>2.2.4</b> Rimuovere tutta la funzionalità non necessaria, ad esempio script, driver, funzioni, sottosistemi, file system e server Web non utilizzati.</p>	<p>Gli standard di protezione dei server devono includere processi per gestire le funzionalità non necessarie con implicazioni specifiche per la sicurezza (ad esempio la rimozione/disabilitazione di FTP o del server Web se il server non eseguirà queste funzioni).</p>

Requisito	Istruzioni
<p><b>2.3</b> Eseguire la cifratura di tutto l'accesso amministrativo non da console, tramite crittografia avanzata. Utilizzare tecnologie quali SSH, VPN o SSL/TLS per la gestione basata su Web e altre attività amministrative non da console.</p>	<p>Se l'amministrazione remota non viene eseguita con l'autenticazione sicura e comunicazioni cifrate, un utente non autorizzato può rilevare informazioni sensibili a livello amministrativo e operativo (ad esempio le password degli amministratori). Un utente non autorizzato può utilizzare queste informazioni per accedere alla rete, divenire un amministratore e sottrarre i dati.</p>
<p><b>2.4</b> I provider di hosting condiviso devono proteggere l'ambiente ospitato e i dati di titolari di carta di ciascuna entità. Questi provider devono soddisfare specifici requisiti come descritto nell'<i>Appendice A: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso</i>.</p>	<p>Questo requisito è destinato ai provider di hosting che forniscono ambienti di hosting condiviso per più client sullo stesso server. Quando tutti i dati si trovano sullo stesso server e sono sotto il controllo di un singolo ambiente, spesso le impostazioni di questi server condivisi non sono gestite dai singoli client, pertanto i client possono aggiungere funzioni non sicure e script che influiscono sulla sicurezza di tutti gli altri ambienti client; di conseguenza, diventa più facile che un utente non autorizzato comprometta i dati di un client e ottenga così l'accesso ai dati di tutti gli altri client. Vedere l'<i>Appendice A</i>:</p>

## Istruzioni per i requisiti 3 e 4: Protezione dei dati di titolari di carta

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

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

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

Requisito	Istruzioni
<p><b>3.1</b> Mantenere al minimo la memorizzazione dei dati dei titolari di carta implementando politiche, procedure e processi per la conservazione e l'eliminazione dei dati, come segue.</p> <p><b>3.1.1</b> Implementare una politica per la conservazione e l'eliminazione dei dati che comprenda:</p> <ul style="list-style-type: none"> <li>▪ Limitazione della quantità dei dati memorizzati e il tempo di conservazione in base alle esigenze aziendali, legali e legislative</li> <li>▪ Processi per la rimozione sicura dei dati quando non sono più necessari</li> <li>▪ Requisiti specifici di conservazione dei dati dei titolari di carta</li> <li>▪ Processo manuale o automatico trimestrale per identificare ed eliminare in modo sicuro i dati dei titolari di carta memorizzati che superano i requisiti di conservazione definiti</li> </ul>	<p>Una politica formale per la conservazione dei dati identifica quali dati devono essere conservati e dove sono collocati in modo da poter essere distrutti o cancellati in modo sicuro non appena non servono più. Al fine di definire dei requisiti di conservazione adeguati, un'entità deve prima comprendere quali siano le sue esigenze aziendali nonché ogni obbligo di natura legale o legislativa che sia valido per il loro settore e/o che riguarda il tipo di dati che viene conservato.</p> <p>La memorizzazione estesa dei dati dei titolari di carte, che va oltre le esigenze aziendali, pone un rischio inutile. I soli dati dei titolari di carte che possono essere conservati dopo l'autorizzazione sono il PAN (primary account number) (reso illeggibile), la data di scadenza, il nome e il codice di servizio.</p> <p>L'implementazione di metodi di eliminazione sicura garantisce che i dati non possano essere recuperati quando non servono più.</p> <p><b>Se non sono necessari, non conservarli!</b></p>

Requisito	Istruzioni
<p><b>3.2 Non memorizzare dati sensibili di autenticazione dopo l'autorizzazione (anche se crittografati).</b></p> <p>I dati sensibili di autenticazione includono i dati citati nei seguenti Requisiti da 3.2.1 a 3.2.3:</p> <p><i><b>Nota:</b> ad Emittenti e società che supportano servizi di emissione è consentita la memorizzazione di dati sensibili di autenticazione in presenza di una giustificazione aziendale e di una memorizzazione sicura dei dati.</i></p>	<p>I dati sensibili di autenticazione sono composti da dati della striscia magnetica (o traccia)<sup>6</sup>, valore o codice di validazione della carta<sup>7</sup>, e dati PIN<sup>8</sup>. <b>La memorizzazione dei dati sensibili di autenticazione dopo l'autorizzazione è vietata.</b> Questi dati sono particolarmente preziosi per gli utenti non autorizzati, in quanto consentono loro di generare carte di pagamento contraffatte e conseguenti transazioni fraudolente. Vedere il documento PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi per la definizione completa di "dati di autenticazione sensibili".</p> <p><i><b>Nota:</b> Alle società che eseguono, facilitano o supportano servizi di emissione è consentito memorizzare dati sensibili di autenticazione SOLO SE hanno un'esigenza aziendale legittima per farlo. Tenere presente che tutti i requisiti PCI DSS si riferiscono ad emittenti e l'unica eccezione per emittenti ed elaboratori di emittenti è che i dati sensibili di autenticazione possono essere conservati in presenza di un motivo legittimo per farlo. Un motivo legittimo è quello necessario per l'esecuzione della funzione che viene fornita dall'emittente e non un motivo di convenienza.</i></p> <p><i>Ciascuno di questi dati deve essere memorizzato in un luogo sicuro ed in conformità ai requisiti PCI DSS e a quelli specifici del marchio di pagamento.</i></p>

<sup>6</sup> Dati codificati nella striscia magnetica utilizzati per l'autorizzazione durante una transazione con carta presente. Questi dati possono essere anche in un chip o in un'altra posizione nella carta. 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 PAN, il nome del titolare della carta, la data di scadenza e il codice di servizio.

<sup>7</sup> Il valore di tre o quattro cifre stampato nel riquadro della firma o a destra di questo riquadro oppure nella parte anteriore di una carta di pagamento utilizzato per verificare le transazioni con carta non presente.

<sup>8</sup> 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.

Requisito	Istruzioni
<p><b>3.2.1</b> Non memorizzare l'intero contenuto delle tracce (dalla striscia magnetica presente sul retro della carta, dati equivalenti contenuti in un chip o in altro luogo). Questi dati sono denominati anche traccia completa, traccia, traccia 1, traccia 2 e dati di striscia magnetica.</p> <p><b>Nota:</b> <i>nel normale svolgimento delle attività, è possibile che sia necessario conservare i seguenti elementi di dati della striscia magnetica:</i></p> <ul style="list-style-type: none"> <li>▪ Nome del titolare della carta</li> <li>▪ PAN (Primary Account Number)</li> <li>▪ Data di scadenza</li> <li>▪ Codice di servizio</li> </ul> <p><i>Per ridurre al minimo il rischio, memorizzare solo gli elementi di dati necessari per l'azienda.</i></p>	<p>Se vengono memorizzati dati a traccia completa, gli utenti non autorizzati che otterranno tali dati potranno riprodurre e vendere carte di pagamento.</p>
<p><b>3.2.2</b> Non memorizzare il codice o il valore di verifica della carta (numero a tre o quattro cifre impresso sulla parte anteriore o posteriore della carta di pagamento) utilizzato per verificare le transazioni con carta non presente.</p>	<p>Lo scopo del codice di validazione della carta è proteggere le transazioni in cui il consumatore e la carta non sono presenti, ad esempio ordini via Internet oppure ordini via posta/telefono (MO/TO). Questi tipi di transazioni possono essere autenticati come provenienti dal proprietario della carta solo richiedendo questo codice di validazione della carta, in quando il proprietario della carta dispone della carta e può leggere il valore. Se questi dati vietati vengono memorizzati e successivamente sottratti, gli individui non autorizzati possono eseguire transazioni Internet e MO/TO fraudolente.</p>
<p><b>3.2.3</b> Non memorizzare il numero di identificazione personale (PIN) o il blocco PIN cifrato.</p>	<p>Questi valori dovrebbero essere noti soltanto al proprietario della carta o alla banca che ha emesso la carta. Se questi dati vietati vengono memorizzati e successivamente sottratti, gli individui non autorizzati possono eseguire transazioni fraudolente di addebito basate su PIN (ad esempio prelievi Bancomat).</p>
<p><b>3.3</b> Mascherare il PAN quando visualizzato (non devono essere visibili più di sei cifre all'inizio e quattro cifre alla fine).</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>▪ <i>questo requisito non si applica ai dipendenti e ad altre parti che hanno l'esigenza aziendale legittima di visualizzare l'intero PAN.</i></li> <li>▪ <i>Questo requisito non sostituisce i requisiti più rigorosi per la visualizzazione dei dati di titolari di carta, ad esempio per ricevute di punti di vendita (POS).</i></li> </ul>	<p>La visualizzazione dell'intero PAN su elementi quali monitor di computer, ricevute di carte di pagamento, fax o rendicontazioni cartacee può comportare il recupero di tali dati da parte di utenti non autorizzati e il loro utilizzo fraudolento. Il PAN può essere visualizzato in forma completa sulle ricevute "copia per l'esercente"; tuttavia, la ricevuta cartacea deve rispettare gli stessi requisiti di sicurezza delle copie elettroniche e seguire le indicazioni dello standard di sicurezza dei dati PCI, in particolare il Requisito 9 sulla sicurezza fisica. Il PAN intero può essere inoltre visualizzato da chi ha un'esigenza aziendale legittima di vederlo.</p> <p>Questo requisito si riferisce anche alla protezione del PAN <u>visualizzato</u> su schermi, ricevute cartacee, ecc. e non deve essere confuso con il Requisito 3.4 per la protezione del PAN quando viene <u>memorizzato</u> in file, database, ecc.</p>

Requisito	Istruzioni
<p><b>2.3</b> Rendere illeggibile il PAN ovunque sia memorizzato (inclusi i dati su supporti digitali portatili, supporti di backup, registri) utilizzando uno dei seguenti approcci:</p> <ul style="list-style-type: none"> <li>▪ Hash one-way basati su crittografia avanzata (l'hash deve essere dell'intero PAN)</li> <li>▪ Troncatura (non si può usare l'hashing per sostituire la parte troncata del PAN)</li> <li>▪ Token e pad indicizzati (i pad devono essere custoditi in un luogo sicuro)</li> <li>▪ Crittografia avanzata con relativi processi e procedure di gestione delle chiavi</li> </ul> <p><i><b>Nota:</b> per un utente non autorizzato è relativamente facile ricostruire i dati PAN originali se ha accesso alla versione troncata e hash del PAN. Nel caso in cui versioni troncata e hash dello stesso PAN siano presenti nell'ambiente di un'entità, andrebbero predisposti ulteriori controlli per verificare che non sia possibile correlare le versioni troncata e hash per ricostruire il PAN originale.</i></p>	<p>La mancanza di protezione dei PAN può consentire agli utenti non autorizzati di visualizzare o scaricare questi dati. I PAN conservati nella memoria principale (database o file flat, ad esempio fogli elettronici su file di testo) e nella memoria non principale (backup, log di audit, log di eccezioni o risoluzione dei problemi) devono essere protetti. I danni derivanti dal furto o dalla perdita dei nastri di backup durante il trasporto possono essere limitati garantendo l'illeggibilità dei PAN mediante operazioni di cifratura, troncatura o hashing. Dal momento che i log di audit, risoluzione dei problemi ed eccezioni devono essere conservati, è possibile impedire la divulgazione dei dati nei log rendendo illeggibili i PAN (oppure rimuovendoli) nei log.</p> <p>Correlando le versioni troncata e hash di un determinato PAN, un utente non autorizzato può facilmente ricavare il valore del PAN originale. I controlli volti ad impedire la correlazione di questi dati aiuteranno a garantire che il PAN originale rimanga illeggibile.</p> <p>Fare riferimento al documento <i>PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi</i> per la definizione di "crittografia avanzata".</p>
<ul style="list-style-type: none"> <li>▪ Hash one-way basati su crittografia avanzata (l'hash deve essere dell'intero PAN)</li> </ul>	<p>Le funzioni hash one-way come SHA (Secure Hash Algorithm) basate su crittografia avanzata possono essere utilizzate per rendere illeggibili i dati dei titolari di carta. Le funzioni di hash sono adatte all'uso quando non è necessario recuperare il numero originale (l'hash one-way è irreversibile).</p> <p>Per rendere più complicata la creazione di rainbow table si consiglia, sebbene non si tratti di un requisito, di inserire un valore seme (salt value) nella funzione hash in aggiunta al PAN.</p>
<ul style="list-style-type: none"> <li>▪ Troncatura (non si può usare l'hashing per sostituire la parte troncata del PAN)</li> </ul>	<p>Lo scopo della troncatura è memorizzare solo una parte del PAN (non oltre le prime sei e le ultime quattro cifre). La tecnica è differente dalla mascheratura, in cui viene memorizzato l'intero PAN, ma in cui il PAN viene mascherato in fase di visualizzazione (ad esempio su schermo, rendiconti, ricevute, ecc. viene visualizzata solo parte del PAN).</p> <p>Questo requisito si riferisce alla protezione del PAN quando viene <u>memorizzato</u> in file, database ecc. e non va confuso con il Requisito 3.3 per la protezione del PAN quando viene <u>visualizzato</u> su schermi, ricevute cartacee, ecc.</p>

Requisito	Istruzioni
<ul style="list-style-type: none"> <li>Token e pad indicizzati (i pad devono essere custoditi in un luogo sicuro)</li> </ul>	<p>Anche token e pad indicizzati possono essere utilizzati per rendere illeggibili i dati dei titolari di carta. Un token indicizzato è un token crittografico che sostituisce il PAN in base a un determinato indice per un valore imprevedibile. Un pad one-time è un sistema in cui una chiave privata, generata in modo casuale, viene utilizzata una sola volta per cifrare un messaggio, che successivamente sarà decifrato utilizzando una chiave e un pad one-time corrispondente.</p>
<ul style="list-style-type: none"> <li>Crittografia avanzata con relativi processi e procedure di gestione delle chiavi</li> </ul>	<p>Lo scopo della cifratura avanzata (vedere la definizione e la lunghezza delle chiavi in <i>PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi</i>) è basare la cifratura su un algoritmo accettato e collaudato nel settore (non un algoritmo proprietario o personale).</p>
<p><b>3.4.1</b> Se si utilizza la cifratura del disco (anziché la cifratura del database a livello di file o colonna), l'accesso logico deve essere gestito in modo indipendente dai meccanismi di controllo dell'accesso al sistema operativo nativo (ad esempio, non utilizzando database di account utente locali). Le chiavi di decifratura non devono essere associate agli account utente.</p>	<p>Lo scopo di questo requisito è gestire l'accettazione della cifratura del disco per rendere illeggibili i dati dei titolari di carte. La cifratura del disco permette di cifrare i dati memorizzati nella memoria di massa di un computer e di decifrare automaticamente le informazioni quando sono richieste da un utente autorizzato. I sistemi di cifratura del disco intercettano le operazioni di lettura e scrittura del sistema operativo ed eseguono le opportune trasformazioni crittografiche senza richiedere azioni all'utente, se non la specifica di una password o di una passphrase all'inizio di una sessione. Sulla base di queste caratteristiche della cifratura del disco, per essere conforme a questo requisito il metodo di cifratura del disco non può avere:</p> <ol style="list-style-type: none"> <li>1) Un'associazione diretta al sistema operativo, oppure</li> <li>2) Chiavi di decifratura associate agli account utente.</li> </ol>
<p><b>3.5</b> Proteggere le chiavi usate per rendere sicuri i dati dei titolari di carta da divulgazione e uso improprio:</p> <p><i>Nota: questo requisito riguarda anche le KEK (key-encrypting keys) usate per proteggere le chiavi di crittografia dei dati—tali KEK devono essere almeno avanzate almeno quanto la chiave di crittografia dei dati.</i></p>	<p>Le chiavi crittografiche devono essere protette in modo avanzato, perché chiunque le ottenga sarà in grado di decifrare i dati. Se utilizzate, le KEK devono essere almeno avanzate almeno quanto la chiave di crittografia dei dati per assicurare un'adeguata protezione della chiave che cifra i dati ed anche dei dati cifrati con tale chiave.</p> <p>Il requisito per proteggere le chiavi da divulgazione e uso improprio si riferisce sia alle chiavi di crittografia dei dati che alle KEK. Dal momento che una KEK può consentire l'accesso a molte chiavi di crittografia dei dati, per questo tipo di chiavi sono necessarie delle misure di protezione rigide. I metodi per una memorizzazione sicura delle KEK comprendono, senza limitazioni, moduli di sicurezza hardware (HSM) e memorizzazione con prova di manomissione con controllo duale e split knowledge.</p>
<p><b>3.5.1</b> Limitare l'accesso alle chiavi di crittografia al minor numero possibile di persone necessarie.</p>	<p>Dovrebbe essere molto limitato il numero di persone che ha accesso alle chiavi di crittografia, di solito solo coloro che hanno responsabilità di custodia delle chiavi.</p>

Requisito	Istruzioni
<p><b>3.5.2</b> Memorizzare le chiavi di crittografia in modo sicuro nel minor numero possibile di posizioni e moduli.</p>	<p>Le chiavi di crittografia devono essere memorizzate in modo sicuro, di solito cifrate con KEK e conservate in un numero molti limitato di posizioni. Non si prevede la cifratura delle KEK, ad ogni modo queste chiavi devono essere protette da divulgazione e uso improprio come indicato al Requisito 3.5. La memorizzazione delle KEK in posizioni separate logicamente e/o fisicamente dalle chiavi di crittografia dei dati riduce il rischio di accesso non autorizzato ad entrambe le chiavi.</p>
<p><b>3.6</b> 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 <b>quanto segue</b>:</p> <p><i>Nota: sono disponibili numerosi standard di settore per la gestione delle chiavi, tra cui il sito del NIST all'indirizzo <a href="http://csrc.nist.gov">http://csrc.nist.gov</a>.</i></p>	<p>La gestione delle chiavi di crittografia è una parte fondamentale della sicurezza continua della soluzione di cifratura. Un valido processo di gestione delle chiavi, manuale o automatico come parte del prodotto di cifratura, gestisce tutti gli elementi chiave da 3.6.1 a 3.6.8.</p>
<p><b>3.6.1</b> Generazione di chiavi di crittografia avanzata</p>	<p>La soluzione di cifratura deve generare chiavi avanzate, come descritto nel documento <i>PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi</i> sotto "crittografia avanzata".</p>
<p><b>3.6.2</b> Distribuzione di chiavi di crittografia sicure</p>	<p>La soluzione di cifratura deve distribuire le chiavi in modo sicuro, vale a dire che le chiavi non vengono distribuite in chiaro e solo ai custodi definiti al punto 3.5.1.</p>
<p><b>3.6.3</b> Memorizzazione di chiavi di crittografia sicure</p>	<p>La soluzione di cifratura deve memorizzare le chiavi in modo sicuro, vale a dire che le chiavi non vengono memorizzate in chiaro (sono cifrate con una chiave di crittografia delle chiavi).</p>
<p><b>3.6.4</b> Modifiche delle chiavi di crittografia per le chiavi giunte al termine del loro periodo di validità (ad esempio, una volta trascorso un periodo di tempo definito e/o dopo la produzione da parte di una determinata chiave di una quantità definita di testo di cifratura), come specificato dal fornitore dell'applicazione associato o dal proprietario delle chiavi, ed in base alle linee guida ed alle migliori pratiche del settore (ad esempio, <i>NIST Special Publication 800-57</i>).</p>	<p>Periodo di crittografia è il periodo durante il quale una determinata chiave di crittografia può essere usata per uno scopo preciso. Le considerazioni per la definizione del periodo di crittografia includono, senza limitazioni, la solidità dell'algoritmo sottostante, le dimensioni o la lunghezza della chiave, il rischio che la chiave possa essere compromessa e la sensibilità dei dati che vengono cifrati.</p> <p>La modifica periodica delle chiavi di crittografia al termine del loro periodo di validità è fondamentale per ridurre il rischio che qualcuno ottenga le chiavi e sia in grado di decifrare i dati.</p> <p>Se sono specificati dal fornitore dell'applicazione di cifratura, seguire i processi o i consigli del fornitore per la modifica periodica delle chiavi. Il proprietario delle chiavi o il custode delle chiavi designato possono anche far riferimento alle migliori pratiche del settore in materia di algoritmi crittografici e gestione delle chiavi, ad esempio <i>NIST Special Publication 800-57</i>, per avere istruzioni in merito al periodo di crittografia per i diversi algoritmi e le lunghezze delle chiavi.</p> <p>Lo scopo di questo requisito riguarda le chiavi utilizzate per criptare dati dei titolari di carta memorizzati, ed ogni rispettiva KEK.</p>

Requisito	Istruzioni
<p><b>3.6.5</b> Ritiro o sostituzione (ad esempio: archiviazione, distruzione e/o revoca) delle chiavi come ritenuto necessario in caso di indebolimento dell'integrità della chiave (ad esempio, partenza di un dipendente a conoscenza di chiavi con testo in chiaro), oppure in presenza del sospetto che le chiavi siano state compromesse.</p> <p><b>Nota:</b> <i>Se ritirate o sostituite le chiavi crittografiche devono essere conservate, queste chiavi devono essere archiviate in modo sicuro (ad esempio usando una KEK). Le chiavi crittografiche archiviate dovrebbero essere usate solo per scopi di decifratura/verifica.</i></p>	<p>Le vecchie chiavi che non sono necessarie o non si usano più vanno ritirate e distrutte per garantire che non possano essere più usate. Se è necessario conservare le vecchie chiavi (ad esempio per supportare i dati cifrati in archivio), si deve applicare loro una protezione avanzata (vedere il successivo punto 3.6.6). La soluzione di cifratura dovrebbe inoltre consentire e facilitare un processo di sostituzione delle chiavi che sono state compromesse (o di cui si sospetta la compromissione).</p>
<p><b>3.6.6</b> Se si utilizzano operazioni manuali di gestione delle chiavi di crittografia con testo in chiaro, tali operazioni devono essere gestite usando "split knowledge" e controllo duale (ad esempio, rendendo necessarie due o tre persone, ciascuna a conoscenza di una sola parte della chiave, per ricostruire l'intera chiave).</p> <p><b>Nota:</b> <i>Esempi di operazioni manuali di gestione delle chiavi includono, senza limitazioni: la generazione, la trasmissione, il caricamento, la memorizzazione e la distruzione delle chiavi.</i></p>	<p>Lo "split knowledge" e il controllo duale delle chiavi sono utilizzati per eliminare la possibilità che una singola persona abbia accesso all'intera chiave. Questo controllo è applicabile alle operazioni di gestione manuale delle chiavi, oppure laddove tale gestione non è implementata dal prodotto di cifratura .</p>
<p><b>3.6.7</b> Prevenzione di tentativi di sostituzione non autorizzata delle chiavi di crittografia</p>	<p>La soluzione di cifratura non dovrebbe consentire o accettare la sostituzione delle chiavi provenienti da fonti non autorizzate o processi imprevisti.</p>
<p><b>3.6.8</b> Obbligo per custodi delle chiavi di crittografia di riconoscere in modo formale che accettano e confermano di conoscere le proprie responsabilità.</p>	<p>Questo processo garantirà che gli individui che agiscono come custodi delle chiavi si impegnino in tale ruolo e comprendano le loro responsabilità.</p>

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

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

<b>Requisito</b>	<b>Istruzioni</b>
<p><b>4.1</b> Usare protocolli di crittografia e sicurezza avanzati (ad esempio, SSL/TLS, IPSEC, SSH, ecc.) per proteggere i dati dei titolari di carta sensibili quando sono trasmessi su reti pubbliche aperte.</p> <p><i>Esempi di reti pubbliche e aperte nell'ambito della valutazione PCI DSS includono, senza limitazioni:</i></p> <ul style="list-style-type: none"><li>▪ <i>Internet</i></li><li>▪ <i>Tecnologie wireless</i></li><li>▪ <i>Comunicazioni GSM (Global System for Mobile)</i></li><li>▪ <i>GPRS (General Packet Radio Service)</i></li></ul>	<p>Le informazioni sensibili devono essere cifrate durante la trasmissione su reti pubbliche, in quanto si verifica con facilità e frequenza che un utente non autorizzato intercetti e/o dirotti i dati in transito.</p> <p>Ad esempio, SSL (Secure Sockets Layer) permette la cifratura delle pagine Web e dei dati immessi al loro interno. Durante l'uso di siti Web protetti con SSL, verificare che nell'URL sia presente la dicitura "https".</p> <p>Tener presente che alcune implementazioni di protocolli (come SSL versione 2.0 e SSH versione 1.0) dispongono di vulnerabilità documentate, quali l'overflow del buffer, che un aggressore può utilizzare per ottenere il controllo del sistema interessato. Qualunque sia il protocollo di sicurezza utilizzato, verificare che sia configurate per usare solo versioni e configurazioni sicure per impedire l'utilizzo di una connessione non sicura.</p>

Requisito	Istruzioni
<p><b>4.1.1</b> Garantire che le reti wireless che trasmettono i dati di titolari di carta o connesse all'ambiente dei dati di titolari di carta utilizzano le pratiche di settore consigliate (ad esempio, IEEE 802.11i) per implementare la crittografia avanzata per l'autenticazione e la trasmissione.</p> <p><i>Nota: l'utilizzo della tecnologia WEP per controllare la sicurezza è stato vietato a partire dal 30 giugno 2010.</i></p>	<p>Gli utenti non autorizzati utilizzano strumenti liberi e ampiamente disponibili per ascoltare le comunicazioni wireless. L'uso di crittografia avanzata può contribuire a limitare la divulgazione di informazioni sensibili attraverso la rete. Molte compromissioni note di dati dei titolari di carte memorizzati solamente nella rete cablata avvengono quando un utente non autorizzato ottiene l'accesso da una rete wireless non protetta. Gli esempi di implementazioni wireless che richiedono crittografia avanzata includono, senza limitazioni, GPRS, GSM, WIFI, satellite e Bluetooth.</p> <p>La crittografia avanzata per l'autenticazione e la trasmissione dei dati dei titolari di carte è necessaria per impedire agli utenti non autorizzati di ottenere accesso alla rete wireless (e ai dati sulla rete) o di utilizzare la rete wireless per raggiungere le reti interne o i dati. La cifratura WEP non dovrebbe mai essere usata come unico mezzo di cifratura dei dati su un canale wireless dal momento che non viene considerata crittografia avanzata, è vulnerabile a causa dei vettori di inizializzazione deboli nel processo di scambio delle chiavi WEP e non dispone della necessaria rotazione delle chiavi. Un aggressore può utilizzare strumenti di cracking basati sulla forza bruta, liberamente disponibili, per superare agevolmente la cifratura WEP.</p> <p>Si dovrebbero aggiornare gli attuali dispositivi wireless (ad esempio con l'upgrade del firmware del punto di accesso a WPA2) per supportare la cifratura avanzata. Se non è possibile aggiornare i dispositivi attuali, si dovrebbero acquistare nuove apparecchiature o implementare altri controlli compensativi per fornire cifratura avanzata.</p>
<p><b>4.2</b> Non inviare mai PAN non cifrati mediante tecnologie di messaggistica degli utenti finali (ad esempio, e-mail, messaggistica istantanea, chat, ecc.).</p>	<p>L'e-mail, la messaggistica istantanea e la chat possono essere facilmente intercettati mediante packet-sniffing durante il recapito attraverso reti interne e pubbliche. Non utilizzare questi strumenti di messaggistica per inviare i PAN, a meno che non dispongano di cifratura avanzata.</p>

## Istruzioni per i requisiti 5 e 6: Utilizzare un programma per la gestione delle vulnerabilità

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

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

Requisito	Istruzioni
<b>5.1</b> Distribuire il software antivirus su tutti i sistemi comunemente colpiti da malware (in particolare PC e server).	<p>Esiste un flusso costante di attacchi che utilizzano exploit pubblicati, spesso di tipo "0 day" (pubblicati e diffusi nelle reti entro un'ora dalla scoperta) contro sistemi altrimenti sicuri. Senza un software antivirus aggiornato regolarmente, queste nuove forme di software dannoso possono attaccare e disabilitare la rete.</p> <p>Il software dannoso può essere scaricato e/o installato inconsapevolmente da Internet, ma i computer risultano vulnerabili anche durante l'uso di dispositivi di memorizzazione rimovibili, quali CD e DVD, memorie e unità disco rigido USB, fotocamere digitali, PDA (Personal Digital Assistant) e altri dispositivi periferici. Senza un software antivirus, questi computer possono divenire punti di accesso alla rete e/o alle informazioni all'interno della rete.</p> <p>Anche se i sistemi comunemente interessati dal software dannoso in genere non comprendono i mainframe e la maggior parte dei sistemi Unix (ulteriori dettagli più avanti), ogni entità deve disporre di un processo conforme al Requisito 6.2 di PCI DSS per identificare e gestire le nuove vulnerabilità di protezione e aggiornare di conseguenza gli standard e i processi di configurazione. Se un altro tipo di soluzione risolve le stesse minacce adottando un'altra metodologia rispetto all'approccio fondato sulla firma, può ancora essere accettabile per soddisfare il requisito.</p> <p>Le tendenze del software dannoso correlate ai sistemi operativi utilizzati da un'entità dovrebbero essere incluse nell'identificazione delle nuove vulnerabilità della protezione, e i metodi per gestire tali nuove tendenze dovrebbero essere integrati negli standard di configurazione dell'azienda e nei meccanismi di protezione, secondo necessità.</p> <p>In generale, non sono comunemente interessati da software dannoso o seguenti sistemi operativi: mainframe e alcuni tipi di server Unix (come AIX, Solaris e HP-Unix). Tuttavia, le tendenze settoriali del software dannoso possono cambiare rapidamente e ogni organizzazione deve rispettare il Requisito 6.2 per identificare e gestire le nuove vulnerabilità di protezione e aggiornare di conseguenza gli standard e i processi di configurazione.</p>

Requisito	Istruzioni
<b>5.1.1</b> Garantire che tutti i programmi antivirus siano in grado di rilevare e rimuovere tutti i tipi di malware nonché garantire una protezione sicura.	È importante proteggersi da <b>TUTTI</b> i tipi e le forme di software dannoso.
<b>5.2</b> Garantire che tutti i meccanismi antivirus siano aggiornati, in esecuzione e in grado di generare log di audit.	Il miglior software antivirus presenta un'efficacia limitata se non dispone delle definizioni dei virus correnti o se non è attivo nella rete o in un singolo computer.  I log di audit consentono di monitorare l'attività dei virus e le reazioni dell'antivirus. Pertanto, è fondamentale che il software antivirus sia configurato per generare log di audit e che questi log siano gestiti in conformità al Requisito 10.

## 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.*

Requisito	Istruzioni
<p><b>6.1</b> Assicurare che tutti i componenti di sistema ed il software siano protetti dalle vulnerabilità note mediante l'installazione delle più recenti patch di sicurezza dei fornitori. Installare patch di sicurezza critiche entro un mese dal rilascio.</p> <p><i>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.</i></p>	<p>Il numero di attacchi che utilizzano exploit pubblicati, spesso di tipo "0 day" (pubblicati entro un'ora), contro sistemi altrimenti sicuri è particolarmente elevato. Senza l'implementazione delle patch più recenti sui sistemi critici nel minor tempo possibile, un utente non autorizzato può utilizzare questi exploit per attaccare e disabilitare la rete. È opportuno assegnare una priorità ai cambiamenti per garantire l'installazione delle patch di protezione critiche sui sistemi importanti o a rischio entro 30 giorni, procedendo con gli aspetti meno rischiosi entro 2-3 mesi.</p>

Requisito	Istruzioni
<p><b>6.2</b> Stabilire un processo per identificare ed assegnare una classificazione di rischio alle vulnerabilità della sicurezza recentemente rilevate.</p> <p><b>Note:</b>  <i>le classificazioni di rischio si dovrebbero basare sulle migliori pratiche del settore. Ad esempio, i criteri per la classificazione di vulnerabilità di rischio elevato possono comprendere un punteggio base CVSS di 4.0 o superiore, e/o una patch del fornitore da questi classificata come "critica", e/o una vulnerabilità che interessa un componente critico del sistema.</i>  <i>La classificazione delle vulnerabilità come riportata al punto 6.2.a è considerata una delle migliori pratiche fino al 30 giugno 2012; dopo tale data, diventerà un requisito.</i></p>	<p>Lo scopo di questo requisito è l'aggiornamento delle organizzazioni in relazione alle nuove vulnerabilità che possono avere un effetto sul loro ambiente.</p> <p>Sebbene sia importante controllare gli annunci dei fornitori contenenti notizie sulle vulnerabilità e sulle patch relative ai loro prodotti, è ugualmente importante controllare i più diffusi newsgroup e mailing list per le vulnerabilità del settore in ordine a vulnerabilità e potenziali soluzioni temporanee di cui il fornitore potrebbe non ancora essere a conoscenza o aver risolto.</p> <p>Una volta che un'organizzazione identifica una vulnerabilità che potrebbe incidere sul suo ambiente, è necessario valutare e classificare il rischio che la vulnerabilità comporta. Ciò richiede la predisposizione di alcuni metodi da parte dell'organizzazione per valutare le vulnerabilità ed attribuire una classificazione di rischio su una base coerente. Pur essendo probabile che in ogni organizzazione siano adottati metodi diversi per la valutazione di una vulnerabilità e per la conseguente assegnazione di una classificazione del rischio in funzione del rispettivo ambiente dei dati dei titolari di carta univoco, è possibile basarsi su sistemi di classificazione del rischio accettati dal settore, ad esempio CVSS. 2.0, NIST SP 800-30, ecc.</p> <p>La classificazione dei rischi (ad esempio come "elevato", "medio" o "basso") consente alle organizzazioni di individuare e risolvere gli elementi di rischio di priorità elevata più rapidamente e ridurre la probabilità che vengano sfruttate le vulnerabilità che costituiscono i rischi più elevati.</p>
<p><b>6.3</b> Sviluppare applicazioni software (interne ed esterne, incluso l'accesso amministrativo tramite Web alle applicazioni) in conformità agli standard PCI DSS (ad esempio, registrazione e autenticazione sicure) e in base alle pratiche di settore consigliate, quindi incorporare la protezione delle informazioni nell'intero ciclo di sviluppo del software. Questi processi devono includere quanto segue:</p>	<p>Senza l'inclusione della sicurezza durante le fasi di definizione dei requisiti, progettazione, analisi e test dello sviluppo del software, le vulnerabilità di protezione possono essere introdotte inavvertitamente o con cattive intenzioni nell'ambiente di produzione.</p>
<p><b>6.3.1</b> Account, ID utente e password di applicazioni personalizzate vengono rimossi prima dell'attivazione o della distribuzione di tali applicazioni ai clienti</p>	<p>Gli account, gli ID utente e le password delle applicazioni personalizzate devono essere rimossi dal codice di produzione prima che l'applicazione diventi attiva o venga rilasciata ai clienti, in quanto questi elementi possono fornire informazioni sul funzionamento dell'applicazione. Il possesso di tali informazioni potrebbe facilitare la compromissione dell'applicazione e dei dati dei titolari di carte correlati.</p>

Requisito	Istruzioni
<p><b>6.3.2</b> Il codice personalizzato viene analizzato prima del rilascio in produzione o della distribuzione ai clienti per identificare eventuali vulnerabilità.</p> <p><i><b>Nota:</b> 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. Le analisi del codice possono essere condotte da personale interno preparato o da terze parti. Le applicazioni Web sono anche soggette a controlli aggiuntivi, se sono pubbliche, per risolvere le minacce costanti e le vulnerabilità dopo l'implementazione, secondo quanto definito nel Requisito 6.6 PCI DSS.</i></p>	<p>Le vulnerabilità di protezione nel codice personalizzato vengono comunemente sfruttate da utenti non autorizzati per accedere a una rete e compromettere i dati dei titolari di carte.</p> <p>Le analisi del codice possono essere eseguite manualmente o con l'ausilio di strumenti di analisi automatici. Gli strumenti di analisi automatici sono dotati di funzionalità che analizzano il codice per rilevare vulnerabilità ed errori di codifica comuni. Sebbene l'analisi automatica rappresenti uno strumento utile, di norma, non dovrebbe costituire l'unico mezzo di analisi del codice su cui fare affidamento. Nel processo di analisi, si dovrebbe coinvolgere un individuo preparato e con esperienza nell'analisi del codice, al fine di identificare questioni riguardanti i codici che per uno strumento automatico siano difficili o addirittura impossibili da identificare. Assegnare le analisi del codice ad una persona che non sia colui che ha sviluppato il codice consente l'esecuzione di un'analisi obiettiva ed indipendente.</p>
<p><b>6.4</b> Seguire i processi e le procedure di controllo delle modifiche per tutte le modifiche apportate ai componenti di sistema. I processi devono includere quanto segue:</p>	<p>Senza controlli di modifica appropriati, le funzionalità di protezione possono essere inavvertitamente o deliberatamente omesse o rese inattive, possono verificarsi problemi di elaborazione o è possibile che venga introdotto del codice dannoso.</p>
<p><b>6.4.1</b> Separare ambienti di sviluppo/test e ambienti di produzione</p>	<p>In considerazione dello stato di costante cambiamento degli ambienti di test e sviluppo, questi tendono ad essere meno sicuri rispetto all'ambiente di produzione. In assenza di un'adeguata separazione tra gli ambienti potrebbe verificarsi la compromissione di ambiente di produzione e dei dati dei titolari di carta a causa delle vulnerabilità in un ambiente di test o di sviluppo.</p>
<p><b>6.4.2</b> Separare le responsabilità tra ambienti di sviluppo/test e ambienti di produzione</p>	<p>Riducendo il numero di membri del personale con accesso all'ambiente di produzione e ai dati dei titolari di carta si limita il rischio e si contribuisce a garantire che l'accesso sia limitato a coloro per i quali è effettivamente necessario.</p> <p>Lo scopo di questo requisito è di garantire che le funzioni di sviluppo/test siano separate dalle funzioni di produzione. Ad esempio, uno sviluppatore può usare un account a livello di amministratore con privilegi elevati per l'ambiente di sviluppo ed avere un account separato con accesso a livello utente per l'ambiente di produzione.</p> <p>In ambienti in cui un individuo ricopre più ruoli (ad esempio sviluppo delle applicazioni ed implementazione di aggiornamenti per i sistemi di produzione), l'assegnazione delle responsabilità dovrebbe avvenire in modo che nessun individuo abbia un controllo end-to-end di un processo senza prevedere un punto di controllo indipendente. Ad esempio, assegnare responsabilità per sviluppo, autorizzazione e monitoraggio a diversi individui.</p>

Requisito	Istruzioni
<p><b>6.4.3</b> I dati di produzione (PAN attivi) sono esclusi dalle attività di test o sviluppo</p>	<p>I controlli di protezione di solito non sono particolarmente rigorosi nell'ambiente di produzione. L'uso dei dati di produzione permette agli utenti non autorizzati di accedere ai dati di produzione (dati dei titolari di carte).</p> <p>I marchi di carte di pagamento e molti acquirenti sono in grado di fornire numeri di conto adatti per i test qualora siano necessari PAN realistici per sottoporre a test la funzionalità del sistema prima del rilascio.</p>
<p><b>6.4.4</b> Rimuovere i dati e gli account di test prima dell'attivazione dei sistemi di produzione</p>	<p>I dati e gli account di test devono essere rimossi dal codice di produzione prima che l'applicazione diventi attiva, in quanto questi elementi possono fornire informazioni sul funzionamento dell'applicazione. Il possesso di tali informazioni potrebbe facilitare la compromissione dell'applicazione e dei dati dei titolari di carte correlati.</p>
<p><b>6.4.5</b> Modificare le procedure di controllo per l'implementazione di patch di sicurezza e modifiche del software. Le procedure devono includere quanto segue:</p>	<p>Senza controlli di modifica adeguati, le funzionalità di protezione possono essere inavvertitamente o deliberatamente omesse o rese inattive, possono verificarsi problemi di elaborazione o è possibile che venga introdotto del codice dannoso. Analogamente, una modifica può influire negativamente sulla funzionalità di un sistema che deve essere modificato per eseguire la procedura di back out.</p>
<p><b>6.4.5.1</b> Documentazione dell'impatto</p>	<p>L'impatto della modifica dovrebbe essere documentato in modo che tutte le parti interessate siano in grado di pianificare accuratamente qualsiasi modifica di elaborazione.</p>
<p><b>6.4.5.2</b> Approvazione documentata per ogni modifica effettuata da parti autorizzate.</p>	<p>L'approvazione delle parti autorizzate indica che una modifica è legittima e autorizzata dall'organizzazione.</p>
<p><b>6.4.5.3</b> Esecuzione del test della funzionalità per verificare che la modifica non influisca negativamente sulla sicurezza del sistema.</p>	<p>Un test approfondito consente di verificare che l'introduzione della modifica non comporti una riduzione della sicurezza dell'ambiente. I test dovrebbero convalidare che, dopo ogni modifica apportata all'ambiente, tutti i controlli di sicurezza esistenti rimangano attivi, siano sostituiti con controlli ugualmente efficaci oppure siano intensificati.</p> <p>Per le modifiche personalizzate del codice, nei test è compresa la verifica che la modifica non abbia introdotto alcuna vulnerabilità di codifica.</p>
<p><b>6.4.5.4</b> Procedure di back-out.</p>	<p>Per ogni modifica devono esistere procedure di back-out nel caso in cui la modifica non riesca, in modo da consentire il ripristino allo stato precedente.</p>

Requisito	Istruzioni
<p><b>6.5</b> Sviluppare applicazioni in base a linee guida di codifica sicura. Prevenire possibili vulnerabilità del codice comuni nei processi di sviluppo del software, incluso quanto segue:</p> <p><b>Nota:</b> <i>le vulnerabilità elencate dal punto 6.5.1 al punto 6.5.9 erano presenti nelle migliori pratiche del settore al momento della pubblicazione di questa versione degli standard PCI DSS. Tuttavia, poiché le migliori pratiche del settore per la gestione delle vulnerabilità sono state aggiornate (ad esempio, la Guida OWASP, la Top 25 SANS CWE, la Codifica Sicura CERT, ecc.), per questi requisiti è necessario utilizzare le migliori pratiche più recenti.</i></p>	<p>Lo strato applicazione è ad alto rischio e può divenire bersaglio di minacce interne ed esterne. Senza la corretta protezione, i dati dei titolari di carte e altre informazioni riservate dell'azienda possono essere esposti, causando danni all'azienda, ai suoi clienti e alla sua reputazione.</p> <p>Come con tutti i requisiti PCI DSS, i requisiti da 6.5.1 a 6.5.5 e da 6.5.7 a 6.5.9 sono i controlli <i>minimi</i> che dovrebbero essere in atto. Questo elenco si compone delle pratiche di codifica sicure, accettate e più comuni al momento della pubblicazione di questa versione degli standard PCI DSS. Mano a mano che le pratiche di codifica sicure accettate dal settore cambiano, le pratiche di codifica organizzative dovrebbero essere ugualmente aggiornate per mantenere la corrispondenza.</p> <p>Gli esempi di risorse di codifica sicure fornite (SANS, CERT e OWASP) rappresentano fonti di riferimento consigliate e sono stati inseriti solo a scopo informativo. Un'organizzazione dovrebbe incorporare le pratiche di codifica sicura del caso come applicabile alla tecnologia specifica del proprio ambiente.</p>

Requisito	Istruzioni
<p><b>6.5.1</b> Injection flaw, in particolare SQL injection. Considerare, inoltre, OS Command Injection, LDAP e XPath injection flaw, nonché altri tipi di injection flaw.</p>	<p>Convalidare l'input per verificare che i dati dell'utente non possano modificare il significato di comandi e query. Injection flaw, in particolare SQL injection, rappresentano il metodo comunemente usato per compromettere le applicazioni. L'injection avviene quando i dati forniti dall'utente vengono inviati a un interprete durante un comando o una query. I dati ostili dell'aggressore inducono l'interprete a eseguire comandi indesiderati o a modificare i dati, e consentono all'aggressore di attaccare i componenti all'interno della rete attraverso l'applicazione, per dare il via ad attacchi di tipo overflow del buffer o per rivelare informazioni riservate e funzionalità dell'applicazione server. Esiste inoltre un metodo diffuso per condurre transazioni fraudolente sui siti Web di e-commerce. Le informazioni delle richieste devono essere convalidate prima dell'invio all'applicazione, ad esempio controllando tutti i caratteri alfabetici, un insieme di caratteri alfabetici e numerici, ecc.</p>
<p><b>6.5.2</b> Overflow del buffer</p>	<p>Verificare che le applicazioni non siano vulnerabili ad attacchi di overflow del buffer. Gli overflow del buffer si verificano quando un'applicazione non dispone degli adeguati controlli di limite sul suo spazio buffer. Per sfruttare una vulnerabilità di overflow del buffer, un aggressore invia ad un'applicazione una quantità di informazioni superiore rispetto a quella che uno dei suoi buffer sia in grado di gestire. Ciò può causare che le informazioni nel buffer vengano spinte fuori dallo spazio di memoria del buffer e collocate nello spazio di memoria eseguibile. Quando ciò si verifica, l'aggressore è in grado di inserire un codice dannoso alla fine del buffer e quindi spingere tale codice nello spazio di memoria eseguibile causando l'overflow del buffer. Questo codice dannoso viene quindi eseguito e spesso consente all'aggressore di accedere in remoto all'applicazione e/o di infettare il sistema.</p>
<p><b>6.5.3</b> Memorizzazione di dati crittografici non sicura</p>	<p>Evitare gli errori di crittografia. Le applicazioni che non usano funzioni di crittografia avanzata in modo corretto per la memorizzazione dei dati sono esposte ad un maggiore rischio di essere compromesse e di esporre i dati dei titolari di carta. Nel caso in cui un aggressore sia in grado di sfruttare i processi crittografici deboli, può ottenere l'accesso con testo in chiaro ai dati crittografati.</p>
<p><b>6.5.4</b> Comunicazioni non sicure</p>	<p>Cifrare in modo appropriato tutte le comunicazioni autenticate e riservate. Le applicazioni che non riescono a cifrare in modo appropriato il traffico di rete usando la crittografia avanzata sono esposte ad un rischio maggiore di compromissione e di esposizione dei dati dei titolari di carta. Nel caso in cui un aggressore sia in grado di sfruttare i processi crittografici deboli, può ottenere il controllo di un'applicazione o addirittura l'accesso con testo in chiaro ai dati crittografati.</p>

Requisito	Istruzioni
<p><b>6.5.5</b> Gestione degli errori non corretta</p>	<p>Non perdere informazioni mediante messaggi di errore o altri mezzi. Le applicazioni possono involontariamente perdere informazioni sulla relativa configurazione e sulle procedure interne, o violare la privacy tramite diversi problemi dell'applicazione. Gli aggressori possono utilizzare questi punti deboli per sottrarre dati sensibili o condurre attacchi più gravi. Inoltre, un'errata gestione degli errori mette a disposizione informazioni che aiutano un utente non autorizzato a compromettere il sistema. Se un utente non autorizzato può creare errori che l'applicazione non è in grado di gestire correttamente, può ottenere informazioni dettagliate sul sistema, creare interruzioni denial-of-service, provocare il fallimento della protezione o causare l'arresto anomalo del server. Ad esempio, il messaggio "password non corretta" comunica che l'ID utente fornito è corretto e che gli sforzi devono essere concentrati solamente sulla password. Utilizzare messaggi d'errore più generici, come "Impossibile verificare i dati".</p>
<p><b>6.5.6</b> Tutte le vulnerabilità "Elevate" identificate nel processo di identificazione delle vulnerabilità (come definito nel Requisito 6.2 PCI DSS).</p> <p><i>Nota: questo requisito è considerato una delle pratiche migliori fino al 30 giugno 2012; dopo tale data, diventerà un requisito</i></p>	<p>Ogni vulnerabilità di livello elevato come individuata nel Requisito 6.2 che potrebbe interessare l'applicazione dovrebbe essere segnalata durante la fase di sviluppo. Ad esempio, una vulnerabilità identificata in una libreria condivisa o nel sistema operativo sottostante andrebbe valutata e risolta prima che l'applicazione venga messa in produzione.</p>
<p>Per applicazioni web ed interfacce di applicazioni (interne o esterne) sono applicabili i seguenti requisiti aggiuntivi:</p>	<p>Applicazioni web, interne ed esterne (rivolte al pubblico), presentano dei rischi di sicurezza univoci sulla base della loro architettura nonché della loro relativa facilità e del verificarsi di compromissioni.</p>
<p><b>6.5.7</b> Cross-site scripting (XSS)</p>	<p>Tutti i parametri devono essere convalidati prima dell'inclusione. Le falle XSS si verificano quando un'applicazione prende i dati forniti dall'utente e li invia a un browser Web senza prima convalidarli o codificarne il contenuto. XSS consente agli aggressori di eseguire script sul browser della vittima, che possono dirottare le sessioni utente, alterare i siti Web, introdurre worm, ecc.</p>

Requisito	Istruzioni
<p><b>6.5.8</b> Controllo di accesso non corretto (come riferimenti a oggetti diretti non sicuri, errore di limitazione dell'accesso URL e scansione trasversale directory)</p>	<p>Non esporre agli utenti riferimenti a oggetti interni. Un riferimento a oggetto diretto si verifica quando uno sviluppatore espone un riferimento a un oggetto di implementazione interno, come un file, una directory, un record di database o una chiave, sotto forma di parametro URL o di modulo. Gli aggressori possono manipolare questi riferimenti per accedere ad altri oggetti senza autorizzazione.</p> <p>Applicare in modo coerente il controllo dell'accesso a livello di presentazione e business logic per tutti gli URL. Spesso l'unico modo in cui un'applicazione protegge le funzionalità sensibili consiste nell'impedire la visualizzazione di collegamenti o URL agli utenti non autorizzati. Gli aggressori possono utilizzare questi punti deboli per accedere ed eseguire operazioni non autorizzate mediante accesso diretto a questi URL.</p> <p>Protezione da scansione trasversale directory. Un aggressore può essere in grado di elencare e navigare la struttura della directory di un sito Web e quindi ottenere accesso ad informazioni non autorizzate ed anche acquisire un'ulteriore comprensione approfondita delle procedure interne del sito per un successivo sfruttamento.</p>
<p><b>5.2.9</b> Cross-site request forgery (CSRF)</p>	<p>Non considerare sicure credenziali di autorizzazione e token inviati automaticamente dai browser. Un attacco CSRF impone al browser di una vittima connessa di inviare una richiesta pre-autenticata a un'applicazione Web vulnerabile, quindi induce il browser della vittima a eseguire un'azione ostile a vantaggio dell'aggressore. CSRF può essere potente quando l'applicazione Web attaccata.</p>
<p><b>6.6</b> Per le applicazioni Web esterne, assicurare una protezione costante da nuove minacce e vulnerabilità e garantire che queste applicazioni siano protette da attacchi noti mediante <i>uno</i> dei seguenti metodi:</p> <ul style="list-style-type: none"> <li>▪ 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</li> <li>▪ Installazione di un firewall di applicazioni Web davanti alle applicazioni Web rivolte al pubblico</li> </ul>	<p>Gli attacchi alle applicazioni con interfaccia Web sono comuni e spesso riusciti, e sono permessi da pratiche di codifica poco attente. Questo requisito di revisione delle applicazioni o di installazione di firewall per le applicazioni Web mira a ridurre notevolmente il numero di compromissioni sulle applicazioni Web per il pubblico, che danno luogo a violazioni dei dati dei titolari di carta.</p> <ul style="list-style-type: none"> <li>▪ Per soddisfare questo requisito, si possono utilizzare metodi o strumenti di valutazione della protezione dalle vulnerabilità automatici o manuali, che rivedono e/o analizzano le vulnerabilità dell'applicazione.</li> <li>▪ I firewall delle applicazioni Web filtrano e bloccano il traffico non essenziale nello strato applicazione. Utilizzato insieme a un firewall di rete, un firewall di applicazioni Web correttamente configurato impedisce gli attacchi dallo strato applicazione nel caso in cui le applicazioni siano configurate o scritte in modo improprio.</li> </ul>

## Istruzioni per i requisiti 7, 8 e 9: Implementazione di rigide misure di controllo dell'accesso

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

Per garantire che solo il personale autorizzato possa accedere a dati critici, occorre mettere in atto sistemi e processi per limitare l'accesso in base alle esigenze e alle responsabilità del ruolo. Per "solo se effettivamente necessario" si intendono situazioni in cui vengono concessi diritti di accesso solo alla quantità minima di dati e privilegi necessari per svolgere una mansione.

Requisito	Istruzioni
<p><b>7.1</b> Limitare l'accesso ai componenti di sistema e ai dati di titolari di carta solo alle persone che svolgono mansioni per le quali tale accesso risulta realmente necessario. Le limitazioni di accesso devono includere quanto segue:</p> <p><b>7.1.1</b> Limitazione dei diritti di accesso a ID utente privilegiati alla quantità minima necessaria per le responsabilità di ruolo</p> <p><b>7.1.2</b> Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale</p> <p><b>7.1.3</b> Requisito per un'approvazione documentata delle parti autorizzate specificando i privilegi necessari.</p> <p><b>7.1.4</b> Implementazione di un sistema di controllo dell'accesso automatico</p>	<p>Quanto maggiore è il numero di persone che hanno accesso ai dati dei titolari di carte, tanto maggiore è il rischio di utilizzo fraudolento di un account utente. Limitando l'accesso alle persone che presentano valide ragioni aziendali per l'accesso, l'organizzazione può impedire l'abuso dei dati dei titolari di carte a causa di inesperienza o premeditazione. Se i diritti di accesso vengono concessi solo alla quantità minima di dati e privilegi necessari per svolgere una mansione, si fa riferimento al concetto di "privilegio minimo" e "solo se effettivamente necessario"; quando i privilegi sono assegnati agli individui in base alla funzione e alla classificazione delle mansioni, si parla di "controllo dell'accesso basato su ruolo" (RBAC). L'imposizione del controllo dell'accesso basato sul ruolo non si limita solo ad una singola applicazione o ad ogni soluzione di autorizzazione specifica. Ad esempio, la tecnologia con l'inclusione, senza limitazioni, di servizi di directory quali Active Directory o LDAP, ACL (Access Control Lists) e TACACS rappresentano delle soluzioni attuabili a condizione che siano configurate in modo adeguato per applicare i principi di "privilegio minimo" e "solo se effettivamente necessario".</p> <p>Le organizzazioni dovrebbero formulare una politica e dei processi chiari per il controllo di accesso ai dati basato sul principio del "solo se effettivamente necessario" ed usando un controllo dell'accesso basato sul ruolo, per definire in che modo ed a chi viene concesso l'accesso, compresi i processi di autorizzazione appropriata del management.</p>

Requisito	Istruzioni
<p><b>7.2</b> 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.</p> <p>Il sistema di controllo dell'accesso deve includere quanto segue:</p> <ul style="list-style-type: none"><li><b>7.2.1</b> Copertura di tutti i componenti di sistema</li><li><b>7.2.2</b> Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale</li><li><b>7.2.3</b> Impostazione predefinita "deny-all"</li></ul> <p><i><b>Nota:</b> alcuni sistemi di controllo dell'accesso sono impostati in modo predefinito su "allow-all" consentendo, pertanto, l'accesso a meno che/finché non viene scritta una regola per negare l'accesso in modo specifico.</i></p>	<p>Senza un meccanismo che limiti l'accesso in base all'effettiva esigenza di un utente, l'utente potrebbe inconsapevolmente ottenere accesso ai dati dei titolari di carte. L'utilizzo di un meccanismo o di un sistema di controllo degli accessi automatizzato è fondamentale per gestire più utenti. Questo sistema dovrebbe essere stabilito in base ai processi e ai criteri di controllo degli accessi dell'organizzazione (compresi "solo se effettivamente necessario" e "controllo dell'accesso basato su ruolo"), dovrebbe gestire l'accesso a tutti i componenti di sistema e dovrebbe disporre di un'impostazione predefinita "deny-all" per garantire che a nessuno venga consentito l'accesso fino a quando non è stata stabilita una regola che concede in modo specifico tale accesso.</p>

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

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

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

Requisito	Istruzioni
<p><b>8.1</b> Assegnare a tutti gli utenti un ID univoco prima di consentire l'accesso ai componenti di sistema o ai dati di titolari di carta.</p>	<p>Garantendo l'identificazione univoca di ogni utente (invece di utilizzare un solo ID per diversi dipendenti), un'organizzazione può mantenere la responsabilità delle azioni e disporre di un effettivo audit trail per ogni dipendente. In questo modo i problemi vengono risolti più velocemente ed è possibile attuare un contenimento quando si rilevano abusi o cattive intenzioni.</p>
<p><b>8.2</b> Oltre ad assegnare un ID univoco , utilizzare almeno uno dei seguenti metodi per l'autenticazione di tutti gli utenti:</p> <ul style="list-style-type: none"> <li>▪ Qualcosa che l'utente conosce, come una password o una passphrase</li> <li>▪ Qualcosa in possesso dell'utente, come un dispositivo token o una smart card</li> <li>▪ Qualcosa che l'utente è, come biometrico</li> </ul>	<p>Questi elementi di autenticazione, se usati in aggiunta agli ID univoci, aiutano a proteggere gli ID univoci degli utenti dalla compromissione (in quanto per un tentativo di compromissione è necessario conoscere sia l'ID univoco che la password o l'altro elemento di autenticazione).</p> <p>Un certificato digitale rappresenta una valida alternativa come forma di tipo di autenticazione "qualcosa in possesso dell'utente" a condizione che sia univoco.</p>

Requisito	Istruzioni
<p><b>8.3</b> Incorporare l'autenticazione a due fattori per l'accesso remoto alla rete (accesso a livello di rete dall'esterno) da parte di dipendenti, amministratori e terze parti. (Ad esempio, RADIUS (Remote Authentication and Dial-in Service) con token; TACACS (Terminal Access Controller Access Control System) con token; oppure altre tecnologie che facilitano l'autenticazione a due fattori.)</p> <p><b>Nota:</b> L' autenticazione a due fattori richiede che per l'autenticazione siano utilizzati due dei tre metodi di autenticazione (vedere il Req. 8.3 per le descrizioni dei metodi di autenticazione) da utilizzare per l'autenticazione. L'utilizzo di un fattore per due volte (ad es. l'uso di due password separate) non si considera come un'autenticazione a due fattori.</p>	<p>L'autenticazione a due fattori richiede due forme di autenticazione per l'accesso a rischio più elevato, ad esempio quello che ha origine all'esterno della rete. Per una maggiore sicurezza, l'organizzazione può prendere in considerazione l'uso dell'autenticazione a due fattori anche per l'accesso a reti con protezione maggiore da reti con protezione minore, ad esempio dai desktop aziendali (minore protezione) ai server/database di produzione con i dati dei titolari di carte (maggiore protezione).</p> <p>Questo requisito è valido per gli utenti con accesso remoto alla rete, nei casi in cui tale accesso potrebbe portare ad accedere all'ambiente dei dati dei titolari di carta.</p> <p>In questo contesto, l'accesso remoto si riferisce all'accesso a livello di rete che ha origine all'esterno della rete di un'entità, da Internet o da un sistema o da una rete "non attendibile", come una terza parte o un dipendente che accedono alla rete dell'entità utilizzando il proprio computer portatile. Ai fini di questo requisito, non viene considerato come accesso remoto l'accesso interno da LAN a LAN (ad esempio, tra due uffici mediante un VPN sicura).</p> <p>Se l'accesso remoto avviene ad una rete di un'entità dotata di adeguata segmentazione, tale che gli utenti in remoto non possono accedere o influire sull'ambiente dei dati dei titolari di carta, per gli standard PCI DSS non sarebbe necessaria un'autenticazione a due fattori per accedere a tale rete. Tuttavia, un'autenticazione a due fattori si rende necessaria per ogni accesso remoto alle reti con accesso all'ambiente dei dati dei titolari di carta, ed è consigliata per tutti gli accessi remoti alle reti dell'entità.</p>
<p><b>8.4</b> Rendere illeggibili tutte le password durante la trasmissione e la memorizzazione su tutti i componenti di sistema utilizzando crittografia avanzata.</p>	<p>Molti dispositivi e applicazioni di rete trasmettono l'ID utente e la password non cifrata sulla rete e/o memorizzano le password senza cifratura. Un utente non autorizzato può facilmente intercettare l'ID utente e la password non cifrati o leggibili utilizzando uno "sniffer" durante la trasmissione o accedendo direttamente a ID utente e password non cifrati nei file in cui sono memorizzati, utilizzando i dati sottratti per l'accesso non autorizzato. Durante la trasmissione, le credenziali dell'utente possono essere cifrate o può essere cifrato il tunnel</p>
<p><b>8.5</b>Garantire una corretta identificazione utente e gestione delle autenticazioni per amministratori e utenti non consumatori su tutti i componenti di sistema nel seguente modo:</p>	<p>Poiché uno di primi passi compiuti da un utente non autorizzato per compromettere un sistema è sfruttare le password deboli o inesistenti, è importante implementare validi processi di autenticazione utente e gestione delle password.</p>
<p><b>8.5.1</b> Controllare le operazioni di aggiunta, eliminazione e modifica di ID utente, credenziali e altri oggetti identificativi.</p>	<p>Per garantire che gli utenti aggiunti ai sistemi siano validi e riconosciuti, l'aggiunta, l'eliminazione e la modifica degli ID utente devono essere gestite e controllate da un piccolo gruppo con la relativa autorità. La capacità di gestire gli ID utente deve essere limitata solo a tale gruppo.</p>

Requisito	Istruzioni
<p><b>8.5.2</b> Verificare l'identità dell'utente prima di eseguire il ripristino delle password.</p>	<p>Molti utenti non autorizzati utilizzano l'ingegneria sociale, ad esempio chiamando un help desk e fingendosi un utente legittimo, per cambiare la loro password in modo da poter utilizzare un ID utente. Prendere in considerazione l'uso di una "domanda segreta" a cui solo l'utente legittimo può rispondere per aiutare gli amministratori a identificare l'utente prima di reimpostare le password. Verificare che tali domande siano ben protette e non condivise.</p>
<p><b>8.5.3</b> Impostare la password per il primo accesso ed il ripristino su un valore univoco per ogni utente e modificarlo immediatamente dopo il primo uso.</p>	<p>Se viene utilizzata la stessa password per ogni nuovo utente impostato, un utente interno, un ex-dipendente o un utente non autorizzato può conoscere o scoprire facilmente la password e utilizzarla per ottenere l'accesso agli account.</p>
<p><b>8.5.4</b> Revocare immediatamente l'accesso per gli utenti non attivi.</p>	<p>Se un dipendente ha lasciato l'azienda e ha tuttora accesso alla rete tramite il suo account utente, potrebbe verificarsi l'accesso inutile o pericoloso ai dati dei titolari di carte. Questo accesso può essere effettuato dall'ex-dipendente o da un utente non autorizzato che sfrutta il vecchio account inutilizzato. Prendere in considerazione l'implementazione di un processo in associazione con le risorse umane per ricevere immediata notifica del licenziamento di un dipendente, in modo che il relativo account utente possa essere immediatamente disattivato.</p>
<p><b>8.5.5</b> Rimuovere/disabilitare gli account utente non attivi almeno ogni 90 giorni.</p>	<p>L'esistenza di account inattivi consente a un utente non autorizzato di sfruttare l'account inutilizzato per accedere potenzialmente ai dati dei titolari di carte.</p>
<p><b>8.5.6</b> Abilitare gli account utilizzati dai fornitori per la gestione in remoto solo durante il periodo di tempo necessario. Monitorare gli account per l'accesso remoto dei fornitori durante l'uso.</p>	<p>Consentendo ai fornitori (ad esempio POS) l'accesso continuo alla rete nel caso debbano supportare i loro sistemi, si aumentano le possibilità di accesso non autorizzato, sia da parte di un utente nell'ambiente del fornitore sia da parte di un utente non autorizzato che trova e utilizza questo punto di ingresso esterno alla rete sempre disponibile.</p> <p>Il monitoraggio dell'accesso del fornitore all'ambiente dei dati dei titolari di carta viene eseguito allo stesso modo di quello adottato per altri utenti, come il personale aziendale. Ciò comprende il monitoraggio e la generazione di registri delle attività come richiesto dai Requisiti 10.1 e 10.2 PCI DSS, e la verifica che l'utilizzo di account remoti dei fornitori avvenga in conformità alla politica secondo le indicazioni contenute nei Requisiti 12.3.8 e 12.3.9.</p>
<p><b>8.5.7</b> Comunicare le procedure e le politiche di autenticazione a tutti gli utenti che hanno accesso ai dati dei titolari di carta.</p>	<p>La comunicazione delle procedure per autenticazione/ password a tutti gli utenti aiuta questi utenti a comprendere e rispettare i criteri, e permette di essere avvisati quando utenti non autorizzati tentano di sfruttare le relative password per accedere ai dati dei titolari di carte (ad esempio chiamando un dipendente e domandando la sua password in modo che il chiamante possa "risolvere un problema").</p>

Requisito	Istruzioni
<p><b>8.5.8</b> Non utilizzare account e password di gruppo, condivisi o generici, o altri metodi di autenticazione.</p>	<p>Se più utenti condividono le medesime credenziali di autenticazione (ad esempio, account utente e password), diventa impossibile assegnare le responsabilità delle azioni o tenerne traccia in modo efficace, in quanto una determinata azione potrebbe essere stata eseguita da qualunque componente del gruppo a conoscenza delle credenziali di autenticazione.</p> <p>Questa esigenza di ID univoci e password complesse viene spesso soddisfatta nell'ambito di funzioni amministrative utilizzando, ad esempio, sudo o SSH in modo che l'amministratore effettui inizialmente il login con il proprio ID univoco e password, per poi collegarsi all'account amministratore mediante sudo o SSH. Spesso i login "direct root" sono disattivati per impedire l'uso di questo account amministrativo condiviso. In questo modo, è possibile mantenere la responsabilità individuale e gli audit trail. Tuttavia, anche con l'uso di strumenti come sudo e SSH, gli effettivi ID amministratore e password dovrebbero soddisfare anche i requisiti PCI DSS (nel caso in cui tali account non siano disattivati) per impedire che vengano usati in modo improprio.</p>
<p><b>8.5.9</b> Modificare le password utente almeno ogni 90 giorni.</p>	<p>Le password avanzate sono la prima linea di difesa nella rete, in quanto un utente non autorizzato spesso tenta in primo luogo di trovare account con password deboli o inesistenti. Il tempo a disposizione di un utente non autorizzato per trovare questi account deboli e compromettere una rete utilizzando un ID utente valido è superiore se le password sono brevi, facili da indovinare o valide per lungo tempo. Le password avanzate possono essere applicate e mantenute secondo questi requisiti attivando le funzionalità di protezione di account e password fornite con il sistema operativo (ad esempio Windows), le reti, i database e altre piattaforme.</p>
<p><b>8.5.10</b> Richiedere una lunghezza minima della password di 7 caratteri.</p>	
<p><b>8.5.11</b> Utilizzare password contenenti valori numerici e alfabetici.</p>	
<p><b>8.5.12</b> Non consentire l'invio di una nuova password uguale a una delle ultime quattro password utilizzate.</p>	<p>Senza i meccanismi di blocco dell'account, un aggressore può tentare in modo continuo di indovinare una password mediante strumenti manuali o automatici (cracking delle password), fino ad avere successo e accedere all'account di un utente.</p>
<p><b>8.5.13</b> Limitare i tentativi di accesso ripetuti bloccando l'ID utente dopo un massimo di sei tentativi.</p>	<p>Se un account è bloccato a causa di un tentativo continuo di indovinare una password, i controlli per ritardare la riattivazione degli account bloccati impediscono all'utente non autorizzato di tentare continuamente di individuare una password (l'interruzione minima prima della riattivazione dell'account è di 30 minuti). Inoltre, se viene richiesta la riattivazione, l'amministratore o l'help desk può verificare che sia il proprietario dell'account la causa del blocco (ad esempio per errori di battitura).</p>
<p><b>8.5.15</b> Se una sessione è inattiva per più di 15 minuti, è necessario che l'utente autentichi di nuovo il terminale o la sessione.</p>	<p>Quando gli utenti si allontanano da un computer attivo con accesso a dati dei titolari di carte o di rete critici, il computer può essere utilizzato da altri in loro assenza, dando luogo all'accesso non autorizzato all'account e/ all'abuso dell'account.</p>

Requisito	Istruzioni
<p><b>8.5.16</b> 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.</p> <p>Consentire l'accesso diretto utente o le query ai database solo agli amministratori del database.</p>	<p>Senza l'autenticazione utente per l'accesso a database e applicazioni, il potenziale di accessi non autorizzati o pericolosi aumenta; inoltre, tale accesso non può essere registrato in quando l'utente non è stato autenticato e quindi non è noto al sistema. Inoltre, l'accesso ai database deve essere consentito solo tramite metodi programmatici (ad esempio stored procedure), anziché mediante accesso diretto al database da parte degli utenti finali (con l'eccezione dei DBA, che possono avere accesso diretto al database per i loro compiti amministrativi).</p>

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

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

Requisito	Istruzioni
<p><b>9.1</b> Utilizzare i controlli dell'accesso alle strutture appropriati per limitare e monitorare gli accessi fisici ai sistemi nell'ambiente dei dati di titolari di carta.</p>	<p>Senza controlli di accesso fisici, le persone non autorizzate possono ottenere accesso all'edificio e alle informazioni sensibili; possono inoltre alterare le configurazioni di sistema, introdurre vulnerabilità nella rete, oppure distruggere o rubare le apparecchiature.</p>
<p><b>9.1.1</b> Utilizzare videocamere o altri meccanismi di controllo dell'accesso per monitorare gli accessi fisici ad aree sensibili. Esaminare i dati raccolti e correlarli con altri. Conservare i dati per almeno tre mesi, se non diversamente richiesto dalle leggi in vigore.</p> <p><b>Nota:</b> per "aree sensibili" si intendono 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.</p>	<p>Durante l'analisi delle violazioni alla protezione, questi controlli possono aiutare a identificare gli individui che accedono fisicamente a queste aree che memorizzano i dati dei titolari di carte. Esempi di aree sensibili comprendono aree server di database aziendali, aree server back-end di una sede di punto vendita che memorizza dati di titolari di carta ed aree di memorizzazione per grandi quantità di dati dei titolari di carta,</p>
<p><b>9.1.2</b> Limitare l'accesso fisico a connettori di rete accessibili pubblicamente.</p> <p>Ad esempio, nelle aree accessibili ai visitatori non dovrebbero essere attivate porte di rete a meno che l'accesso alla rete non sia espressamente autorizzato.</p>	<p>Limitando l'accesso ai connettori di rete è possibile impedire che utenti non autorizzati effettuino il collegamento a tali connettori disponibili, ottenendo accesso alle risorse della rete interna. È possibile valutare la disattivazione dei connettori di rete quando non sono in uso, riattivandoli solo quando necessario. Nelle aree pubbliche, quali le sale conferenze, è possibile creare reti private per consentire a fornitori e visitatori di accedere solo a Internet, in modo che non penetrino nella rete interna.</p>

Requisito	Istruzioni
<p><b>9.1.3</b> Limitare l'accesso fisico a punti di accesso wireless, gateway, dispositivi portatili, hardware di rete e comunicazione e linee di telecomunicazione.</p>	<p>Senza la protezione dell'accesso a componenti e dispositivi wireless, gli utenti non autorizzati possono utilizzare i dispositivi wireless incustoditi dell'azienda per accedere alle risorse di rete, o persino per connettere i loro dispositivi alla rete wireless, ottenendo accesso non autorizzato. Inoltre, la protezione di hardware di comunicazione e di rete impedisce agli utenti non autorizzati di intercettare il traffico di rete o di collegare fisicamente i loro dispositivi alle risorse di rete cablate dell'entità.</p> <p>Prendere in considerazione lo spostamento di hardware di comunicazione e di rete, di gateway e di punti di accesso wireless in aree sicure, ad esempio all'interno di armadi con serratura o sale server. Per le reti wireless, garantire l'attivazione di cifratura avanzata. Prendere in considerazione anche l'attivazione del blocco automatico dei dispositivi palmari wireless dopo un lungo periodo di inattività, e l'impostazione dei dispositivi affinché richiedano una password all'accensione.</p>
<p><b>9.2</b> Sviluppare procedure che consentono di distinguere facilmente tra personale in sede e visitatori, in particolare in aree che permettono l'accesso ai dati di titolari di carta.</p>	<p>Senza l'uso di sistemi badge e controlli all'ingresso, gli utenti non autorizzati possono facilmente accedere all'edificio per rubare, disattivare, interrompere o distruggere sistemi critici e dati dei titolari di carte. Per un controllo ottimale, implementare un sistema di accesso a tessera o badge all'interno e all'esterno delle aree di lavoro che contengono i dati dei titolari di carte.</p> <p>La predisposizione dell'identificazione dei visitatori autorizzati in modo da poterli facilmente distinguerli dal personale in sede impedisce che a visitatori non autorizzati venga concesso l'accesso ad aree contenenti dati dei titolari di carta.</p>
<p><b>9.3</b> Accertarsi che tutti i visitatori vengano gestiti nel modo seguente:</p>	<p>I controlli sui visitatori sono importanti per ridurre la capacità degli utenti non autorizzati di accedere agli edifici (e, potenzialmente, ai dati dei titolari di carte).</p>
<p><b>9.3.1</b> Siano autorizzati prima di accedere alle aree in cui i dati di titolari di carta sono elaborati o custoditi.</p>	<p>I controlli sui visitatori sono importanti per garantire che i visitatori accedano solo alle aree a cui sono autorizzati, che siano identificabili come visitatori (in modo che il personale possa controllarne le attività) e che il loro accesso sia limitato solo alla durata della visita legittima.</p>
<p><b>9.3.2</b> Ricevano un token fisico (ad esempio, una tessera magnetica o un dispositivo di accesso) con scadenza, che identifica i visitatori non come personale in sede.</p>	
<p><b>9.3.3</b> Restituiscano il token fisico prima di lasciare la struttura o in corrispondenza della data di scadenza.</p>	
<p><b>9.4</b> Utilizzare un registro visitatori per conservare un audit trail fisico dell'attività dei visitatori. Documentare il nome del visitatore, l'azienda rappresentata e il personale in sede che autorizza l'accesso fisico sul registro. Conservare questo registro per almeno tre mesi, se non diversamente richiesto dalla legge.</p>	<p>Un registro dei visitatori che documenta informazioni minime sul visitatore è facile ed economico da mantenere e può offrire assistenza, in caso di un'indagine su una violazione dei dati, nell'identificazione dell'accesso fisico a un edificio o un locale, e potenzialmente ai dati dei titolari di carte. Prendere in considerazione l'implementazione di registri all'ingresso degli edifici e soprattutto nelle zone in cui sono presenti i dati dei titolari di carte.</p>

Requisito	Istruzioni
<p><b>9.5</b> 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.</p>	<p>Se conservati in un ambiente non sicuro, i backup contenenti i dati dei titolari di carte possono essere facilmente persi, rubati o copiati per scopi pericolosi. Per una memorizzazione sicura, prendere in considerazione un contratto con un'azienda che si occupa di conservazione di dati commerciali o, per un'entità più piccola, l'uso di una cassetta di sicurezza presso una banca.</p>
<p><b>9.6</b> Proteggere fisicamente tutti i supporti.</p>	<p>I dati dei titolari di carte sono soggetti a visualizzazione, copia o scansione non autorizzate se sono trasferiti senza protezione su supporti portatili o rimovibili, stampati o lasciati sulla scrivania.</p>
<p><b>9.7</b> Mantenere un rigido controllo sulla distribuzione interna o esterna di qualsiasi tipo di supporto, incluso quanto segue:</p>	<p>Procedure e processi che aiutano a proteggere i dati dei titolari di carte sui supporti distribuiti agli utenti interni e/o esterni. Senza tali procedure i dati possono essere persi o rubati e utilizzati per scopi fraudolenti.</p>
<p><b>9.7.1</b> Classificare i supporti in modo da poter determinare la sensibilità dei dati.</p>	<p>È importante che i supporti siano identificati in modo che il loro stato di classificazione possa essere facilmente rilevato. Per i supporti che non sono identificati come riservati non è possibile predisporre una protezione adeguata o possono essere persi o rubati.</p>
<p><b>9.7.2</b> Inviare il supporto tramite un corriere affidabile o un altro metodo di consegna che possa essere monitorato in modo appropriato.</p>	<p>I supporti possono essere rubati o persi se inviati tramite un metodo non rintracciabile, ad esempio la posta tradizionale. Utilizzare i servizi di un corriere sicuro per consegnare i supporti che possono contenere dati dei titolari di carte, così da utilizzare i loro sistemi di tracking per mantenere l'inventario e la posizione delle spedizioni.</p>
<p><b>9.8</b> Accertarsi che il management approvi tutti i supporti che vengono spostati da un'area protetta (in particolare quando i supporti vengono distribuiti a singoli utenti).</p>	<p>Per i dati dei titolari di carte che lasciano le aree sicure senza un processo approvato dal management può verificarsi la perdita o il furto degli stessi. Senza un processo definito, la posizione dei supporti non viene rintracciata e non esiste un processo sulla destinazione dei dati o sulla loro protezione.</p>
<p><b>9.9</b> Mantenere un rigido controllo sulla conservazione e sull'accessibilità dei supporti.</p>	<p>Senza metodi di inventario attenti e controlli di storage, potrebbe non essere possibile accorgersi del furto o della mancanza di supporti per diverso tempo.</p>
<p><b>9.9.1</b> Conservare in modo appropriato i registri di inventario per tutti i supporti ed eseguire tali inventari almeno una volta all'anno.</p>	<p>Se i supporti non vengono inventariati, potrebbe non essere possibile accorgersi del furto o della mancanza di supporti per diverso tempo oppure non accorgersene affatto.</p>
<p><b>9.10</b> Distruggere i supporti quando non sono più necessari per scopi aziendali o legali, come segue:</p>	<p>La mancata adozione di misure per distruggere le informazioni contenute sui dischi rigidi, unità portatili, CD/DVD o su carta prima dell'eliminazione, può dar modo ad utenti non autorizzati di recuperare le informazioni dai supporti eliminati, determinando una compromissione dei dati. Ad esempio, gli individui non autorizzati possono utilizzare una tecnica chiamata "dumpster diving", con la quale</p>
<p><b>9.10.1</b> Stracciare, bruciare o mandare al macero i materiali cartacei in modo che i dati di titolari di carta non possano essere ricostruiti.</p>	

Requisito	Istruzioni
<b>9.10.2</b> Rendere i dati di titolari di carta su supporti elettronici non recuperabili, in modo che non sia possibile ricostruirli.	ricercano nei cestini e nella spazzatura, informazioni che possono usare per lanciare un attacco.  Esempi di metodi che consentono una distruzione sicura dei supporti elettronici comprendono cancellazione, smagnetizzazione o distruzione fisica (come tritare o distruggere i dischi rigidi).

## Istruzioni per i requisiti 10 e 11: 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, se non impossibile, determinare la causa di una compromissione di dati.*

Requisito	Istruzioni
<b>10.1</b> 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.	È fondamentale disporre di un processo o di un sistema che colleghi l'accesso dell'utente ai componenti di sistema, in particolare per gli utenti con privilegi di amministrazione. Questo sistema genera log di audit e consente di ricondurre le attività sospette a un utente specifico. I team legali attivati dopo un incidente fanno affidamento su questi log per avviare le indagini.
<b>10.2</b> Implementare audit trail automatici per tutti i componenti di sistema per ricostruire i seguenti eventi:	La generazione di audit trail sulle attività sospette avverte l'amministratore di sistema, invia dati ad altri meccanismi di monitoraggio (ad esempio i sistemi di rilevamento delle intrusioni) e fornisce una cronologia da utilizzare a seguito di un incidente. La registrazione dei seguenti eventi consente ad un'organizzazione di identificare e tenere traccia delle attività potenzialmente dannose.
<b>10.2.1</b> Tutti gli accessi utente ai dati di titolari di carta	Gli utenti non autorizzati potrebbero arrivare a conoscere un account utente con accesso ai sistemi nel ambiente dei dati dei titolari di carta, oppure potrebbero creare un nuovo account non autorizzato per accedere ai dati dei titolari di carta. La registrazione di tutti gli accessi individuali ai dati dei titolari di carta può individuare quali account possono essere stati compromessi o usati in modo improprio.
<b>10.2.2</b> Tutte le azioni intraprese da un utente con privilegi di utente root o amministratore	Account con maggiori privilegi, come di "amministratore" o "root", hanno il potenziale di influire in modo significativo sulla sicurezza o sulla funzionalità operativa di un sistema. Senza un log delle attività eseguite, un'organizzazione non è in grado di ricondurre ogni questione risultante da un errore amministrativo o dall'uso improprio di privilegi all'individuo o all'azione specifica.
<b>10.2.3</b> Accesso a tutti gli audit trail	Gli utenti non autorizzati spesso cercano di modificare i log di audit per nascondere le loro azioni e con la registrazione degli accessi per un'organizzazione è possibile ricondurre eventuali incongruenze o potenziali manomissioni dei log ad un singolo account,
<b>10.2.4</b> Tentativi di accesso logico non validi	Gli utenti non autorizzati sulla rete spesso eseguono più tentativi di accesso sui sistemi di destinazione. Vari tentativi di login non riusciti possono rappresentare un'indicazione dei tentativi di accesso di un utente non autorizzato facendo ricorso a "forza bruta" o cercando di indovinare una password.

Requisito	Istruzioni
<b>10.2.5</b> Uso dei meccanismi di identificazione e autenticazione	<p>Se non è possibile sapere chi erano gli utenti presenti al momento in cui si è verificato un incidente, non è possibile identificare gli account che possono essere usati. Inoltre, gli utenti non autorizzati possono tentare di manipolare i controlli di autenticazione per cercare di superarli o di spacciarsi per un account valido. Le attività comprese, senza limitazione, la scalata di privilegi o le modifiche ai permessi di accesso possono segnalare l'uso non autorizzato dei meccanismi di autenticazione di un sistema.</p>
<b>10.2.6</b> Inizializzazione dei registri di audit	<p>La disattivazione dei log di audit prima di eseguire delle attività illecite è un obiettivo comune degli utenti non autorizzati che non vogliono essere scoperti. L'inizializzazione dei log di audit potrebbe indicare che la funzione di log è stata disattivata da un utente per nascondere le sue azioni.</p>
<b>10.2.7</b> Creazione ed eliminazione di oggetti a livello di sistema	<p>Software dannoso, come malware, spesso crea o sostituisce oggetti a livello di sistema sul sistema di destinazione per controllarne una determinata funzione o operazione.</p> <p>Fare riferimento al documento <i>PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi</i> per la definizione di "oggetti a livello di sistema".</p>
<p><b>10.3</b> Registrare almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento:</p> <ul style="list-style-type: none"> <li><b>10.3.1</b> Identificazione utente</li> <li><b>10.3.2</b> Tipo di evento</li> <li><b>10.3.3</b> Data e ora</li> <li><b>10.3.4</b> Indicazione di successo o fallimento</li> <li><b>10.3.5</b> Origine dell'evento</li> <li><b>4.3.6</b> Identità o nome dell'elemento interessato (dati, componente di sistema o risorsa)</li> </ul>	<p>Registrando queste voci per gli eventi registrabili nel punto 10.2, è possibile identificare rapidamente una potenziale compromissione e disporre di dettagli sufficienti per sapere chi, cosa, dove, come e quando.</p>

Requisito	Istruzioni
<p><b>10.4</b> Utilizzando la tecnologia per la sincronizzazione dell'ora, sincronizzare tutti gli orologi e gli orari critici del sistema ed assicurare che sia implementato quanto segue per l'acquisizione, la distribuzione e la memorizzazione dell'ora.</p> <p><i>Nota: NTP (Network Time Protocol) è un esempio di tecnologia per la sincronizzazione dell'ora.</i></p> <p><b>10.4.1</b> I sistemi critici hanno l'ora esatta e coerente</p> <p><b>10.4.2</b> I dati dell'ora sono protetti</p> <p><b>10.4.3</b> Le impostazioni dell'ora sono ricevute da sorgenti per l'orario accettate dal settore</p>	<p>La tecnologia per la sincronizzazione dell'ora viene utilizzata per sincronizzare gli orologi su sistemi multipli. Quando utilizzata in modo corretto, questa tecnologia è in grado di sincronizzare gli orologi su un numero elevato di sistemi entro una frazione di secondo l'uno dall'altro. Alcuni dei problemi che possono verificarsi quando gli orologi non sono sincronizzati in modo corretto comprendono, senza limitazioni, rendere difficile se non impossibile il confronto di file di registro di diversi sistemi per stabilire la sequenza esatta di eventi (elemento fondamentale per l'analisi forense nel caso di una violazione), ed impedire i protocolli crittografici come SSH il cui funzionamento corretto si basa sull'ora assoluta. Per i team legali attivati dopo un incidente, la precisione e la coerenza dell'ora tra tutti i sistemi e l'ora di ciascuna attività è fondamentale per determinare come sono stati compromessi i sistemi.</p> <p>Per assicurare che l'ora sia coerente, idealmente, in un'entità, dovrebbero esserci solo pochi server interni di rilevamento dell'orario (centrale). Questi server ricevono dati UTC (Coordinated Universal Time) direttamente da server per il rilevamento dell'orario esterni conosciuti ed affidabili, via radio, satelliti GPS o altre fonti di rete esterne, e comunicano tra loro per garantire la precisione dell'orario. Altri sistemi ricevono poi l'orario da questi server.</p> <p>Se un utente non autorizzato ha accesso alla rete, spesso tenta di cambiare gli indicatori di data/ora delle sue azioni all'interno dei log di audit per impedire il rilevamento delle sue attività. Un utente non autorizzato può anche cercare di modificare direttamente l'orologio di un componente di sistema per nascondere la propria presenza, ad esempio modificando l'orologio di sistema ad un'ora precedente. Per questi motivi, è importante che l'orario sia preciso su tutti i sistemi e che i dati relativi all'orario siano protetti da modifiche o accessi non autorizzati. I dati relativi all'orario comprendono parametri e metodi utilizzati per impostare l'orologio di ogni sistema.</p> <p>Ulteriori informazioni su NTP sono disponibili sul sito Web <a href="http://www.ntp.org">www.ntp.org</a>, comprese le informazioni su ora, standard e server di rilevamento dell'ora.</p>
<p><b>10.5</b> Proteggere gli audit trail in modo che non possano essere modificati.</p>	<p>Spesso un utente non autorizzato che ha ottenuto accesso alla rete tenta di modificare i log di audit per celare le sue attività. Senza un'adeguata protezione dei log di audit non è possibile garantirne la completezza, la precisione e l'integrità; inoltre, i log di audit possono rivelarsi uno strumento di indagine inutile dopo una compromissione.</p>

Requisito	Istruzioni
<p><b>10.5.1</b> Limitare la visualizzazione degli audit trail a coloro che realmente necessitano di tali informazioni per scopi aziendali.</p> <p><b>10.5.2</b> Proteggere i file di audit trail da modifiche non autorizzate.</p> <p><b>10.5.3</b> Eseguire immediatamente il backup dei file di audit trail su un server di registro centralizzato o un supporto difficile da modificare.</p> <p><b>10.5.4</b> Scrivere registri per tecnologie rivolte al pubblico su un server di registro sulla LAN interna.</p>	<p>Una protezione adeguata dei log di audit comprende un solido controllo degli accessi (che limita l'accesso ai registri "solo se effettivamente necessario") e l'uso della separazione interna (per rendere più difficile l'individuazione e la modifica dei registri). Scrivendo i log da tecnologie rivolte al pubblico, quali wireless, firewall, DNS e server di posta, il rischio di modifica dei registri è ridotto, in quanto sono più sicuri all'interno della rete interna.</p>
<p><b>10.5.5</b> Utilizzare un meccanismo di monitoraggio dell'integrità dei file o un software di rilevamento delle modifiche sui registri per accertarsi che i dati di registro esistenti non possano essere modificati senza generare avvisi (sebbene l'aggiunta di nuovi dati non dovrebbe generare avvisi).</p>	<p>I sistemi di monitoraggio dell'integrità dei file controllano e segnalano le modifiche ai file critici. Ai fini del monitoraggio dell'integrità dei file, un'entità di solito controlla i file che in genere non cambiano, ma che se sono modificati indicano una potenziale compromissione. Per i file di registro (che cambiano spesso), è opportuno monitorare, ad esempio, quando un file viene eliminato, aumenta o riduce notevolmente le sue dimensioni, o altri indicatori di manomissione del file di registro da parte di un utente non autorizzato. Sono disponibili sia strumenti commerciali sia applicazioni open source per monitorare l'integrità dei file.</p>
<p><b>10.6</b> 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.</p> <p><i>Nota: gli strumenti di raccolta, analisi e generazione di avvisi per i log possono essere utilizzati ai fini della conformità al requisito 10.6.</i></p>	<p>Molte violazioni avvengono per giorni o mesi prima di essere rilevate. Il controllo quotidiano dei registri riduce al minimo la durata e l'esposizione di una potenziale violazione. Il processo di revisione dei registri non deve essere manuale: si può considerare l'uso di strumenti di raccolta, analisi e generazione di avvisi, in particolare per le entità con numerosi server.</p>
<p><b>10.7</b> 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).</p>	<p>La conservazione dei registri per almeno un anno è dovuta al fatto che spesso serve tempo per individuare una compromissione avvenuta o in corso, e consente agli investigatori di disporre di una cronologia sufficiente per determinare il periodo interessato da una potenziale violazione e i sistemi coinvolti. Con la disponibilità immediata dei registri di tre mesi, un'entità può identificare rapidamente e ridurre al minimo l'impatto di una violazione dei dati. La conservazione dei nastri di backup fuori sede può richiedere tempi superiori per il ripristino dei dati, l'analisi e l'identificazione dei dati o dei sistemi interessati.</p>

## Requisito 11: Eseguire regolarmente test dei sistemi e processi di protezione

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

Requisito	Istruzioni
<p><b>11.1</b> Verificare la presenza di punti di accesso wireless e rilevare punti di accesso wireless non autorizzati almeno su base trimestrale.</p> <p><b>Nota:</b> I metodi che si possono utilizzare nel processo comprendono, senza limitazioni, scansioni della rete wireless, controlli di tipo fisico e logico di infrastrutture e componenti di sistema, NAC (Network Access Control) o IDS/IPS wireless.</p> <p>Qualunque sia il metodo adottato, questo deve essere in grado di rilevare ed identificare qualsiasi dispositivo non autorizzato.</p>	<p>L'implementazione e/o lo sfruttamento della tecnologia wireless all'interno di una rete rappresentano uno dei percorsi più noti agli utenti non autorizzati per ottenere l'accesso alla rete e ai dati dei titolari di carte. Se viene installato un dispositivo o una rete wireless senza che l'azienda ne sia a conoscenza, un aggressore potrebbe accedere alla rete con facilità e in modo "invisibile".</p> <p>Dispositivi wireless non autorizzati possono essere nascosti all'interno di un computer o di un altro componente di sistema o collegati ad esso, oppure essere collegati direttamente ad una porta o a un dispositivo di rete, come uno switch o un router. Ogni dispositivo non autorizzato di questo tipo potrebbe costituire un punto di accesso non autorizzato all'ambiente.</p> <p>In considerazione della facilità con cui un punto di accesso wireless può essere unito alla rete, della difficoltà a rilevarne la presenza e del maggiore rischio posto dai dispositivi wireless non autorizzati, queste scansioni vanno eseguite anche in presenza di un criterio che impedisce l'uso della tecnologia wireless.</p> <p>Le dimensioni e la complessità di un determinato ambiente stabiliranno gli strumenti ed i processi adeguati da utilizzare per fornire un'assicurazione sufficiente che nell'ambiente non sia stato installato un punto di accesso wireless non autorizzato.</p> <p>Ad esempio: Nel caso di un singolo chiosco di vendita indipendente in un centro commerciale, dove tutti i componenti di comunicazione sono inseriti in contenitori a prova di manomissione e con chiusura di garanzia, l'esecuzione di un'accurata ispezione fisica del chiosco spesso può essere sufficiente per garantire che non sia stato installato o connesso un punto di accesso wireless non autorizzato. Tuttavia, in un ambiente in cui sono presenti nodi multipli (come in un negozio di grandi dimensioni, un call centre, un'area server o un centro dati), l'esecuzione di un'accurata ispezione fisica diventa più difficile a causa del numero di componenti di sistema e punti di rete in cui un dispositivo di accesso wireless non autorizzato potrebbe essere installato o nascosto. In questo caso, è possibile combinare più metodi per soddisfare il requisito, ad esempio abbinando l'esecuzione di ispezioni fisiche del sistema ai risultati di un analizzatore wireless.</p> <p>Le soluzioni NAC (Network access control) possono eseguire l'autenticazione del dispositivo e la gestione della configurazione per impedire la connessione alla rete di sistemi non autorizzati, o la connessione di dispositivi non autorizzati a sistemi autorizzati sulla rete.</p> <p>Un'organizzazione dovrebbe disporre, all'interno del suo piano di risposta agli incidenti, di procedure documentate da seguire nel caso venga rilevato un punto di accesso wireless non autorizzato. È opportuno configurare un IDS/IPS wireless affinché generi automaticamente un avviso, ma il piano deve anche documentare le procedure di risposta se viene rilevato un dispositivo non autorizzato</p>

Requisito	Istruzioni
<p><b>11.2</b>Eseguire scansioni di vulnerabilità della rete interne ed esterne almeno una volta ogni tre mesi e dopo ogni cambiamento significativo apportato alla rete (ad esempio, installazione di nuovi componenti di sistema, modifica della topologia della rete, modifica delle regole del firewall o aggiornamento di un prodotto).</p> <p><i><b>Nota:</b> non è necessario completare quattro scansioni trimestrali per la conformità iniziale a PCI DSS, se il valutatore verifica che 1) il risultato della scansione più recente era positivo, 2) l'entità dispone di politiche e procedure documentate che richiedono l'esecuzione di scansioni trimestrali e 3) ogni vulnerabilità rilevata dalla scansione è stata corretta nel modo dimostrato da una nuova scansione. Per gli anni successivi alla scansione PCI DSS iniziale, è necessario eseguire quattro scansioni trimestrali con esito positivo.</i></p>	<p>durante una scansione wireless manuale.</p> <p>Una scansione delle vulnerabilità è uno strumento automatico eseguito su server e dispositivi di rete interni ed esterni, studiato per esporre le potenziali vulnerabilità nelle reti che possono essere individuate e sfruttate da utenti non autorizzati. Una volta identificati questi punti deboli, l'entità li corregge e ripete la scansione per verificare che le vulnerabilità siano state corrette.</p> <p>All'atto della valutazione PCI DSS iniziale di un'entità, è possibile che non siano ancora state eseguite quattro scansioni trimestrali. Se il risultato della scansione più recente soddisfa i criteri di una scansione di passaggio, ed esistono criteri e procedure per le scansioni trimestrali future, lo scopo di questo requisito può considerarsi soddisfatto. Non è necessario ritardare una valutazione "sul posto" per questo requisito a causa della mancanza di quattro scansioni, purché queste condizioni siano soddisfatte.</p>

Requisito	Istruzioni
<p><b>11.2.1</b> Eseguire scansioni di vulnerabilità interne ogni tre mesi.</p>	<p>Un processo definito per l'identificazione delle vulnerabilità sui sistemi interni nell'ambiente dei dati dei titolari di carta richiede l'esecuzione di scansioni di vulnerabilità trimestrali. L'identificazione e la risoluzione delle vulnerabilità in modo tempestivo, riduce le probabilità che una vulnerabilità venga sfruttata e quindi la potenziale compromissione di un componente di sistema o dei dati dei titolari di carta.</p> <p>Le vulnerabilità che costituiscono i rischi più elevati per l'ambiente (ad esempio, classificate come "Elevate" in base al Requisito 6.2) dovrebbero essere risolte con la massima priorità.</p> <p>Poiché, durante l'anno, le reti interne possono subire modifiche continue, è possibile che un'entità possa non avere scansioni complete per le vulnerabilità interne. Per un'entità lo scopo è quello di avere a disposizione un programma valido di gestione delle vulnerabilità che le permetta di risolvere le vulnerabilità rilevate in tempi ragionevoli. Come minimo, le vulnerabilità "elevate" devono essere risolte tempestivamente.</p> <p>Le scansioni per le vulnerabilità interne possono essere eseguite da personale interno qualificato che sia ragionevolmente indipendente dai componenti di sistema sottoposti a scansione (ad esempio, un amministratore del firewall non dovrebbe eseguire la scansione del firewall), oppure un'entità può scegliere di far eseguire queste scansioni da un fornitore di scansioni approvato (ASV, Approved Scanning Vendor) riconosciuto da PCI SSC, da un QSA o da un'altra azienda specializzata in scansioni delle vulnerabilità.</p>
<p><b>11.2.2</b> Far eseguire le scansioni esterne della vulnerabilità trimestrali ad un fornitore di scansioni approvato (ASV) autorizzato da PCI SSC.</p> <p><i>Nota: le scansioni esterne delle vulnerabilità trimestrali devono essere eseguite da un fornitore di scansioni approvato (ASV) e autorizzato da PCI SSC. Le scansioni dopo le modifiche della rete possono essere eseguite da personale interno.</i></p>	<p>Poiché le reti esterne sono esposte ad un rischio più elevato di compromissione, le scansioni esterne delle vulnerabilità devono essere eseguita da ASV di PCI SSC.</p> <p>Gli ASV sono tenuti a seguire una serie di criteri di scansione e rendicontazione stabiliti da PCI SSC nella Guida del programma per i fornitori di scansioni approvati.</p>
<p><b>11.2.3</b> Eseguire scansioni interne ed esterne dopo ogni modifica significativa.</p> <p><i>Nota: Le scansioni dopo le modifiche possono essere eseguite da personale interno.</i></p>	<p>La scansione di un ambiente, successivamente all'introduzione di una modifica significativa, assicura che le modifiche siano state apportate in modo adeguato così da non compromettere la sicurezza dell'ambiente a seguito della modifica. Potrebbe non essere necessario effettuare la scansione dell'intero ambiente dopo una modifica. Ad ogni modo, tutti i componenti di sistema interessati dalla modifica dovranno essere sottoposti a scansione.</p>

Requisito	Istruzioni
<p><b>11.3</b> 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:</p> <ul style="list-style-type: none"><li><b>11.3.1</b> Test di penetrazione a livello di rete</li><li><b>11.3.2</b> Test di penetrazione a livello di applicazione</li></ul>	<p>Il test di penetrazione ha come scopo la simulazione di una situazione di attacco nel mondo reale con l'obiettivo di stabilire fino a che punto un aggressore sarebbe in grado di penetrare nell'ambiente. In questo modo un'entità, disponendo di un'idea più chiara dell'esposizione potenziale, può elaborare una strategia per difendersi dagli attacchi.</p> <p>Un test di penetrazione è diverso da una scansione della vulnerabilità, essendo un processo attivo che può comprendere lo sfruttamento delle vulnerabilità identificate. Spesso, l'esecuzione di una scansione delle vulnerabilità rappresenta uno dei primi passi che una persona che esegue test di penetrazione effettua per comprendere una strategia di attacco, pur non essendo l'unico passo. Anche se una scansione delle vulnerabilità non rileva alcuna vulnerabilità conosciuta, la persona che esegue il test di penetrazione spesso acquisirà una conoscenza sufficiente del sistema per identificare eventuali lacune della sicurezza.</p> <p>I test di penetrazione sono generalmente un processo estremamente manuale. Sebbene possano essere utilizzati alcuni strumenti automatici, la persona che esegue il test deve utilizzare la propria conoscenza dei sistemi per penetrare in un ambiente. Spesso la persona che esegue i test incatena insieme vari tipi di exploit con l'obiettivo di bucare gli strati di difesa. Ad esempio, se la persona che esegue i test individua un modo per accedere al server di un'applicazione, userà il server compromesso come punto per organizzare un nuovo attacco sulla base delle risorse a cui il server ha accesso. In questo modo l'esecutore del test è in grado di simulare i metodi cui ricorre un aggressore per identificare ogni area che presenta un potenziale punto debole nell'ambiente di cui è necessario occuparsi.</p>

Requisito	Istruzioni
<p><b>11.4</b> Utilizzare sistemi di rilevamento e/o di prevenzione delle intrusioni per monitorare tutto il traffico in corrispondenza del perimetro dell'ambiente dei dati di titolari di carta nonché ai punti critici all'interno dell'ambiente stesso e segnalare possibili rischi al personale addetto.</p> <p>Mantenere aggiornati tutti i sistemi, basi e firme di rilevamento e prevenzione delle intrusioni.</p>	<p>I sistemi di rilevamento e/o prevenzione delle intrusioni (IDS/IPS) operano un confronto del traffico in entrata nella rete con "firme" e/o comportamenti conosciuti di migliaia di tipi di compromissione (strumenti per hacker, cavalli di Troia ed altro malware) ed inviano avvisi e/o fermano il tentativo in corso. Senza un approccio proattivo al rilevamento di attività non autorizzate mediante questi strumenti, gli attacchi alle risorse del computer (o l'abuso di tali risorse) potrebbero non essere rilevati in tempo reale. Gli avvisi di protezione generati da questi strumenti dovrebbero essere monitorati, al fine di fermare i tentativi di intrusione.</p> <p>I dispositivi IDS/IPS dovrebbero essere implementati in modo da monitorare il traffico in entrata e in uscita in corrispondenza del perimetro dell'ambiente dei dati dei titolari di carta (CDE) nonché ai punti critici all'interno dell'ambiente stesso. I punti critici all'interno del CDE possono includere server di database che memorizzano i dati dei titolari di carta, posizioni di memorizzazione delle chiavi crittografiche, reti di elaborazione o altri componenti di sistemi sensibili come determinato dall'ambiente dell'entità e documentato nella valutazione dei rischi.</p> <p>Sebbene esistano attualmente molti dispositivi IDS/IPS in grado di monitorare più punti all'interno del CDE mediante un singolo dispositivo, è importante tener conto della maggiore esposizione che può verificarsi a seguito del guasto di tale singolo dispositivo. Pertanto, è importante incorporare un'adeguata ridondanza nell'infrastruttura IDS/IPS.</p> <p>Esistono migliaia di tipi di compromissione, e molti altri vengono scoperti quotidianamente. I motori di scansioni e le firme stantie sui dispositivi IDS/IPS non saranno in grado di identificare le nuove vulnerabilità che potrebbero dar luogo a violazioni non rilevate. I fornitori di questi prodotti mettono a disposizione aggiornamenti frequenti, spesso giornalieri, che dovrebbero essere valutati ed applicati su base regolare.</p>

Requisito	Istruzioni
<p><b>11.5</b> Distribuire gli strumenti di monitoraggio dell'integrità dei file per segnalare al personale modifiche non autorizzate di file system, file di configurazione o file di contenuto critici; inoltre, configurare il software in modo che esegua confronti di file critici almeno una volta alla settimana.</p> <p><b>Nota:</b> 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).</p>	<p>Gli strumenti di monitoraggio dell'integrità dei file (FIM) controllano e segnalano le modifiche ai file critici. Sono disponibili sia strumenti commerciali sia applicazioni open source per monitorare l'integrità dei file. Se non vengono implementati correttamente e l'output del FIM non è monitorato, un utente non autorizzato potrebbe modificare il contenuto dei file di configurazione, i programmi del sistema operativo o i file eseguibili delle applicazioni. Tali modifiche non autorizzate, se non vengono rilevate, possono rendere inefficaci i controlli di protezione esistenti e/o dare luogo al furto dei dati dei titolari di carte senza impatto percettibile sulla normale elaborazione.</p>

## Istruzioni per il requisito 12: Gestire una politica di sicurezza delle informazioni

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

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

Requisito	Istruzioni
<p><b>12.1</b> Stabilire, pubblicare, conservare e rendere disponibile una politica di sicurezza conforme a quanto indicato di seguito:</p> <p><b>12.1.1</b> Risponde a tutti i requisiti PCI DSS.</p>	<p>Un criterio di protezione delle informazioni dell'azienda crea la roadmap per l'implementazione delle misure di protezione per proteggere le sue risorse più preziose. Una politica di sicurezza rigida definisce il livello di sicurezza per l'intera società e consente al personale di sapere quali sono le aspettative nei loro confronti in termini di sicurezza. Tutto il personale deve essere a conoscenza della sensibilità dei dati e delle proprie responsabilità in termini di protezione.</p>
<p><b>12.1.2</b> Include un processo annuale che identifica minacce e vulnerabilità e che consente di ottenere una valutazione formale dei rischi. (Esempi di metodologie per la valutazione dei rischi includono, senza limitazioni, OCTAVE, ISO 27005 e NIST SP 800-30).</p>	<p>Una valutazione dei rischi consente all'organizzazione di individuare le minacce e le vulnerabilità connesse che hanno il potenziale di influire negativamente sulla sua attività. Si può quindi procedere ad assegnare in modo efficace le risorse per implementare controlli volti a ridurre la probabilità e/o il potenziale impatto della minaccia che si verifica.</p> <p>L'esecuzione di valutazioni dei rischi con cadenza almeno annuale consente all'organizzazione di tenersi aggiornata sulle modifiche organizzative e sulle minacce, tendenze e tecnologie future,</p>
<p><b>12.1.3</b> Includa una revisione almeno annuale ed esegua gli aggiornamenti quando si apportano modifiche all'ambiente.</p>	<p>Le minacce alla sicurezza e i metodi di protezione si evolvono rapidamente durante l'anno. Senza l'aggiornamento dei criteri di protezione per riflettere le modifiche di rilievo, le nuove misure di protezione per combattere queste minacce non vengono applicate.</p>
<p><b>12.2</b> 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).</p>	<p>Le procedure di sicurezza operativa giornaliere fungono da "istruzioni alla scrivania" che il personale può utilizzare nelle attività quotidiane di manutenzione e amministrazione del sistema. Le procedure di sicurezza operativa non documentate porteranno al fatto che il personale non comprende l'intero scopo dell'attività svolta, processi che non possono essere ripetuti facilmente dai nuovi dipendenti e potenziali lacune in questi processi che potrebbero consentire a un utente non autorizzato di ottenere l'accesso a sistemi e risorse critici.</p>

Requisito	Istruzioni
<p><b>12.3</b> Sviluppare politiche che regolano l'uso per le tecnologie critiche (ad esempio, tecnologie di accesso remoto, wireless, supporti elettronici rimovibili, laptop, tablet, PDA, uso della posta elettronica e di Internet) e definire l'uso corretto di queste tecnologie. Accertarsi che tali politiche richiedano quanto segue:</p>	<p>I criteri di utilizzo del personale possono sia vietare l'uso di determinati dispositivi e altre tecnologie in base alla politica dell'azienda, sia fornire una guida all'uso e all'implementazione corretti per il personale. Se non sono disponibili criteri di utilizzo, il personale può utilizzare le tecnologie in violazione delle politiche dell'azienda, consentendo pertanto agli utenti non autorizzati di accedere ai sistemi critici e ai dati dei titolari di carte. Un esempio può essere l'impostazione inconsapevole di reti wireless prive di protezione. Per garantire il rispetto degli standard aziendali e l'implementazione delle sole tecnologie approvate, prendere in considerazione la limitazione dell'implementazione ai soli team operativi, impedendo al personale generico/non specializzato di installare queste tecnologie.</p>
<p><b>12.3.1</b> Approvazione esplicita delle parti autorizzate</p>	<p>Senza la richiesta dell'approvazione esplicita per l'implementazione di queste tecnologie, un singolo membro del personale può implementare una soluzione per un'esigenza aziendale percepita aprendo inconsapevolmente un enorme falla che mette sistemi critici e dati a disposizione degli utenti non autorizzati.</p>
<p><b>12.3.2</b> Autenticazione per l'uso della tecnologia</p>	<p>Se la tecnologia viene implementata senza la corretta autenticazione (ID utente e password, token, VPN, ecc.), gli individui non autorizzati possono facilmente utilizzare questa tecnologia non protetta per accedere a sistemi critici e dati dei titolari di carte.</p>
<p><b>12.3.3</b> Un elenco di tutti i dispositivi di questo tipo e del personale autorizzato all'accesso</p>	<p>Gli individui non autorizzati possono violare la sicurezza fisica e inserire i loro dispositivi nella rete come "back door." Il personale può anche ignorare le procedure ed installare dispositivi. Un inventario accurato con una corretta etichettatura dei dispositivi consente una rapida identificazione delle installazioni non approvate. Prendere in considerazione l'applicazione di una convenzione di denominazione ufficiale per i dispositivi, quindi etichettare e registrare tutti i dispositivi insieme a controlli dell'inventario ben definiti. Inoltre, un'etichettatura logica si può utilizzare con informazioni come codici che collegano il dispositivo al suo proprietario, informazioni di contatto e scopo.</p>
<p><b>12.3.4</b> Etichettatura dei dispositivi con indicazione di proprietario, informazioni di contatto e scopo</p>	
<p><b>12.3.5</b> Usi accettabili della tecnologia</p>	<p>Definendo l'uso aziendale accettabile e la posizione di dispositivi e tecnologie approvati dall'azienda, la società è in grado di gestire e controllare al meglio le lacune nella configurazione e nei controlli operativi, per garantire che non venga aperta una "back door" tramite la quale un utente non autorizzato può accedere ai sistemi critici e ai dati dei titolari di carte.</p>
<p><b>12.3.6</b> Posizioni di rete accettabili per le tecnologie</p>	
<p><b>12.3.7</b> Elenco di prodotti approvati dalla società</p>	
<p><b>12.3.8</b> Disconnessione automatica delle sessioni per tecnologie di accesso remoto dopo un periodo di tempo specifico di inattività</p>	<p>Nelle tecnologie di accesso remoto vengono spesso inserite "back door" per le risorse critiche e i dati dei titolari di carte. Scollegando le tecnologie di accesso remoto quando non sono in uso (per esempio quelle utilizzate per supportare i sistemi dal fornitore del POS, da altri rivenditori o da partner aziendali), l'accesso e i rischi per la rete vengono ridotti al minimo. Prendere in considerazione l'uso di controlli per scollegare i dispositivi dopo 15 minuti di inattività. Vedere anche il Requisito 8.5.6 per ulteriori informazioni su questo argomento.</p>
<p><b>12.3.9</b> Attivazione di tecnologie di accesso remoto per fornitori e partner aziendali solo quando necessario, con disattivazione immediata dopo l'uso</p>	

Requisito	Istruzioni
<p><b>12.3.10</b> Per il personale che accede ai dati dei titolari di carta utilizzando tecnologie di accesso remoto, proibire la copia, lo spostamento o la memorizzazione dei dati dei titolari di carta su dischi rigidi locali e supporti elettronici rimovibili, a meno che ciò non sia stato espressamente autorizzato per un'esigenza aziendale specifica.</p>	<p>Verificare che tutto il personale sia consapevole delle proprie responsabilità di non memorizzare o copiare i dati dei titolari di carta sul proprio personal computer locale o su altri supporti, l'azienda dovrebbe disporre di una politica che vieta chiaramente tali attività ad eccezione del personale che sia stato espressamente autorizzato ad agire in tal senso. Tale eventuale personale autorizzato ha la responsabilità di garantire che i dati dei titolari di carta in suo possesso siano gestiti in conformità ai requisiti PCI DSS, poiché tale ambiente remoto del personale viene ora considerato parte dell'ambiente dei dati dei titolari di carte dell'organizzazione.</p>
<p><b>12.4</b> Assicurare che nelle procedure e nella politica per la sicurezza siano definite in modo chiaro le responsabilità in termini di protezione delle informazioni per tutto il personale.</p>	<p>Senza l'assegnazione di ruoli e responsabilità di protezione chiaramente definiti, potrebbero verificarsi interazioni incoerenti con il gruppo di protezione, che portano a un'implementazione non sicura delle tecnologie o l'uso di tecnologie non aggiornate e poco sicure.</p>
<p><b>12.5</b> Assegnare a un utente singolo o a un team le seguenti responsabilità di gestione della sicurezza delle informazioni:</p> <p><b>12.5.1</b> Stabilire, documentare e distribuire le politiche e le procedure di sicurezza.</p> <p><b>12.5.2</b> Monitorare ed esaminare avvisi e informazioni sulla sicurezza e distribuirli al personale appropriato.</p> <p><b>12.5.3</b> Stabilire, documentare e distribuire le procedure di risposta ed escalation in caso di problemi di sicurezza per garantire una gestione tempestiva ed efficiente di tutte le situazioni.</p> <p><b>12.5.4</b> Amministrare gli account utente, incluse aggiunte, eliminazioni e modifiche</p> <p><b>12.5.5</b> Monitorare e controllare tutti gli accessi ai dati.</p>	<p>Ogni persona o team con responsabilità di gestione della sicurezza delle informazioni deve essere chiaramente consapevole delle sue responsabilità e delle attività correlate tramite criteri specifici. Senza questa responsabilità, le lacune nei processi possono aprire l'accesso a risorse critiche o dati dei titolari di carte.</p>
<p><b>12.6</b> Implementare un programma formale di consapevolezza della sicurezza per rendere tutto il personale consapevole dell'importanza della sicurezza dei dati di titolari di carta.</p>	<p>Se il personale non viene istruito sulle proprie responsabilità di sicurezza, le misure di protezione e i processi implementati potrebbero divenire inefficaci a causa di errori o azioni intenzionali.</p>

Requisito	Istruzioni
<p><b>12.6.1</b> Formare il personale al momento dell'assunzione e almeno una volta all'anno.</p> <p><i>Nota: i metodi possono essere diversi in funzione del ruolo svolto dal personale e del loro livello di accesso ai dati dei titolari di carta.</i></p>	<p>Se il programma di conoscenza della sicurezza non prevede sessioni di aggiornamento periodiche, i processi e le procedure di sicurezza potrebbero essere dimenticati o ignorati, provocando l'esposizione delle risorse critiche e dei dati dei titolari di carte. I temi principali e di approfondimento della formazione iniziale e periodica possono differire in funzione delle mansioni del personale e dovrebbero essere personalizzati in base al tipo di destinatari a cui si rivolgono. Ad esempio, le sessioni per gli amministratori del database possono concentrarsi su specifici processi e controlli tecnici, mentre la formazione per i cassieri dei negozi di vendita al dettaglio può concentrarsi sulle procedure per transazioni sicure.</p> <p>Prendere in considerazione la possibilità di inserire degli aggiornamenti di consapevolezza continui per mantenere i dipendenti al corrente delle politiche e delle procedure in vigore. Anche il metodo di somministrazione può variare in funzione del tipo di destinatari o di formazione. Ad esempio, la formazione iniziale ed annuale può essere effettuata mediante una sessione di formazione formale diretta o basata su computer, mentre gli aggiornamenti periodici continui possono avvenire mediante e-mail, poster, newsletter, ecc.</p>
<p><b>12.6.2</b> Richiedere al personale di certificare almeno una volta all'anno di aver letto e compreso la politica e le procedure di sicurezza.</p>	<p>La richiesta di un'attestazione da parte del personale in forma scritta o elettronica aiuta a garantire che abbiano letto e compreso i criteri e le procedure di protezione e che si siano impegnati e continuano ad impegnarsi a rispettarli.</p>
<p><b>12.7</b> Sottoporre il personale potenziale a screening prima dell'assunzione per ridurre al minimo il rischio di attacchi da fonti interne. Esempi di indagini sulla storia personale sono informazioni su impieghi precedenti, precedenti penali, storico del credito e controlli delle referenze.</p> <p><i>Nota: Per quel personale potenziale da assumere per determinate posizioni come cassieri di negozi, che hanno accesso a un solo numero di carta alla volta durante una transazione, questo requisito è solo consigliato.</i></p>	<p>L'esecuzione di approfondite indagini di base prima dell'assunzione del personale che dovrà accedere ai dati dei titolari di carte riduce il rischio di uso non autorizzato dei PAN e di altri dati dei titolari di carte da parte di individui con precedenti penali o discutibili. Si prevede che un'azienda disponga di una politica e di un processo per il controllo dei precedenti, che include il processo decisionale che valuta se i risultati del controllo avranno un impatto sulla decisione di assunzione (e quale sarà tale impatto).</p> <p>Per essere efficace, il livello di indagini sulla storia personale dovrebbe essere adeguato alla posizione in questione. Ad esempio, per le posizioni che richiedono responsabilità maggiori o che consentono l'accesso amministrativo a sistemi o dati critici possono richiedere delle indagini sulla storia personale più approfondite rispetto a posizioni che prevedono livelli inferiori di responsabilità e di accesso. Potrebbe rivelarsi opportuno anche per il processo di copertura di trasferimenti interni, in cui personale con posizioni con un livello di rischio inferiore e che per il quale non sia stata eseguita un'indagine approfondita sulla storia personale, viene promosso o trasferito a posizioni con maggiori responsabilità e livello di accesso più elevato.</p>

Requisito	Istruzioni
<p><b>12.8</b> Se i dati di titolari di carta sono condivisi con provider di servizi, gestire e implementare politiche e procedure per i provider di servizi per includere quanto segue:</p>	<p>Se un esercente o un provider di servizi condivide i dati dei titolari di carte con un provider di servizi, tali provider dovranno applicare requisiti specifici per garantire la protezione continua di questi dati.</p>
<p><b>12.8.1</b> Conservare un elenco dei provider di servizi.</p>	<p>Tenere traccia di tutti i provider di servizi permette di identificare dove si estendono i rischi potenziali all'esterno dell'organizzazione.</p>
<p><b>12.8.2</b> Conservare un accordo scritto in base al quale il provider di servizi si assume la responsabilità della protezione dei dati di titolari di carta di cui entra in possesso.</p>	<p>La conferma dei provider di servizi ne evidenzia l'impegno a mantenere la sicurezza dei dati dei titolari di carte che ottengono dai clienti, rendendoli pertanto responsabili.</p>
<p><b>12.8.3</b> Accertarsi che esista un processo definito per incaricare i provider di servizi, che includa tutte le attività di dovuta diligenza appropriate prima dell'incarico.</p>	<p>Il processo garantisce che qualsiasi coinvolgimento di un provider di servizi sia attentamente esaminato da un'organizzazione a livello interno, comprendendo un'analisi dei rischi prima di stabilire una relazione formale con il provider.</p>
<p><b>12.8.4</b> Conservare un programma per monitorare lo stato di conformità agli standard PCI DSS dei provider di servizi con cadenza almeno annuale.</p>	<p>La conoscenza dello stato di conformità PCI DSS di un provider di servizi garantisce il loro rispetto degli stessi requisiti a cui è soggetta l'organizzazione.</p> <p>Se il provider di servizi offre vari servizi, questo requisito è valido solo per quei servizi effettivamente erogati al cliente, e solo per quei servizi che rientrano nell'ambito per la valutazione PCI DSS per il cliente. Ad esempio, se un provider offre servizi firewall/IDS e ISP, un cliente che utilizza solo il servizio firewall/IDS inserirebbe solo tale servizio nell'ambito della propria valutazione PCI DSS.</p>
<p><b>12.9</b> Implementare un piano di risposta agli incidenti. Prepararsi a rispondere immediatamente a una violazione del sistema.</p>	<p>Senza un piano di risposta agli incidenti di protezione correttamente divulgato, letto e compreso dalle parti responsabili, la confusione o la mancanza di una risposta unificata potrebbero causare ulteriori tempi di inattività del business, un'inutile esposizione ai mezzi di informazione e responsabilità legali.</p>
<p><b>12.9.1</b> Creare il piano di risposta agli incidenti da attuare in caso di violazione del sistema. Accertarsi che il piano includa almeno i seguenti elementi:</p> <ul style="list-style-type: none"> <li>▪ Ruoli, responsabilità e strategie di comunicazione e contatto in caso di violazione, nonché notifiche ai marchi di pagamento</li> <li>▪ Procedure specifiche di risposta agli incidenti</li> <li>▪ Procedure di ripristino e continuità delle attività aziendali</li> <li>▪ Processi di backup dei dati</li> <li>▪ Analisi dei requisiti legali per la segnalazione delle violazioni</li> <li>▪ Copertura e risposte per tutti i componenti di sistema critici</li> <li>▪ Riferimenti e descrizioni delle procedure di risposta agli incidenti adottate dai marchi di pagamento</li> </ul>	<p>Il piano di risposta agli incidenti dovrebbe essere completo e contenere tutti gli elementi importanti che consentono all'azienda di rispondere in modo efficace nel caso di una violazione che influisca sui dati dei titolari di carte.</p>

Requisito	Istruzioni
<p><b>12.9.2</b> Eseguire un test del piano almeno una volta all'anno.</p>	<p>Senza il test, è possibile che vengano trascurati passaggi chiave che potrebbero determinare una maggiore esposizione durante un incidente.</p> <p>Se nel corso dell'ultimo anno il piano di risposta agli incidenti è stato attivato nella sua interezza, coprendo tutti i componenti dello stesso, una revisione dettagliata dell'incidente in questione e la sua risposta possono essere sufficienti a fornire un test adatto. Se invece solo alcuni dei componenti del piano sono stati attivati di recente, i restanti componenti dovranno essere sottoposti a test. Nel caso in cui nessun componente del piano sia stato attivato nel corso degli ultimi 12 mesi, il test annuale dovrà riguardare tutti i componenti del piano.</p>
<p><b>12.9.3</b> Nominare personale specifico disponibile 24 ore al giorno, 7 giorni su 7 in caso di emergenza.</p>	<p>Senza un team di risposta agli incidenti formato e prontamente disponibile, possono verificarsi danni estesi alla rete, e i dati e i sistemi critici potrebbero essere "inquinati" da una gestione inappropriata dei sistemi bersagliati. Questo può minare la riuscita di un'indagine successiva all'incidente. Se non sono disponibili risorse interne, valutare l'appalto a un fornitore che mette a disposizione tali servizi.</p>
<p><b>12.9.4</b> Formare in modo appropriato il personale addetto al controllo delle violazioni della sicurezza.</p>	
<p><b>12.9.5</b> Includere allarmi dai sistemi di rilevamento e prevenzione delle intrusioni e dai sistemi di monitoraggio dell'integrità dei file.</p>	<p>Questi sistemi di monitoraggio sono pensati per porre l'attenzione sui potenziali rischi per i dati, sono fondamentali per intraprendere azioni rapide per impedire una violazione e devono essere inclusi nei processi di risposta agli incidenti.</p>
<p><b>12.9.6</b> Sviluppare un processo che consenta di correggere e migliorare il piano di risposta agli incidenti tenendo conto delle lezioni apprese e degli ultimi sviluppi nel settore.</p>	<p>L'integrazione delle "lezioni apprese" nel piano di risposta agli incidenti dopo un incidente aiuta a mantenere aggiornato il piano e a reagire correttamente alle minacce emergenti e ai trend della sicurezza.</p>

## Istruzioni per il requisito A.1: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso

### **Requisito A.1: I provider di hosting condiviso proteggono 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.

Requisito	Istruzioni
<p><b>A.1</b> 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:</p> <p>Il provider di hosting è tenuto a soddisfare questi requisiti, oltre a tutte le altre sezioni rilevanti degli standard PCI DSS.</p> <p><b>Nota:</b> anche se un provider di hosting soddisfa tutti questi requisiti, la conformità dell'entità che utilizza tale provider di hosting non è automaticamente garantita. Ogni entità deve soddisfare i requisiti e ottenere la convalida della conformità agli standard PCI DSS, come applicabile.</p>	<p>L'Appendice A di PCI DSS è destinata ai provider di hosting condiviso che desiderano fornire ai clienti di esercenti e/o provider di servizi un ambiente di hosting compatibile con PCI DSS. Questi passaggi devono essere rispettati in aggiunta a tutti gli altri requisiti PCI DSS pertinenti.</p>
<p><b>A.1.1</b> Garantire che ogni entità esegua processi con accesso esclusivo al proprio ambiente dei dati di titolari di carta.</p>	<p>Se un esercente o un provider di servizi può eseguire le sue applicazioni sul server condiviso, tali applicazioni devono essere eseguite con l'ID utente dell'esercente o del provider, anziché come utente privilegiato. Un utente privilegiato avrà accesso agli altri ambienti dei dati dei titolari di carte di tutti gli altri esercenti e provider di servizi, oltre che al proprio.</p>
<p><b>A.1.2</b> Limitare l'accesso e i privilegi di ciascuna entità esclusivamente al relativo ambiente di dati di titolari di carta.</p>	<p>Per garantire che l'accesso e i privilegi siano limitati, in modo tale che ogni esercente o provider di servizi abbia accesso solamente al suo ambiente dei dati dei titolari di carte, prendere in considerazione quanto segue: (1) privilegi dell'ID utente sul server Web dell'esercente o del provider di servizi; (2) autorizzazioni di lettura, scrittura ed esecuzione file concesse; (3) autorizzazioni di scrittura nei file binari del sistema concesse; (4) autorizzazioni concesse per i file di registro dell'esercente o del provider di servizi; (5) controlli per garantire che un esercente o provider di servizi non possa monopolizzare le risorse di sistema.</p>
<p><b>A.1.3</b> 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.</p>	<p>I registri dovrebbero essere disponibili in un ambiente di hosting condiviso, in modo che gli esercenti e i provider di servizi possano accedere e rivedere i registri specifici per il loro ambiente dei dati dei titolari di carte.</p>
<p><b>A.1.4</b> 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</p>	<p>I provider di hosting condiviso devono disporre di processi per garantire una risposta rapida nel caso sia necessaria un'indagine forense su una compromissione, fino al livello di dettagli appropriato, in modo che siano disponibili</p>

Requisito	Istruzioni
servizi ospitato.	i dettagli del singolo esercente o provider di servizi.

## Appendice A: PCI DSS: Documenti correlati

I seguenti documenti sono stati creati per una migliore comprensione degli standard PCI DSS, dei requisiti e della responsabilità per la conformità.

Documento	Destinatari
<i>Requisiti PCI DSS e procedure di valutazione della sicurezza</i>	Tutti gli esercenti e i provider di servizi
<i>Navigazione in PCI DSS: Comprensione dello scopo dei requisiti</i>	Tutti gli esercenti e i provider di servizi
<i>PCI DSS: Questionario, istruzioni e linee guida per l'autovalutazione</i>	Tutti gli esercenti e i provider di servizi
<i>PCI DSS: Questionario di autovalutazione A e Attestato</i>	Esercenti idonei <sup>9</sup>
<i>PCI DSS: Questionario di autovalutazione B e Attestato</i>	Esercenti idonei <sup>9</sup>
<i>PCI DSS: Questionario di autovalutazione C-VT e Attestato</i>	Esercenti idonei <sup>9</sup>
<i>PCI DSS: Questionario di autovalutazione C e Attestato</i>	Esercenti idonei <sup>9</sup>
<i>PCI DSS: Questionario di autovalutazione D e Attestato</i>	Esercenti e provider di servizi idonei <sup>9</sup>
<i>PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi</i>	Tutti gli esercenti e i provider di servizi

<sup>9</sup> Per determinare il questionario di autovalutazione appropriato, fare riferimento al documento PCI DSS: Questionario, istruzioni e linee guida per l'autovalutazione, "Scelta del questionario SAQ e dell'attestato più appropriati per la propria azienda".