



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

Comprensione dello scopo dei requisiti

Versione 1.2

Ottobre 2008

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 ai nuovi standard PCI DSS v1.2 e implementare modifiche minori apportate dopo la versione originale v1.1.</i>

Sommario

Modifiche del documento	i
Prefazione	iii
Dati dei titolari di carta e dati sensibili di autenticazione	1
<i>Posizione dei dati dei titolari di carta e dei dati sensibili di autenticazione</i>	<i>2</i>
<i>Dati della traccia 1 e dati della traccia 2</i>	<i>3</i>
Istruzioni correlate per lo standard di sicurezza dei dati PCI.....	4
Istruzioni per i requisiti 1 e 2: Sviluppo e gestione di una rete sicura	5
<i>Requisito 1: Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta</i>	<i>5</i>
<i>Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di sicurezza</i>	<i>10</i>
Istruzioni per i requisiti 3 e 4: Protezione dei dati di titolari di carta	13
<i>Requisito 3: Proteggere i dati di titolari di carta memorizzati</i>	<i>13</i>
<i>Requisito 4: Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche.....</i>	<i>19</i>
Istruzioni per i requisiti 5 e 6: Utilizzare un programma per la gestione delle vulnerabilità	21
<i>Requisito 5: Utilizzare e aggiornare regolarmente il software antivirus</i>	<i>21</i>
<i>Requisito 6: Sviluppare e gestire sistemi e applicazioni protette</i>	<i>23</i>
Istruzioni per i requisiti 7, 8 e 9: Implementazione di rigide misure di controllo dell'accesso	29
<i>Requisito 7: Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario</i>	<i>29</i>
<i>Requisito 8: Assegnare un ID univoco a chiunque abbia accesso a un computer</i>	<i>30</i>
<i>Requisito 9: Limitare l'accesso fisico ai dati di titolari di carta</i>	<i>34</i>
Istruzioni per i requisiti 10 e 11: Monitoraggio e test delle reti regolari	38
<i>Requisito 10: Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta</i>	<i>38</i>
<i>Requisito 11: Eseguire regolarmente test dei sistemi e processi di protezione.....</i>	<i>41</i>
Istruzioni per il requisito 12: Gestire una politica di sicurezza delle informazioni	43
<i>Requisito 12: Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori</i>	<i>43</i>
Istruzioni per il requisito A.1: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso	49
Appendice A: PCI DSS: Documenti correlati	51

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 v1.2*.

I requisiti di PCI DSS sono applicabili a tutti i componenti di sistema inclusi nell'ambiente dei dati di titolari di carta o collegati ad esso. L'ambiente dei dati dei titolari di carta è la parte di rete che contiene dati dei titolari di carta o dati sensibili di autenticazione, tra cui componenti di rete, server e applicazioni.

- 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, database, autenticazione, e-mail, proxy, NTP (Network Time Protocol) e DNS (Domain Name Server).
- Le applicazioni includono, senza limitazioni, tutte le applicazioni acquistate e personalizzate, comprese applicazioni interne ed esterne (Internet).

Una segmentazione di rete adeguata, che isola i sistemi che memorizzano, elaborano o trasmettono i dati dei titolari di carta da quelli che non eseguono tali operazioni, 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 pertinenti alla 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 PCI SSC di società Qualified Security Assessors è disponibile all'indirizzo: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf.

Dati dei titolari di carta e dati sensibili di autenticazione

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 esauriente; il solo scopo è quello di illustrare i diversi tipi di requisiti applicabili a ciascun elemento di dati.

I dati dei titolari di carta sono definiti dal numero PAN (o numero di carta di credito) e dagli altri dati ottenuti durante una transazione di pagamento, compresi i seguenti elementi dei dati (ulteriori dettagli sono disponibili più avanti nella tabella):

- PAN
- Nome titolare di carta
- Data di scadenza
- Codice di servizio
- Dati sensibili di autenticazione: (1) dati della striscia magnetica, (2) CAV2, CID, CVC2, CVV2, (3) PIN e dati di blocco PIN

Il PAN (Primary Account Number) è il fattore determinante nell'applicabilità dei requisiti PCI DSS e degli standard PA-DSS. Se il PAN non viene memorizzato, elaborato o trasmesso, gli standard PCI DSS e PA-DSS non sono applicabili.

	Elemento di dati	Memorizzazione consentita	Protezione richiesta	Req. PCI DSS 3, 4
Dati di titolari di carta	PAN	Sì	Sì	Sì
	Nome titolare di carta ¹	Sì	Sì ¹	No
	Codice di servizio ¹	Sì	Sì ¹	No
	Data di scadenza ¹	Sì	Sì ¹	No
Dati sensibili di autenticazione²	Dati completi della striscia magnetica ³	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/Blocco PIN	No	N/A	N/A

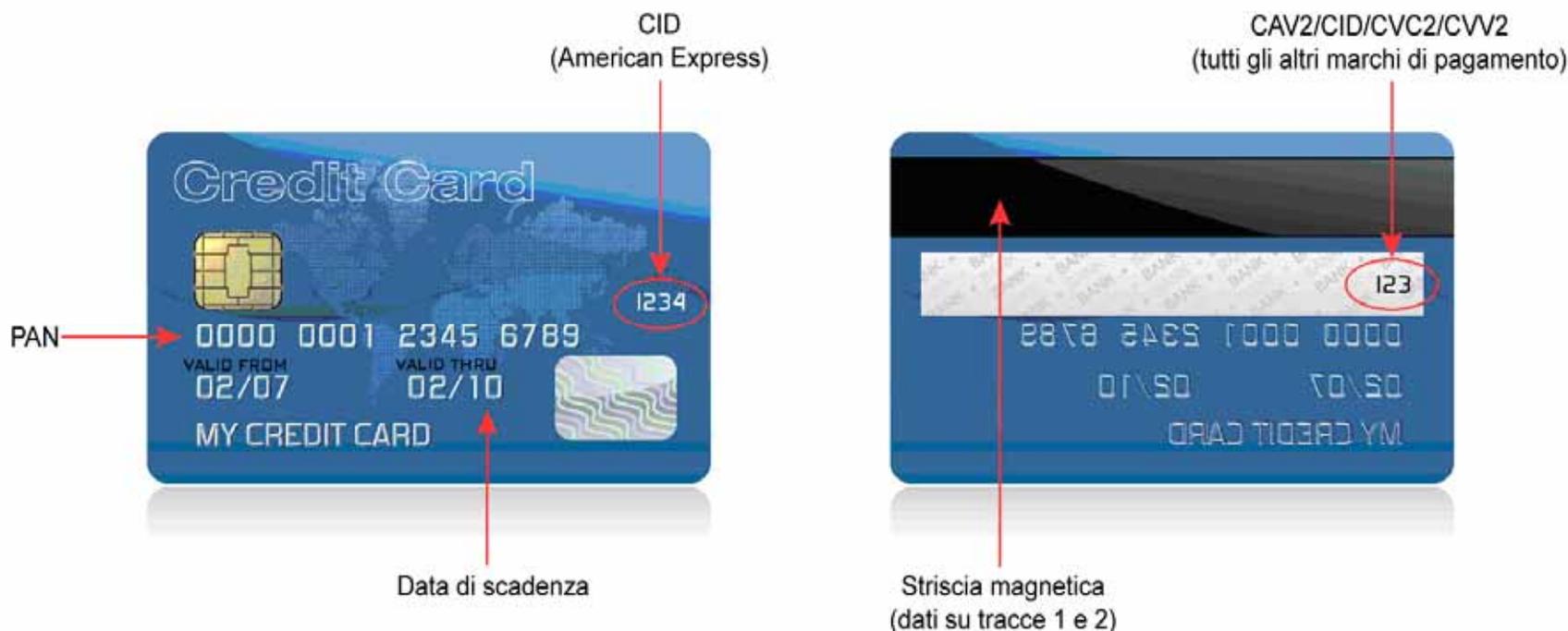
¹ Questi elementi di dati devono essere protetti se memorizzati insieme al PAN. Tale protezione rientra in base ai requisiti PCI DSS nella protezione generale dell'ambiente dei titolari di carta. Inoltre, altre leggi (ad esempio, correlate alla protezione dei dati personali, alla privacy, al furto di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

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

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

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

I dati di autenticazione sensibili sono costituiti da dati della striscia magnetica (su traccia)⁴, valore o codice di validazione della carta⁵ e dati PIN⁶. **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. Vedere il documento *PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi* per la definizione completa di "dati di autenticazione sensibili". 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.



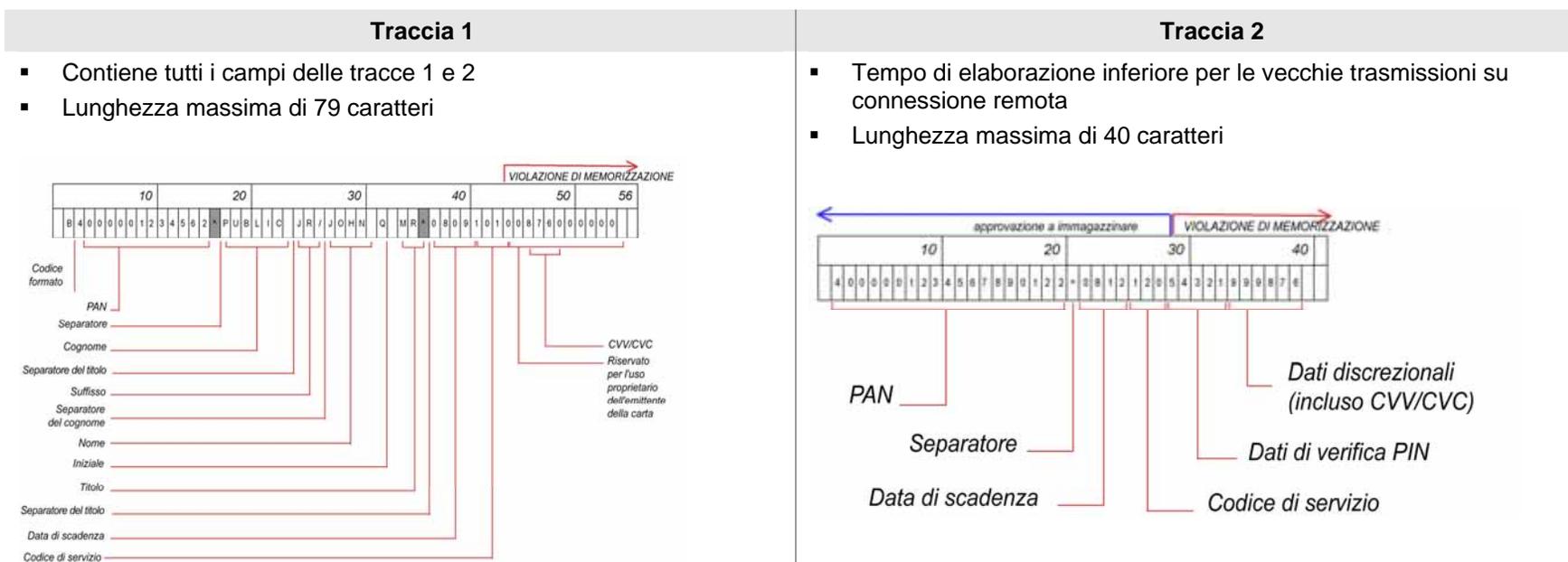
⁴ Dati codificati nella striscia magnetica utilizzati per l'autorizzazione durante una transazione con carta presente. Questi dati sono presenti anche nell'immagine della striscia magnetica sul chip o in un'altra posizione sulla carta. Le entità non possono conservare tutti i dati completi della striscia magnetica dopo l'autorizzazione della transazione. I soli elementi dei dati di traccia che possono essere conservati sono il numero PAN, il nome del titolare della carta, la data di scadenza e il codice di servizio.

⁵ 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.

⁶ 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.



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 sicurezza

Protezione dei dati di titolari di carta

- Requisito 3: Proteggere i dati di titolari di carta memorizzati
Requisito 4: Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche

Utilizzare un programma per la gestione delle vulnerabilità

- Requisito 5: Utilizzare e aggiornare regolarmente il software antivirus
Requisito 6: Sviluppare e gestire sistemi e applicazioni protette

Implementazione di rigide misure di controllo dell'accesso

- Requisito 7: Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario
Requisito 8: Assegnare un ID univoco a chiunque abbia accesso a un computer
Requisito 9: Limitare l'accesso fisico ai dati di titolari di carta

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

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

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

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

Requisito	Istruzioni
1.1 Stabilire standard di configurazione del firewall e del router che includano:	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.
1.1.1 Un processo formale per l'approvazione e il test di tutte le connessioni esterne alla rete e le modifiche apportate alla configurazione di firewall e router	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.
1.1.2 Un diagramma aggiornato della rete con tutte le connessioni ai dati dei titolari di carta, comprese eventuali reti wireless	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.

Requisito	Istruzioni
<p>1.1.3 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>1.1.4 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>1.1.5 La documentazione e la giustificazione aziendale per l'uso di tutti i servizi, i protocolli e le porte consentite, inclusa la documentazione delle funzioni di sicurezza implementate per i protocolli considerati non sicuri</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>
<p>1.1.6 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>

Requisito	Istruzioni
<p>1.2 Creare una configurazione del firewall che limiti le connessioni tra le reti non attendibili e qualsiasi componente di sistema nell'ambiente dei dati di titolari di carta.</p> <p><i>Nota: una "rete non attendibile" è una qualsiasi rete esterna alle reti che appartengono all'entità sottoposta a revisione e/o che l'entità non è in grado di controllare o gestire.</i></p>	<p>È fondamentale installare una protezione di rete, nello specifico un firewall, tra la rete attendibile interna e qualsiasi altra rete non attendibile esterna e/o che l'entità non è in grado di controllare o gestire. La mancata implementazione di questa misura comporta la vulnerabilità dell'entità all'accesso non autorizzato da parte di utenti o software dannosi.</p> <p>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>1.2.1 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>1.2.2 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>
<p>1.2.3 Installazione di firewall perimetrali tra le reti wireless e l'ambiente dati dei titolari di carta e configurazione di questi firewall affinché impediscano tutto il traffico dall'ambiente wireless o controllino il traffico qualora sia necessario per lo svolgimento dell'attività</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>

Requisito	Istruzioni
<p>1.3 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 i dati dei titolari di carte). Se è consentito l'accesso diretto tra sistemi pubblici e sistemi che memorizzano i dati dei titolari di carte, la protezione offerta dal firewall viene superata e i componenti di sistema che memorizzano i dati dei titolari di carte sono esposti alla compromissione.</p>
<p>1.3.1 Implementare una zona DMZ per limitare il traffico in entrata e in uscita ai soli protocolli necessari per l'ambiente dei dati di titolari di carta.</p>	<p>Questi requisiti intendono 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 esterno non attendibile in una rete non attendibile).</p>
<p>1.3.2 Limitare il traffico Internet in entrata agli indirizzi IP all'interno della zona DMZ.</p>	
<p>1.3.3 Non consentire nessun percorso diretto per il traffico in entrata o in uscita tra Internet e l'ambiente dei dati di titolari di carta.</p>	<p>La zona demilitarizzata (DMZ) è la parte del firewall rivolta verso la rete Internet pubblica e gestisce le connessioni tra Internet 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>1.3.4 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 corollaria chiamata "uso di filtri in uscita".</p>
<p>1.3.5 Limitare il traffico in uscita dall'ambiente dei dati di titolari di carta a Internet in modo che il traffico in uscita possa accedere solo agli indirizzi IP all'interno della zona DMZ.</p>	<p>La zona DMZ deve inoltre valutare tutto il traffico in uscita dalla rete per garantire che segua regole prestabilite. Affinché la zona DMZ svolga correttamente questa funzione, le connessioni dalla rete a qualsiasi indirizzo esterno alla rete non devono essere consentite se prima non ne è stata valutata la legittimità da parte della zona DMZ.</p>

Requisito	Istruzioni
<p>1.3.6 Implementare un controllo efficiente, anche noto come "dynamic packet filtering" (ossia che consente solo alle connessioni già "stabilite" di accedere alla rete).</p>	<p>Un firewall che esegue l'ispezione dei pacchetti "stateful" mantiene lo stato di ogni connessione al firewall. Grazie alla conservazione dello stato, il firewall 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>1.3.7 Posizionamento del database in una zona di rete interna, separata dalla zona DMZ</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>1.3.8 Implementare un IP-masquerading per evitare che gli indirizzi interni vengano tradotti e resi noti su Internet, tramite lo spazio indirizzi RFC 1918. Utilizzare tecnologie NAT (Network Address Translation), ad esempio PAT (Port Address Translation).</p>	<p>IP-masquerading, 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>1.4 Installare firewall personali (software) su tutti i computer portatili e i computer di proprietà dei dipendenti con connettività diretta a Internet (ad esempio, laptop utilizzati dai dipendenti), che vengono utilizzati per accedere alla rete aziendale.</p>	<p>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>

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

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

Requisito	Istruzioni
<p>2.1 Modificare sempre le impostazioni predefinite del fornitore prima di installare un sistema su una rete, ad esempio, password, stringhe di comunità SNMP (Simple Network Management Protocol) ed eliminazione di account non necessari.</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 compromettere i sistemi. Queste impostazioni sono note nelle comunità degli hacker e aumentano la vulnerabilità agli attacchi del sistema.</p>
<p>2.1.1 Per gli ambienti wireless connessi all'ambiente dei dati di titolari di carta o che trasmettono tali dati, modificare le impostazioni predefinite del fornitore wireless, incluse, senza limitazione, chiavi di cifratura wireless predefinite, password e stringhe di comunità SNMP. Accertarsi che le impostazioni di sicurezza dei dispositivi wireless consentano l'uso della tecnologia di cifratura avanzata per l'autenticazione e la trasmissione.</p>	<p>Molti utenti installano questi dispositivi senza l'approvazione della direzione 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, quali WPA/WPA2.</p>
<p>2.2 Sviluppare standard di configurazione per tutti i componenti di sistema. Accertarsi che questi standard risolvano tutte le vulnerabilità della sicurezza note e siano coerenti con gli standard di hardening accettati dal settore.</p>	<p>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. Visitare questi tre siti Web di esempio dove è possibile ottenere ulteriori informazioni sulle migliori pratiche industriali che possono aiutare nell'implementazione degli standard di configurazione: www.nist.gov, www.sans.org, www.cisecurity.org.</p>

Requisito	Istruzioni
<p>2.2.1 Implementare una sola funzione principale per server.</p>	<p>Questo requisiti 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"> 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. 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. <p>Questo requisito è pensato per i server (in genere basati su Unix, Linux o Windows), ma non per i sistemi mainframe.</p>
<p>2.2.2 Disattivare tutti i servizi e i protocolli non necessari e non protetti (che non sono strettamente necessari per eseguire la funzione specifica del dispositivo).</p>	<p>Come affermato nel punto 1.1.7, 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 questi servizi e protocolli siano sempre disabilitati all'implementazione di nuovi server, questo requisito deve essere parte degli standard di configurazione dell'organizzazione e dei processi correlati.</p>
<p>2.2.3 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>2.2.4 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>
<p>2.3 Cifratura di tutto l'accesso amministrativo non da console. Utilizzare tecnologie quali SSH, VPN o SSL/TLS per la gestione basata su Web e altre attività amministrative non da console.</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>

Requisito	Istruzioni
<p>2.4 I provider di hosting condiviso devono proteggere l'ambiente ospitato e i dati 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'Appendice A.</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

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

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

Requisito	Istruzioni
3.1 Limitare il più possibile la memorizzazione dei dati di titolari di carta. Sviluppare una politica per la conservazione e l'eliminazione dei dati. Limitare la quantità di dati memorizzati e il tempo di conservazione in base alle esigenze aziendali, legali e/o legislative, come documentato nella politica per la conservazione dei dati.	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 sono il numero PAN (reso illeggibile), la data di scadenza, il nome e il codice di servizio. Se non sono necessari, non conservarli!
3.2 Non memorizzare dati sensibili di autenticazione dopo l'autorizzazione (anche se crittografati). I dati sensibili di autenticazione includono i dati citati nei seguenti Requisiti, da 3.2.1 a 3.2.3:	I dati di autenticazione sensibili sono costituiti da dati della striscia magnetica (su traccia) ⁷ , valore o codice di validazione della carta ⁸ e dati PIN ⁹ . La memorizzazione dei dati sensibili di autenticazione dopo l'autorizzazione è vietata. Questi dati sono particolarmente preziosi per gli utenti non autorizzati, in quanto consentono loro di generare carte di pagamento contraffatte e conseguenti transazioni fraudolente. Vedere il documento <i>PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi</i> per la definizione completa di "dati di autenticazione sensibili".

⁷ Dati codificati nella striscia magnetica utilizzati per l'autorizzazione durante una transazione con carta presente. Questi dati sono presenti anche nell'immagine della striscia magnetica sul chip o in un'altra posizione sulla 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 numero PAN, il nome del titolare della carta, la data di scadenza e il codice di servizio.

⁸ 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.

⁹ 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>3.2.1 Non memorizzare l'intero contenuto delle tracce della striscia magnetica (presente sul retro della carta, 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><i>Nota: nel normale svolgimento delle attività, è possibile che sia necessario conservare i seguenti elementi di dati della striscia magnetica:</i></p> <ul style="list-style-type: none"> ▪ Nome del titolare della carta ▪ PAN (Primary Account Number) ▪ Data di scadenza ▪ Codice di servizio <p><i>Per ridurre al minimo il rischio, memorizzare solo gli elementi di dati necessari.</i></p> <p><i>Nota: vedere il documento PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi per ulteriori informazioni.</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 nel mondo.</p>
<p>3.2.2 Non memorizzare il codice o il valore di validazione della carta (numero di tre o quattro cifre stampato sulla parte anteriore o posteriore della carta di pagamento) utilizzato per verificare le transazioni con carta non presente.</p> <p><i>Nota: vedere il documento PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi per ulteriori informazioni.</i></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>3.2.3 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 di addebito basate su PIN fraudolente (ad esempio prelievi Bancomat).</p>

Requisito	Istruzioni
<p>3.3 Mascherare il PAN quando visualizzato (non devono essere visibili più di sei cifre all'inizio e quattro cifre alla fine)</p> <p><i>Note:</i></p> <ul style="list-style-type: none"> ▪ <i>Questo requisito non si applica ai dipendenti e ad altre parti che hanno l'esigenza specifica di visualizzare il numero PAN intero.</i> ▪ <i>Questo requisito non sostituisce i requisiti più rigorosi per la visualizzazione dei dati di titolari di carta, ad esempio per ricevute di punti di vendita (POS).</i> 	<p>La visualizzazione dell'intero numero 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 numero 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 numero PAN intero può essere inoltre visualizzato da chi ha un'esigenza aziendale legittima di vedere l'intero numero PAN.</p>
<p>3.4 Rendere illeggibile almeno il numero PAN ovunque sia memorizzato (inclusi i dati su supporti digitali portatili, supporti di backup, registri) utilizzando uno dei seguenti approcci:</p> <ul style="list-style-type: none"> ▪ Hash one-way basati su crittografia avanzata ▪ Troncatura ▪ Token e pad indicizzati (i pad devono essere custoditi in un luogo sicuro) 	<p>La mancanza di protezione dei numeri PAN può consentire agli utenti non autorizzati di visualizzare o scaricare questi dati. I numeri 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 numeri 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 numeri PAN (oppure rimuovendoli o mascherandoli) nei log. Fare riferimento al documento <i>PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi</i> per la definizione di "crittografia avanzata".</p> <p>Le funzioni di hash one-way (ad esempio SHA-1) basate sulla cifratura avanzata possono essere utilizzate per rendere illeggibili i dati dei titolari di carte. Le funzioni di hash sono adatte all'uso quando non è necessario recuperare il numero originale (l'hash one-way è irreversibile).</p> <p>L'intento 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 numero PAN, ma in cui il PAN viene mascherato in fase di visualizzazione (ad esempio su schermo, rendiconti, ricevute, ecc. viene visualizzata solo parte del numero PAN).</p> <p>Anche token e possono essere utilizzati per rendere illeggibili i dati dei titolari di carte. Un token indicizzato è un token crittografico che sostituisce il PAN in base a un dato indice per un valore imprevedibile. Un pad one-time è un sistema in cui viene 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>

Requisito	Istruzioni
<ul style="list-style-type: none"> ▪ Crittografia avanzata con relativi processi e procedure di gestione delle chiavi. <p><i>Il PAN è l'informazione MINIMA sull'account che deve essere resa illeggibile.</i></p> <p><i>Note:</i></p> <ul style="list-style-type: none"> ▪ <i>In caso di problemi nel rendere illeggibile il numero PAN, consultare l'Appendice B: Controlli compensativi.</i> ▪ <i>La "crittografia avanzata" viene definita nel documento PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi.</i> 	<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>3.4.1 Se si utilizza la cifratura del disco (anziché la cifratura del database a livello di file o colonna), l'accesso logico deve essere gestito in modo indipendente dai meccanismi di controllo dell'accesso al sistema operativo nativo (ad esempio, non utilizzando database di account 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 la conformità a questo requisito il metodo di cifratura del disco non può avere:</p> <ol style="list-style-type: none"> 1) Un'associazione diretta al sistema operativo. 2) Chiavi di decifratura associate agli account utente.
<p>3.5 Proteggere le chiavi di crittografia utilizzate per la cifratura dei dati di titolari di carta da divulgazione e uso improprio:</p>	<p>Le chiavi crittografiche devono essere protette in modo avanzato, perché chiunque le ottenga sarà in grado di decifrare i dati.</p>
<p>3.5.1 Limitare l'accesso alle chiavi di crittografia al minor numero possibile di persone necessarie.</p>	<p>Dovrebbero essere poche le persone che hanno accesso alle chiavi di crittografia, di solito coloro che hanno responsabilità di custodia delle chiavi.</p>
<p>3.5.2 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 chiavi di crittografia delle chiavi, e conservate in poche posizioni.</p>

Requisito	Istruzioni
3.6 Documentare e implementare completamente tutti i processi e le procedure di gestione delle chiavi di crittografia utilizzate per la cifratura dei dati di titolari di carta, incluso quanto segue:	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.
3.6.1 Generazione di chiavi di crittografia avanzate	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".
3.6.2 Distribuzione sicura delle chiavi di crittografia	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 in 3.5.1.
3.6.3 Memorizzazione sicura delle chiavi di crittografia	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).
3.6.4 Modifica periodica di chiavi di crittografia <ul style="list-style-type: none"> • In base a quanto richiesto e consigliato dall'applicazione associata (ad esempio, re-keying), preferibilmente in modo automatico • Almeno una volta all'anno 	Se sono specificati dal fornitore dell'applicazione di cifratura, seguire i processi o i consigli del produttore per la modifica periodica delle chiavi. La modifica annuale delle chiavi di crittografia è fondamentale per ridurre il rischio che qualcuno ottenga le chiavi e sia in grado di decifrare i dati.
3.6.5 Ritiro o sostituzione di chiavi di crittografia precedentemente o potenzialmente compromesse	Le vecchie chiavi che non sono più in uso o necessarie devono essere ritirate e distrutte per garantire che le chiavi non siano più in uso. Se è necessario conservare le vecchie chiavi (ad esempio per supportare i dati cifrati in archivio), è necessario applicare loro una protezione avanzata (vedere il punto 3.6.6). La soluzione di cifratura dovrebbe inoltre consentire e facilitare un processo di sostituzione delle chiavi che sono state compromesse (o che si sospetta lo siano state).
3.6.6 Uso della procedura "split knowledge" e definizione del controllo duale delle chiavi	La tecnica "split knowledge" il controllo duale delle chiavi sono utilizzati per eliminare la possibilità che una singola persona abbia accesso all'intera chiave. Questo controllo è generalmente applicabile ai sistemi di crittografia manuale delle chiavi, o laddove la gestione delle chiavi non è implementata dal prodotto di cifratura. Questo tipo di controllo viene generalmente implementato all'interno dei moduli di sicurezza hardware.

Requisito	Istruzioni
3.6.7 Prevenzione di tentativi di sostituzione non autorizzata delle chiavi di crittografia	La soluzione di cifratura non dovrebbe consentire o accettare la sostituzione delle chiavi provenienti da fonti non autorizzate o processi imprevisti.
3.6.8 Obbligo per i custodi delle chiavi di crittografia di firmare una dichiarazione in cui accettano e confermano di conoscere le proprie responsabilità.	Questo processo garantirà che i singoli individui si impegnino nel ruolo di custodi delle chiavi e comprendano le loro responsabilità.

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

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

Requisito	Istruzioni
<p>4.1 Utilizzare protocolli di crittografia e sicurezza avanzati, quali SSL/TLS o IPSEC, per proteggere i dati sensibili di titolari di carta durante la trasmissione su reti pubbliche e aperte.</p> <p><i>Esempi di rete pubbliche e aperte nell'ambito della valutazione PCI DSS sono:</i></p> <ul style="list-style-type: none">▪ <i>Internet</i>▪ <i>Tecnologie wireless</i>▪ <i>Comunicazioni GSM (Global System for Mobile)</i>▪ <i>GPRS (General Packet Radio Service)</i>	<p>Le informazioni sensibili devono essere cifrate durante la trasmissione su reti pubbliche, in quanto è facile e comune che un utente non autorizzato intercetti e/o dirotti i dati in transito. 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>Le versioni di SSL precedenti a v3.0 contengono vulnerabilità documentate, quali l'overflow del buffer, che un aggressore può utilizzare per ottenere il controllo del sistema interessato.</p>

Requisito	Istruzioni
<p>4.1.1 Garantire che le reti wireless che trasmettono i dati di titolari di carta o connesse all'ambiente dei dati di titolari di carta utilizzano le pratiche di settore consigliate (ad esempio, IEEE 802.11i) per implementare la cifratura avanzata per l'autenticazione e la trasmissione.</p> <ul style="list-style-type: none"> ▪ <i>Per le nuove implementazioni wireless, non è consentito implementare la tecnologia WEP dopo il 31 marzo 2009.</i> ▪ <i>Per le implementazioni wireless correnti, non è consentito utilizzare la tecnologia WEP dopo il 30 giugno 2010.</i> 	<p>Gli utenti non autorizzati utilizzano strumenti liberi e ampiamente disponibili per ascoltare le comunicazioni wireless. L'uso della cifratura appropriata può impedire l'eavesdropping e la divulgazione di informazioni sensibili sulla 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.</p> <p>La cifratura 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. WEP non utilizza la cifratura avanzata. La cifratura WEP non dovrebbe mai essere utilizzata da sola, in quanto è vulnerabile ai vettori iniziali (IV) deboli nel processo di scambio delle chiavi WEP e non dispone della rotazione delle chiavi. Un aggressore può utilizzare strumenti di cracking basati sulla forza bruta, liberamente disponibili, per superare la cifratura WEP.</p> <p>I dispositivi wireless correnti dovrebbero essere aggiornati (ad esempio Con l'upgrade del firmware del punto di accesso a WPA) per supportare la cifratura avanzata. Se i dispositivi correnti non possono essere aggiornati, è necessario acquistare nuovi apparecchi.</p> <p>Se le reti wireless utilizzano WEP, non dovrebbero avere accesso agli ambienti dei dati dei titolari di carte.</p>
<p>4.2 Non inviare mai i numeri PAN non cifrati mediante tecnologie di messaggistica degli utenti finali (ad esempio, e-mail, messaggistica istantanea, chat).</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 numeri PAN, a meno che non dispongano di funzioni di cifratura.</p>

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

Requisito 5: Utilizzare e aggiornare regolarmente il software antivirus

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

Requisito	Istruzioni
5.1 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. 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 dal software dannoso i sistemi operativi mainframe e alcuni server Unix (ad esempio 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
5.1.1 Garantire che tutti i programmi antivirus siano in grado di rilevare e rimuovere tutti i tipi di malware nonché garantire una protezione sicura.	È importante proteggersi da TUTTI i tipi e le forme di software dannoso.
5.2 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.

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>6.1 Garantire che su tutti i componenti di sistema e il software siano installate le patch di sicurezza più recenti. Installare patch di sicurezza critiche entro un mese dal rilascio.</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>
<p>6.2 Stabilire un processo per identificare le vulnerabilità della sicurezza recentemente rilevate (ad esempio, attraverso un abbonamento a servizi di notifica gratuiti disponibili in Internet). Aggiornare gli standard di configurazione secondo il Requisito 2.2 PCI DSS per risolvere nuovi problemi di vulnerabilità.</p>	<p>L'intenzione di questo requisito è far sì che le organizzazioni si tengano aggiornate sulle nuove vulnerabilità al fine di proteggere opportunamente la rete, incorporando le vulnerabilità nuove e pertinenti nei relativi standard di configurazione.</p>
<p>6.3 Sviluppare applicazioni software in base agli standard PCI DSS (ad esempio, autenticazione e registrazione sicure) e alle pratiche di settore consigliate, quindi incorporare la protezione delle informazioni nell'intero ciclo di sviluppo del software. Questi processi devono includere quanto segue:</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>

Requisito	Istruzioni
<p>6.3.1 Test di tutte le patch di sicurezza e delle modifiche della configurazione del software prima della distribuzione</p> <p>6.3.1.1 Convalida di tutto l'input (per prevenire cross-site scripting, injection flaw, esecuzione di file pericolosi, ecc.)</p> <p>6.3.1.2 Convalida del processo di gestione degli errori appropriato</p> <p>6.3.1.3 Convalida del processo di memorizzazione di dati crittografici sicuro</p> <p>6.3.1.4 Convalida di comunicazioni sicure</p> <p>6.3.1.5 Convalida di un processo di controllo dell'accesso basato su ruoli (RBAC, Role-Based Access Control) appropriato</p>	<p>Garantire che tutte le installazioni e le modifiche vengano eseguite come previsto e che non vi siano funzioni impreviste, indesiderate o dannose.</p>
<p>6.3.2 Ambienti di sviluppo, test e produzione separati</p>	<p>Spesso gli ambienti di sviluppo e test sono meno sicuri dell'ambiente di produzione. Senza un'adeguata separazione, l'ambiente di produzione e i dati dei titolari di carte possono essere a rischio, a causa di vulnerabilità o processi interni deboli.</p>
<p>6.3.3 Responsabilità assegnate agli ambienti di sviluppo, test e produzione separate</p>	<p>In questo modo si riduce il numero di personale con accesso all'ambiente di produzione e ai dati dei titolari di carte, garantendo che l'accesso sia limitato solo a chi ne ha davvero bisogno.</p>
<p>6.3.4 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>6.3.5 Dati e account di test vengono rimossi 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>

Requisito	Istruzioni
<p>6.3.6 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>
<p>6.3.7 Il codice personalizzato viene analizzato prima del rilascio in produzione o della distribuzione ai clienti per identificare eventuali vulnerabilità</p> <p><i>Nota: questo requisito per le analisi del codice si applica a tutti i codici personalizzati (interni ed esterni), come parte della durata del ciclo di sviluppo del sistema richiesto nel Requisito 6.3 PCI DSS. Le analisi del codice possono essere condotte da personale interno preparato. 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. Le persone che conoscono le tecniche di codifica sicura dovrebbero rivedere il codice per identificarne le vulnerabilità.</p>
<p>6.4 Seguire le procedure di controllo delle modifiche per tutte le modifiche da apportare ai componenti di sistema. Le procedure devono includere quanto segue:</p>	<p>Senza controlli di modifica del software 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. Se i criteri del personale interessato per i controlli di base e i controlli di accesso al sistema non sono adeguati, esiste il rischio che individui non autorizzati o poco istruiti ottengano accesso illimitato al codice del software, che i dipendenti licenziati abbiano la possibilità di compromettere i sistemi e che le azioni non autorizzate non vengano rilevate.</p>
<p>6.4.1 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>6.4.2 Approvazione del management delle parti interessate</p>	<p>L'approvazione del management indica che una modifica è legittima e autorizzata dall'organizzazione.</p>

Requisito	Istruzioni
<p>6.4.3 Test della funzionalità operativa</p>	<p>Un test approfondito consente di verificare che tutte le azioni siano previste, che i rendiconti siano precisi, che la reazione a tutte le possibili condizioni di errore sia corretta, ecc.</p>
<p>6.4.4 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>
<p>6.5 Sviluppare tutte le applicazioni Web (interne, esterne e con accesso amministrativo all'applicazione tramite Web) in base alle linee guida di codifica sicura, quali le linee guida <i>Open Web Application Security Project</i>. Prevenire possibili vulnerabilità del codice comuni nei processi di sviluppo del software, incluso quanto segue:</p> <p><i>Nota: le vulnerabilità elencate dal punto 6.5.1 al punto 6.5.10 erano presenti nella guida OWASP al momento della pubblicazione degli standard PCI DSS v1.2. Tuttavia, in caso di aggiornamento della guida OWASP, è necessario utilizzare la versione più recente per questi requisiti.</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 esposte, causando danni all'azienda, ai suoi clienti e alla sua reputazione.</p>
<p>6.5.1 XSS (Cross-Site Scripting)</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>
<p>6.5.2 Injection flaw, in particolare SQL injection. Considerare, inoltre, 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. Gli Injection flaw, in particolare SQL injection, sono comuni nelle applicazioni Web. 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 Web devono essere convalidate prima dell'invio all'applicazione Web, ad esempio controllando tutti i caratteri alfabetici, un insieme di caratteri alfabetici e numerici, ecc.</p>

Requisito	Istruzioni
6.5.3 Esecuzione di file pericolosi	<p>Convalidare l'input per verificare che l'applicazione non accetti nomi file o file di utenti non previsti. Il codice vulnerabile all'inclusione di file remoti (RFI) consente agli aggressori di includere codice e dati ostili, dando luogo ad attacchi devastanti come la totale compromissione del server. Gli attacchi basati sull'esecuzione di file pericolosi influiscono su PHP, XML e su qualsiasi framework che accetti file e nomi file dagli utenti.</p>
6.5.4 Riferimenti a oggetti diretti non sicuri	<p>Non esporre riferimenti a oggetti interni agli utenti. 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>
6.5.5 Cross-site request forgery (CSRF)	<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>
6.5.6 Perdita di informazioni e gestione degli errori non appropriata	<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 Web 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>

Requisito	Istruzioni
6.5.7 Violazione dell'autenticazione e gestione delle sessioni	Autenticare in modo corretto gli utenti e proteggere le credenziali degli account e i token di sessione. Le credenziali degli account e i token di sessione spesso non vengono protetti accuratamente. Gli aggressori compromettono password, chiavi o token di autenticazione per assumere l'identità di altri utenti.
6.5.8 Memorizzazione di dati crittografici non sicura	Evitare gli errori di crittografia. Le applicazioni Web utilizzano raramente le funzioni di crittografia in modo corretto per proteggere dati e credenziali. Gli aggressori possono utilizzare i dati protetti in modo debole per il furto di identità e altri crimini, ad esempio frodi basate su carte di credito.
6.5.9 Comunicazioni non sicure	Cifrare in modo appropriato tutte le comunicazioni autenticate e riservate. Le applicazioni spesso non riescono a cifrare il traffico di rete quando è necessario proteggere le comunicazioni sensibili.
6.5.10 Mancata limitazione dell'accesso URL	Applicare in modo coerente il controllo dell'accesso a livello di presentazione e business logic per tutti gli URL. Spesso un'applicazione protegge le funzionalità sensibili solo impedendo 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.
6.6 Per le applicazioni Web esterne, assicurare una protezione costante da nuove minacce e vulnerabilità e garantire che queste applicazioni siano protette da attacchi noti mediante <i>uno</i> dei seguenti metodi: <ul style="list-style-type: none"> ▪ Analisi delle applicazioni Web rivolte al pubblico tramite strumenti o metodi di valutazione della sicurezza delle applicazioni manuali o automatici, almeno una volta all'anno e dopo ogni modifica ▪ Installazione di un firewall di applicazioni Web davanti alle applicazioni Web rivolte al pubblico 	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 carte. <ul style="list-style-type: none"> ▪ 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. ▪ 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. Vedere <i>Supplemento informativo: Requisito 6.6 Analisi del codice e firewall a livello di applicazione</i> (www.pcisecuritystandards.org) per ulteriori informazioni.

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>7.1 Limitare l'accesso ai componenti di sistema e ai dati di titolari di carta solo alle persone per le cui mansioni è realmente necessario. Le limitazioni di accesso devono includere quanto segue:</p> <p>7.1.1 Limitazione dei diritti di accesso a ID utente privilegiati alla quantità minima necessaria per le responsabilità di ruolo</p> <p>7.1.2 Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale</p> <p>7.1.3 Richiesta di un modulo di autorizzazione firmato dal management che specifica i privilegi necessari</p> <p>7.1.4 Implementazione di un sistema di controllo dell'accesso automatico</p>	<p>Maggiore è il numero di persone che hanno accesso ai dati dei titolari di carte, 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 "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'organizzazione dovrebbe creare criteri e processi chiari per il controllo dell'accesso ai dati basate sull'effettiva esigenza di conoscenza e sul controllo dell'accesso basato su ruolo, al fine di definire come concedere l'accesso e a chi.</p>
<p>7.2 Stabilire un meccanismo per i componenti di sistemi con più utenti per limitare l'accesso in base alla reale necessità di un utente e impostare "deny all" per impedire ogni accesso se non specificatamente consentito. Il sistema di controllo dell'accesso deve includere quanto segue:</p> <p><i>Nota: 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.</i></p> <p>7.2.1 Copertura di tutti i componenti di sistema</p> <p>7.2.2 Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale</p> <p>7.2.3 Impostazione predefinita "deny-all"</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.

Requisito	Istruzioni
<p>8.1 Assegnare a tutti gli utenti un ID univoco prima di consentire l'accesso ai componenti di sistema o ai dati di titolari di carta.</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>8.2 Oltre ad assegnare un ID univoco, adottare almeno uno dei seguenti metodi per autenticare tutti gli utenti:</p> <ul style="list-style-type: none"> ▪ Password o passphrase ▪ Autenticazione a due fattori (ad esempio, dispositivi token, smart card, biometrica o chiavi pubbliche) 	<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>8.3 Incorporare l'autenticazione a due fattori per l'accesso remoto alla rete (accesso a livello di rete dall'esterno) da parte di dipendenti, amministratori e terze parti. Utilizzare tecnologie, quali RADIUS (Remote Authentication and Dial-In Service) o TACACS (Terminal Access Controller Access Control System) con token oppure VPN (basata su SSL/TLS o IPSEC) con certificati singoli.</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>8.4 Rendere tutte le password illeggibili durante la trasmissione e la memorizzazione su tutti i componenti di sistema tramite la crittografia avanzata (definita nel documento <i>PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi</i>).</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 cifrate nei file in cui sono memorizzati, utilizzando i dati sottratti per l'accesso non autorizzato.</p>
<p>8.5 Mettere in atto la gestione delle autenticazioni e delle password utente per utenti non consumatori e amministratori in tutti i componenti del 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>

Requisito	Istruzioni
<p>8.5.1 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>
<p>8.5.2 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>8.5.3 Impostare la password per il primo accesso su un valore univoco per ogni utente e modificarla immediatamente dopo il primo uso.</p>	<p>Se viene utilizzata la stessa password per ogni 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>8.5.4 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, è possibile 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>8.5.5 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>8.5.6 Abilitare gli account utilizzati dai fornitori per la gestione in remoto solo durante il periodo di tempo necessario.</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. Vedere anche 12.3.8 e 12.3.9 per ulteriori informazioni su questo argomento.</p>
<p>8.5.7 Comunicare le procedure e le politiche relative alle password a tutti gli utenti con accesso ai dati di titolari di carta.</p>	<p>La comunicazione delle procedure per le 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
8.5.8 Non utilizzare account e password di gruppo, condivisi o generici.	Se più utenti condividono lo stesso account 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 membro del gruppo che condivide account e password.
8.5.9 Modificare le password utente almeno ogni 90 giorni.	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 rete, i database e altre piattaforme.
8.5.10 Richiedere una lunghezza minima della password di 7 caratteri.	
8.5.11 Utilizzare password contenenti valori numerici e alfabetici.	
8.5.12 Non consentire l'invio di una nuova password uguale a una delle ultime quattro password utilizzate.	
8.5.13 Limitare i tentativi di accesso ripetuti bloccando l'ID utente dopo un massimo di sei tentativi.	Senza i meccanismi di blocco dell'account, un aggressore può tentare in modo continuo di indovinare una password mediante strumenti manuali o automatici (cracking delle password), fino ad avere successo e accedere all'account di un utente.
8.5.14 Impostare la durata del blocco a un minimo di 30 minuti o finché l'amministratore non abilita l'ID utente.	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).
8.5.15 Se una sessione è inattiva per oltre 15 minuti, l'utente deve immettere nuovamente la password per riattivare il terminale.	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.

Requisito	Istruzioni
<p>8.5.16 Autenticare tutti gli accessi al database contenente i dati di titolari di carta. Sono compresi gli accessi da applicazioni, amministratori e tutti gli altri utenti.</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 di titolari di carta

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

Requisito	Istruzioni
<p>9.1 Utilizzare i controlli dell'accesso alle strutture appropriati per limitare e monitorare gli accessi fisici ai sistemi nell'ambiente dei dati di titolari di carta.</p>	<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>9.1.1 Utilizzare videocamere o altri meccanismi di controllo dell'accesso per monitorare gli accessi fisici ad aree sensibili. Esaminare i dati raccolti e correlarli con altri. Conservare i dati per almeno tre mesi, se non diversamente richiesto dalle leggi in vigore.</p> <p><i>Nota: per "aree sensibili" si intendono centri dati, aree server e aree che ospitano sistemi di memorizzazione dei dati di titolari di carta. Ciò esclude le aree in cui vi sono i terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio.</i></p>	<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.</p>
<p>9.1.2 Limitare l'accesso fisico a connettori di rete accessibili pubblicamente.</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>
<p>9.1.3 Limitare l'accesso fisico a punti di accesso wireless, gateway e dispositivi portatili.</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. Prendere in considerazione lo spostamento di gateway e punti di accesso wireless in aree sicure, ad esempio all'interno di armadi con serratura o sale server. Verificare che sia attivata la cifratura avanzata. Attivare il blocco automatico dei dispositivi palmari wireless dopo un lungo periodo di inattività, e impostare i dispositivi affinché richiedano una password all'accensione.</p>

Requisito	Istruzioni
<p>9.2 Sviluppare procedure che consentono a tutto il personale di distinguere facilmente tra dipendenti e visitatori, in particolare in aree che permettono l'accesso ai dati di titolari di carta.</p> <p><i>Ai fini del presente requisito, per "dipendente" si intende un dipendente a tempo pieno o part-time, un dipendente con contratto a tempo determinato, un collaboratore o consulente che svolge le sue prestazioni in sede. Per "visitatore" si intende un fornitore, un ospite di un dipendente, un tecnico dell'assistenza o chiunque abbia necessità di accedere alla struttura per un breve periodo di tempo, solitamente non più di un giorno.</i></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>9.3 Accertarsi che tutti i visitatori vengano gestiti nel modo seguente:</p> <p>9.3.1 Ricevono l'autorizzazione appropriata prima di accedere alle aree in cui i dati di titolari di carta sono elaborati o custoditi.</p> <p>9.3.2 Ricevono un token fisico (ad esempio, una tessera magnetica o un dispositivo di accesso) che scade e che identifica i visitatori come non dipendenti.</p> <p>9.3.3 Restituiscono il token fisico prima di lasciare la struttura o in corrispondenza della data di scadenza.</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>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 i dipendenti possano controllarne le attività) e che il loro accesso sia limitato solo alla durata della visita legittima.</p>
<p>9.4 Utilizzare un registro visitatori per conservare un audit trail fisico dell'attività dei visitatori. Documentare il nome del visitatore, l'azienda rappresentata e il dipendente che autorizza l'accesso fisico sul registro. Conservare questo registro per almeno tre mesi, se non diversamente richiesto dalla legge.</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>
<p>9.5 Conservare i backup dei supporti in un luogo sicuro, preferibilmente in una struttura esterna, quale un luogo alternativo o 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>

Requisito	Istruzioni
9.6 Proteggere fisicamente tutti i supporti cartacei ed elettronici contenenti dati di titolari di carta.	I dati dei titolari di carte sono soggetti a visualizzazione, copia o scansione non autorizzate se sono trasferiti senza protezione su supporti portatili, stampati o lasciati sulla scrivania. Prendere in considerazione procedure e processi per 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.
9.7 Mantenere un rigido controllo sulla distribuzione interna o esterna di qualsiasi tipo di supporto che contenga dati di titolari di carta, incluso quanto segue:	
9.7.1 Classificare il supporto in modo che possa essere identificato come riservato.	I supporti non identificati come riservati potrebbero non essere trattati con la cura necessaria e quindi potrebbero essere persi o rubati. Includere un processo di classificazione dei supporti nelle procedure consigliate nel precedente Requisito 9.6.
9.7.2 Inviare il supporto tramite un corriere affidabile o un altro metodo di consegna che possa essere monitorato in modo appropriato.	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.
9.8 Accertarsi che il management approvi tutti i supporti contenenti i dati di titolari di carta che vengono spostati da un'area protetta (in particolare quando i supporti vengono distribuiti a singoli utenti).	I dati dei titolari di carte che lasciano le aree sicure senza un processo approvato dal management possono portare alla perdita o al furto di dati. Senza un processo, la posizione dei supporti non viene rintracciata e non esiste un processo sulla destinazione dei dati o sulla loro protezione. Includere lo sviluppo di un processo approvato dal management per il trasferimento dei supporti nelle procedure consigliate nel precedente Requisito 9.6.
9.9 Mantenere rigidi controlli sulla memorizzazione e sull'accesso a supporti contenenti dati di titolari di carta.	Senza metodi di inventario attenti e controlli di storage, potrebbe non essere possibile accorgersi del furto o della mancanza di supporti per diverso tempo. Includere lo sviluppo di un processo per limitare l'accesso ai supporti contenenti dati dei titolari di carte nelle procedure consigliate nel precedente Requisito 9.6.
9.9.1 Conservare in modo appropriato i registri di inventario per tutti i supporti ed eseguire tali inventari almeno una volta all'anno.	Se i supporti non vengono inventariati, potrebbe non essere possibile accorgersi del furto o della mancanza di supporti per diverso tempo. Includere lo sviluppo di un processo per l'inventario dei supporti e la memorizzazione sicura nelle procedure consigliate nel precedente Requisito 9.6.

Requisito	Istruzioni
9.10 Distruggere i supporti contenenti dati di titolari di carta quando non sono più necessari per scopi aziendali o legali, come segue:	Se non vengono compiuti i passi per distruggere le informazioni contenute sui dischi rigidi del PC, su CD e su carta, lo smaltimento di tali informazioni può dare luogo a compromissioni e comportare perdite finanziarie o di reputazione. Ad esempio, gli individui non autorizzati possono utilizzare una tecnica chiamata "dumpster diving", con la quale ricercano nei cestini e nella spazzatura, utilizzando le informazioni trovate per lanciare un attacco. Includere lo sviluppo di un processo per la corretta distruzione dei supporti contenenti dati dei titolari di carte, comprendendo la corretta conservazione di tali supporti prima della distruzione, nelle procedure consigliate nel precedente Requisito 9.6.
9.10.1 Stracciare, bruciare o mandare al macero i materiali cartacei in modo che i dati di titolari di carta non possano essere ricostruiti.	
9.10.2 Rendere i dati di titolari di carta su supporti elettronici non recuperabili, in modo che non sia possibile ricostruirli.	

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 determinare la causa di una compromissione di dati.

Requisito	Istruzioni
<p>10.1 Stabilire un processo per collegare tutti gli accessi ai componenti di sistema (in particolare l'accesso eseguito con privilegi di amministratore, ad esempio come utente root) a ciascun utente.</p>	<p>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.</p>
<p>10.2 Implementare audit trail automatizzati per tutti i componenti del sistema per ricostruire i seguenti eventi:</p> <ul style="list-style-type: none"> 10.2.1 Tutti i singoli accessi di utenti a dati di titolari di carta 10.2.2 Tutte le azioni intraprese da un utente con privilegi di utente root o amministratore 10.2.3 Accesso a tutti gli audit trail 10.2.4 Tentativi di accesso logico non validi 10.2.5 Uso di meccanismi di identificazione e autenticazione 10.2.6 Inizializzazione di log di audit 10.2.7 Creazione ed eliminazione di oggetti a livello di sistema 	<p>Gli utenti non autorizzati sulla rete spesso eseguono più tentativi di accesso sui sistemi di destinazione. 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.</p>

Requisito	Istruzioni
<p>10.3 Registrare almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento:</p> <ul style="list-style-type: none"> 10.3.1 Identificazione utente 10.3.2 Tipo di evento 10.3.3 Data e ora 10.3.4 Indicazione di successo o fallimento 10.3.5 Origine dell'evento 10.3.6 Identità o nome dell'elemento interessato (dati, componente di sistema o risorsa) 	<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>
<p>10.4 Sincronizzare tutti gli orologi e gli orari critici del sistema.</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. Per i team legali attivati dopo un incidente, l'ora di ciascuna attività è fondamentale per determinare come sono stati compromessi i sistemi. Un utente non autorizzato può inoltre tentare di modificare direttamente l'ora su un server di riferimento orario, se le limitazioni di accesso non sono adeguate, per cambiare l'ora di accesso alla rete da parte dell'utente non autorizzato.</p>
<p>10.5 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>
<ul style="list-style-type: none"> 10.5.1 Limitare la visualizzazione degli audit trail a coloro che realmente necessitano di tali informazioni per scopi aziendali. 10.5.2 Proteggere i file di audit trail da modifiche non autorizzate. 10.5.3 Eseguire immediatamente il backup dei file di audit trail su un server di registro centralizzato o un supporto difficile da modificare. 10.5.4 Scrivere registri per tecnologie rivolte al pubblico su un server di registro sulla LAN interna. 	<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>

Requisito	Istruzioni
<p>10.5.5 Utilizzare un meccanismo di monitoraggio dell'integrità dei file e un software di rilevamento delle modifiche di log per accertarsi che i dati di log esistenti non possano essere modificati senza generare avvisi (non per l'aggiunta di nuovi dati)</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>10.6 Esaminare i registri per tutti i componenti di sistema almeno una volta al giorno. Le analisi dei log devono includere i server che eseguono funzioni di sicurezza, quali i servizi antintrusione IDS (Intrusion Detection System), i server di autenticazione, autorizzazione e accounting (AAA), 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>10.7 Conservare la cronologia dell'audit trail per almeno un anno, con un minimo di tre mesi di disponibilità immediata per l'analisi (ad esempio, online, archiviazione o recuperabile da backup).</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 interessati. 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>11.1 Verificare la presenza di punti di accesso wireless utilizzando un analizzatore wireless almeno una volta ogni tre mesi oppure distribuendo un IDS/IPS wireless per identificare tutti i dispositivi wireless in uso.</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". Inoltre, possono essere utilizzati analizzatori wireless, scanner di porte e altri strumenti di rete che rilevano i dispositivi wireless.</p> <p>Viste la facilità con cui un punto di accesso wireless può essere unito alla rete, la difficoltà di rilevarne la presenza e il maggiore rischio posto dai dispositivi wireless non autorizzati, queste scansioni devono essere eseguite anche quando esiste un criterio che impedisce l'uso della tecnologia wireless.</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 durante una scansione wireless manuale.</p>
<p>11.2 Eseguire scansioni interne ed esterne della rete almeno una volta ogni tre mesi e dopo ogni cambiamento significativo apportato alla rete (ad esempio, l'installazione di nuovi componenti di sistema, la modifica della topologia della rete, la modifica delle regole del firewall o l'aggiornamento di un prodotto)</p> <p><i>Nota: le scansioni esterne delle vulnerabilità trimestrali devono essere eseguite da un fornitore di scansioni approvato (ASV) e qualificato da PCI SSC. Le scansioni dopo le modifiche della rete possono essere eseguite dal personale interno della società.</i></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 e identificare le porte 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>11.3 Eseguire test di penetrazione esterna ed interna almeno una volta all'anno e dopo ogni aggiornamento o modifica significativa dell'infrastruttura o dell'applicazione (quale un aggiornamento del sistema operativo, l'aggiunta all'ambiente di una subnet o di un server Web). Questi test di penetrazione devono includere quanto segue:</p> <p>11.3.1 Test di penetrazione a livello di rete</p> <p>11.3.2 Test di penetrazione a livello di applicazione</p>	<p>I test di penetrazione a livello di rete e di applicazione sono diversi dalle scansioni delle vulnerabilità, in quanto i test di penetrazione sono manuali, tentano di sfruttare alcune delle vulnerabilità identificate nelle scansioni e comprendono tecniche utilizzate dagli utenti non autorizzati per trarre vantaggio da processi o sistemi con protezione debole.</p> <p>Prima della messa in produzione di applicazioni, dispositivi di rete e sistemi, è opportuno rafforzarli e proteggerli utilizzando le migliori pratiche di protezione (Requisito 2.2). Le scansioni delle vulnerabilità e i test di penetrazione esporranno le vulnerabilità rimanenti che potrebbero essere individuate e sfruttate in seguito da un aggressore.</p>
<p>11.4 Utilizzare sistemi di rilevamento e/o di prevenzione delle intrusioni per monitorare tutto il traffico nell'ambiente dei dati di titolari di carta e segnalare possibili rischi al personale addetto. Mantenere tutti i sistemi di rilevamento e prevenzione delle intrusioni aggiornati.</p>	<p>Questi strumenti confrontano il traffico in arrivo nella rete con "definizioni" note di migliaia di tipi di compromissione (strumenti per hacker, cavalli di Troia e altro malware) e inviano avvisi e/o fermano il tentativo in corso. Senza un approccio proattivo al rilevamento di attività non autorizzate 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>Esistono migliaia di tipi di compromissione, e molti altri vengono scoperti quotidianamente. Le versioni stantie di questi sistemi non disporranno di definizioni correnti e non identificheranno le nuove vulnerabilità che potranno portare a violazioni non rilevate. I fornitori di questi prodotti forniscono aggiornamenti frequenti, spesso giornalieri.</p>
<p>11.5 Distribuire il software di monitoraggio dell'integrità dei file per segnalare al personale modifiche non autorizzate di file system, file di configurazione o file di contenuto critici; inoltre, configurare il software in modo che esegua confronti di file critici almeno una volta alla settimana.</p> <p><i>Nota: ai fini del monitoraggio dell'integrità dei file, i file critici sono solitamente file che non cambiano frequentemente, ma la cui modifica può indicare la compromissione, effettiva o potenziale, del sistema. In genere, i prodotti per il monitoraggio dell'integrità dei file sono preconfigurati con file critici per il sistema operativo in uso. Altri file critici, ad esempio quelli per applicazioni personalizzate, devono essere valutati e definiti dall'entità (ossia dall'esercente o dal provider di servizi).</i></p>	<p>I sistemi 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 dipendenti e collaboratori

Una politica di sicurezza rigida definisce il livello di sicurezza per l'intera società e spiega ai dipendenti quali sono le aspettative nei loro confronti in termini di sicurezza. Tutti i dipendenti devono essere a conoscenza della sensibilità dei dati e delle proprie responsabilità in termini di protezione. Ai fini del presente requisito, per "dipendente" si intende un dipendente a tempo pieno o part-time, un dipendente con contratto a tempo determinato, un collaboratore o consulente che svolge le sue prestazioni in sede.

Requisito	Istruzioni
<p>12.1 Stabilire, pubblicare, conservare e rendere disponibile una politica di sicurezza conforme a quanto indicato di seguito:</p> <p>12.1.1 Risponde a tutti i requisiti PCI DSS.</p> <p>12.1.2 Include un processo annuale che identifica minacce e vulnerabilità e che consente di ottenere una valutazione dei rischi formale.</p> <p>12.1.3 Include una revisione almeno una volta l'anno e aggiornamenti in caso di cambiamenti dell'ambiente</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 ai dipendenti di sapere quali sono le aspettative nei loro confronti in termini di sicurezza. Tutti i dipendenti devono essere a conoscenza della sensibilità dei dati e delle proprie responsabilità in termini di protezione.</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 queste modifiche, le nuove misure di protezione per combattere queste minacce non vengono applicate.</p>
<p>12.2 Sviluppare procedure di sicurezza operativa giornaliere coerenti con i requisiti di questa specifica (ad esempio, procedure per la manutenzione degli account utente e procedure di revisione dei registri).</p>	<p>Le procedure di sicurezza operativa giornaliere fungono da "istruzioni alla scrivania" che i dipendenti possono utilizzare nelle loro attività di manutenzione e amministrazione del sistema quotidiane. Le procedure di sicurezza operativa non documentate porteranno a dipendenti che non comprendono l'intero scopo delle loro attività, 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>12.3 Sviluppare politiche di uso per tecnologie per dipendenti critiche (ad esempio, tecnologie di accesso remoto, wireless, supporti elettronici rimovibili, laptop, PDA, uso della posta elettronica e di Internet) per definire l'uso corretto di queste tecnologie per tutti i dipendenti e i collaboratori esterni. Accertarsi che tali politiche richiedano quanto segue:</p>	<p>I criteri di utilizzo dei dipendenti 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 i dipendenti. Se non sono disponibili criteri di utilizzo, i dipendenti possono 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 ai dipendenti generici/non specializzati di installare queste tecnologie.</p>
<p>12.3.1 Approvazione esplicita del management</p>	<p>Senza la richiesta dell'approvazione esplicita del management per queste tecnologie, un utente può implementare una soluzione per un'esigenza aziendale percepita aprendo inconsapevolmente un enorme falla che mette sistemi critici e dati a disposizione degli utenti non autorizzati.</p>
<p>12.3.2 Autenticazione per l'uso della tecnologia</p>	<p>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>12.3.3 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". I dipendenti possono inoltre bypassare procedure e dispositivi di installazione. Un inventario accurato con una corretta etichettatura dei dispositivi consente una rapida identificazione delle installazioni non approvate. Prendere in considerazione l'applicazione di una convenzione di denominazione ufficiale per i dispositivi, quindi etichettare e registrare tutti i dispositivi insieme a controlli dell'inventario ben definiti.</p>
<p>12.3.4 Etichettatura di dispositivi con proprietario, informazioni di contatto e scopo</p>	
<p>12.3.5 Usi accettabili delle tecnologie</p>	
<p>12.3.6 Posizioni di rete accettabili per le tecnologie</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>12.3.7 Elenco di prodotti approvati dalla società</p>	
<p>12.3.8 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</p>

Requisito	Istruzioni
<p>12.3.9 Attivazione di tecnologie di accesso remoto per fornitori solo quando necessario, con disattivazione immediata dopo l'uso</p>	<p>sistemi dal POS o da altri rivenditori), 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>12.3.10 Durante l'accesso ai dati di titolari di carta tramite tecnologie di accesso remoto, vietare la copia, lo spostamento e la memorizzazione dei dati di titolari di carta su dischi rigidi locali e supporti elettronici rimovibili.</p>	<p>Per garantire che i dipendenti siano consapevoli delle loro responsabilità di non memorizzare o copiare i dati dei titolari di carte sul loro personal computer locale o su altri supporti, l'azienda dovrebbe disporre di un criterio che vieta chiaramente tali attività.</p>
<p>12.4 Accertarsi che la politica e le procedure di sicurezza definiscano chiaramente le responsabilità in termini di protezione delle informazioni per tutti i dipendenti e i collaboratori.</p>	<p>Senza l'assegnazione di ruoli e responsabilità di protezione chiaramente definiti, potrebbero verificarsi interazioni incoerenti con il gruppo di protezione, che portano a un'implementazione non sicura delle tecnologie o l'uso di tecnologie non aggiornate e poco sicure.</p>
<p>12.5 Assegnare a un utente singolo o a un team le seguenti responsabilità di gestione della sicurezza delle informazioni:</p> <ul style="list-style-type: none"> 12.5.1 Definizione, documentazione e distribuzione delle politiche e delle procedure di sicurezza 12.5.2 Monitoraggio e analisi degli avvisi e delle informazioni sulla sicurezza e distribuzione al personale appropriato 12.5.3 Definizione, documentazione e distribuzione di procedure di risposta ed escalation in caso di problemi di sicurezza per garantire una gestione tempestiva ed efficiente di tutte le situazioni 12.5.4 Amministrazione di account utente, incluse aggiunte, eliminazione e modifiche 12.5.5 Monitoraggio e controllo di tutti gli accessi ai dati 	<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>12.6 Implementare un programma formale di consapevolezza della sicurezza per rendere tutti i dipendenti consapevoli dell'importanza della sicurezza dei dati di titolari di carta.</p>	<p>Se gli utenti non sono istruiti sulle loro responsabilità di sicurezza, le misure di protezione e i processi implementati potrebbero divenire inefficaci a causa di errori o azioni intenzionali dei dipendenti.</p>

Requisito	Istruzioni
<p>12.6.1 Formare i dipendenti al momento dell'assunzione e almeno una volta all'anno.</p>	<p>Se il programma di conoscenza della sicurezza non include sessioni di aggiornamento annuali, 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.</p>
<p>12.6.2 Richiedere ai dipendenti di certificare almeno una volta all'anno che hanno letto e compreso la politica e le procedure di sicurezza della società.</p>	<p>Richiedere ai dipendenti una conferma (ad esempio In forma scritta o elettronica) per garantire che abbiano letto e compreso i criteri e le procedure di protezione e che si impegnino a rispettarli.</p>
<p>12.7 Sottoporre i potenziali dipendenti a screening (vedere la definizione di "dipendente" al punto 9.2 riportato sopra) prima di assumerli per ridurre al minimo il rischio di attacchi da fonti interne. <i>Per i dipendenti, quali i cassieri di un negozio, che hanno accesso a un solo numero di carta alla volta, questo requisito è solo consigliato.</i></p>	<p>L'esecuzione di approfondite indagini di base prima dell'assunzione dei dipendenti che dovranno accedere ai dati dei titolari di carte riduce il rischio di uso non autorizzato dei numeri 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>12.8 Se i dati di titolari di carta sono condivisi con provider di servizi, gestire e implementare politiche e procedure per i provider di servizi per includere quanto segue:</p>	<p>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>12.8.1 Conservare un elenco dei provider di servizi.</p>	<p>La conoscenza dei provider di servizi permette di identificare dove si estendono i rischi potenziali all'esterno dell'organizzazione.</p>
<p>12.8.2 Conservare un accordo scritto in base al quale il provider di servizi si assume la responsabilità della protezione dei dati di titolari di carta di cui entra in possesso.</p>	<p>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>12.8.3 Accertarsi che esista un processo definito per incaricare i provider di servizi, che includa tutte le attività di dovuta diligenza appropriate prima dell'incarico.</p>	<p>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>12.8.4 Conservare un programma per monitorare lo stato di conformità agli standard PCI DSS dei provider di servizi.</p>	<p>La conoscenza dello stato di conformità PCI DSS di un provider di servizi garantisce ulteriormente il loro rispetto degli stessi requisiti a cui è soggetta un'organizzazione.</p>

Requisito	Istruzioni
12.9 Implementare un piano di risposta agli incidenti. Prepararsi a rispondere immediatamente a una violazione del sistema.	Senza un piano di risposta agli incidenti di protezione correttamente divulgato, letto e compreso dalle parti responsabili, la confusione o la mancanza di una risposta unificata potrebbero causare ulteriori tempi di inattività del business, un'inutile esposizione ai mezzi di informazione e responsabilità legali.
12.9.1 Creare il piano di risposta agli incidenti da attuare in caso di violazione del sistema. Accertarsi che il piano includa almeno i seguenti elementi: <ul style="list-style-type: none"> ▪ Ruoli, responsabilità e strategie di comunicazione e contatto in caso di violazione, nonché notifiche ai marchi di pagamento ▪ Procedure specifiche di risposta agli incidenti ▪ Procedure di ripristino e continuità delle attività aziendali ▪ Processi di backup dei dati ▪ Analisi dei requisiti legali per la segnalazione delle violazioni ▪ Copertura e risposte per tutti i componenti di sistema critici ▪ Riferimenti e descrizioni delle procedure di risposta agli incidenti adottate dai marchi di pagamento 	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.
12.9.2 Eseguire un test del piano almeno una volta all'anno.	Senza il test, è possibile che vengano trascurati passaggi chiave che potrebbero limitare l'esposizione durante un incidente.
12.9.3 Nominare personale specifico disponibile 24 ore al giorno, 7 giorni su 7 in caso di emergenza.	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.
12.9.4 Formare in modo appropriato il personale addetto al controllo delle violazioni della sicurezza.	

Requisito	Istruzioni
12.9.5 Includere allarmi dai sistemi di rilevamento e prevenzione delle intrusioni e dai sistemi di monitoraggio dell'integrità dei file.	Questi sistemi di monitoraggio sono pensati per porre l'attenzione sui potenziali rischi per i dati, sono fondamentali per intraprendere azioni rapide per impedire una violazione e devono essere inclusi nei processi di risposta agli incidenti.
12.9.6 Sviluppare un processo che consenta di correggere e migliorare il piano di risposta agli incidenti tenendo conto delle lezioni apprese e degli ultimi sviluppi nel settore.	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.

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

Requisito A.1: Protezione di dati di titolari di carta da parte dei provider di hosting condiviso

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>A.1 Proteggere l'ambiente e i dati di ogni entità ospitata (esercente, provider di servizi o altra entità), nei modi previsti dal punto A.1.1 al punto A.1.4:</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><i>Nota: anche se un provider di hosting soddisfa tutti questi requisiti, la conformità dell'entità che utilizza tale provider di hosting non è automaticamente garantita. Ogni entità deve soddisfare i requisiti e ottenere la convalida della conformità agli standard PCI DSS, come applicabile.</i></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>A.1.1 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>A.1.2 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>

Requisito	Istruzioni
A.1.3 Accertarsi che le funzioni di audit trail e di generazione dei registri siano abilitate e siano univoche per l'ambiente dei dati di titolari di carta di ciascuna entità e che siano coerenti con il Requisito 10 PCI DSS.	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.
A.1.4 Abilitare processi per fornire tutte le informazioni necessarie per un'indagine legale tempestiva in caso di violazione di dati di un esercente o un provider di servizi ospitato	I provider di hosting condiviso devono disporre di processi per garantire una risposta rapida nel caso sia necessaria un'indagine forense su una compromissione, fino al livello di dettagli appropriato, in modo che siano disponibili i dettagli del singolo esercente o provider di servizi.

Appendice 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 ¹⁰
<i>PCI DSS: Questionario di autovalutazione B e Attestato</i>	Esercenti ¹⁰
<i>PCI DSS: Questionario di autovalutazione C e Attestato</i>	Esercenti ¹⁰
<i>PCI DSS: Questionario di autovalutazione D e Attestato</i>	Esercenti ¹⁰ e tutti i provider di servizi
<i>PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi</i>	Tutti gli esercenti e i provider di servizi

¹⁰ 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".