



**Settore delle carte di pagamento (PCI)  
Standard di protezione dei dati  
Questionario di autovalutazione D  
e Attestato di conformità**

---

**Tutti gli altri esercenti idonei per  
il questionario SAQ**  
Per l'uso con PCI DSS versione 3.2

Aprile 2016

## Modifiche del documento

Data	Versione PCI DSS	Revision e SAQ	Descrizione
Ottobre 2008	1.2		Allineare il contenuto con il nuovo standard PCI DSS v1.2 e implementare modifiche minori apportate dopo la versione originale v1.1.
Ottobre 2010	2.0		Allineare il contenuto ai nuovi requisiti e procedure di test PCI DSS v2.0.
Febbraio 2014	3.0		Allineare il contenuto con i requisiti PCI DSS v3.0 e le procedure di test e incorporare ulteriori opzioni di risposta.
Aprile 2015	3.1		Aggiornato per allinearlo a PCI DSS v3.1. Per informazioni dettagliate sulle modifiche di PCI DSS, fare riferimento a <i>PCI DSS - Riepilogo delle modifiche di PCI DSS dalla versione 3.0 alla 3.1</i> .
Luglio 2015	3.1	1.1	Aggiornato per rimuovere i riferimenti alle “migliore pratiche” prima del 30 giugno 2015 e per rimuovere l’opzione di reporting PCI DSS v2 per il Requisito 11.3.
Aprile 2016	3.2	1.0	Aggiornato per allinearlo a PCI DSS v3.2. Per informazioni dettagliate sulle modifiche di PCI DSS, fare riferimento a <i>PCI DSS - Riepilogo delle modifiche di PCI DSS dalla versione 3.1 alla 3.2</i> .

# Sommario

<b>Modifiche del documento</b> .....	<b>i</b>
<b>Operazioni preliminari</b> .....	<b>iii</b>
<b>Passaggi per il completamento dell'autovalutazione PCI DSS</b> .....	<b>iii</b>
<b>Comprensione del questionario di autovalutazione</b> .....	<b>iii</b>
<i>Test previsti</i> .....	<i>iv</i>
<b>Completamento del questionario di autovalutazione</b> .....	<b>iv</b>
<b>Guida per la non applicabilità di determinati requisiti specifici</b> .....	<b>v</b>
<i>Comprendere la differenza tra Non applicabile e Non testato</i> .....	<i>v</i>
<b>Eccezione legale</b> .....	<b>vi</b>
<b>Sezione 1 - Informazioni sulla valutazione</b> .....	<b>1</b>
<b>Sezione 2 - Questionario di autovalutazione D per esercenti</b> .....	<b>4</b>
<b>Sviluppo e gestione di sistemi e reti sicure</b> .....	<b>4</b>
<i>Requisito 1 - Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta</i> .....	<i>4</i>
<i>Requisito 2 - Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione</i> .....	<i>10</i>
<b>Protezione dei dati dei titolari di carta</b> .....	<b>17</b>
<i>Requisito 3 - Proteggere i dati dei titolari di carta memorizzati</i> .....	<i>17</i>
<i>Requisito 4 - Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche</i> .....	<i>25</i>
<b>Utilizzare un programma per la gestione delle vulnerabilità</b> .....	<b>27</b>
<i>Requisito 5 - Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus</i> .....	<i>27</i>
<i>Requisito 6 - Sviluppare e gestire sistemi e applicazioni protette</i> .....	<i>29</i>
<b>Implementazione di rigide misure di controllo dell'accesso</b> .....	<b>40</b>
<i>Requisito 7 - Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario</i> .....	<i>40</i>
<i>Requisito 8 - Individuare e autenticare l'accesso ai componenti di sistema</i> .....	<i>42</i>
<i>Requisito 9 - Limitare l'accesso fisico ai dati dei titolari di carta</i> .....	<i>49</i>
<b>Monitoraggio e test delle reti regolari</b> .....	<b>58</b>
<i>Requisito 10 - Registrare e monitorare tutti gli accessi a risorse di rete e dati dei titolari di carta</i> ..	<i>58</i>
<i>Requisito 11 - Eseguire regolarmente test dei sistemi e processi di protezione</i> .....	<i>65</i>
<b>Gestire una politica di sicurezza delle informazioni</b> .....	<b>73</b>
<i>Requisito 12 - Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale</i> .....	<i>73</i>
<b>Appendice A - Requisiti PCI DSS aggiuntivi</b> .....	<b>81</b>
<i>Appendice A1 - Requisiti PCI DSS aggiuntivi per provider di hosting condiviso</i> .....	<i>81</i>
<i>Appendice A2 - Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale</i> .....	<i>81</i>
<i>Appendice A3 - Convalida aggiuntiva delle entità designate (DESV)</i> .....	<i>82</i>
<b>Appendice B - Foglio di lavoro - Controlli compensativi</b> .....	<b>83</b>
<b>Appendice C - Spiegazione di non applicabilità</b> .....	<b>84</b>
<b>Appendice D - Spiegazione dei requisiti non testati</b> .....	<b>85</b>
<b>Sezione 3 - Dettagli su convalida e attestato</b> .....	<b>86</b>

## Operazioni preliminari

Il modulo SAQ D per esercenti è valido per gli esercenti idonei al questionario SAQ che non rispondono ai criteri richiesti per altri tipi di SAQ. Esempi di ambienti di esercenti che potrebbero avvalersi di SAQ D sono, senza limitazione:

- Esercenti di E-commerce che accettano i dati dei titolari di carta nel sito Web
- Esercenti che utilizzano la memorizzazione elettronica dei dati di titolari di carta
- Esercenti che non memorizzano i dati dei titolari di carta in formato elettronico ma che non rispondono ai criteri di un altro tipo di SAQ
- Esercenti con ambienti che potrebbero rispondere ai requisiti di un altro tipo di SAQ, ma con altri requisiti PCI DSS applicabili al proprio ambiente

Sebbene molte aziende che completano il questionario SAQ D debbano convalidare la propria conformità a ogni requisito PCI DSS, alcune aziende con modelli di business molto specifici possono trovare non applicabili alcuni requisiti. Fare riferimento alla guida seguente per informazioni sull'esclusione di alcuni requisiti specifici.

## Passaggi per il completamento dell'autovalutazione PCI DSS

1. Identificare il questionario SAQ per il proprio ambiente. Per informazioni, consultare il documento *Istruzioni e linee guida per l'autovalutazione* sul sito Web PCI SSC.
2. Accertarsi che il proprio ambiente sia del giusto ambito e che risponda ai criteri di idoneità per il questionario SAQ che si sta utilizzando.
3. Valutare il proprio ambiente per la conformità ai requisiti PCI DSS.
4. Completare tutte le sezioni di questo documento:
  - Sezione 1 (Parti 1 e 2 dell'AOC) - Informazioni sulla valutazione e riepilogo esecutivo
  - Sezione 2 - Questionario di autovalutazione PCI DSS (SAQ D)
  - Sezione 3 (Parti 3 e 4 dell'AOC) - Dettagli su convalida e attestato e piano d'azione per i requisiti non conformi (se applicabile)
5. Inviare il questionario SAQ e l'Attestato di conformità (AOC), insieme ad eventuale altra documentazione richiesta (ad esempio, i rapporti delle scansioni ASV) al proprio acquirente, al marchio di pagamento o ad altra entità richiedente.

## Comprensione del questionario di autovalutazione

Le domande contenute nella colonna "Domanda PCI DSS" del presente questionario di autovalutazione si basano sui requisiti specificati negli standard PCI DSS.

Sono inoltre state fornite risorse aggiuntive a supporto del processo di valutazione che forniscono indicazioni sui requisiti PCI DSS e sulla procedura di compilazione del questionario di autovalutazione. Di seguito è disponibile una panoramica di alcune di queste risorse:

Documento	Include:
PCI DSS <i>(Requisiti PCI DSS e procedure di valutazione della sicurezza)</i>	<ul style="list-style-type: none"> <li>• Istruzioni sulla determinazione dell'ambito</li> <li>• Istruzioni sullo scopo di tutti i requisiti PCI DSS</li> <li>• Dettagli delle procedure di test</li> <li>• Istruzioni sui controlli compensativi</li> </ul>
Documenti relativi a istruzioni e linee guida SAQ	<ul style="list-style-type: none"> <li>• Informazioni su tutti i questionari SAQ e sui relativi criteri di idoneità</li> <li>• Come determinare quale questionario SAQ è adatto</li> </ul>

Documento	Include:
	alla propria azienda
<i>Glossario, abbreviazioni e acronimi PCI DSS e PA-DSS</i>	<ul style="list-style-type: none"> <li>• Descrizioni e definizioni dei termini utilizzati in PCI DSS e nei questionari di autovalutazione</li> </ul>

Queste e altre risorse sono disponibili sul sito Web PCI SSC ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)). Le aziende sono invitate a esaminare gli standard PCI DSS e altri documenti di supporto prima di iniziare una valutazione.

### Test previsti

Le istruzioni fornite nella colonna “Test previsti” si basano sulle procedure di test contenute negli standard PCI DSS e forniscono una descrizione dettagliata dei tipi di attività di test che devono essere eseguiti al fine di verificare la conformità a un requisito. I dettagli completi delle procedure di test per ogni requisito sono disponibili negli standard PCI DSS.

### Completamento del questionario di autovalutazione

Per ogni domanda vengono fornite diverse risposte tra cui scegliere per indicare lo stato della propria azienda in merito al requisito specificato. **È possibile selezionare una sola risposta per ogni domanda.**

Nella tabella riportata di seguito viene fornita una descrizione del significato di ogni risposta:

Risposta	Quando utilizzare questa risposta:
<b>Sì</b>	Il test previsto è stato eseguito e tutti gli elementi del requisito sono stati soddisfatti come indicato.
<b>Sì con CCW</b> (Foglio di lavoro - Controllo compensativo)	<p>Il test previsto è stato eseguito e il requisito risulta soddisfatto grazie all’ausilio di un controllo compensativo.</p> <p>Tutte le risposte di questa colonna richiedono il completamento di un Foglio di lavoro - Controllo compensativo (CCW) presente nell’Appendice B del questionario SAQ.</p> <p>Negli standard PCI DSS vengono fornite tutte le informazioni sull’utilizzo dei controlli compensativi e le istruzioni sulla procedura di completamento del foglio di lavoro.</p>
<b>No</b>	Alcuni o tutti gli elementi del requisito non sono stati soddisfatti, sono in fase di implementazione o richiedono ulteriori test prima di sapere se sono effettivamente in uso.
<b>N/A</b> (non applicabile)	<p>Il requisito non si applica all’ambiente dell’azienda. (Per consultare alcuni esempi, vedere la <i>Guida per la non applicabilità di determinati requisiti specifici</i> riportata di seguito.)</p> <p>Tutte le risposte di questa colonna richiedono una spiegazione di supporto disponibile nell’Appendice C del questionario SAQ.</p>
<b>Non testato</b>	<p>Il requisito non è stato preso in considerazione nella valutazione e non è stato testato in alcun modo. (Vedere <i>Comprendere le differenze tra Non applicabile e Non testato</i> di seguito per alcuni esempi su come utilizzare questa opzione.)</p> <p>Tutte le risposte di questa colonna richiedono una spiegazione di supporto disponibile nell’Appendice D del questionario SAQ.</p>

## Guida per la non applicabilità di determinati requisiti specifici

Sebbene molte aziende che completano il questionario SAQ D debbano convalidare la propria conformità a ogni requisito PCI DSS, alcune aziende con modelli di business molto specifici possono trovare non applicabili alcuni requisiti. Ad esempio, una società che non utilizza una tecnologia wireless in alcun modo non può garantire la conformità ai requisiti indicati nelle sezioni degli standard PCI DSS specifiche per la gestione di tale tecnologia. Analogamente, un'azienda che non memorizza in formato elettronico i dati dei titolari di carta non dovrà convalidare i requisiti relativi alla memorizzazione sicura dei dati dei titolari di carta (ad esempio Requisiti 3.4).

Esempi di requisiti con applicabilità specifica includono:

- Fornire una risposta alle domande specifiche sulla protezione della tecnologia wireless (ad esempio, requisiti 1.2.3, 2.1.1 e 4.1.1) solo se tale tecnologia è disponibile nella propria rete. Tenere presente che occorre comunque fornire una risposta al requisito 11.1 (uso di processi per identificare punti di accesso wireless non autorizzati) anche se la propria rete non prevede la tecnologia wireless, perché il processo rileva eventuali intrusioni o dispositivi non autorizzati che possono essere stati aggiunti a vostra insaputa.
- Fornire una risposta alle domande specifiche sullo delle applicazioni e sul codice protetto (requisiti 6.3 e 6.5), solo se la propria azienda sviluppa applicazioni personalizzate.
- Fornire una risposta alle domande per i requisiti 9.1.1 e 9.3 solo per strutture con "aree sensibili" come definite nel presente documento: per "aree sensibili" si intendono centri dati, aree server e aree che ospitano sistemi di memorizzazione, elaborazione o trasmissione dei dati dei titolari di carta. Ciò esclude le aree in cui sono presenti solo terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio, ma comprende le sale server back-office di negozi di vendita al dettaglio in cui sono memorizzati dati dei titolari di carta e aree di memorizzazione per grandi quantità di tali dati.

Se si ritiene che alcuni requisiti non siano applicabili nel proprio ambiente, selezionare l'opzione "N/A" per il requisito in questione e completare il foglio di lavoro "Spiegazione di non applicabilità" presente nell'Appendice C per ogni voce "N/A".

### **Comprendere la differenza tra Non applicabile e Non testato**

È necessario verificare che i requisiti considerati non applicabili a un ambiente lo siano veramente. Utilizzando l'esempio della tecnologia wireless di cui sopra, affinché un'azienda possa selezionare "N/A" per i requisiti 1.2.3, 2.1.1 e 4.1.1, l'azienda deve prima confermare di non disporre di tecnologie wireless nel proprio CDE o che si colleghino al proprio CDE. Una volta confermato, l'azienda può selezionare "N/A" per i requisiti specifici.

Se un requisito è escluso completamente dalla revisione senza alcuna considerazione sulla sua *eventuale* applicabilità, è necessario selezionare l'opzione "Non testato". Esempi di situazioni in cui si verifica questo fenomeno sono:

- A un'azienda viene richiesto dal proprio acquirente di convalidare un sottoinsieme di requisiti, ad esempio utilizzando un approccio prioritario per la convalida di determinate pietre miliari.
- Un'azienda può desiderare di convalidare un nuovo controllo di sicurezza che incide solo su un sottoinsieme di requisiti, ad esempio l'implementazione di una nuova metodologia di cifratura che richiede la valutazione dei requisiti PCI DSS 2, 3 e 4.
- Un'azienda fornitrice di servizi può offrire un servizio che copre un numero limitato di requisiti PCI DSS, ad esempio un provider di storage fisico può desiderare di convalidare i controlli di sicurezza fisica per il requisito PCI DSS 9 della propria struttura di storage.

In questi scenari, l'azienda intende convalidare solo alcuni requisiti PCI DSS, anche se altri requisiti sono validi per il suo ambiente.

## **Eccezione legale**

Se la propria azienda è soggetta a una restrizione di natura legale che le impedisce di soddisfare un requisito PCI DSS, selezionare la colonna “No” specifica di quel requisito e completare l’attestato corrispondente nella Parte 3.

## Sezione 1 - Informazioni sulla valutazione

### Istruzioni per l'invio

Il presente documento deve essere compilato come dichiarazione dei risultati dell'autovalutazione dell'esercente unitamente a *Requisiti e procedure di valutazione della sicurezza PCI DSS*. Completare tutte le sezioni. L'esercente è tenuto a garantire che ogni sezione sia stata completata dalle parti interessate, come applicabile. Contattare l'acquirente (banca dell'esercente) o i marchi di pagamento per determinare le procedure di reporting e invio.

### Parte 1. Informazioni Esercente e Azienda qualificata per la valutazione (QSA)

#### Parte 1a. Informazioni sull'organizzazione dell'esercente

Ragione sociale:		DBA (doing business as):	
Nome referente:		Mansione:	
Telefono:		E-mail:	
Indirizzo ufficio:		Città:	
Stato/Provincia:		Paese:	CAP:
URL:			

#### Parte 1b. Informazioni sull'azienda qualificata per la valutazione (se applicabile)

Ragione sociale:			
Nome referente QSA principale:		Mansione:	
Telefono:		E-mail:	
Indirizzo ufficio:		Città:	
Stato/Provincia:		Paese:	CAP:
URL:			

### Parte 2. Riepilogo esecutivo

#### Parte 2a. Tipo di esercente (selezionare tutte le risposte pertinenti)

- Rivenditore
  Telecomunicazioni
  Negozi di alimentari e supermercati  
 Distributori di benzina
  E-Commerce
  Ordini via posta/telefono (MOTO)  
 Altro (specificare):

Quali tipi di canali di pagamento offre l'azienda?

- Ordini via posta/telefono (MOTO)  
 E-Commerce  
 Con carta presente (contatto diretto)

Quali sono i canali di pagamento coperti dal presente questionario SAQ?

- Ordini via posta/telefono (MOTO)  
 E-Commerce  
 Con carta presente (contatto diretto)

**Nota:** se la propria azienda dispone di un canale o una procedura di pagamento non inclusi nel presente questionario SAQ, consultare l'acquirente o il marchio di pagamento in merito alla convalida degli altri canali.

### Parte 2b. Descrizione delle attività relative alla carta di pagamento

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

### Parte 2c. Sedi

Elenco dei tipi di struttura (ad esempio, punti vendita, uffici, centri dati, call center ecc.) e riepilogo delle sedi incluse nella revisione PCI DSS.

Tipo di struttura	Numero di strutture di questo tipo	Sedi della struttura (città, paese)
<i>Esempio: punti vendita</i>	3	<i>Boston, MA, Stati Uniti</i>

### Parte 2d. Applicazione di pagamento

L'azienda utilizza una o più applicazioni di pagamento?  Sì  No

Fornire le seguenti informazioni in ordine alle Applicazioni di pagamento utilizzate dalla propria azienda:

Nome applicazione di pagamento	Versione numero	Fornitore dell'applicazione	L'applicazione è inclusa nell'elenco PA-DSS?	Data di scadenza dell'elenco PA-DSS (se applicabile)
			<input type="checkbox"/> Sì <input type="checkbox"/> No	
			<input type="checkbox"/> Sì <input type="checkbox"/> No	
			<input type="checkbox"/> Sì <input type="checkbox"/> No	
			<input type="checkbox"/> Sì <input type="checkbox"/> No	
			<input type="checkbox"/> Sì <input type="checkbox"/> No	

### Parte 2e. Descrizione dell'ambiente

Fornire una descrizione **di alto livello** dell'ambiente coperto da questa valutazione.

*Ad esempio:*

- *Connessioni interne ed esterne all'ambiente dei dati dei titolari di carta.*
- *Componenti di sistema critici interni all'ambiente dei dati dei titolari di carta, ai database, ai server Web ecc. e qualsiasi altro componente di pagamento necessario, come applicabile.*

L'azienda utilizza la segmentazione di rete per definire l'ambito del proprio ambiente PCI

Sì  No

<p>DSS? (Consultare la sezione “Segmentazione di rete” di PCI DSS per indicazioni sulla segmentazione di rete.)</p>	
---	--

**Parte 2f. Provider di servizi di terzi**

<p>L'azienda utilizza un responsabile dell'integrazione e rivenditore qualificati (QIR)?</p> <p>Se sì:</p> <p>Nome dell'azienda QIR:</p> <p>Singolo nome QIR:</p> <p>Descrizione dei servizi forniti dal QIR:</p>	<p><input type="checkbox"/> Sì <input type="checkbox"/> No</p>
---	--

<p>L'azienda condivide i dati dei titolari di carta con provider di servizi di terzi (ad esempio responsabile dell'integrazione e rivenditore qualificati (QIR), gateway, elaboratori pagamenti, provider di servizi di pagamento (PSP), società di hosting Web, agenti per la prenotazione di voli aerei, agenti del programma fedeltà, ecc.)?</p>	<p><input type="checkbox"/> Sì <input type="checkbox"/> No</p>
---	--

**Se sì:**

Nome del provider di servizi:	Descrizione dei servizi forniti:

**Nota:** il Requisito 12.8 si applica a tutte le entità presenti in questo elenco.

## Sezione 2 - Questionario di autovalutazione D per esercenti

**Nota:** le domande seguenti sono numerate in base ai requisiti PCI DSS e alle procedure di test, secondo quanto definito nel documento Requisiti PCI DSS e procedure di valutazione della sicurezza.

Data di completamento dell'autovalutazione:

### Sviluppo e gestione di sistemi e reti sicure

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

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Si	Si con CCW	No	N/A	Non testato
1.1	Sono stati stabiliti e implementati standard di configurazione del firewall e del router tali da includere quanto segue:					
1.1.1	È presente un processo formale per l'approvazione e il test di tutte le connessioni esterne alla rete e le modifiche apportate alla configurazione del firewall e del router?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	(a) È presente un diagramma di rete aggiornato che documenta tutte le connessioni tra ambiente dei dati dei titolari di carta e altre reti, comprese eventuali reti wireless?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) È presente un processo volto a garantire il costante aggiornamento del diagramma?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	(a) È presente un diagramma aggiornato che mostra tutti i flussi dei dati dei titolari di carta sui sistemi e sulle reti?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) È presente un processo volto a garantire il costante aggiornamento del diagramma?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Si	Si con CCW	No	N/A	Non testato
1.1.4	(a) È richiesto e presente un firewall per ogni connessione Internet e tra tutte le zone demilitarizzate (DMZ) e la zona della rete interna?	<ul style="list-style-type: none"> <li>Analizzare gli standard di configurazione del firewall</li> <li>Osservare le configurazioni di rete per verificare che sia presente un firewall</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Il diagramma di rete attuale è coerente con gli standard di configurazione del firewall?	<ul style="list-style-type: none"> <li>Confrontare gli standard di configurazione del firewall per diagramma di rete attuale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	Sono stati assegnati e documentati i gruppi, i ruoli e le responsabilità per la gestione logica dei componenti di rete negli standard di configurazione del firewall e del router?	<ul style="list-style-type: none"> <li>Analizzare gli standard di configurazione di firewall e router</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	(a) Gli standard di configurazione del firewall e del router includono un elenco documentato di servizi, protocolli e porte, comprese la giustificazione e l'approvazione aziendali per ciascuno?	<ul style="list-style-type: none"> <li>Analizzare gli standard di configurazione di firewall e router</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Sono stati identificati tutti i servizi, i protocolli e le porte non sicuri e le funzioni di sicurezza sono state documentate e implementate per ciascuno di essi?	<ul style="list-style-type: none"> <li>Analizzare gli standard di configurazione di firewall e router</li> <li>Esaminare le configurazioni di firewall e router</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.7	(a) Gli standard di configurazione di firewall e router richiedono una revisione dei set di regole del firewall e del router almeno ogni sei mesi?	<ul style="list-style-type: none"> <li>Analizzare gli standard di configurazione di firewall e router</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) La revisione dei set di regole di firewall e router viene effettuata almeno ogni sei mesi?	<ul style="list-style-type: none"> <li>Esaminare la documentazione prodotta dalle revisioni dei firewall</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Si	Si con CCW	No	N/A	Non testato
1.2	Le configurazioni di firewall e router limitano le connessioni tra le reti non attendibili e qualsiasi sistema nell'ambiente dei dati di titolari di carta nel modo seguente:  <b>Nota:</b> una "rete non attendibile" è una qualsiasi rete esterna alle reti che appartengono all'entità sottoposta a revisione e/o che l'entità non è in grado di controllare o gestire.					
1.2.1	(a) Il traffico in entrata e in uscita è limitato a quello indispensabile per l'ambiente dei dati dei titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Il resto del traffico in entrata e in uscita viene negato in modo specifico, ad esempio utilizzando un comando esplicito "deny all" o un comando implicito di negazione dopo un'istruzione "allow".	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	I file di configurazione del router vengono protetti contro l'accesso non autorizzato e vengono sincronizzati, ad esempio la configurazione in esecuzione (o attiva) corrisponde alla configurazione all'avvio (utilizzata in caso di riavvio delle macchine)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Sono stati installati i firewall perimetrali tra le reti wireless e l'ambiente dei dati dei titolari di carta e tali firewall sono stati configurati in modo da negare o controllare (se necessario per gli scopi aziendali) solo il traffico autorizzato tra l'ambiente wireless e l'ambiente dei dati dei titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Si	Si con CCW	No	N/A	Non testato
1.3	È vietato l'accesso pubblico diretto tra Internet e i componenti di sistema nell'ambiente dei dati di titolari di carta, come segue:					
1.3.1	È implementata una zona DMZ per limitare il traffico in entrata ai soli componenti di sistema che forniscono servizi, protocolli e porte autorizzati accessibili pubblicamente?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.2	Il traffico Internet in entrata è stato limitato agli indirizzi IP all'interno della zona DMZ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.3	Sono state implementate delle misure anti-spoofing per rilevare gli indirizzi IP di origine contraffatti e per impedire loro di accedere alla rete? (Ad esempio, bloccare il traffico proveniente da Internet con un indirizzo interno.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.4	Viene autorizzato in modo esplicito il traffico in uscita dall'ambiente dei dati di titolari di carta ad Internet?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.5	Sono consentite nella rete solo le connessioni già stabilite?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.3.6	I componenti di sistema che memorizzano dati dei titolari di carta (come un database) sono collocati in una zona di rete interna, separata dalla zona DMZ e da altre reti non attendibili?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Si	Si con CCW	No	N/A	Non testato
1.3.7 (a) Sono in atto misure volte a impedire la divulgazione di indirizzi IP privati e informazioni di routing ad Internet?  <b>Nota: i metodi per oscurare l'indirizzamento IP possono includere, senza limitazioni:</b> <ul style="list-style-type: none"> <li>NAT (Network Address Translation);</li> <li>posizionamento di server contenenti dati dei titolari di carta dietro server/firewall proxy;</li> <li>rimozione o filtraggio di annunci di instradamento per reti private che utilizzano indirizzamento registrato;</li> <li>uso interno di spazio indirizzi RFC1918 invece degli indirizzi registrati.</li> </ul>	<ul style="list-style-type: none"> <li>Esaminare le configurazioni di firewall e router</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Sono autorizzate eventuali divulgazioni ad entità esterne di indirizzi IP privati e di informazioni di routing?	<ul style="list-style-type: none"> <li>Esaminare le configurazioni di firewall e router</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.4 (a) È stato installato ed è attivo il firewall personale (o funzionalità equivalente) su tutti i dispositivi mobili (inclusi quelli di proprietà dell'azienda e/o dei dipendenti) con connettività a Internet se all'esterno della rete (ad esempio, laptop utilizzati dai dipendenti) e quali vengono utilizzati anche per accedere al CDE?	<ul style="list-style-type: none"> <li>Analizzare le politiche e gli standard di configurazione</li> <li>Esaminare i dispositivi mobili e/o di proprietà dei dipendenti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Il firewall personale (o funzionalità equivalente) è configurato in base a impostazioni specifiche, è in esecuzione in modo attivo e non è modificabile da parte degli utenti di dispositivi mobili e/o di proprietà dei dipendenti?	<ul style="list-style-type: none"> <li>Analizzare le politiche e gli standard di configurazione</li> <li>Esaminare i dispositivi mobili e/o di proprietà dei dipendenti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Si	Si con CCW	No	N/A	Non testato
1.5	Le politiche di sicurezza e le procedure operative per la gestione dei firewall sono: <ul style="list-style-type: none"> <li>▪ documentate;</li> <li>▪ in uso;</li> <li>▪ note a tutte le parti coinvolte?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche di sicurezza e le procedure operative</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
2.1	(a) I valori predefiniti del fornitore vengono sempre modificati prima di installare un sistema in rete? <i>Questo vale per TUTTE le password predefinite, incluse, senza limitazioni, quelle utilizzate da sistemi operativi, software che fornisce servizi di sicurezza, account di applicazioni e sistemi, terminali POS (Point-Of-Sale), applicazioni di pagamento, stringhe di comunità SNMP (Simple Network Management Protocol), ecc.</i>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Esaminare la documentazione del fornitore</li> <li>▪ Osservare le configurazioni di sistema e le impostazioni account</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>				
	(b) Gli account predefiniti non necessari vengono rimossi o disattivati prima dell'installazione di un sistema sulla rete?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Analizzare la documentazione del fornitore</li> <li>▪ Esaminare le configurazioni di sistema e le impostazioni account</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>				
2.1.1	Per gli ambienti wireless connessi all'ambiente dei dati di titolari di carta o che trasmettono tali dati, sono stati modificati tutti i valori predefiniti del fornitore wireless al momento dell'installazione, come segue:						
	(a) Sono state modificate le chiavi di cifratura predefinite al momento dell'installazione e vengono modificate ogni volta che un utente a conoscenza delle chiavi lascia l'azienda o cambia sede?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Analizzare la documentazione del fornitore</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>				
	(b) Le stringhe di comunità SNMP predefinite sui	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le</li> </ul>	<input type="checkbox"/>				

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
dispositivi wireless sono state modificate al momento dell'installazione?	procedure <ul style="list-style-type: none"> <li>▪ Analizzare la documentazione del fornitore</li> <li>▪ Consultare il personale</li> <li>▪ Esaminare le configurazioni del sistema</li> </ul>					
(c) Le password/passphrase predefinite sui punti di accesso sono state modificate al momento dell'installazione?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Consultare il personale</li> <li>▪ Esaminare le configurazioni del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) Il firmware sui dispositivi wireless è aggiornato per supportare la cifratura avanzata per l'autenticazione e la trasmissione su reti wireless?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Analizzare la documentazione del fornitore</li> <li>▪ Esaminare le configurazioni del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(e) Sono state modificate altre impostazioni predefinite del fornitore wireless relative alla sicurezza, se applicabili?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Analizzare la documentazione del fornitore</li> <li>▪ Esaminare le configurazioni del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
2.2 (a) Sono stati sviluppati standard di configurazione per tutti i componenti di sistema e sono coerenti con gli standard di System Hardening che sono accettati dal settore?  <i>Fonti di standard di System Hardening accettati dal settore possono comprendere, senza limitazione, enti quali SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), International Organization for Standardization (ISO) e Center for Internet Security (CIS).</i>	<ul style="list-style-type: none"> <li>▪ Analizzare gli standard di configurazione del sistema</li> <li>▪ Analizzare gli standard di hardening accettati dal settore</li> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Sono aggiornati gli standard di configurazione del sistema in caso di identificazione di nuovi problemi di vulnerabilità, secondo quanto definito al Requisito 6.1?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Quando si configurano nuovi sistemi, vengono applicati gli standard di configurazione del sistema?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
(d) Gli standard di configurazione del sistema comprendono quanto segue: <ul style="list-style-type: none"> <li>• Modifica di tutti i valori predefiniti del fornitore ed eliminazione di account predefiniti non necessari?</li> <li>• Implementazione di una sola funzione principale per server per impedire la coesistenza sullo stesso server di funzioni che richiedono livelli di sicurezza diversi?</li> <li>• Abilitazione di servizi, protocolli, daemon, ecc. necessari, come richiesto per la funzione del sistema?</li> <li>• Implementazione di funzioni di sicurezza aggiuntive per servizi, protocolli o daemon necessari considerati non sicuro?</li> <li>• Configurazione di parametri di sicurezza del sistema per evitare un uso improprio?</li> <li>• Rimozione di tutta la funzionalità non necessaria, ad esempio script, driver, funzioni, sottosistemi, file system e server Web non utilizzati?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare gli standard di configurazione del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.1 (a) È implementata una sola funzione primaria per server, per evitare la coesistenza sullo stesso server di funzioni che richiedono livelli di sicurezza diversi?  <i>Ad esempio, server Web, database server e DNS devono essere implementati su server separati.</i>	<ul style="list-style-type: none"> <li>▪ Esaminare le configurazioni del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) In caso di utilizzo di tecnologie di virtualizzazione, viene implementata una sola funzione primaria per dispositivo o componente di sistema virtuale?	<ul style="list-style-type: none"> <li>▪ Esaminare le configurazioni del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
2.2.2 (a) Sono abilitati solo i servizi, protocolli, daemon ecc. necessari come richiesto per la funzione del sistema (sono disabilitati i servizi e protocolli che non sono strettamente necessari per eseguire la funzione specifica di un dispositivo)?	<ul style="list-style-type: none"> <li>Analizzare gli standard di configurazione</li> <li>Esaminare le configurazioni del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.2 (b) Tutti i servizi, i daemon o i protocolli non sicuri attivi sono giustificati a fronte di standard di configurazione documentati?	<ul style="list-style-type: none"> <li>Analizzare gli standard di configurazione</li> <li>Consultare il personale</li> <li>Esaminare le impostazioni di configurazione</li> <li>Confrontare i servizi attivati ecc. in base alle giustificazioni documentate</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.2.3 Sono state documentate e implementate le funzioni di sicurezza aggiuntive per servizi, protocolli o daemon necessari considerati non sicuri? <i>Nota: laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.</i>	<ul style="list-style-type: none"> <li>Analizzare gli standard di configurazione</li> <li>Esaminare le impostazioni di configurazione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
2.2.4	(a) Gli amministratori di sistema e/o il personale che si occupa della configurazione dei componenti di sistema conoscono in modo approfondito le impostazioni dei parametri di sicurezza per i componenti di sistema in questione?	▪ Consultare il personale	<input type="checkbox"/>				
	(b) Le impostazioni dei parametri di sicurezza comuni del sistema sono comprese negli standard di configurazione del sistema?	▪ Analizzare gli standard di configurazione del sistema	<input type="checkbox"/>				
	(c) Le impostazioni dei parametri di sicurezza sono impostate correttamente sui componenti di sistema?	<ul style="list-style-type: none"> <li>▪ Esaminare i componenti di sistema</li> <li>▪ Esaminare le impostazioni dei parametri di sicurezza</li> <li>▪ Confrontare le impostazioni degli standard di configurazione del sistema</li> </ul>	<input type="checkbox"/>				
2.2.5	(a) È stata rimossa tutta la funzionalità non necessaria, ad esempio script, driver, funzioni, sottosistemi, file system e server Web non utilizzati?	▪ Esaminare i parametri di sicurezza sui componenti di sistema	<input type="checkbox"/>				
	(b) Tutte le funzioni abilitate sono documentate e supportano una configurazione sicura?	<ul style="list-style-type: none"> <li>▪ Analizzare la documentazione</li> <li>▪ Esaminare i parametri di sicurezza sui componenti di sistema</li> </ul>	<input type="checkbox"/>				
	(c) Sui componenti di sistema sono presenti solo funzionalità documentate?	<ul style="list-style-type: none"> <li>▪ Analizzare la documentazione</li> <li>▪ Esaminare i parametri di sicurezza sui componenti di sistema</li> </ul>	<input type="checkbox"/>				
2.3	<p>È stata eseguita la cifratura dell'accesso amministrativo non da console come segue:</p> <p><b>Nota:</b> laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.</p>						

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
	(a) È stata eseguita la cifratura di tutto l'accesso amministrativo non da console con crittografia avanzata? Viene richiamato un sistema di cifratura avanzata prima della richiesta della password dell'amministratore?	<ul style="list-style-type: none"> <li>▪ Esaminare i componenti di sistema</li> <li>▪ Esaminare le configurazioni del sistema</li> <li>▪ Osservare un accesso amministratore</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) I servizi di sistema e i file dei parametri sono configurati in modo da impedire l'uso di Telnet e di altri comandi di accesso remoto non sicuri?	<ul style="list-style-type: none"> <li>▪ Esaminare i componenti di sistema</li> <li>▪ Esaminare servizi e file</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) L'accesso amministratore alle interfacce di gestione basate su Web è cifrato con un metodo di crittografia avanzata?	<ul style="list-style-type: none"> <li>▪ Esaminare i componenti di sistema</li> <li>▪ Osservare un accesso amministratore</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(d) Per la tecnologia in uso, viene implementata una crittografia avanzata in conformità alle migliori pratiche di settore e/o alle raccomandazioni del fornitore?	<ul style="list-style-type: none"> <li>▪ Esaminare i componenti di sistema</li> <li>▪ Analizzare la documentazione del fornitore</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.4	(a) Viene mantenuto un inventario per i componenti dei sistemi che rientrano nell'ambito degli standard PCI DSS, compreso un elenco di componenti hardware e software e una descrizione della funzione/dell'uso di ciascuno?	<ul style="list-style-type: none"> <li>▪ Esaminare l'inventario del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) L'inventario documentato viene aggiornato?	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Le politiche di sicurezza e le procedure operative per la gestione delle impostazioni predefinite del fornitore e dei parametri di sicurezza sono: <ul style="list-style-type: none"> <li>▪ documentate;</li> <li>▪ in uso;</li> <li>▪ note a tutte le parti coinvolte?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche di sicurezza e le procedure operative</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.6	<i>Questo requisito si applica solo ai provider di servizi.</i>						

## Protezione dei dati dei titolari di carta

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

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Si con CCW	No	N/A	Non testato
3.1	Le politiche, le procedure e i processi per la conservazione e l'eliminazione dei dati sono implementati come indicato di seguito:					
(a)	La quantità dei dati memorizzati e il tempo di conservazione sono limitati in base alle esigenze aziendali, legali e/o legislative?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b)	Sono stati adottati processi definiti per l'eliminazione sicura dei dati dei titolari di carta quando questi dati non sono più necessari per scopi legali, legislativi e/o aziendali?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c)	Sono presenti requisiti specifici di conservazione dei dati dei titolari di carta? <i>Ad esempio, è necessario conservare i dati dei titolari di carta per un periodo X per scopi aziendali Y.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d)	È presente un processo trimestrale per identificare ed eliminare in modo sicuro i dati dei titolari di carta memorizzati che superano i requisiti di conservazione definiti?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(e)	Tutti i dati dei titolari di carta memorizzati soddisfano i requisiti contenuti nella politica di conservazione dei dati?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
3.2	(a) Questa procedura di test si applica solo agli emittenti.						
	(b) Questa procedura di test si applica solo agli emittenti.						
	(c) I dati sensibili di autenticazione vengono eliminati o resi non recuperabili dopo il completamento del processo di autorizzazione?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	(d) Tutti i sistemi aderiscono ai seguenti requisiti relativi alla non memorizzazione di dati sensibili di autenticazione dopo l'autorizzazione (anche se cifrati)?						
3.2.1	<p>L'intero contenuto delle tracce della striscia magnetica (presente sul retro della carta, contenuto in un chip o in altro luogo) non viene memorizzato dopo l'autorizzazione?</p> <p><i>Questi dati sono denominati anche traccia completa, traccia, traccia 1, traccia 2 e dati della striscia magnetica.</i></p> <p><b>Nota:</b> nel normale svolgimento delle attività, è possibile che sia necessario conservare i seguenti elementi di dati della striscia magnetica:</p> <ul style="list-style-type: none"> <li>Nome del titolare della carta</li> <li>PAN (Primary Account Number)</li> <li>Data di scadenza</li> <li>Codice di servizio</li> </ul> <p><i>Per ridurre al minimo il rischio, memorizzare solo gli elementi di dati necessari per l'azienda.</i></p>	<ul style="list-style-type: none"> <li>Esaminare le origini dei dati tra cui: <ul style="list-style-type: none"> <li>Dati di transazioni in entrata</li> <li>Tutti i registri</li> <li>File di cronologia</li> <li>File di traccia</li> <li>Schema del database</li> <li>Contenuto del database</li> </ul> </li> </ul>	<input type="checkbox"/>				

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
3.2.2	Il codice o il valore di verifica della carta (numero di tre o quattro cifre impresso sulla parte anteriore o sul retro di una carta di pagamento) non viene memorizzato dopo l'autorizzazione?	<ul style="list-style-type: none"> <li>▪ Esaminare le origini dei dati tra cui:               <ul style="list-style-type: none"> <li>• Dati di transazioni in entrata</li> <li>• Tutti i registri</li> <li>• File di cronologia</li> <li>• File di traccia</li> <li>• Schema del database</li> <li>• Contenuto del database</li> </ul> </li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Il numero di identificazione personale (PIN) o il blocco PIN cifrato non viene memorizzato dopo l'autorizzazione?	<ul style="list-style-type: none"> <li>▪ Esaminare le origini dei dati tra cui:               <ul style="list-style-type: none"> <li>• Dati di transazioni in entrata</li> <li>• Tutti i registri</li> <li>• File di cronologia</li> <li>• File di traccia</li> <li>• Schema del database</li> <li>• Contenuto del database</li> </ul> </li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.3	<p>Il PAN completo viene mascherato quando visualizzato (non devono essere visibili più di sei cifre all'inizio e quattro cifre alla fine) per renderlo visibile solo al personale autorizzato?</p> <p><b>Nota:</b> questo requisito non sostituisce i requisiti più rigorosi per la visualizzazione dei dati dei titolari di carta, ad esempio requisiti legali o del marchio di carta di pagamento per ricevute di punti di vendita (POS).</p>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Analizzare i ruoli che hanno la necessità di accedere alle visualizzazioni del PAN completo</li> <li>▪ Esaminare le configurazioni del sistema</li> <li>▪ Osservare le visualizzazioni del PAN</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
<p>3.4 Il numero PAN è reso illeggibile ovunque memorizzato (inclusi repository dei dati, supporti digitali portatili, supporti di backup e i log di audit) utilizzando uno dei seguenti approcci?</p> <ul style="list-style-type: none"> <li>▪ Hash unidirezionali basati su crittografia avanzata (l'hash deve essere dell'intero PAN)</li> <li>▪ Troncatura (non si può usare l'hashing per sostituire la parte troncata del PAN)</li> <li>▪ Token e pad indicizzati (i pad devono essere custoditi in un luogo sicuro)</li> <li>▪ Crittografia avanzata con relativi processi e procedure di gestione delle chiavi.</li> </ul> <p><i>Nota: per un utente non autorizzato è relativamente facile ricostruire i dati PAN originali se ha accesso alla versione troncata e hash del PAN. Nel caso in cui la versione troncata e quella hash dello stesso PAN siano generate presenti nell'ambiente di un'entità, andrebbero predisposti ulteriori controlli per verificare che non sia possibile correlare la versione troncata e hash per ricostruire il PAN originale.</i></p>	<ul style="list-style-type: none"> <li>▪ Esaminare la documentazione del fornitore</li> <li>▪ Esaminare i repository di dati</li> <li>▪ Esaminare i supporti rimovibili</li> <li>▪ Esaminare i log di audit, inclusi i log delle applicazioni di pagamento</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<p>3.4.1 Se si utilizza la cifratura su disco (anziché la cifratura del database a livello di file o colonna), l'accesso viene gestito come segue:</p> <p><i>Nota: questo requisito si applica in aggiunta a tutti gli altri requisiti di gestione delle chiavi e di cifratura PCI DSS.</i></p> <p>(a) L'accesso logico ai file system cifrati è gestito in modo separato e indipendente dai meccanismi nativi di controllo dell'accesso e autenticazione del sistema operativo (ad esempio, evitando di utilizzare i database di account utente locali)?</p>	<ul style="list-style-type: none"> <li>▪ Esaminare le configurazioni del sistema</li> <li>▪ Osservare il processo di autenticazione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
	(b) Le chiavi crittografiche sono memorizzate in modo sicuro (ad esempio, su un supporto rimovibile adeguatamente protetto con controlli di accesso rigorosi)?	<ul style="list-style-type: none"> <li>Osservare i processi</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) I dati dei titolari di carta su supporti rimovibili sono cifrati in ogni posizione di memorizzazione? <i>Nota: se la cifratura del disco non è utilizzata per cifrare supporti rimovibili, è necessario rendere illeggibili i dati memorizzati sul supporto in questione utilizzando altri metodi.</i>	<ul style="list-style-type: none"> <li>Esaminare le configurazioni del sistema</li> <li>Osservare i processi</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Le chiavi utilizzate per garantire la protezione dei dati di titolari di carta memorizzati da divulgazione e uso improprio sono protette come segue: <i>Nota: questo requisito si applica alle chiavi utilizzate per cifrare i dati dei titolari di carta memorizzati e alle chiavi di cifratura delle chiavi (KEK) utilizzate per proteggere le chiavi di cifratura dei dati. Tali KEK devono essere avanzate almeno quanto la chiave di cifratura dei dati.</i>						
3.5.1	<i>Questo requisito si applica solo ai provider di servizi.</i>						
3.5.2	L'accesso alle chiavi utilizzate per la crittografia è limitato al minor numero possibile di persone necessarie?	<ul style="list-style-type: none"> <li>Esaminare gli elenchi di accesso utente</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
3.5.3 Le chiavi di crittografia segrete e private vengono utilizzate per cifrare/decifrare costantemente i dati dei titolari di carta in uno (o più) dei seguenti modi? <ul style="list-style-type: none"> <li>▪ Cifrate con chiave KEK avanzata almeno quanto la chiave di cifratura dei dati che viene memorizzata separatamente dalle chiavi di cifratura dei dati</li> <li>▪ Interne a un dispositivo crittografico protetto (come un modulo di sicurezza (host) hardware (HSM) o un dispositivo di punto di interazione approvato PTS)</li> <li>▪ Come almeno due componenti o condivisioni di chiavi a lunghezza integrale, in conformità a un metodo accettato nel settore</li> </ul> <p><i>Nota: non è necessario memorizzare le chiavi pubbliche in uno di questi moduli.</i></p>	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure documentate</li> <li>▪ Esaminare le configurazioni di sistema e i luoghi di conservazione delle chiavi, incluse le chiavi KEK</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.5.4 Le chiavi utilizzate per la crittografia sono custodite nel minor numero possibile di luoghi?	<ul style="list-style-type: none"> <li>▪ Esaminare i luoghi di conservazione delle chiavi</li> <li>▪ Osservare i processi</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6 (a) Tutti i processi e le procedure di gestione delle chiavi di crittografia utilizzati per la cifratura dei dati di titolari di carta sono completamente documentati e implementati?	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure di gestione delle chiavi</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) <i>Questa procedura di test si applica solo ai provider di servizi.</i>						
(c) I processi e le procedure per la gestione delle chiavi sono implementati in modo da rendere necessario quanto segue:						
3.6.1 Le procedure per le chiavi di crittografia comprendono la generazione di chiavi avanzate?	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure di gestione delle chiavi</li> <li>▪ Osservare il metodo di generazione delle chiavi</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
3.6.2	Le procedure per le chiavi di crittografia comprendono la distribuzione di chiavi di crittografia sicure?	<ul style="list-style-type: none"> <li>Analizzare le procedure di gestione delle chiavi</li> <li>Osservare le procedure di distribuzione di chiavi</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.3	Le procedure per le chiavi di crittografia comprendono la memorizzazione di chiavi di crittografia sicure?	<ul style="list-style-type: none"> <li>Analizzare le procedure di gestione delle chiavi</li> <li>Osservare il metodo di conservazione sicura delle chiavi</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4	Le procedure per le chiavi di crittografia comprendono modifiche delle chiavi di crittografia per le chiavi giunte al termine del loro periodo di validità (ad esempio, una volta trascorso un periodo di tempo definito e/o dopo la produzione da parte di una determinata chiave di una quantità definita di testo di cifratura), come specificato dal fornitore dell'applicazione associato o dal proprietario delle chiavi, ed in base alle linee guida ed alle migliori pratiche del settore (ad esempio, NIST Special Publication 800-57)?	<ul style="list-style-type: none"> <li>Analizzare le procedure di gestione delle chiavi</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5	(a) Le procedure per chiavi di crittografia comprendono il ritiro o la sostituzione (ad esempio: archiviazione, distruzione e/o revoca) delle chiavi di crittografia in caso di indebolimento dell'integrità della chiave (ad esempio, partenza di un dipendente a conoscenza di chiavi con testo in chiaro)?	<ul style="list-style-type: none"> <li>Analizzare le procedure di gestione delle chiavi</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Le procedure per le chiavi di crittografia comprendono la sostituzione di chiavi potenzialmente o effettivamente compromesse?	<ul style="list-style-type: none"> <li>Analizzare le procedure di gestione delle chiavi</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) In caso di conservazione di chiavi di crittografia ritirate o sostituite, queste chiavi vengono usate solo per fini di decifratura o verifica e non usate per operazioni di cifratura?	<ul style="list-style-type: none"> <li>Analizzare le procedure di gestione delle chiavi</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
3.6.6 Se si utilizzano le operazioni di gestione delle chiavi in chiaro, le procedure relative alle chiavi di crittografia includono “split knowledge” e controllo duale delle chiavi di crittografia, come segue: <ul style="list-style-type: none"> <li>▪ Le procedure di “split knowledge” richiedono che i componenti principali siano controllati da almeno due utenti che conoscono soltanto i relativi componenti principali?</li> </ul> E <ul style="list-style-type: none"> <li>▪ Le procedure di controllo duale richiedono che almeno due utenti effettuino operazioni di gestione delle chiavi e nessuno abbia accesso ai materiali di autenticazione (ad esempio, password o chiavi) dell'altro.</li> </ul> <p><i>Nota: esempi di operazioni manuali di gestione delle chiavi includono, senza limitazioni: la generazione, la trasmissione, il caricamento, la memorizzazione e la distruzione delle chiavi.</i></p>	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure di gestione delle chiavi</li> <li>▪ Consultare il personale e/o</li> <li>▪ Osservare i processi</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.7 Le procedure per le chiavi di crittografia comprendono la prevenzione di tentativi di sostituzione non autorizzata delle chiavi?	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure</li> <li>▪ Consultare il personale e/o</li> <li>▪ Osservare i processi</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8 Ai custodi delle chiavi viene richiesto di riconoscere in modo formale (in forma scritta o elettronica) che accettano e confermano di conoscere le proprie responsabilità come custodi delle chiavi?	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure</li> <li>▪ Analizzare la documentazione o altra prova</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.7 Le politiche di sicurezza e le procedure operative per la protezione dei dati dei titolari di carta sono: <ul style="list-style-type: none"> <li>▪ documentate;</li> <li>▪ in uso;</li> <li>▪ note a tutte le parti coinvolte?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche di sicurezza e le procedure operative</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### Requisito 4 - Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Si	Si con CCW	No	N/A	Non testato
4.1 (a) I protocolli di sicurezza e di crittografia avanzata sono stati utilizzati per proteggere i dati sensibili dei titolari di carta durante la trasmissione su reti pubbliche e aperte? <i>Nota: laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.</i> <i>Esempi di reti pubbliche e aperte includono, senza limitazioni: Internet, tecnologie wireless, (compresi 802.11 e Bluetooth), tecnologie cellulari (ad es. le comunicazioni Global System for Mobile, GSM), CDMA (Code Division Multiple Access) e GPRS (General Packet Radio Service).</i>	<ul style="list-style-type: none"> <li>Analizzare gli standard documentati</li> <li>Analizzare le politiche e le procedure</li> <li>Analizzare tutte località in cui si trasmettono o ricevono i dati dei titolari di carta</li> <li>Esaminare le configurazioni del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Vengono accettati solo certificati e/o chiavi affidabili?	<ul style="list-style-type: none"> <li>Osservare le trasmissioni in ingresso e in uscita</li> <li>Esaminare le chiavi e i certificati</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Sono implementati protocolli di sicurezza per utilizzare solo configurazioni sicure e non supportare versioni o configurazioni non sicure?	<ul style="list-style-type: none"> <li>Esaminare le configurazioni del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) Viene implementato il livello di crittografia corretto per la metodologia in uso (controllare i suggerimenti, le pratiche consigliate del fornitore)?	<ul style="list-style-type: none"> <li>Analizzare la documentazione del fornitore</li> <li>Esaminare le configurazioni del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(e) Per le implementazioni TLS, è abilitato TLS durante la trasmissione o la ricezione dei dati dei titolari di carta? <i>Ad esempio, per le implementazioni basate su browser:</i> <ul style="list-style-type: none"> <li>"HTTPS" viene visualizzato come protocollo dell'URL del browser;</li> <li>i dati dei titolari di carta vengono richiesti solo se "HTTPS" viene visualizzato come parte dell'URL.</li> </ul>	<ul style="list-style-type: none"> <li>Esaminare le configurazioni del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Si	Si con CCW	No	N/A	Non testato
4.1.1	Le migliori pratiche di settore sono state utilizzate per implementare la cifratura avanzata per l'autenticazione e la trasmissione per le reti wireless che trasmettono i dati dei titolari di carta o connesse all'ambiente dei dati dei titolari di carta?  <div style="background-color: #cccccc; height: 15px; width: 100%;"></div>	<ul style="list-style-type: none"> <li>▪ Analizzare gli standard documentati</li> <li>▪ Analizzare le reti wireless</li> <li>▪ Esaminare le impostazioni di configurazione del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.2	(a) I PAN sono resi illeggibili o sicuri con crittografia avanzata ogni volta che vengono inviati utilizzando tecnologie di messaggistica degli utenti finali (ad esempio e-mail, messaggistica istantanea, SMS, chat, ecc.)?	<ul style="list-style-type: none"> <li>▪ Osservare i processi</li> <li>▪ Analizzare le trasmissioni in uscita</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Sono in atto politiche in cui viene indicato che i PAN non protetti non si devono inviare mediante tecnologie di messaggistica degli utenti finali?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Le politiche di sicurezza e le procedure operative per la cifratura delle trasmissioni dei dati dei titolari di carta sono: <ul style="list-style-type: none"> <li>▪ documentate;</li> <li>▪ in uso;</li> <li>▪ note a tutte le parti coinvolte?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche di sicurezza e le procedure operative</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Utilizzare un programma per la gestione delle vulnerabilità

### Requisito 5 - Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Si	Si con CCW	No	N/A	Non testato
5.1	È stato installato un software antivirus su tutti i sistemi comunemente colpiti da software dannoso?	<ul style="list-style-type: none"> <li>Esaminare le configurazioni del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Tutti i programmi antivirus sono in grado di rilevare, rimuovere e proteggere da tutti i tipi conosciuti di software dannoso (ad esempio virus, cavalli di Troia, worm, spyware, adware e rootkit)?	<ul style="list-style-type: none"> <li>Analizzare la documentazione del fornitore</li> <li>Esaminare le configurazioni del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Vengono eseguite valutazioni periodiche per identificare e valutare l'evoluzione delle minacce malware e confermare se i sistemi considerati in genere non colpiti dal software dannoso continuano a essere sicuri?	<ul style="list-style-type: none"> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Tutti i meccanismi antivirus sono mantenuti come segue:						
	(a) Il software antivirus e le definizioni sono aggiornati?	<ul style="list-style-type: none"> <li>Esaminare le politiche e le procedure</li> <li>Esaminare le configurazioni antivirus, inclusa l'installazione principale</li> <li>Esaminare i componenti di sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Sono attivati e vengono eseguiti aggiornamenti automatici e scansioni periodiche?	<ul style="list-style-type: none"> <li>Esaminare le configurazioni antivirus, inclusa l'installazione principale</li> <li>Esaminare i componenti di sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Tutti i meccanismi antivirus generano log di audit e, questi log sono conservati in base al Requisito 10.7 PCI DSS?	<ul style="list-style-type: none"> <li>Esaminare le configurazioni antivirus</li> <li>Analizzare i processi di conservazione dei log</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Si	Si con CCW	No	N/A	Non testato
5.3	<p>Tutti i meccanismi antivirus sono:</p> <ul style="list-style-type: none"> <li>▪ Attivamente in esecuzione?</li> <li>▪ Non disattivabili o modificabili dagli utenti?</li> </ul> <p><i>Nota: è possibile disattivare temporaneamente le soluzioni antivirus solo in caso di esigenza tecnica legittima, come autorizzato dalla direzione per ogni singolo caso. Se è necessario disattivare la protezione antivirus per un motivo specifico, è opportuno essere autorizzati formalmente. Potrebbe essere necessario implementare ulteriori misure di sicurezza per il periodo di tempo in cui la protezione antivirus non è attiva.</i></p>	<ul style="list-style-type: none"> <li>▪ Esaminare le configurazioni antivirus</li> <li>▪ Esaminare i componenti di sistema</li> <li>▪ Osservare i processi</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.4	<p>Le politiche di sicurezza e le procedure operative per la protezione dei sistemi contro il malware sono:</p> <ul style="list-style-type: none"> <li>▪ documentate;</li> <li>▪ in uso;</li> <li>▪ note a tutte le parti coinvolte?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche di sicurezza e le procedure operative</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Requisito 6 - Sviluppare e gestire sistemi e applicazioni protette

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
<p>6.1 È presente un processo per individuare vulnerabilità alla sicurezza, incluso quanto segue:</p> <ul style="list-style-type: none"> <li>Utilizzo di fonti esterne attendibili di informazioni sulle vulnerabilità?</li> <li>Assegnazione di una classificazione dei rischi alle vulnerabilità che include l'identificazione di tutte le vulnerabilità ad "alto rischio" e "critiche"?</li> </ul> <p><b>Nota:</b> le classificazioni dei rischi devono essere basate sulle migliori pratiche di settore nonché sulla valutazione del potenziale impatto. Ad esempio, i criteri per la classificazione delle vulnerabilità possono tenere in considerazione il punteggio base CVSS e/o la classificazione del fornitore e/o il tipo di sistemi interessati.</p> <p><i>I metodi per la valutazione delle vulnerabilità e l'assegnazione delle valutazioni dei rischi variano in base all'ambiente aziendale e alla strategia di valutazione dei rischi. Le classificazioni dei rischi devono almeno identificare tutte le vulnerabilità ad "alto rischio" per l'ambiente. Oltre alla classificazione dei rischi, le vulnerabilità possono essere considerate "critiche" se rappresentano una minaccia imminente per l'ambiente, influiscono sui sistemi critici e/o comportano una potenziale compromissione se non risolte. Esempi di sistemi critici includono sistemi di sicurezza, dispositivi e sistemi rivolti al pubblico, database e altri sistemi che memorizzano, elaborano o trasmettono i dati dei titolari di carta.</i></p>	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure</li> <li>Consultare il personale</li> <li>Osservare i processi</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
6.2	(a) Tutti i componenti di sistema e il software sono protetti dalle vulnerabilità note mediante l'installazione delle patch di sicurezza dei fornitori?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure</li> </ul>	<input type="checkbox"/>				
	(b) Sono state installate patch di protezione critiche entro un mese dal relativo rilascio? <i>Nota: le patch di sicurezza critiche vanno identificate in conformità al processo di classificazione dei rischi definito nel Requisito 6.1.</i>	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure</li> <li>Esaminare i componenti di sistema</li> <li>Confrontare elenco delle patch di sicurezza installate con gli elenchi delle ultime patch del fornitore</li> </ul>	<input type="checkbox"/>				
6.3	(a) I processi di sviluppo del software si fondano su migliori pratiche e/o standard di settore?	<ul style="list-style-type: none"> <li>Analizzare i processi di sviluppo del software</li> <li>Osservare i processi</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>				
	(b) La sicurezza delle informazioni è compresa per l'intera durata del ciclo di sviluppo del software?	<ul style="list-style-type: none"> <li>Analizzare i processi di sviluppo del software</li> <li>Osservare i processi</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>				
	(c) Le applicazioni software sono sviluppate in conformità agli standard PCI DSS (ad esempio autenticazione e registrazione sicure)?	<ul style="list-style-type: none"> <li>Analizzare i processi di sviluppo del software</li> <li>Osservare i processi</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>				
	(d) I processi di sviluppo software garantiscono quanto segue ai punti 6.3.1-6.3.2:						
6.3.1	Gli account, gli ID utenti e le password di sviluppo, test e/o applicazioni personalizzate vengono rimossi prima dell'attivazione delle applicazioni o del loro rilascio agli utenti?	<ul style="list-style-type: none"> <li>Analizzare i processi di sviluppo del software</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>				

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
<p>6.3.2 Il codice personalizzato viene rivisto prima del rilascio per la produzione o per i clienti per identificare eventuali vulnerabilità del codice (mediante processi manuali o automatici) come segue:</p> <ul style="list-style-type: none"> <li>▪ Le modifiche del codice sono analizzate da utenti singoli diversi dall'autore del codice originario e da utenti esperti di tecniche di analisi del codice e pratiche di codifica sicure?</li> <li>▪ Le analisi del codice garantiscono che il codice venga sviluppato in base a linee guida di codifica sicure?</li> <li>▪ Le correzioni appropriate vengono implementate prima del rilascio?</li> <li>▪ I risultati dell'analisi del codice vengono esaminati e approvati dal management prima del rilascio?</li> </ul> <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. Le analisi del codice possono essere condotte da personale interno preparato o da terze parti. Le applicazioni Web rivolte al pubblico sono anche soggette a controlli aggiuntivi, per risolvere le minacce costanti e le vulnerabilità dopo l'implementazione, secondo quanto definito nel Requisito 6.6 PCI DSS.</i></p>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Consultare il personale</li> <li>▪ Esaminare le modifiche recenti e modificare i record</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4	I processi e le procedure di controllo delle modifiche sono seguiti per tutte le modifiche apportate ai componenti di sistema per comprendere quanto segue:					
6.4.1	<p>(a) Gli ambienti di sviluppo/test sono separati dall'ambiente di produzione?</p> <ul style="list-style-type: none"> <li>▪ Analizzare i processi e le procedure di controllo delle modifiche</li> <li>▪ Esaminare la documentazione di rete e le configurazioni del dispositivo di rete</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
	(b) È stato adottato un controllo degli accessi per favorire la separazione tra gli ambienti di sviluppo/test e gli ambienti di produzione?	<ul style="list-style-type: none"> <li>▪ Analizzare i processi e le procedure di controllo delle modifiche</li> <li>▪ Esaminare le impostazioni di controllo dell'accesso</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.2	Esiste una separazione di responsabilità tra il personale assegnato agli ambienti di sviluppo/test e il personale assegnato all'ambiente di produzione?	<ul style="list-style-type: none"> <li>▪ Analizzare i processi e le procedure di controllo delle modifiche</li> <li>▪ Osservare i processi</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.3	I dati di produzione (PAN attivi) <b>non</b> vengono utilizzati per le attività di test o sviluppo?	<ul style="list-style-type: none"> <li>▪ Analizzare i processi e le procedure di controllo delle modifiche</li> <li>▪ Osservare i processi</li> <li>▪ Consultare il personale</li> <li>▪ Esaminare i dati del test</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.4	Vengono rimossi dai componenti di sistema account e dati di test prima che il sistemi diventi attivo/entri in produzione?	<ul style="list-style-type: none"> <li>▪ Analizzare i processi e le procedure di controllo delle modifiche</li> <li>▪ Osservare i processi</li> <li>▪ Consultare il personale</li> <li>▪ Esaminare i sistemi di produzione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
6.4.5 (a) Le procedure di controllo delle modifiche sono documentate e richiedono quanto segue? <ul style="list-style-type: none"> <li>documentazione dell'impatto;</li> <li>approvazione documentata del controllo delle modifiche prodotta da parti autorizzate;</li> <li>test della funzionalità per verificare che la modifica non influisca negativamente sulla sicurezza del sistema;</li> <li>procedure di back-out.</li> </ul>	<ul style="list-style-type: none"> <li>Analizzare i processi e le procedure di controllo delle modifiche</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) I seguenti fattori vengono richiesti e documentati per tutte le modifiche:						
6.4.5.1 Documentazione dell'impatto?	<ul style="list-style-type: none"> <li>Tenere traccia delle modifiche per aggiornare la documentazione di controllo</li> <li>Esaminare la documentazione di controllo delle modifiche</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.5.2 Approvazione documentata delle parti autorizzate?	<ul style="list-style-type: none"> <li>Tenere traccia delle modifiche per aggiornare la documentazione di controllo</li> <li>Esaminare la documentazione di controllo delle modifiche</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.5.3 (a) Test della funzionalità per verificare che la modifica non influisca negativamente sulla sicurezza del sistema?	<ul style="list-style-type: none"> <li>Tenere traccia delle modifiche per aggiornare la documentazione di controllo</li> <li>Esaminare la documentazione di controllo delle modifiche</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Per le modifiche del codice personalizzate, test degli aggiornamenti per verificare la conformità al Requisito 6.5 PCI DSS prima del rilascio in produzione?	<ul style="list-style-type: none"> <li>Tenere traccia delle modifiche per aggiornare la documentazione di controllo</li> <li>Esaminare la documentazione di controllo delle modifiche</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
6.4.5.4	Procedure di back-out?	<ul style="list-style-type: none"> <li>▪ Tenere traccia delle modifiche per aggiornare la documentazione di controllo</li> <li>▪ Esaminare la documentazione di controllo delle modifiche</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.4.6	Al completamento di una modifica significativa, tutti i requisiti PCI DSS rilevanti sono implementati su tutte le reti e tutti i sistemi nuovi o modificati e la documentazione viene aggiornata come applicabile?  <i><b>Nota:</b> questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.</i>	<ul style="list-style-type: none"> <li>▪ Tenere traccia delle modifiche per aggiornare la documentazione di controllo</li> <li>▪ Esaminare la documentazione di controllo delle modifiche</li> <li>▪ Consultare il personale</li> <li>▪ Osservare le reti o i sistemi interessati</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
6.5	(a) I processi di sviluppo software si occupano delle vulnerabilità di codifica comuni?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Gli sviluppatori vengono formati almeno una volta all'anno sulle tecniche di codifica sicure aggiornate, inclusi i metodi per evitare le vulnerabilità di codifica comuni?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Le applicazioni vengono sviluppate in base a linee guida di codifica sicura per proteggere le applicazioni quanto meno dalle seguenti vulnerabilità:  <b>Nota:</b> le vulnerabilità elencate dal punto 6.5.1 al punto 6.5.10 erano presenti nelle migliori pratiche di settore al momento della pubblicazione di questa versione dello standard PCI DSS. Tuttavia, poiché le migliori pratiche di settore per la gestione delle vulnerabilità sono state aggiornate (ad esempio OWASP, SANS CWE Top 25, CERT Secure Coding ecc.), per questi requisiti è necessario utilizzare le migliori pratiche più recenti.					
6.5.1	Le tecniche di codifica si occupano degli injection flaw, in particolare di SQL injection?  <b>Nota:</b> Considerare, inoltre, OS Command Injection, LDAP e XPath injection flaw, nonché altri tipi di injection flaw.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.2	Le tecniche di codifica si occupano delle vulnerabilità di buffer overflow?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.3	Le tecniche di codifica si occupano della memorizzazione di dati crittografici non sicura?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
6.5.4	Le tecniche di codifica si occupano delle comunicazioni non sicure?	<ul style="list-style-type: none"> <li>Esaminare le policy e le procedure di sviluppo software</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.5	Le tecniche di codifica si occupano della gestione degli errori non corretta?	<ul style="list-style-type: none"> <li>Esaminare le policy e le procedure di sviluppo software</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.6	Le tecniche di codifica si occupano di tutte le vulnerabilità "elevate" individuate nel processo di identificazione delle vulnerabilità (come definito nel Requisito 6.1 PCI DSS)?	<ul style="list-style-type: none"> <li>Esaminare le policy e le procedure di sviluppo software</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Per le applicazioni Web e le interfacce delle applicazioni (interne o esterne), le applicazioni vengono sviluppate in base a linee guida di codifica sicura per proteggere le applicazioni dalle seguenti vulnerabilità aggiuntive:							
6.5.7	Le tecniche di codifica si occupano delle vulnerabilità di cross-site scripting (XSS)?	<ul style="list-style-type: none"> <li>Esaminare le policy e le procedure di sviluppo software</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.8	Le tecniche di codifica si occupano del controllo di accesso non corretto (quali riferimenti a oggetti diretti non sicuri, errore di limitazione dell'accesso URL, errore di scansione trasversale directory ed errore di limitazione dell'accesso utente alle funzioni)?	<ul style="list-style-type: none"> <li>Esaminare le policy e le procedure di sviluppo software</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.5.9	Le tecniche di codifica si occupano del cross-site request forgery (CSRF)?	<ul style="list-style-type: none"> <li>Esaminare le policy e le procedure di sviluppo software</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
6.5.10	Le tecniche di codifica si occupano di violazione dell'autenticazione e gestione delle sessioni?	<ul style="list-style-type: none"> <li>▪ Esaminare le policy e le procedure di sviluppo software</li> <li>▪ Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
<p>6.6 Per le applicazioni Web esterne, viene assicurata in modo costante la protezione da nuove minacce e vulnerabilità e queste applicazioni sono protette da attacchi noti applicando <i>uno</i> dei seguenti metodi?</p> <ul style="list-style-type: none"> <li>▪ Analisi delle applicazioni Web rivolte al pubblico tramite strumenti o metodi manuali o automatici di valutazione della sicurezza della vulnerabilità delle applicazioni, come segue: <ul style="list-style-type: none"> <li>- Almeno una volta all'anno</li> <li>- dopo ogni modifica;</li> <li>- da un'organizzazione specializzata in sicurezza delle applicazioni;</li> <li>- che almeno tutte le vulnerabilità elencate nel Requisito 6.5 vengano incluse nella valutazione;</li> <li>- che tutte le vulnerabilità vengano corrette;</li> <li>- Che l'applicazione venga nuovamente valutata dopo le correzioni</li> </ul> </li> </ul> <p><b>Nota:</b> la valutazione non corrisponde alle scansioni delle vulnerabilità eseguite in base al Requisito 11.2.</p> <p>- O -</p> <ul style="list-style-type: none"> <li>▪ installazione di una soluzione tecnica automatica che rileva e impedisce gli attacchi basati sul Web (ad esempio, un firewall per applicazioni Web) nel seguente modo: <ul style="list-style-type: none"> <li>- posta davanti alle applicazioni Web rivolte al pubblico per rilevare ed evitare attacchi basati su Web;</li> <li>- in esecuzione e aggiornata secondo necessità;</li> <li>- in grado di generare log di audit;</li> <li>- configurata in modo da bloccare gli attacchi basati sul Web o da generare un avviso investigato immediatamente.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare i processi documentati</li> <li>▪ Consultare il personale</li> <li>▪ Esaminare i record di valutazioni di sicurezza delle applicazioni</li> <li>▪ Esaminare le impostazioni di configurazione del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
6.7	Le politiche di sicurezza e le procedure operative per lo sviluppo e la manutenzione di applicazioni e sistemi sicuri sono: <ul style="list-style-type: none"> <li>▪ documentate;</li> <li>▪ in uso;</li> <li>▪ note a tutte le parti coinvolte?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche di sicurezza e le procedure operative</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Implementazione di rigide misure di controllo dell'accesso

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

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
7.1	L'accesso ai componenti di sistema e ai dati di titolari di carta è limitato solo alle persone per le cui mansioni è realmente necessario, come segue:						
	<ul style="list-style-type: none"> <li>▪ È presente un documento scritto per il controllo dell'accesso che integra i seguenti elementi?               <ul style="list-style-type: none"> <li>• Definizione delle esigenze di accessi e assegnazioni dei privilegi per ogni ruolo</li> <li>• Limitazione dell'accesso a ID utente con privilegi alla quantità minima necessaria per le responsabilità di ruolo</li> <li>• assegnazione dell'accesso basata sulla classificazione e sulla funzione del ruolo del personale;</li> <li>• Approvazione documentata (elettronicamente o per iscritto) da parte di terzi autorizzati per tutti gli accessi, incluso l'elenco di privilegi specifici approvati</li> </ul> </li> </ul>	▪ Esaminare la politica scritta di controllo dell'accesso	<input type="checkbox"/>				
7.1.1	Sono state definite le esigenze di accesso per ogni ruolo, inclusi: <ul style="list-style-type: none"> <li>▪ Componenti di sistema e risorse dati di cui ogni ruolo ha bisogno per accedere alla relativa mansione?</li> <li>▪ Livello di privilegio necessario (ad esempio, utente, amministratore, ecc.) per accedere alle risorse?</li> </ul>	▪ Esaminare i ruoli e le esigenze di accesso	<input type="checkbox"/>				
7.1.2	L'accesso agli ID utente con privilegi è limitato come segue: <ul style="list-style-type: none"> <li>▪ Alla quantità minima necessaria per le responsabilità di ruolo?</li> <li>▪ Assegnato solo a ruoli che necessitano specificatamente tale accesso privilegiato?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> <li>▪ Consultare i membri del management</li> <li>▪ Analizzare gli ID utente con privilegi</li> </ul>	<input type="checkbox"/>				

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
7.1.3	L'accesso viene assegnato in base alla classificazione e alla funzione del singolo ruolo del personale?	<ul style="list-style-type: none"> <li>Consultare i membri del management</li> <li>Analizzare gli ID utente</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.1.4	L'approvazione documentata delle parti autorizzate viene richiesta specificando i privilegi necessari?	<ul style="list-style-type: none"> <li>Analizzare gli ID utente</li> <li>Confrontare con le approvazioni documentate</li> <li>Confrontare i privilegi assegnati con le approvazioni documentate</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Per i componenti di sistema, è presente un sistema di controllo dell'accesso per limitarlo in base alla reale necessità di un utente ed è impostato su "deny all" se non specificatamente consentito, come segue:						
7.2.1	Sono presenti sistemi di controllo dell'accesso su tutti i componenti di sistema?	<ul style="list-style-type: none"> <li>Analizzare la documentazione del fornitore</li> <li>Esaminare le impostazioni di configurazione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.2.2	I sistemi di controllo dell'accesso sono configurati in modo che i privilegi vengano assegnati agli utenti in base alla classificazione e alla funzione del ruolo?	<ul style="list-style-type: none"> <li>Analizzare la documentazione del fornitore</li> <li>Esaminare le impostazioni di configurazione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.2.3	I sistemi di controllo dell'accesso dispongono di un'impostazione predefinita "deny-all"?	<ul style="list-style-type: none"> <li>Analizzare la documentazione del fornitore</li> <li>Esaminare le impostazioni di configurazione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Le politiche di sicurezza e le procedure operative per la limitazione dell'accesso ai dati dei titolari di carta sono: <ul style="list-style-type: none"> <li>documentate;</li> <li>in uso;</li> <li>note a tutte le parti coinvolte?</li> </ul>	<ul style="list-style-type: none"> <li>Esaminare le politiche di sicurezza e le procedure operative</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
8.1	Sono state definite e applicate le politiche e le procedure per i controlli di gestione dell'identificazione dell'utente per utenti non consumatori e amministratori in tutti i componenti del sistema, come segue:					
8.1.1	A tutti gli utenti viene assegnato un ID univoco prima di consentire loro l'accesso a componenti del sistema o dati di titolari di carta?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.2	Le operazioni di aggiunta, eliminazione e modifica di ID utente, credenziali e altri oggetti identificativi sono controllate, in modo che gli ID utente siano implementati solo come autorizzati (incluso con privilegi specificati)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.3	L'accesso per gli utenti non attivi viene disattivato o rimosso immediatamente?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.1.4	Gli account utente non attivi vengono rimossi o disabilitati entro 90 giorni?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
8.1.5	(a) Gli account utilizzati da terzi per accedere, fornire supporto o manutenzione ai componenti di sistema mediante accesso remoto sono abilitati solo durante il periodo di tempo necessario e disabilitati se non in uso?	<ul style="list-style-type: none"> <li>Analizzare le procedure delle password</li> <li>Consultare il personale</li> <li>Osservare i processi</li> </ul>	<input type="checkbox"/>				
	(b) Gli account per l'accesso in remoto di terzi vengono monitorati durante l'uso?	<ul style="list-style-type: none"> <li>Consultare il personale</li> <li>Osservare i processi</li> </ul>	<input type="checkbox"/>				
8.1.6	(a) I tentativi di accesso ripetuti sono limitati bloccando l'ID utente dopo un massimo di sei tentativi?	<ul style="list-style-type: none"> <li>Analizzare le procedure delle password</li> <li>Esaminare le impostazioni di configurazione del sistema</li> </ul>	<input type="checkbox"/>				
	(b) <i>Questa procedura di test si applica solo ai provider di servizi.</i>						
8.1.7	Una volta che un account utente è bloccato, la durata del blocco è impostata almeno su 30 minuti oppure fino a quando l'amministratore non abilita nuovamente l'ID utente?	<ul style="list-style-type: none"> <li>Analizzare le procedure delle password</li> <li>Esaminare le impostazioni di configurazione del sistema</li> </ul>	<input type="checkbox"/>				
8.1.8	Se una sessione è inattiva per più di 15 minuti, agli utenti viene richiesto di effettuare nuovamente l'autenticazione (ad esempio immettere di nuovo la password) per riattivare il terminale o la sessione?	<ul style="list-style-type: none"> <li>Analizzare le procedure delle password</li> <li>Esaminare le impostazioni di configurazione del sistema</li> </ul>	<input type="checkbox"/>				
8.2	Oltre ad assegnare un ID univoco, viene adottato uno o più dei seguenti metodi per autenticare tutti gli utenti? <ul style="list-style-type: none"> <li>qualcosa che l'utente conosce, come una password o una passphrase;</li> <li>Qualcosa in possesso dell'utente, come un dispositivo token o una smart card</li> <li>qualcosa che l'utente è, come un elemento biometrico.</li> </ul>	<ul style="list-style-type: none"> <li>Analizzare le procedure delle password</li> <li>Osservare i processi di autenticazione</li> </ul>	<input type="checkbox"/>				

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
8.2.1	(a) Si utilizza la crittografia avanzata per rendere illeggibili tutte le credenziali di autenticazione (quali password/passphrase) durante la trasmissione e la memorizzazione su tutti i componenti di sistema?	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure delle password</li> <li>▪ Analizzare la documentazione del fornitore</li> <li>▪ Esaminare le impostazioni di configurazione del sistema</li> <li>▪ Osservare i file delle password</li> <li>▪ Osservare le trasmissioni di dati</li> </ul>	<input type="checkbox"/>				
	(b) Questa procedura di test si applica solo ai provider di servizi.						
8.2.2	L'identità dell'utente viene verificata prima di modificare le credenziali di autenticazione, ad esempio ripristinando la password, fornendo nuovi token o generando nuove chiavi?	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure di autenticazione</li> <li>▪ Osservare il personale</li> </ul>	<input type="checkbox"/>				
8.2.3	(a) I parametri delle password utente vengono configurati per richiedere che password/passphrase soddisfino i seguenti requisiti? <ul style="list-style-type: none"> <li>• Lunghezza minima della password di 7 caratteri</li> <li>• Presenza di caratteri numerici e alfabetici</li> </ul> In alternativa, le password/passphrase devono presentare una complessità e solidità pari almeno ai parametri indicati sopra.	<ul style="list-style-type: none"> <li>▪ Esaminare le impostazioni di configurazione del sistema per verificare i parametri delle password</li> </ul>	<input type="checkbox"/>				
	(b) Questa procedura di test si applica solo ai provider di servizi.						
8.2.4	(a) Le password/passphrase degli utenti vengono modificate almeno una volta ogni 90 giorni?	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure delle password</li> <li>▪ Esaminare le impostazioni di configurazione del sistema</li> </ul>	<input type="checkbox"/>				
	(b) Questa procedura di test si applica solo ai provider di servizi.						

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
8.2.5	(a) La nuova password/passphrase specificata deve essere diversa dalle ultime quattro password/passphrase utilizzate?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Questa procedura di test si applica solo ai provider di servizi.					
8.2.6	Le password/passphrase sono impostate su un valore univoco per ciascun utente per il primo accesso e al ripristino e ogni utente modifica la propria password immediatamente dopo il primo accesso?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.3	Tutto il singolo accesso amministrativo non da console e tutto l'accesso remoto al CDE vengono protetti mediante l'autenticazione a più fattori, nel modo seguente?  <b>Nota:</b> l'autenticazione a più fattori richiede l'utilizzo di almeno due dei tre metodi di autenticazione (fare riferimento al Requisito 8.2 PCI DSS per le descrizioni dei metodi di autenticazione). Utilizzare due volte un fattore (ad esempio, l'uso di due password separate) non viene considerato come un'autenticazione a più fattori.					
8.3.1	È stata integrata l'autenticazione a più fattori per tutto l'accesso non da console al CDE per il personale con l'accesso amministrativo?  <b>Nota:</b> questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
8.3.2	È stata integrata l'autenticazione a più fattori per tutto l'accesso remoto alla rete (sia utente che amministratore e incluso l'accesso di terzi per supporto o manutenzione) originato al di fuori della rete dall'entità?	<ul style="list-style-type: none"> <li>▪ Esaminare le configurazioni del sistema</li> <li>▪ Osservare la connessione del personale in remoto</li> </ul>	<input type="checkbox"/>				
8.4	(a) Le procedure e le politiche di autenticazione vengono documentate e comunicate a tutti gli utenti?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Analizzare il metodo di distribuzione</li> <li>▪ Consultare il personale</li> <li>▪ Consultare gli utenti</li> </ul>	<input type="checkbox"/>				
	(b) Le procedure e le politiche di autenticazione includono quanto segue? <ul style="list-style-type: none"> <li>• Istruzioni sulla selezione di credenziali di autenticazione avanzata</li> <li>• Istruzioni su come gli utenti dovrebbero proteggere le proprie credenziali di autenticazione</li> <li>• Istruzioni per non riutilizzare le password utilizzate precedentemente</li> <li>• Istruzioni su come gli utenti devono modificare le password in caso di sospetta compromissione delle password</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Analizzare la documentazione fornita agli utenti</li> </ul>	<input type="checkbox"/>				
8.5	Account e password di gruppo, condivisi o generici o altri metodi di autenticazione sono vietati come segue: <ul style="list-style-type: none"> <li>• Gli ID e gli account utente generici sono disabilitati o rimossi.</li> <li>• Non esistono ID utente condivisi per le attività di amministrazione del sistema e per altre funzioni critiche.</li> <li>• Gli ID utente condivisi e generici non vengono utilizzati per gestire i componenti di sistema.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Esaminare gli elenchi di ID utente</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>				

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
8.5.1	Questo requisito si applica solo ai provider di servizi.						
8.6	<p>Laddove vengano utilizzati altri meccanismi di autenticazione (ad esempio, token di sicurezza fisici o logici, smart card, certificati, ecc.), l'uso di questi meccanismi viene assegnato come segue?</p> <ul style="list-style-type: none"> <li>I meccanismi di autenticazione devono essere assegnati a un singolo account e non vanno condivisi tra più account.</li> <li>Vanno adottati controlli fisici e/o logici per assicurare che solo un account determinato possa utilizzare tale meccanismo di accesso.</li> </ul>	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure</li> <li>Consultare il personale</li> <li>Esaminare le impostazioni di configurazione del sistema e/o i controlli fisici</li> </ul>	<input type="checkbox"/>				
8.7	L'accesso a eventuali database contenenti dati dei titolari di carta (incluso l'accesso da parte di applicazioni, amministratori e altri utenti) è limitato come segue:						
	(a) Tutti gli accessi, le query e le azioni dell'utente (ad esempio, spostamento, copia, eliminazione) sul database si verificano solo tramite metodi programmatici (ad esempio, procedure memorizzate)?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure di autenticazione dei database</li> <li>Esaminare le impostazioni di configurazione di database e applicazioni</li> </ul>	<input type="checkbox"/>				
	(b) L'accesso diretto utente o le query ai database è limitato solo agli amministratori del database?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure di autenticazione dei database</li> <li>Esaminare le impostazioni di controllo dell'accesso al database</li> <li>Esaminare le impostazioni di configurazione dell'applicazione del database</li> </ul>	<input type="checkbox"/>				

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
(c) Gli ID di applicazione possono essere usati solo dalle applicazioni (e non da singoli utenti o altri processi)?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure di autenticazione dei database</li> <li>▪ Esaminare le impostazioni di controllo dell'accesso al database</li> <li>▪ Esaminare le impostazioni di configurazione dell'applicazione del database</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.8 Le politiche di sicurezza e le procedure operative per l'identificazione e l'autenticazione sono: <ul style="list-style-type: none"> <li>▪ documentate;</li> <li>▪ in uso;</li> <li>▪ note a tutte le parti coinvolte?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Esaminare le politiche di sicurezza e le procedure operative</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
9.1	I controlli dell'accesso alle strutture appropriati sono utilizzati per limitare e monitorare gli accessi fisici ai sistemi nell'ambiente dei dati di titolari di carta?	<ul style="list-style-type: none"> <li>▪ Osservare i controlli di accesso fisici</li> <li>▪ Osservare il personale</li> </ul>	<input type="checkbox"/>				
9.1.1	(a) Sono presenti videocamere o meccanismi di controllo dell'accesso (o entrambi) per monitorare gli accessi fisici ad aree sensibili?  <i>Nota: Per "aree sensibili" si intende centri dati, aree server e aree che ospitano sistemi di memorizzazione, elaborazione o trasmissione dei dati di titolari di carta. Ciò esclude le aree rivolte al pubblico in cui vi sono i terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio.</i>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Osservare i meccanismi di monitoraggio fisici</li> <li>▪ Osservare le funzionalità di protezione</li> </ul>	<input type="checkbox"/>				
	(b) Le videocamere o meccanismi di controllo dell'accesso (o entrambi) sono protetti da manomissione o disabilitazione?	<ul style="list-style-type: none"> <li>▪ Osservare i processi</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>				
	(c) I dati raccolti dalle videocamere e/o dai meccanismi di controllo dell'accesso vengono analizzati e correlati con altri dati?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Consultare il personale di sicurezza</li> </ul>	<input type="checkbox"/>				
	(d) I dati raccolti dalle videocamere e/o da altri meccanismi di controllo dell'accesso vengono memorizzati per almeno tre mesi, se non diversamente richiesto dalla legge?	<ul style="list-style-type: none"> <li>▪ Analizzare i processi di conservazione dei dati</li> <li>▪ Osservare la memorizzazione dei dati</li> <li>▪ Consultare il personale di sicurezza</li> </ul>	<input type="checkbox"/>				

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
9.1.2 Sono stati adottati i controlli fisici e/o logici per limitare l'accesso ai connettori di rete pubblicamente accessibili? <i>Ad esempio, i connettori di rete che si trovano nelle aree pubbliche e nelle aree accessibili ai visitatori potrebbero essere disattivati e attivati solo quando l'accesso alla rete è autorizzato esplicitamente. In alternativa, è possibile implementare i processi per garantire che i visitatori siano scortati costantemente nelle aree con connettori di rete attivi.</i>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Consultare il personale</li> <li>▪ Osservare le posizioni</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.1.3 Viene limitato l'accesso fisico a punti di accesso wireless, gateway, dispositivi portatili, hardware di rete e comunicazione e linee di telecomunicazione?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Consultare il personale</li> <li>▪ Osservare i dispositivi</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.2 (a) Le procedure sono elaborate per consentire di distinguere facilmente tra personale in sede e visitatori, tra cui: <ul style="list-style-type: none"> <li>• individuazione di nuovo personale in sede o visitatori (ad esempio, assegnando tessere magnetiche);</li> <li>• modifica dei requisiti di accesso;</li> <li>• revoca dell'identificazione scaduta del personale in sede o dei visitatori (ad esempio, tessere magnetiche).</li> </ul> <i>Ai fini del Requisito 9, per "personale in sede" si intendono le persone assunte a tempo pieno o part-time, le persone con contratto a tempo determinato, i collaboratori o i consulenti che sono fisicamente presenti presso i locali dell'entità. Per "visitatore" si intende un fornitore, un ospite del personale in sede, un tecnico dell'assistenza o chiunque abbia necessità di accedere alla struttura per un breve periodo di tempo, solitamente non più di un giorno.</i>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Consultare il personale</li> <li>▪ Osservare i metodi di identificazione (ad es. tessere magnetiche)</li> <li>▪ Osservare i processi dei visitatori</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Si	Si con CCW	No	N/A	Non testato
(b) I metodi di identificazione (come le tessere magnetiche ID) identificano chiaramente i visitatori e consentono una facile distinzione tra personale in sede e visitatori?	<ul style="list-style-type: none"> <li>▪ Osservare i metodi di identificazione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) L'accesso al sistema di tessere magnetiche è limitato al personale autorizzato?	<ul style="list-style-type: none"> <li>▪ Osservare i controlli fisici e i controlli di accesso per il sistema di tessere magnetiche</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.3 L'accesso fisico per il personale in sede alle aree sensibili viene controllato come segue: <ul style="list-style-type: none"> <li>▪ L'accesso viene autorizzato e basato sulla mansione dell'utente?</li> <li>▪ L'accesso viene revocato immediatamente in caso di licenziamento?</li> <li>▪ In caso di licenziamento, i meccanismi di accesso fisici, quali chiavi, schede di accesso, ecc., vengono restituiti o disattivati?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> <li>▪ Esaminare gli elenchi di controllo dell'accesso</li> <li>▪ Osservare il personale in sede</li> <li>▪ Confrontare gli elenchi di dipendenti licenziati agli elenchi di controllo dell'accesso</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4 L'identificazione e l'accesso dei visitatori viene gestito come indicato di seguito:						
9.4.1 I visitatori ricevono l'autorizzazione prima di accedere e devono essere sempre scortati nelle aree in cui i dati dei titolari di carta sono elaborati o custoditi?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Osservare i processi dei visitatori, inclusa la modalità di controllo dell'accesso</li> <li>▪ Consultare il personale</li> <li>▪ Osservare i visitatori e l'uso delle tessere magnetiche</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4.2 (a) I visitatori vengono identificati e ricevono una tessera magnetica o altro strumento di identificazione che consente di distinguere visivamente i visitatori dal personale in sede?	<ul style="list-style-type: none"> <li>▪ Osservare l'uso delle tessere magnetiche di personale e visitatori</li> <li>▪ Esaminare l'identificazione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Si	Si con CCW	No	N/A	Non testato
	(b) Le tessere magnetiche dei visitatori o gli altri strumenti di identificazione hanno una scadenza?	<ul style="list-style-type: none"> <li>▪ Osservare il processo</li> <li>▪ Esaminare l'identificazione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4.3	Ai visitatori viene chiesto di restituire la tessera magnetica o altro strumento di identificazione prima di lasciare la struttura o in corrispondenza della data di scadenza?	<ul style="list-style-type: none"> <li>▪ Osservare i processi</li> <li>▪ Osservare i visitatori che lasciando la struttura</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.4.4	(a) Viene utilizzato un registro dei visitatori per registrare gli accessi fisici alla struttura nonché alle aree computer e ai centri dati in cui vengono memorizzati o trasmessi i dati di titolari di carta?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Esaminare il registro dei visitatori</li> <li>▪ Osservare i processi dei visitatori</li> <li>▪ Esaminare la conservazione dei log</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Il registro dei visitatori contiene il nome del visitatore, l'azienda rappresentata e il personale in sede che autorizza l'accesso fisico?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Esaminare il registro dei visitatori</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Il registro dei visitatori viene conservato per almeno tre mesi?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure</li> <li>▪ Esaminare la conservazione del registro dei visitatori</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.5	Tutti i supporti sono protetti fisicamente (inclusi, senza limitazione, computer, supporti elettronici rimovibili, ricevute cartacee, resoconti cartacei e fax)? <i>Ai fini del Requisito 9, per "supporti" si intendono tutti i supporti elettronici e cartacei contenenti dati di titolari di carta.</i>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure per proteggere fisicamente i supporti</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.5.1	La posizione in cui i backup dei supporti vengono memorizzati viene analizzata almeno annualmente per verificare che la memorizzazione sia sicura?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure per la revisione delle posizioni dei supporti fuori sede</li> <li>▪ Consultare il personale di sicurezza</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Si	Si con CCW	No	N/A	Non testato
9.6	(a) La distribuzione interna ed esterna di qualsiasi tipo di supporto è rigorosamente controllata?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure per la distribuzione dei supporti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) I controlli devono includere quanto segue:						
9.6.1	Il supporto è classificato in modo da poter determinare la sensibilità dei dati?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure per la classificazione dei supporti</li> <li>Consultare il personale di sicurezza</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.2	Il supporto viene inviato tramite un corriere affidabile o un altro metodo di consegna che può essere adeguatamente monitorato?	<ul style="list-style-type: none"> <li>Consultare il personale</li> <li>Esaminare i registri di controllo e la documentazione della distribuzione dei supporti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.6.3	L'approvazione del management viene concessa prima dello spostamento dei supporti (soprattutto quando i supporti vengono distribuiti agli individui)?	<ul style="list-style-type: none"> <li>Consultare il personale</li> <li>Esaminare i registri di controllo e la documentazione della distribuzione dei supporti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.7	Sono in atto controlli adeguati per la memorizzazione e l'accesso ai supporti?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.7.1	(a) I registri di inventario per tutti i supporti sono stati conservati in modo appropriato?	<ul style="list-style-type: none"> <li>Esaminare i registri di inventario</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Gli inventari periodici dei supporti vengono eseguiti almeno una volta l'anno?	<ul style="list-style-type: none"> <li>Esaminare i registri di inventario</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Si	Si con CCW	No	N/A	Non testato
9.8	(a) Tutti i supporti vengono distrutti quando non sono più necessari per scopi aziendali o legali?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure di distruzione periodica dei supporti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) È presente una politica per la distruzione periodica dei supporti che definisce i requisiti per i seguenti aspetti? <ul style="list-style-type: none"> <li>Verificare che i materiali cartacei vengano stracciati tramite trinciatrice, bruciati o macerati in modo da garantire ragionevolmente che tali materiali non potranno essere ricostruiti.</li> <li>I contenitori utilizzati per il materiale da distruggere devono essere sicuri.</li> <li>I dati dei titolari di carta su supporti elettronici devono essere resi irrecuperabili (ad esempio tramite un programma di pulizia sicuro in conformità a standard di settore accettati per l'eliminazione sicura oppure distruggendo fisicamente i supporti).</li> </ul>	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure di distruzione periodica dei supporti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) La distruzione avviene in base alle seguenti modalità:						
9.8.1	(a) I materiali cartacei sono stati distrutti utilizzando una trinciatrice, bruciati o disintegrati, in modo che non sia possibile ricostruire i dati dei titolari di carta?	<ul style="list-style-type: none"> <li>Consultare il personale</li> <li>Esaminare le procedure</li> <li>Osservare i processi</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) I contenitori usati per conservare i materiali che contengono le informazioni da distruggere sono protetti per impedire l'accesso al contenuto?	<ul style="list-style-type: none"> <li>Esaminare la sicurezza dei contenitori di conservazione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.8.2	Si rendono irrecuperabili i dati dei titolari di carta su supporti elettronici (ad esempio tramite un programma di pulizia basato su standard di settore accettati per l'eliminazione sicura oppure in altro modo attraverso la distruzione fisica dei supporti) in modo da rendere impossibile la ricostruzione dei dati dei titolari di carta?	<ul style="list-style-type: none"> <li>Osservare i processi</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Si con CCW	No	N/A	Non testato
9.9 I dispositivi che acquisiscono i dati delle carte di pagamento attraverso un'interazione fisica diretta con la carta vengono protetti contro manomissioni e sostituzioni, come indicato di seguito?  <b>Nota:</b> questo requisito si applica ai dispositivi che leggono le carte utilizzati nelle transazioni con carta presente (ovvero, tessera magnetica o dip) nel punto vendita. Questo requisito non si applica ai componenti per l'immissione manuale, quali tastiere di computer o tastierini di POS.						
(a) Le politiche e le procedure prevedono che venga conservato un elenco di tali dispositivi?	▪ Analizzare le politiche e le procedure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Le politiche e le procedure richiedono che i dispositivi siano sottoposti a un'ispezione periodica per controllare eventuali manomissioni o sostituzioni?	▪ Analizzare le politiche e le procedure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Le politiche e le procedure impongono la corretta formazione del personale che deve essere a conoscenza del comportamento sospetto e segnalare le manomissioni o le sostituzioni dei dispositivi?	▪ Analizzare le politiche e le procedure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.1 (a) L'elenco dei dispositivi include quanto segue? <ul style="list-style-type: none"> <li>• Marca, modello del dispositivo</li> <li>• Posizione del dispositivo (ad esempio, l'indirizzo della sede o della struttura in cui si trova il dispositivo)</li> <li>• Numero di serie del dispositivo o altro metodo di identificazione univoca</li> </ul>	▪ Esaminare l'elenco dei dispositivi	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) L'elenco è accurato e aggiornato?	▪ Osservare i dispositivi e le relative posizioni e confrontarli con l'elenco	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) L'elenco di dispositivi viene aggiornato quando i dispositivi vengono aggiunti, riposizionati, messi fuori uso ecc.?	▪ Consultare il personale	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Si	Si con CCW	No	N/A	Non testato
9.9.2 (a) Le superfici del dispositivo vengono ispezionate periodicamente per rilevare manomissioni (ad esempio, aggiunta di skimmer di carte ai dispositivi) o sostituzioni (ad esempio, controllando il numero di serie o le caratteristiche del dispositivo per verificare che non sia stato sostituito con un dispositivo fraudolento), come indicato di seguito?  <i>Nota: esempi di indicazioni che un dispositivo potrebbe essere stato alterato o sostituito includono raccordi o cavi innestati nel dispositivo, etichette di sicurezza mancanti o modificate, involucri rotti o di colori diversi o modifiche al numero di serie o altri contrassegni esterni.</i>	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> <li>▪ Osservare i processi di ispezione e confrontare con processi definiti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Il personale è a conoscenza delle procedure per ispezionare i dispositivi?	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.9.3 Il personale è stato debitamente formato per essere a conoscenza dei tentativi di alterazione o sostituzione dei dispositivi, con inclusione di quanto segue?						
(a) Il materiale formativo per il personale dei punti vendita include quanto segue? <ul style="list-style-type: none"> <li>• Verifica dell'identità di eventuali terzi che sostengono di essere addetti alle riparazioni o alla manutenzione, prima di consentire loro l'autorizzazione a modificare o risolvere i problemi dei dispositivi.</li> <li>• Divieto di installare, sostituire o restituire dispositivi in assenza di verifica.</li> <li>• Massima attenzione al comportamento sospetto in prossimità dei dispositivi (ad esempio, tentativi di persone sconosciute di disconnettere o aprire i dispositivi).</li> <li>• Segnalazione di comportamento sospetto e indicazioni di alterazione o sostituzione del dispositivo al personale appropriato (ad esempio, un manager o un addetto alla sicurezza).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare i materiali di formazione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
	(b) Il personale dei punti vendita ha seguito la giusta formazione e conosce le procedure necessarie per individuare e segnalare i tentativi di manomissione o sostituzione dei dispositivi?	<ul style="list-style-type: none"> <li>▪ Consultare il personale presso le sedi POS</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.10	Le politiche di sicurezza e le procedure operative per la limitazione dell'accesso fisico ai dati dei titolari di carta sono: <ul style="list-style-type: none"> <li>▪ documentate;</li> <li>▪ in uso;</li> <li>▪ note a tutte le parti coinvolte?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Esaminare le politiche di sicurezza e le procedure operative</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Monitoraggio e test delle reti regolari

### Requisito 10 - Registrare e monitorare tutti gli accessi a risorse di rete e dati dei titolari di carta

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
10.1	(a) Gli audit trail sono attivi e funzionanti per i componenti di sistema?	<ul style="list-style-type: none"> <li>▪ Osservare i processi</li> <li>▪ Consultare l'amministratore di sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) L'accesso ai componenti di sistema è collegato ad ogni singolo utente?	<ul style="list-style-type: none"> <li>▪ Osservare i processi</li> <li>▪ Consultare l'amministratore di sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2	Sono stati implementati audit trail automatizzati per tutti i componenti del sistema per ricostruire i seguenti eventi:						
10.2.1	Tutti i singoli accessi di utenti a dati di titolari di carta?	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> <li>▪ Osservare i log di audit</li> <li>▪ Esaminare le impostazioni dei relativi log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.2	Tutte le azioni intraprese da un utente con privilegi di utente root o amministratore?	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> <li>▪ Osservare i log di audit</li> <li>▪ Esaminare le impostazioni dei relativi log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.3	Accesso a tutti gli audit trail?	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> <li>▪ Osservare i log di audit</li> <li>▪ Esaminare le impostazioni dei relativi log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.4	Tentativi di accesso logico non validi?	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> <li>▪ Osservare i log di audit</li> <li>▪ Esaminare le impostazioni dei relativi log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
10.2.5	Uso e modifiche dei meccanismi di identificazione e autenticazione (compresi, a titolo esemplificativo, creazione di nuovi account, incremento dei privilegi, ecc.) e tutte le modifiche, le aggiunte e le eliminazioni agli account dell'applicazione con privilegi root o di amministratore?	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> <li>▪ Osservare i log di audit</li> <li>▪ Esaminare le impostazioni dei relativi log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.6	Inizializzazione, arresto o pausa dei log di audit?	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> <li>▪ Osservare i log di audit</li> <li>▪ Esaminare le impostazioni dei relativi log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.2.7	Creazione ed eliminazione di oggetti a livello di sistema?	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> <li>▪ Osservare i log di audit</li> <li>▪ Esaminare le impostazioni dei relativi log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3	Vengono registrate le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento:						
10.3.1	Identificazione utente?	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> <li>▪ Osservare i log di audit</li> <li>▪ Esaminare le impostazioni dei relativi log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.2	Tipo di evento?	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> <li>▪ Osservare i log di audit</li> <li>▪ Esaminare le impostazioni dei relativi log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.3	Data e ora?	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> <li>▪ Osservare i log di audit</li> <li>▪ Esaminare le impostazioni dei relativi log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
10.3.4	Indicazione di successo o fallimento?	<ul style="list-style-type: none"> <li>Consultare il personale</li> <li>Osservare i log di audit</li> <li>Esaminare le impostazioni dei relativi log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.5	Origine dell'evento?	<ul style="list-style-type: none"> <li>Consultare il personale</li> <li>Osservare i log di audit</li> <li>Esaminare le impostazioni dei relativi log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.3.6	Identità o nome del dato interessato, componente di sistema o risorsa?	<ul style="list-style-type: none"> <li>Consultare il personale</li> <li>Osservare i log di audit</li> <li>Esaminare le impostazioni dei relativi log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.4	<p>Tutti gli orologi e gli orari critici del sistema sono sincronizzati utilizzando la tecnologia per la sincronizzazione dell'ora? Tale tecnologia viene aggiornata?</p> <p><b>Nota:</b> NTP (Network Time Protocol) è un esempio di tecnologia per la sincronizzazione dell'ora.</p>	<ul style="list-style-type: none"> <li>Analizzare gli standard e i processi di configurazione dell'ora</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.4.1	Sono stati implementati i seguenti processi per i sistemi cruciali per avere un orario corretto e uniforme:						
	(a) Solo i server di rilevamento dell'orario centrali designati ricevono i segnali orari da sorgenti esterne e tali segnali si basano su International Atomic Time o UTC?	<ul style="list-style-type: none"> <li>Analizzare gli standard e i processi di configurazione dell'ora</li> <li>Esaminare i parametri di sistema relativi all'ora</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Laddove esiste più di un server di riferimento orario, i server comunicano tra loro per mantenere un orario esatto?	<ul style="list-style-type: none"> <li>Analizzare gli standard e i processi di configurazione dell'ora</li> <li>Esaminare i parametri di sistema relativi all'ora</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
(c) I sistemi ricevono le informazioni orarie soltanto dai server centrali designati.	<ul style="list-style-type: none"> <li>Analizzare gli standard e i processi di configurazione dell'ora</li> <li>Esaminare i parametri di sistema relativi all'ora</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.4.2 I dati dell'ora sono protetti come segue:	<ul style="list-style-type: none"> <li>Esaminare le configurazioni di sistema e le impostazioni per la sincronizzazione dell'ora</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(a) L'accesso ai dati dell'ora è limitato solo al personale per il quale l'accesso a tali dati sia effettivamente necessario?						
(b) Le modifiche alle impostazioni dell'ora su sistemi critici sono registrate, monitorate ed esaminate?	<ul style="list-style-type: none"> <li>Esaminare le configurazioni di sistema e le impostazioni e i log per la sincronizzazione dell'ora</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.4.3 Le impostazioni dell'ora vengono ricevute da fonti specifiche accettate dal settore? (Ciò al fine di evitare la modifica dell'ora da parte di utenti non autorizzati.) <i>Facoltativamente, tali aggiornamenti possono essere cifrati con una chiave simmetrica ed è possibile creare elenchi di controllo dell'accesso che specifichino gli indirizzi IP dei computer client ai quali verranno forniti gli aggiornamenti di ora (per evitare un uso non autorizzato dei server di rilevamento dell'ora interni).</i>	<ul style="list-style-type: none"> <li>Esaminare le configurazioni del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.5 Gli audit trail sono protetti in modo che non possano essere modificati, come segue:						
10.5.1 La visualizzazione degli audit trail è limitata a coloro che realmente necessitano di tali informazioni per scopi aziendali?	<ul style="list-style-type: none"> <li>Consultare gli amministratori di sistema</li> <li>Esaminare le configurazioni di sistema e le autorizzazioni</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.5.2 I file di audit trail sono protetti in modo da non consentire modifiche non autorizzate tramite meccanismi di controllo dell'accesso, separazione fisica e/o di rete?	<ul style="list-style-type: none"> <li>Consultare gli amministratori di sistema</li> <li>Esaminare le configurazioni di sistema e le autorizzazioni</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
10.5.3	Viene eseguito il backup dei file di audit trail su un server dei log o un supporto centralizzato difficile da modificare?	<ul style="list-style-type: none"> <li>Consultare gli amministratori di sistema</li> <li>Esaminare le configurazioni di sistema e le autorizzazioni</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.5.4	I registri per le tecnologie rivolte al pubblico (ad esempio wireless, firewall, DNS, e-mail) vengono scritti su un server di registro o un supporto sicuro, centralizzato e interno?	<ul style="list-style-type: none"> <li>Consultare gli amministratori di sistema</li> <li>Esaminare le configurazioni di sistema e le autorizzazioni</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.5.5	Vengono utilizzati un meccanismo di monitoraggio dell'integrità dei file o 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)?	<ul style="list-style-type: none"> <li>Esaminare le impostazioni, i file monitorati e i risultati delle attività di monitoraggio</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.6	<p>I registri e gli eventi di sicurezza per tutti i componenti di sistema vengono analizzati al fine di identificare anomalie o attività sospette, come indicato di seguito?</p> <p><b>Nota:</b> gli strumenti di raccolta, analisi e generazione di avvisi per i log possono essere utilizzati ai fini della conformità al requisito 10.6.</p>						

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
10.6.1	(a) Sono state definite politiche e procedure scritte per rivedere gli elementi seguenti almeno quotidianamente, manualmente o tramite strumenti di registro? <ul style="list-style-type: none"> <li>• Tutti gli eventi di sicurezza.</li> <li>• Registri di tutti i componenti di sistema che memorizzano, elaborano o trasmettono CHD e/o SAD.</li> <li>• Registri di tutti i componenti di sistema critici.</li> <li>• Registri di tutti i server e componenti di sistema che eseguono funzioni di sicurezza (ad esempio, firewall, sistemi di rilevamento intrusioni/sistemi di prevenzione intrusioni IDS/IPS, server di autenticazione, server di ridirezionamento e-commerce).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure di sicurezza</li> </ul>	<input type="checkbox"/>				
	(b) I registri e gli eventi di sicurezza menzionati sopra vengono analizzati almeno una volta al giorno?	<ul style="list-style-type: none"> <li>▪ Osservare i processi</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>				
10.6.2	(a) Sono state definite politiche e procedure di sicurezza scritte per rivedere periodicamente i registri e tutti gli altri componenti di sistema, manualmente o tramite strumenti di registro, in base alle politiche e alla strategia di gestione del rischio dell'azienda?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure di sicurezza</li> </ul>	<input type="checkbox"/>				
	(b) Le analisi di tutti gli altri componenti di sistema vengono eseguite in conformità alle politiche e alle strategie di gestione del rischio dell'azienda?	<ul style="list-style-type: none"> <li>▪ Analizzare la documentazione di valutazione dei rischi</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>				
10.6.3	(a) Sono state definite politiche e procedure di sicurezza scritte per il follow-up di eccezioni e anomalie identificate durante il processo di revisione?	<ul style="list-style-type: none"> <li>▪ Analizzare le politiche e le procedure di sicurezza</li> </ul>	<input type="checkbox"/>				
	(b) Viene eseguito il follow-up per le eccezioni e le anomalie?	<ul style="list-style-type: none"> <li>▪ Osservare i processi</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>				

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
10.7	(a) Sono state adottate politiche e procedure di conservazione dei log di audit che impongono che i log siano conservati per almeno un anno, con un minimo di tre mesi di disponibilità immediata per l'analisi (ad esempio, online, archiviazione o recuperabile da backup)?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure di sicurezza</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) I log di audit vengono conservati per almeno un anno?	<ul style="list-style-type: none"> <li>Consultare il personale</li> <li>Esaminare i log di audit</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) Sono immediatamente disponibili per l'analisi almeno i log degli ultimi tre mesi?	<ul style="list-style-type: none"> <li>Consultare il personale</li> <li>Osservare i processi</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.8	<i>Questo requisito si applica solo ai provider di servizi.</i>						
10.9	Le politiche di sicurezza e le procedure operative per il monitoraggio di tutti gli accessi alle risorse di rete e ai dati dei titolari di carta sono: <ul style="list-style-type: none"> <li>documentate;</li> <li>in uso;</li> <li>note a tutte le parti coinvolte?</li> </ul>	<ul style="list-style-type: none"> <li>Analizzare le politiche di sicurezza e le procedure operative</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Requisito 11 - Eseguire regolarmente test dei sistemi e processi di protezione**

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Si con CCW	No	N/A	Non testato
11.1 (a) I processi per il rilevamento e l'identificazione dei punti di accesso wireless autorizzati e non autorizzati vengono implementati almeno a cadenza trimestrale?  <i>Nota: i metodi che si possono utilizzare nel processo comprendono, senza limitazioni, scansioni della rete wireless, controlli di tipo fisico e logico di infrastrutture e componenti di sistema, NAC (Network Access Control) o IDS/IPS wireless. Qualunque sia il metodo adottato, questo deve essere in grado di rilevare e identificare qualsiasi dispositivo non autorizzato.</i>	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) La metodologia rileva e identifica ogni punto di accesso wireless non autorizzato, compreso, come minimo, quanto segue? <ul style="list-style-type: none"> <li>Schede WLAN inserite nei componenti di sistema</li> <li>Dispositivi portatili o mobili collegati ai componenti di sistema per creare un punto di accesso wireless (ad esempio, con USB, ecc.)</li> <li>Dispositivi wireless collegati a una porta o a un dispositivo di rete</li> </ul>	<ul style="list-style-type: none"> <li>Valutare la metodologia</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) La scansione wireless finalizzata a identificare i punti di accesso wireless autorizzati e non autorizzati viene eseguita con cadenza trimestrale per tutte le strutture e i componenti di sistema?	<ul style="list-style-type: none"> <li>Esaminare l'output delle scansioni wireless recenti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(d) In caso di utilizzo del monitoraggio automatico (ad esempio, IDS/IPS wireless, NAC, ecc.), tale monitoraggio è configurato per generare avvisi per il personale?	<ul style="list-style-type: none"> <li>Esaminare le impostazioni di configurazione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.1.1	Viene mantenuto un inventario dei punti di accesso wireless autorizzati e viene documentata una giustificazione aziendale per tutti i punti di accesso wireless autorizzati?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Si con CCW	No	N/A	Non testato
11.1.2	(a) Il piano di risposta agli incidenti definisce e richiede una risposta in caso di rilevamento di punti di accesso wireless non autorizzati?	<ul style="list-style-type: none"> <li>Esaminare il piano di risposta agli incidenti (vedere il requisito 12.10)</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Viene intrapresa un'azione quando si rilevano punti di accesso wireless non autorizzati?	<ul style="list-style-type: none"> <li>Consultare il personale responsabile</li> <li>Ispezionare le scansioni wireless recenti e le relative risposte</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2	<p>Sono state eseguite 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), come segue?</p> <p><b>Nota:</b> è possibile unire più rapporti delle scansioni per il processo di scansione trimestrale per accertarsi che sia stata eseguita la scansione di tutti i sistemi e siano state risolte tutte le vulnerabilità applicabili. Potrebbe essere necessaria una documentazione ulteriore per verificare che le vulnerabilità non corrette siano in fase di correzione.</p> <p>Per la conformità iniziale a PCI DSS, non è necessario che vengano completati quattro scansioni trimestrali positive se il valutatore verifica che 1) il risultato della scansione più recente era positivo, 2) l'entità dispone di politiche e procedure documentate che richiedono l'esecuzione di scansioni trimestrali e 3) le vulnerabilità rilevate nei risultati della scansione sono state corrette nel modo dimostrato da una nuova scansione. Per gli anni successivi alla revisione PCI DSS iniziale, è necessario eseguire quattro scansioni trimestrali con esito positivo.</p>						
11.2.1	(a) Vengono eseguite scansioni interne di vulnerabilità trimestrali?	<ul style="list-style-type: none"> <li>Analizzare i rapporti delle scansioni</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Si con CCW	No	N/A	Non testato
(b) Il processo di scansioni interne trimestrali risolve tutte le vulnerabilità "Elevate" e comprende nuove scansioni fino alla risoluzione di tutte le vulnerabilità "Elevate" (come definito nel Requisito 6.1 PCI DSS)?	<ul style="list-style-type: none"> <li>Analizzare i rapporti delle scansioni</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Le scansioni interne trimestrali vengono eseguite da una risorsa interna o da una terza parte qualificata e, se applicabile, l'esecutore del test è indipendente dall'organizzazione (non necessariamente un QSA o un ASV)?	<ul style="list-style-type: none"> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.2 (a) Vengono eseguite scansioni esterne di vulnerabilità trimestrali? <i>Nota: le scansioni esterne delle vulnerabilità trimestrali devono essere eseguite da un fornitore di prodotti di scansione approvato (ASV) e autorizzato dall'Ente responsabile degli standard di protezione PCI (PCI SSC). Fare riferimento alla Guida del programma ASV pubblicata sul sito Web PCI SSC per le responsabilità dei clienti relative alle scansioni, la preparazione delle scansioni, ecc.</i>	<ul style="list-style-type: none"> <li>Analizzare i risultati dai quattro trimestri più recenti di scansioni delle vulnerabilità esterne</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) I risultati delle scansioni esterne trimestrali soddisfano i requisiti della Guida del programma per i fornitori di scansioni approvati (ad esempio nessuna vulnerabilità classificata superiore a 4.0 dal CVSS e nessun errore automatico)?	<ul style="list-style-type: none"> <li>Analizzare i risultati di ogni scansione trimestrale esterna e ripetere la scansione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Le scansioni esterne di vulnerabilità trimestrali vengono eseguite dal fornitore di prodotti di scansione approvato (ASV) PCI SSC?	<ul style="list-style-type: none"> <li>Analizzare i risultati di ogni scansione trimestrale esterna e ripetere la scansione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.2.3 (a) Le scansioni interne ed esterne vengono eseguite, e ripetute se necessario, dopo ogni modifica significativa? <i>Nota: le scansioni devono essere eseguite da personale qualificato.</i>	<ul style="list-style-type: none"> <li>Esaminare e associare la documentazione di controllo delle modifiche e i report di scansione</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Si con CCW	No	N/A	Non testato
(b) Il processo di scansione comprende nuove scansioni fino a quando: <ul style="list-style-type: none"> <li>• Per le scansioni esterne, non esistano vulnerabilità a cui sia assegnato un punteggio superiore a 4.0 da parte del CVSS.</li> <li>• Per le scansioni interne, sia stato conseguito un risultato positivo oppure siano state risolte tutte le vulnerabilità "Elevate" in base alla definizione contenuta nel Requisito 6.1 PCI DSS?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare i rapporti delle scansioni</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(c) Le scansioni vengono eseguite da una risorsa interna o da una terza parte qualificata e, ove applicabile, l'esecutore del test è indipendente dall'organizzazione (non necessariamente un QSA o un ASV)?	<ul style="list-style-type: none"> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.3 La metodologia dei test di penetrazione include quanto segue? <ul style="list-style-type: none"> <li>▪ È basata sugli approcci ai test di penetrazione accettati dal settore (ad esempio, NIST SP800-115).</li> <li>▪ Include la copertura dell'intero perimetro dell'ambiente dei dati dei titolari di carta e i dei sistemi critici.</li> <li>▪ Include i test dall'interno e dall'esterno della rete.</li> <li>▪ Comprende i test per convalidare eventuali controlli di segmentazione e riduzione della portata.</li> <li>▪ Definisce i test di penetrazione a livello di applicazione affinché includano almeno le vulnerabilità elencate nel Requisito 6.5.</li> <li>▪ Definisce i test di penetrazione a livello di rete affinché includano componenti che supportano le funzioni di rete nonché i sistemi operativi.</li> <li>▪ Include la revisione e la valutazione delle minacce e delle vulnerabilità verificatesi negli ultimi 12 mesi.</li> <li>▪ Specifica la conservazione dei risultati dei test di penetrazione e dei risultati delle attività di correzione.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Esaminare la metodologia dei test di penetrazione</li> <li>▪ Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Si con CCW	No	N/A	Non testato	
11.3.1	(a) I test di penetrazione <i>esterna</i> vengono eseguiti, come richiesto dalla metodologia definita, almeno una volta l'anno e dopo ogni modifica significativa dell'infrastruttura o dell'applicazione (come un aggiornamento del sistema operativo, l'aggiunta all'ambiente di una subnet o di un server Web)?	<ul style="list-style-type: none"> <li>Esaminare la portata del lavoro</li> <li>Esaminare i risultati dai test di penetrazione esterna più recenti</li> </ul>	<input type="checkbox"/>				
	(b) I test sono eseguiti da una risorsa interna o da una terza parte esterna qualificata e, ove applicabile, l'esecutore del test è indipendente dall'organizzazione (non necessariamente un QSA o un ASV)?	<ul style="list-style-type: none"> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>				
11.3.2	(a) I test di penetrazione <i>interna</i> vengono eseguiti, come richiesto dalla metodologia definita, almeno una volta l'anno e dopo ogni modifica significativa dell'infrastruttura o dell'applicazione (come un aggiornamento del sistema operativo, l'aggiunta all'ambiente di una subnet o di un server Web)?	<ul style="list-style-type: none"> <li>Esaminare la portata del lavoro</li> <li>Esaminare i risultati dai test di penetrazione interna più recenti</li> </ul>	<input type="checkbox"/>				
	(b) I test sono eseguiti da una risorsa interna o da una terza parte esterna qualificata e, ove applicabile, l'esecutore del test è indipendente dall'organizzazione (non necessariamente un QSA o un ASV)?	<ul style="list-style-type: none"> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>				
11.3.3	Le vulnerabilità sfruttabili individuate durante il test di penetrazione vengono corrette e il test viene ripetuto per verificare le correzioni?	<ul style="list-style-type: none"> <li>Esaminare i risultati dei test di penetrazione</li> </ul>	<input type="checkbox"/>				
11.3.4	Se si utilizza la segmentazione per isolare l'ambiente dei dati dei titolari di carta da altre reti:						
	(a) Sono state definite procedure dei test di penetrazione per testare tutti i metodi di segmentazione e confermare che sono funzionali ed efficaci, e isolare tutti i sistemi che non rientrano nell'ambito dai sistemi che rientrano nel CDE?	<ul style="list-style-type: none"> <li>Esaminare i controlli di segmentazione</li> <li>Analizzare la metodologia dei test di penetrazione</li> </ul>	<input type="checkbox"/>				

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
	(b) I test di penetrazione volti a verificare i controlli di segmentazione rispondono ai seguenti criteri? <ul style="list-style-type: none"> <li>Vengono eseguiti almeno una volta all'anno e dopo eventuali modifiche ai controlli/metodi di segmentazione.</li> <li>Coprono tutti i controlli/metodi di segmentazione in uso.</li> <li>Verificano che i metodi di segmentazione siano funzionali ed efficaci e isolino tutti i sistemi che non rientrano nell'ambito dai sistemi che rientrano nel CDE.</li> </ul>	<ul style="list-style-type: none"> <li>Esaminare i risultati dai test di penetrazione più recenti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(c) I test sono eseguiti da una risorsa interna o da una terza parte esterna qualificata e, ove applicabile, l'esecutore del test è indipendente dall'organizzazione (non necessariamente un QSA o un ASV)?	<ul style="list-style-type: none"> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.3.4.1	<i>Questo requisito si applica solo ai provider di servizi.</i>						
11.4	(a) Sono state adottate tecniche di rilevamento delle intrusioni e/o di prevenzione delle intrusioni che rilevano e/o prevengono le intrusioni nella rete al fine di monitorare tutto il traffico: <ul style="list-style-type: none"> <li>in corrispondenza del perimetro dell'ambiente dei dati dei titolari di carta;</li> <li>in corrispondenza dei punti critici nell'ambiente dei dati dei titolari di carta.</li> </ul>	<ul style="list-style-type: none"> <li>Esaminare le configurazioni del sistema</li> <li>Esaminare i diagrammi di rete</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Le tecniche di rilevamento delle intrusioni e/o di prevenzione delle intrusioni sono state configurate per avvertire il personale di violazioni sospette?	<ul style="list-style-type: none"> <li>Esaminare le configurazioni del sistema</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Si con CCW	No	N/A	Non testato
	(c) Vengono tenuti aggiornati tutti i sistemi, le basi e le firme di rilevamento e prevenzione delle intrusioni?	<ul style="list-style-type: none"> <li>Esaminare le configurazioni IDS/IPS</li> <li>Esaminare la documentazione del fornitore</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.5	<p>(a) È stato implementato un meccanismo di rilevamento delle modifiche (ad esempio, strumenti di monitoraggio dell'integrità file) per rilevare modifiche non autorizzate (incluse modifiche, aggiunte ed eliminazioni) a file di sistema, di configurazione o di contenuti critici?</p> <p><i>Tra gli esempi di file che devono essere monitorati:</i></p> <ul style="list-style-type: none"> <li>Eseguibili di sistema</li> <li>eseguibili di applicazioni</li> <li>File di configurazione e parametri</li> <li>File memorizzati centralmente, di cronologia o archiviazione, di registro e audit</li> <li>File critici ulteriori determinati dall'entità (ad esempio, tramite la valutazione dei rischi o altri mezzi)</li> </ul>	<ul style="list-style-type: none"> <li>Osservare le impostazioni di sistema e i file monitorati</li> <li>Esaminare le impostazioni di configurazione del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<p>(b) Il meccanismo di rilevamento delle modifiche è stato configurato per segnalare al personale le modifiche non autorizzate (incluse modifiche, aggiunte ed eliminazioni) ai file di sistema, di configurazione o di contenuti critici? Questi strumenti eseguono confronti di file critici almeno una volta alla settimana?</p> <p><b>Nota:</b> ai fini del rilevamento delle modifiche, i file critici sono solitamente file che non cambiano frequentemente, ma la cui modifica può indicare la compromissione, effettiva o potenziale, del sistema. I meccanismi di rilevamento delle modifiche come i prodotti per il monitoraggio dell'integrità dei file sono generalmente preconfigurati con file critici per il sistema operativo in uso. Altri file critici, ad esempio quelli per applicazioni personalizzate, devono essere valutati e definiti dall'entità (ossia dall'esercente o dal provider di servizi).</p>	<ul style="list-style-type: none"> <li>Osservare le impostazioni di sistema e i file monitorati</li> <li>Analizzare i risultati delle attività di monitoraggio</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
11.5.1	È stato adottato un processo per rispondere a eventuali avvisi generati dalla soluzione di rilevamento delle modifiche?	<ul style="list-style-type: none"> <li>▪ Esaminare le impostazioni di configurazione del sistema</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11.6	Le politiche di sicurezza e le procedure operative per il monitoraggio e il test della sicurezza sono: <ul style="list-style-type: none"> <li>• documentate;</li> <li>• in uso;</li> <li>• note a tutte le parti coinvolte?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Esaminare le politiche di sicurezza e le procedure operative</li> <li>▪ Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Gestire una politica di sicurezza delle informazioni

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

**Nota:** ai fini del Requisito 12, per “personale” si intende un dipendente a tempo pieno o part-time, un dipendente con contratto a tempo determinato, un collaboratore o consulente che svolge le sue prestazioni in sede o che abbia in altro modo accesso all’ambiente dei dati dei titolari di carta della società.

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
12.1	È stata definita, pubblicata, gestita e diffusa una politica per la sicurezza tra tutto il personale interessato?	<ul style="list-style-type: none"> <li>Analizzare la politica di sicurezza delle informazioni</li> </ul>	<input type="checkbox"/>				
12.1.1	La politica di sicurezza viene rivista almeno una volta all’anno e aggiornata quando l’ambiente cambia?	<ul style="list-style-type: none"> <li>Analizzare la politica di sicurezza delle informazioni</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>				
12.2	(a) È stato implementato un processo di valutazione dei rischi annuale che <ul style="list-style-type: none"> <li>identifichi risorse critiche, minacce e vulnerabilità;</li> <li>consenta di ottenere una formale analisi dei rischi documentata?</li> </ul> <i>Esempi di metodologie per la valutazione dei rischi includono, senza limitazioni, OCTAVE, ISO 27005 e NIST SP 800-30.</i>	<ul style="list-style-type: none"> <li>Analizzare il processo annuale di valutazione dei rischi</li> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>				
	(b) Il processo di valutazione dei rischi viene eseguito almeno una volta all’anno e in occasione di modifiche significative all’ambiente (ad esempio, acquisizione, fusione, trasferimento, ecc.)?	<ul style="list-style-type: none"> <li>Analizzare la documentazione di valutazione dei rischi</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>				

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
12.3	<p>Sono state sviluppate politiche che regolano l'uso per tecnologie critiche per definire l'uso corretto di queste tecnologie? Tali politiche richiedono quanto segue:</p> <p><b>Nota:</b> esempi di tecnologie critiche comprendono, senza limitazioni, accesso remoto e tecnologie wireless, laptop, tablet, supporti elettronici rimovibili, uso della posta elettronica e di Internet.</p>						
12.3.1	Approvazione esplicita delle parti autorizzate per l'uso delle tecnologie?	<ul style="list-style-type: none"> <li>Analizzare le politiche di utilizzo</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.2	Autenticazione per l'uso della tecnologia?	<ul style="list-style-type: none"> <li>Analizzare le politiche di utilizzo</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.3	Un elenco di tutti i dispositivi di questo tipo e del personale autorizzato all'accesso?	<ul style="list-style-type: none"> <li>Analizzare le politiche di utilizzo</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.4	Un metodo per determinare accuratamente e rapidamente proprietario, informazioni di contatto e scopo (ad esempio, etichettatura, codifica e/o inventariazione dei dispositivi)?	<ul style="list-style-type: none"> <li>Analizzare le politiche di utilizzo</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.5	Usi accettabili delle tecnologie?	<ul style="list-style-type: none"> <li>Analizzare le politiche di utilizzo</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.6	Posizioni di rete accettabili per le tecnologie?	<ul style="list-style-type: none"> <li>Analizzare le politiche di utilizzo</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.3.7	Elenco di prodotti approvati dalla società?	<ul style="list-style-type: none"> <li>Analizzare le politiche di utilizzo</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
12.3.8	Disconnessione automatica delle sessioni per tecnologie di accesso remoto dopo un periodo di tempo specifico di inattività?	<ul style="list-style-type: none"> <li>Analizzare le politiche di utilizzo</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>				
12.3.9	Attivazione di tecnologie di accesso remoto per fornitori e partner aziendali solo quando necessario, con disattivazione immediata dopo l'uso?	<ul style="list-style-type: none"> <li>Analizzare le politiche di utilizzo</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>				
12.3.10	(a) Per il personale che ha accesso ai dati dei titolari di carta tramite tecnologie di accesso remoto, la politica specifica il divieto di copiare, spostare o memorizzare tali dati su dischi rigidi locali e supporti elettronici rimovibili salvo espressa autorizzazione per una specifica esigenza aziendale?  <i>Laddove è presente un'esigenza aziendale autorizzata, le politiche che regolano l'uso devono richiedere la protezione dei dati in conformità a tutti i requisiti PCI DSS applicabili.</i>	<ul style="list-style-type: none"> <li>Analizzare le politiche di utilizzo</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>				
	(b) Per il personale in possesso di opportuna autorizzazione, la politica richiede la protezione dei dati dei titolari di carta in conformità ai Requisiti PCI DSS?	<ul style="list-style-type: none"> <li>Analizzare le politiche di utilizzo</li> <li>Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>				
12.4	La politica e le procedure per la sicurezza delle informazioni definiscono chiaramente le responsabilità in termini di protezione delle informazioni per tutto il personale?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure di sicurezza delle informazioni</li> <li>Consultare un campione di personale responsabile</li> </ul>	<input type="checkbox"/>				
12.4.1	<i>Questo requisito si applica solo ai provider di servizi.</i>						
12.5	(a) La responsabilità per la sicurezza delle informazioni è assegnata in modo formale ad un CSO (Chief Security Officer) o a un altro membro del management esperto in sicurezza?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure di sicurezza delle informazioni</li> </ul>	<input type="checkbox"/>				
	(b) Le seguenti responsabilità per la gestione della sicurezza delle informazioni sono state assegnate a una singola persona o a un team?						

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
12.5.1	Definizione, documentazione e distribuzione delle politiche e delle procedure di sicurezza?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure di sicurezza delle informazioni</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.5.2	Monitoraggio e analisi degli avvisi e delle informazioni sulla sicurezza e distribuzione al personale appropriato?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure di sicurezza delle informazioni</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
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?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure di sicurezza delle informazioni</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.5.4	Amministrazione di account utente, incluse aggiunte, eliminazione e modifiche?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure di sicurezza delle informazioni</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.5.5	Monitoraggio e controllo di tutti gli accessi ai dati?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure di sicurezza delle informazioni</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.6	(a) È in atto un programma formale di consapevolezza della sicurezza per rendere tutto il personale consapevole delle procedure e dei criteri di protezione dei dati dei titolari di carta?	<ul style="list-style-type: none"> <li>Analizzare il programma di consapevolezza della sicurezza</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	(b) Le procedure inserite nel programma di consapevolezza della sicurezza comprendono quanto segue:						
12.6.1	(a) Il programma di consapevolezza della sicurezza mette a disposizione diversi strumenti di comunicazione e formazione dei dipendenti (ad esempio, poster, lettere, promemoria, formazione basata su Web, riunioni e promozioni)?  <b>Nota:</b> i metodi possono essere diversi in funzione del ruolo svolto dal personale e del loro livello di accesso ai dati dei titolari di carta.	<ul style="list-style-type: none"> <li>Analizzare il programma di consapevolezza della sicurezza</li> <li>Analizzare le procedure legate al programma di consapevolezza della sicurezza</li> <li>Analizzare i record di partecipazione al programma di consapevolezza della sicurezza</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)					
		Sì	Sì con CCW	No	N/A	Non testato	
(b) È prevista la formazione del personale al momento dell'assunzione ed almeno una volta all'anno?	<ul style="list-style-type: none"> <li>Esaminare le procedure e la documentazione del programma di consapevolezza della sicurezza</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
(c) I dipendenti hanno completato la formazione sulla consapevolezza e conoscono l'importanza della sicurezza dei dati dei titolari di carta?	<ul style="list-style-type: none"> <li>Consultare il personale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
12.6.2	Al personale viene richiesto di certificare, almeno una volta all'anno, di aver letto e compreso la politica e le procedure di sicurezza?	<ul style="list-style-type: none"> <li>Esaminare le procedure e la documentazione del programma di consapevolezza della sicurezza</li> </ul>	<input type="checkbox"/>				
12.7	<p>Il personale potenziale (fare riferimento alla definizione di "personale" di cui sopra) viene sottoposto a screening prima dell'assunzione per ridurre al minimo il rischio di attacchi da fonti interne?</p> <p><i>Esempi di indagini sulla storia personale sono informazioni su impieghi precedenti, precedenti penali, storico del credito e controlli delle referenze.</i></p> <p><b>Nota:</b> per quel personale potenziale da assumere per determinate posizioni come cassieri di negozi, che hanno accesso a un solo numero di carta alla volta durante una transazione, questo requisito è solo consigliato.</p>	<ul style="list-style-type: none"> <li>Consultare la direzione del reparto per le risorse umane</li> </ul>	<input type="checkbox"/>				
12.8	Vengono mantenute e implementate politiche e procedure per gestire i provider di servizi con cui vengono condivisi i dati dei titolari di carta o che potrebbero incidere sulla sicurezza dei dati dei titolari di carta, come segue:						
12.8.1	È stato conservato un elenco di provider di servizi, inclusa una descrizione dei servizi forniti?	<ul style="list-style-type: none"> <li>Analizzare le politiche e le procedure</li> <li>Osservare i processi</li> <li>Analizzare un elenco dei provider di servizi</li> </ul>	<input type="checkbox"/>				

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
12.8.2	<p>Si conserva un accordo scritto in base al quale il provider di servizi si assume la responsabilità della protezione dei dati dei titolari di carta di cui entra in possesso o che memorizza, elabora o trasmette in altro modo per conto del cliente o nella misura in cui questi potrebbe avere un impatto sulla sicurezza dell'ambiente dei dati dei titolari di carta del cliente?</p> <p><b>Nota:</b> la formulazione corretta di un riconoscimento dipende dall'accordo tra le due parti, dai dettagli del servizio fornito e dalle responsabilità assegnate a ciascuna delle parti. Il riconoscimento non deve includere la formulazione corretta fornita nel presente requisito.</p>	<ul style="list-style-type: none"> <li>Osservare i contratti scritti</li> <li>Analizzare le politiche e le procedure</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.3	Esiste un processo definito per incaricare i provider di servizi, che includa tutte le attività di "due diligence" appropriate prima dell'incarico?	<ul style="list-style-type: none"> <li>Osservare i processi</li> <li>Analizzare le politiche e le procedure e la documentazione di supporto</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.4	È stato conservato un programma per monitorare lo stato di conformità agli standard PCI DSS dei provider di servizi con cadenza almeno annuale?	<ul style="list-style-type: none"> <li>Osservare i processi</li> <li>Analizzare le politiche e le procedure e la documentazione di supporto</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.8.5	Vengono conservate le informazioni su quali requisiti PCI DSS vengono gestiti da ogni provider di servizi e quali vengono gestiti dall'entità?	<ul style="list-style-type: none"> <li>Osservare i processi</li> <li>Analizzare le politiche e le procedure e la documentazione di supporto</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.9	<i>Questo requisito si applica solo ai provider di servizi.</i>						
12.10	È stato implementato un piano di risposta in preparazione alla risposta immediata a una violazione del sistema che includa quanto segue:						

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
12.10.1 (a) È stato creato un piano di risposta da implementare in caso di violazione del sistema?	<ul style="list-style-type: none"> <li>▪ Analizzare il piano di risposta agli incidenti</li> <li>▪ Analizzare le procedure per il piano di risposta agli incidenti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(b) Il piano include almeno i seguenti elementi?						
<ul style="list-style-type: none"> <li>• Ruoli, responsabilità e strategie di comunicazione e contatto in caso di violazione, nonché notifiche ai marchi di pagamento</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure per il piano di risposta agli incidenti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• Procedure specifiche di risposta agli incidenti</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure per il piano di risposta agli incidenti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• Procedure di ripristino e continuità delle attività aziendali</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure per il piano di risposta agli incidenti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• Processi di backup dei dati</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure per il piano di risposta agli incidenti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• Analisi dei requisiti legali per la segnalazione di violazioni</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure per il piano di risposta agli incidenti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• Copertura e risposte per tutti i componenti di sistema critici</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure per il piano di risposta agli incidenti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"> <li>• Riferimenti e descrizioni delle procedure di risposta agli incidenti adottate dai marchi di pagamento</li> </ul>	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure per il piano di risposta agli incidenti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.2 Il piano viene rivisto e testato almeno annualmente, inclusi tutti gli elementi elencati nel Requisito 12.10.1?	<ul style="list-style-type: none"> <li>▪ Analizzare le procedure per il piano di risposta agli incidenti</li> <li>▪ Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.3 Per rispondere a eventuali problemi è disponibile personale specifico 24 ore su 24, 7 giorni alla settimana?	<ul style="list-style-type: none"> <li>▪ Osservare i processi</li> <li>▪ Analizzare le politiche</li> <li>▪ Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
12.10.4	Viene fornita la formazione appropriata al personale con responsabilità di risposta a violazioni della sicurezza?	<ul style="list-style-type: none"> <li>▪ Osservare i processi</li> <li>▪ Analizzare le procedure per il piano di risposta agli incidenti</li> <li>▪ Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.5	Nel piano di risposta agli incidenti sono inclusi gli avvisi emessi dai sistemi di monitoraggio della sicurezza?	<ul style="list-style-type: none"> <li>▪ Osservare i processi</li> <li>▪ Analizzare le procedure per il piano di risposta agli incidenti</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.10.6	È stato sviluppato e messo in atto un processo per la modifica e il miglioramento del piano di risposta agli incidenti in base a quanto appreso e per incorporare gli sviluppi del settore?	<ul style="list-style-type: none"> <li>▪ Osservare i processi</li> <li>▪ Analizzare le procedure per il piano di risposta agli incidenti</li> <li>▪ Consultare il personale responsabile</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12.11	<i>Questo requisito si applica solo ai provider di servizi.</i>						

## Appendice A - Requisiti PCI DSS aggiuntivi

### Appendice A1 - Requisiti PCI DSS aggiuntivi per provider di hosting condiviso

Questa appendice non viene utilizzata per le valutazioni dell' esercente.

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

Domanda PCI DSS		Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
			Sì	Sì con CCW	No	N/A	Non testato
A2.1	<p>Per i terminali POS POI (e i punti di terminazione SSL/TLS a cui si connettono) che utilizzano SSL e/o TLS iniziale:</p> <ul style="list-style-type: none"> <li>È confermato che i dispositivi non sono soggetti a eventuali exploit noti per SSL/TLS iniziale</li> <li>O:</li> <li>È in atto un piano formale di migrazione e riduzione dei rischi in base al Requisito A2.2?</li> </ul>	<ul style="list-style-type: none"> <li>Analizzare la documentazione (ad esempio, documentazione del fornitore, dettagli di configurazione del sistema/della rete, ecc.) che verifica che i dispositivi POS POI non siano soggetti a eventuali exploit noti per SSL/TLS iniziale</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Domanda PCI DSS	Test previsti	Risposta (Selezionare una risposta per ogni domanda.)				
		Sì	Sì con CCW	No	N/A	Non testato
A2.2	<p>È in atto un piano formale di migrazione e di riduzione dei rischi per tutte le implementazioni che utilizzano SSL e/o TLS iniziale (diverso da quanto consentito in A2.1), che include:</p> <ul style="list-style-type: none"> <li>▪ descrizione dell'utilizzo, inclusi il tipo di dati trasmessi, i tipi e il numero di sistemi che utilizzano e/o supportano SSL/TLS iniziale come tipo di ambiente;</li> <li>▪ risultati della valutazione dei rischi e controlli per la riduzione dei rischi in atto;</li> <li>▪ descrizione dei processi per ricercare eventuali nuove vulnerabilità associate a SSL/TLS iniziale;</li> <li>▪ descrizione dei processi di controllo delle modifiche implementati per accertarsi che SSL/TLS iniziale non venga implementato nei nuovi ambienti;</li> <li>▪ panoramica del piano del progetto di migrazione inclusa la data di completamento della migrazione prevista non oltre il 30 giugno 2018?</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A2.3	<i>Questo requisito si applica solo ai provider di servizi.</i>					

### Appendice A3 - Convalida aggiuntiva delle entità designate (DESV)

Questa appendice si applica solo alle entità designate da un acquirente o un marchio di pagamento che richiedono la convalida aggiuntiva di requisiti PCI DSS esistenti. Le entità che richiedono la convalida in questo appendice devono utilizzare il modello di reporting aggiuntivo DESV e l'Attestato di conformità aggiuntivo per il reporting e consultare l'acquirente e/o il marchio di pagamento applicabile per le procedure di invio.

## Appendice B - Foglio di lavoro - Controlli compensativi

Utilizzare questo foglio di lavoro per definire i controlli compensativi per qualsiasi requisito per il quale è stata selezionata la risposta "Sì con CCW".

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

Per informazioni sui controlli compensativi e per istruzioni su come completare il presente foglio di lavoro, consultare le appendici B, C e D degli standard PCI DSS.

### Numero e definizione del requisito:

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





## Sezione 3 - Dettagli su convalida e attestato

### Parte 3. Convalida PCI DSS

Questo AOC si basa sui risultati annotati nel questionario SAQ D (Sezione 2), datato (*data di completamento SAQ*).

In base ai risultati documentati nel questionario SAQ D indicato sopra, i firmatari di cui alle Parti 3b-3d, come applicabile, dichiarano il seguente stato di conformità dell'entità identificata nella Parte 2 di questo documento: (*selezionare un'opzione*):

<input type="checkbox"/>	<p><b>Conforme:</b> Tutte le sezioni del questionario PCI DSS SAQ sono state completate e a tutte le domande è stato risposto in modo affermativo, determinando una valutazione di <b>CONFORMITÀ</b> globale; pertanto (<i>Ragione sociale esercente</i>) ha dimostrato la massima conformità agli standard PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non conforme:</b> non tutte le sezioni del questionario PCI DSS SAQ sono state completate o non a tutte le domande è stata fornita una risposta affermativa, determinando una valutazione di <b>NON CONFORME</b> globale; pertanto (<i>Ragione sociale esercente</i>) non ha dimostrato la massima conformità agli standard PCI DSS.</p> <p><b>Data di destinazione</b> per conformità:</p> <p>è possibile che a un'entità che invia questo modulo con lo stato "Non conforme" venga richiesto di completare il Piano d'azione presente nella Parte 4 del presente documento. <i>Consultare il proprio acquirente o il marchio di pagamento prima di completare la Parte 4.</i></p>						
<input type="checkbox"/>	<p><b>Conforme ma con eccezione legale:</b> uno o più requisiti sono stati contrassegnati con "No" a causa di una restrizione legale che impedisce di rispondere al requisito. Questa opzione richiede un'ulteriore revisione da parte dell'acquirente o del marchio di pagamento.</p> <p><i>Se selezionata, completare quanto segue:</i></p> <table border="1" data-bbox="289 1129 1409 1304"> <thead> <tr> <th>Requisito interessato</th> <th>Dettagli su come il vincolo legale impedisce la conformità ai requisiti</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Requisito interessato	Dettagli su come il vincolo legale impedisce la conformità ai requisiti				
Requisito interessato	Dettagli su come il vincolo legale impedisce la conformità ai requisiti						

### Parte 3a. Riconoscimento dello stato

I firmatari confermano:

(*Selezionare tutte le risposte pertinenti*)

<input type="checkbox"/>	Il questionario di autovalutazione D PCI DSS, versione ( <i>versione di SAQ</i> ), è stato completato in base alle istruzioni qui fornite.
<input type="checkbox"/>	Tutte le informazioni contenute nel questionario SAQ e in questo attestato rappresentano in modo onesto i risultati della mia valutazione sotto tutti gli aspetti.
<input type="checkbox"/>	Ho verificato con il fornitore dell'applicazione di pagamento che il mio sistema di pagamento non memorizza dati sensibili di autenticazione dopo l'autorizzazione.
<input type="checkbox"/>	Ho letto gli standard PCI DSS e accetto di garantire sempre la massima conformità a tali standard in ogni momento, in base a quanto applicabile al mio ambiente.
<input type="checkbox"/>	Se il mio ambiente cambia, accetto di dover rivalutare l'ambiente e implementare eventuali requisiti PCI DSS in base alle necessità.

### Parte 3a. Riconoscimento dello stato (continua)

<input type="checkbox"/>	Nessuna prova della memorizzazione dei dati della traccia completa <sup>1</sup> , dei dati CAV2, CVC2, CID o CVV2 <sup>2</sup> oppure dei dati PIN <sup>3</sup> dopo che l'autorizzazione alla transazione è stata individuata su QUALSIASI sistema esaminato durante questa valutazione.
<input type="checkbox"/>	Le scansioni ASV vengono completate dal Fornitore di prodotti di scansione approvato (ASV) PCI SSC (Nome ASV)

### Parte 3b. Attestato esercente

<i>Firma del funzionario esecutivo dell'esercente</i> ↑	<i>Data:</i>
<i>Nome del funzionario esecutivo dell'esercente:</i>	<i>Mansione:</i>

### Parte 3c. Riconoscimento dell'azienda qualificata per la valutazione (QSA) (se applicabile)

Se un QSA è stato coinvolto o aiutato durante questa valutazione, descrivere il ruolo ricoperto:	
--	--

<i>Firma del funzionario espressamente autorizzato dell'azienda QSA</i> ↑	<i>Data:</i>
<i>Nome del funzionario espressamente autorizzato:</i>	<i>Azienda QSA:</i>

### Parte 3d. Coinvolgimento dell'azienda interna per la valutazione (ISA) (se applicabile)

Se un ISA è stato coinvolto o aiutato durante questa valutazione, identificare il personale ISA e descrivere il ruolo ricoperto:	
--	--

### Parte 4. Piano d'azione per i requisiti non conformi

Selezionare la risposta appropriata per "Conforme ai requisiti PCI DSS" per ogni requisito. In caso di

<sup>1</sup> Dati codificati nella striscia magnetica o dati equivalenti su un chip utilizzati per l'autorizzazione durante una transazione con carta presente. Le entità non possono conservare i dati della traccia completa dopo l'autorizzazione della transazione. I soli elementi dei dati di traccia che possono essere conservati sono il PAN, la data di scadenza e il nome del titolare della carta.

<sup>2</sup> Il valore di tre o quattro cifre stampato nel riquadro della firma o nella parte anteriore di una carta di pagamento utilizzato per verificare le transazioni con carta non presente.

<sup>3</sup> Numero di identificazione personale inserito dal titolare della carta durante una transazione con carta presente e/o blocco PIN cifrato presente all'interno del messaggio di transazione.

risposta negativa a uno dei requisiti, è necessario fornire la data in cui si prevede che la Società sarà conforme al requisito e una breve descrizione delle azioni che verranno intraprese per soddisfare il requisito. Consultare il proprio acquirente o il marchio di pagamento prima di completare la Parte 4.

Requisito PCI DSS	Descrizione del requisito	Conforme ai requisiti PCI DSS (Selezionarne uno)		Data della soluzione e azioni (Se è stata selezionata l'opzione "NO" per un qualsiasi requisito)
		Sì	NO	
1	Installare e gestire una configurazione firewall per proteggere i dati dei titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
2	Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione	<input type="checkbox"/>	<input type="checkbox"/>	
3	Proteggere i dati dei titolari di carta memorizzati	<input type="checkbox"/>	<input type="checkbox"/>	
4	Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche	<input type="checkbox"/>	<input type="checkbox"/>	
5	Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus	<input type="checkbox"/>	<input type="checkbox"/>	
6	Sviluppare e gestire sistemi e applicazioni protette	<input type="checkbox"/>	<input type="checkbox"/>	
7	Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario	<input type="checkbox"/>	<input type="checkbox"/>	
8	Individuare e autenticare l'accesso ai componenti di sistema	<input type="checkbox"/>	<input type="checkbox"/>	
9	Limitare l'accesso fisico ai dati dei titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
10	Registrare e monitorare tutti gli accessi a risorse di rete e dati dei titolari di carta	<input type="checkbox"/>	<input type="checkbox"/>	
11	Eseguire regolarmente test dei sistemi e processi di protezione	<input type="checkbox"/>	<input type="checkbox"/>	
12	Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale	<input type="checkbox"/>	<input type="checkbox"/>	
Appendice A2	Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale	<input type="checkbox"/>	<input type="checkbox"/>	

