



**Payment Card Industry (PCI)  
Data Security Standard  
Questionario di autovalutazione**

---

**Istruzioni e linee guida**

**Versione 2.0**

Ottobre 2010

## Modifiche del documento

---

Data	Versione	Descrizione
1 ottobre 2008	1.2	Allineare il contenuto con i nuovi standard PCI DSS v1.2 e implementare modifiche minori apportate dopo la versione originale v1.1.
28 ottobre 2010	2.0	Allineare il contenuto ai nuovi standard PCI DSS v2.0 e chiarire i tipi di ambienti SAQ ed i criteri di idoneità. Aggiunta di SAQ C-VT per esercenti di terminali virtuali basati su Web

## Sommario

---

<b>Istruzioni e linee guida Versione 2.0 Ottobre 2010.....</b>	<b>1</b>
<b>Modifiche del documento .....</b>	<b>2</b>
<b>Informazioni sul documento .....</b>	<b>4</b>
<b>Autovalutazione PCI DSS: Compatibilità .....</b>	<b>5</b>
<b>PCI DSS: Documenti correlati .....</b>	<b>6</b>
<b>Panoramica del questionario di autovalutazione (SAQ).....</b>	<b>7</b>
<b>Perché è importante la conformità agli standard PCI DSS?.....</b>	<b>8</b>
<b>Suggerimenti generali e strategie per prepararsi per la convalida della conformità</b>	<b>9</b>
<b>Scelta del questionario di autovalutazione e dell'attestato più appropriati per la propria azienda.....</b>	<b>12</b>
SAQ A – Esercenti con carta non presente, tutte le funzioni per i dati di titolari di carta sono fornite dall'esterno.....	12
SAQ B - Esercenti che utilizzano solo macchinette stampigliatrici oppure solo terminali per connessione in uscita indipendenti. Nessuna memorizzazione elettronica dei dati dei titolari di carta.	14
SAQ C-VT – Esercenti con terminali virtuali basati su Web, Nessuna memorizzazione elettronica dei dati dei titolari di carta .....	14
SAQ C – Esercenti con sistemi di pagamento connessi a Internet, nessuna memorizzazione elettronica dei dati dei titolari di carta .....	15
SAQ D – Tutti gli altri esercenti e provider di servizi definiti da un marchio di pagamento come idonei alla compilazione del questionario SAQ .....	16
<b>Guida per la non applicabilità di determinati requisiti specifici.....</b>	<b>17</b>
<b>Istruzioni per il completamento del questionario SAQ .....</b>	<b>17</b>
<b>Qual è il questionario più adatto all'ambiente della propria azienda?.....</b>	<b>18</b>

## Informazioni sul documento

---

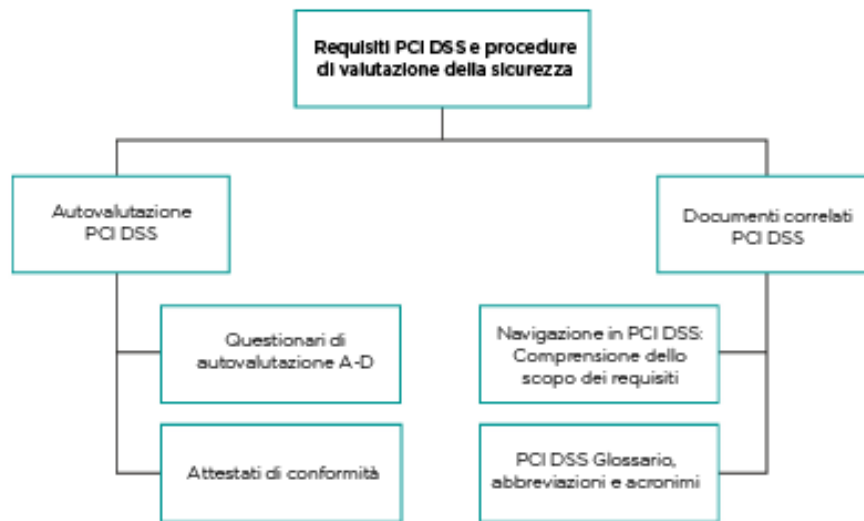
Questo documento è stato sviluppato per aiutare gli esercenti e i provider di servizi a comprendere il questionario di autovalutazione (SAQ, Self-Assessment Questionnaire) degli standard di sicurezza (DSS, Data Security Standard) PCI. Leggere completamente il documento per comprendere il motivo per cui gli standard PCI DSS sono importanti per la propria azienda, le possibili strategie da utilizzare per facilitare la convalida della conformità e determinare se la propria azienda dispone dei requisiti necessari per completare una delle versioni del questionario più brevi. Nelle sezioni seguenti vengono fornite tutte le informazioni necessarie sul questionario di autovalutazione PCI DSS.

- Autovalutazione PCI DSS: Compatibilità
- PCI DSS: Documenti correlati
- Panoramica del questionario di autovalutazione (SAQ)
- Perché è importante la conformità agli standard PCI DSS?
- Suggerimenti generali e strategie per prepararsi per la convalida della conformità
- Scelta del questionario e dell'attestato più appropriati per la propria azienda
- Guida per la non applicabilità di determinati requisiti specifici
- Istruzioni per il completamento del questionario SAQ
- Qual è il questionario più adatto all'ambiente della propria azienda?

## Autovalutazione PCI DSS: Compatibilità

Gli standard di sicurezza dei dati PCI e i documenti correlati rappresentano una serie comune di strumenti e misurazioni del settore che consentono di gestire in modo più sicuro le informazioni riservate. Gli standard forniscono una struttura azionabile per lo sviluppo di un processo per la protezione dei dati dei clienti affidabile, che comprende la prevenzione, il rilevamento e la risposta a problemi di sicurezza. Per limitare il rischio di violazioni della sicurezza e ridurre l'impatto, è importante che tutte le entità che memorizzano, elaborano o trasmettono dati di titolari di carta agiscano nel rispetto di tali standard. Il grafico seguente mostra gli strumenti che aiutano le diverse entità interessate a garantire la conformità agli standard di sicurezza dei dati PCI e ad eseguire la relativa autovalutazione.

Questi ed altri documenti correlati sono disponibili all'indirizzo [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).



## PCI DSS: Documenti correlati

I seguenti documenti sono stati creati per una migliore comprensione degli standard PCI DSS e dei questionari di autovalutazione appropriati da parte di esercenti e provider di servizi.

Documento	Destinatari
<i>PCI DSS: Requisiti e procedure di valutazione della sicurezza</i>	Tutti gli esercenti e i provider di servizi
<i>Navigazione in PCI DSS: Comprensione dello scopo dei requisiti</i>	Tutti gli esercenti e i provider di servizi
<i>PCI DSS: Istruzioni e linee guida per l'autovalutazione</i>	Tutti gli esercenti e i provider di servizi
<i>PCI DSS: Questionario di autovalutazione A e Attestato</i>	Esercenti idonei <sup>1</sup>
<i>PCI DSS: Questionario di autovalutazione B e Attestato</i>	Esercenti idonei <sup>1</sup>
<i>PCI DSS: Questionario di autovalutazione C-VT e Attestato</i>	Esercenti idonei <sup>1</sup>
<i>PCI DSS: Questionario di autovalutazione C e Attestato</i>	Esercenti idonei <sup>1</sup>
<i>PCI DSS: Questionario di autovalutazione D e Attestato</i>	Esercenti e provider di servizi idonei <sup>1</sup>
<i>PCI Data Security Standard e Payment Application Data Security Standard: Glossario, abbreviazioni e acronimi</i>	Tutti gli esercenti e i provider di servizi

<sup>1</sup> Per stabilire il Questionario di autovalutazione più adatto, fare riferimento a "Scelta del questionario SAQ e dell'attestato più appropriati per la propria azienda", a pagina 12 del presente documento.

## Panoramica del questionario di autovalutazione (SAQ)

---

Il *questionario di autovalutazione della conformità agli standard di sicurezza dei dati PCI* è uno strumento di convalida che assiste esercenti e provider di servizi nell'autovalutazione della propria conformità agli standard di sicurezza dei dati delle carte di pagamento (PCI DSS). Per soddisfare diversi scenari, sono disponibili tre versioni del questionario di autovalutazione PCI DSS. Questo documento è stato sviluppato per aiutare le aziende a scegliere il questionario più appropriato alle loro esigenze.

Il questionario di autovalutazione PCI DSS è uno strumento di convalida per esercenti e provider di servizi che non sono tenuti a presentare un Rapporto sulla conformità per la valutazione della sicurezza dei dati in sede, in conformità a *Requisiti PCI DSS e procedure di valutazione della sicurezza* come può essere richiesto dal proprio acquirente o marchio di pagamento. Consultare l'acquirente o il marchio di pagamento per informazioni dettagliate sui requisiti di convalida PCI DSS.

Il questionario di autovalutazione degli standard PCI DSS è costituito dai seguenti componenti:

1. Domande correlate ai requisiti PCI DSS, appropriate per provider di servizi ed esercenti: vedere la sezione "Scelta del questionario SAQ e dell'attestato più appropriati per la propria azienda" nel presente documento.
2. Attestato di conformità: L'Attestato rappresenta l'autocertificazione della propria idoneità ad eseguire e aver effettivamente eseguito un'autovalutazione PCI DSS.

## Perché è importante la conformità agli standard PCI DSS?

---

I membri del PCI Security Standards Council (American Express, Discover, JCB, MasterCard e Visa) controllano continuamente casi di compromissione dei dati dei clienti. Questi casi riguardano l'intera gamma di aziende, da aziende di piccole dimensioni a esercenti e provider di servizi molto grandi.

Una violazione della sicurezza e la successiva compromissione dei dati della carta di pagamento hanno effetti di vasta portata sulle entità interessate, tra cui:

1. Obbligo di notifica alle autorità regolatorie
2. Danni alla reputazione
3. Perdita di clienti
4. Possibili responsabilità finanziarie (ad esempio, sanzioni regolatorie e altre sanzioni e multe)
5. Cause legali

L'analisi post-mortem dei danni ha mostrato i punti deboli comuni in termini di sicurezza che sono risolti dagli standard di sicurezza dei dati PCI, ma che non erano stati presi in considerazione nelle aziende in cui si sono verificati tali problemi. Gli standard PCI DSS includono requisiti dettagliati esattamente per questo motivo, ossia per ridurre al minimo la possibilità di compromettere la sicurezza dei dati e i conseguenti effetti.

In base ad alcune indagini eseguite successivamente, sono state rilevate alcune violazioni degli standard PCI DSS comuni, incluse senza limitazione:

- Memorizzazione di dati della striscia magnetica (requisito 3.2). È importante tenere presente che molte entità danneggiate non sono a conoscenza del fatto che i relativi sistemi memorizzano questi dati.
- Controlli dell'accesso inadeguati dovuti a sistemi POS per esercenti installati in modo non corretto, che consentono ad utenti non autorizzati di accedere ad aree destinate ai fornitori di POS (requisiti 7.1, 7.2, 8.2 e 8.3)
- Impostazioni di sistema e password predefinite non modificate dal momento della configurazione del sistema (requisito 2.1)
- Servizi non necessari e non sicuri che non vengono rimossi o protetti al momento della configurazione del sistema (requisiti 2.2.2 e 2.2.4)
- Applicazioni Web codificate in modo scadente che portano a problemi di SQL Injection e altre vulnerabilità e consentono di accedere al database contenente i dati dei titolari di carta di direttamente dal sito Web (requisito 6.5)
- Patch di sicurezza mancanti e obsolete (requisito 6.1)
- Perdita dei log (requisito 10)
- Mancanza di meccanismi di monitoraggio (mediante revisioni di log, rilevazione/prevenzione delle intrusioni, analisi delle vulnerabilità trimestrali e sistemi di monitoraggio dell'integrità dei file) (requisiti 10.6, 11.2, 11.4 e 11.5)
- Segmentazione di rete implementata in modo insufficiente che determina l'esposizione inconsapevole dell'ambiente dei dati dei titolari di carta attraverso punti deboli in altre parti della rete che non sono state protette in conformità agli standard PCI SS (ad esempio, da punti di accesso wireless non sicuri e vulnerabilità introdotte tramite posta elettronica dei dipendenti ed esplorazione Web) (requisiti 1.2, 1.3 e 1.4)

## Suggerimenti generali e strategie per prepararsi per la convalida della conformità

---

Di seguito alcuni suggerimenti generali e strategie per convalidare la propria conformità agli standard PCI DSS. Questi suggerimenti possono aiutare a eliminare i dati non necessari, isolare i dati necessari in aree centralizzate definite e controllate e limitare l'ambito della convalida della conformità agli standard PCI DSS. Ad esempio, eliminando i dati che non sono necessari e/o isolando i dati di cui si ha bisogno in aree controllate e definite, è possibile eliminare dall'ambito della propria autovalutazione sistemi e reti che non memorizzano, elaborano, o trasmettono i dati dei titolari di carta e che non si collegano a sistemi che lo fanno.

1. **Dati sensibili di autenticazione (includono il contenuto completo della traccia della striscia magnetica o del chip, i codici e i valori di validazione della carta, PIN e blocchi PIN):**
  - a. Accertarsi di ***non memorizzare mai questi dati***.
  - b. In caso di dubbio, contattare il fornitore del sistema POS per verificare se il prodotto e la versione software in uso memorizza tali dati. In alternativa, prendere in esame l'assunzione di un Qualified Security Assessor (QSA) in grado di fornire il supporto necessario per determinare se dati sensibili di autenticazione sono memorizzati, registrati o acquisiti dal sistema in uso.
2. **In qualità di esercente, chiedere al fornitore del sistema POS informazioni sulla sicurezza del sistema in uso, ponendo le seguenti domande consigliate:**
  - a. Il mio software POS è convalidato per gli standard PA-DSS? (Fare riferimento all'elenco PCI SSC di Applicazioni di pagamento convalidate).
  - b. Il mio software POS memorizza dati della striscia magnetica (dati su traccia) o blocchi PIN? In tal caso, poiché questa memorizzazione è vietata, può aiutarmi a eliminare tali dati nel tempo più breve possibile?
  - c. Il mio software POS memorizza i PAN (Primary Account Number)? In tal caso, poiché questa memorizzazione deve essere protetta, in che modo il POS protegge tali dati?
  - d. È in atto un processo per creare un elenco dei file scritti dall'applicazione con un riepilogo del contenuto di ciascun file che consenta di verificare che tali dati di cui è vietata la conservazione non siano realmente memorizzati?
  - e. Il sistema POS richiede l'installazione di firewall per proteggere il mio sistema da un accesso non autorizzato?
  - f. Sono necessarie password complesse e univoche per accedere ai miei sistemi? Può confermare che non vengono utilizzate password comuni o predefinite per accedere al mio sistema e ai sistemi di altri esercenti suoi clienti?
  - g. Le impostazioni e le password predefinite sono state modificate nei sistemi e nei database che fanno parte del sistema POS?
  - h. Tutti i servizi non necessari e non sicuri sono stati rimossi dai sistemi e dai database che fanno parte del sistema POS?
  - i. Può accedere in remoto al mio sistema POS? In tal caso, ha implementato controlli appropriati per impedire ad altre persone di accedere al mio sistema POS, ad esempio metodi di accesso remoto sicuri e non tramite password comuni o predefinite? Con quale frequenza accede al mio sistema POS in remoto e perché? Chi è autorizzato ad accedere al mio sistema POS in remoto?
  - j. Tutti i sistemi e i database che fanno parte del sistema POS sono stati aggiornati con tutte le patch di sicurezza applicabili?

- k. La funzionalità di creazione di file di log è attivata per i sistemi e i database che fanno parte del sistema POS?
- l. Se le versioni precedenti del mio software POS prevedevano la memorizzazione dei dati su traccia, questa funzione è stata rimossa dall'attuale versione del software POS? È stata utilizzata una funzionalità per la pulizia del sistema sicura per rimuovere questi dati?

### 3. Dati di titolari di carta — Se non sono necessari, non conservarli!

- a. Le regole dei marchi di pagamento consentono la memorizzazione del numero PAN (Personal Account Number, numero account personale), della data di scadenza, del nome del titolare e del codice di servizio.
- b. Fare un inventario di tutti i motivi e i luoghi in cui si conservano questi dati. Se i dati non sono più necessari per uno scopo aziendale significativo, considerarne l'eliminazione.
- c. Determinare se la conservazione di tali dati e il processo aziendale basato su tale conservazione giustificano i seguenti rischi:
  - i. Compromissione dei dati
  - ii. Necessità di ulteriori azioni per proteggere tali dati nel rispetto degli standard PCI DSS
  - iii. Necessità di azioni di manutenzione continue per rimanere conformi agli standard PCI DSS nel tempo

### 4. Dati di titolari di carta — Se sono necessari, consolidarli e isolarli.

È possibile limitare l'ambito di una valutazione della conformità agli standard PCI DSS conservando i dati in un ambiente specifico e isolando tali dati mediante l'uso di un'adeguata segmentazione di rete. Ad esempio, se i dipendenti navigano in Internet e ricevono un messaggio e-mail sullo stesso computer o sullo stesso segmento di rete utilizzato per i dati di titolari di carta, considerare la segmentazione (isolamento) di tali dati in un computer o in un segmento di rete specifico (ad esempio, mediante router o firewall). Un isolamento efficiente dei dati di titolari di carta consente di concentrare i propri sforzi per garantire la conformità agli standard PCI DSS solo sulla parte isolata anziché su tutti i computer.

### 5. Controlli compensativi

È possibile considerare controlli compensativi per la maggior parte dei requisiti PCI DSS quando un'entità non è in grado di soddisfare le specifiche tecniche di un requisito, ma ha posto in essere altri controlli sufficienti a mitigare il rischio associato a tale requisito attraverso dei controlli alternativi. Se la società non dispone del controllo completo indicato negli standard PCI DSS ma ha attivato altri controlli che soddisfano la definizione PCI DSS di controlli compensativi (vedere "Controlli compensativi" nell'Appendice SAQ applicabile e il documento *PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi* disponibile all'indirizzo [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)), la società dovrebbe fare quanto segue:

- a. Rispondere "Sì" alla domanda del questionario SAQ e, nella colonna "Speciale", annotare l'uso di ciascun controllo compensativo utilizzato per soddisfare un requisito.
- b. Rivedere la sezione "Controlli compensativi" nell'appendice B del questionario SAQ applicabile e documentare l'uso di tali controlli completando il corrispondente foglio di lavoro nell'Appendice C del SAQ.
- c. Completare un foglio di lavoro dei controlli compensativi per ciascun requisito soddisfatto con un controllo di questo tipo.
- d. Inviare tutti i fogli di lavoro dei controlli compensativi, insieme al questionario completato e/o all'attestato, in base alle istruzioni dell'acquirente o del marchio di pagamento.

## 6. Formazione ed assistenza professionale

- a. Se si desidera ricevere istruzioni e linee guida da un professionista della sicurezza per garantire la conformità e completare il questionario SAQ, non esitare. Considerare, tuttavia, che, sebbene sia possibile scegliere qualsiasi professionista della sicurezza si desidera, solo i professionisti inclusi nell'elenco di Qualified Security Assessor (QSA) di PCI SSC sono riconosciuti come QSA e formati da PCI SSC. Questo elenco è disponibile all'indirizzo [https://www.pcisecuritystandards.org/pdfs/pci\\_qsa\\_list.pdf](https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf).
- b. PCI Security Standards Council (SSC) mette a disposizione una serie di risorse formative per promuovere la consapevolezza della sicurezza nell'ambito del settore delle carte di pagamento. Queste risorse comprendono formazione PCI DSS per Internal Security Assessor (ISA) e formazione sugli standard. Anche il sito Web di PCI SCC rappresenta una fonte primaria di risorse aggiuntive, tra cui:
- La *Guida* di navigazione in PCI DSS
  - Il *PCI DSS e PA-DSS Glossario, abbreviazioni e acronimi*
  - FAQ
  - Webinar
  - Supplementi informativi e linee guida
  - Attestati di conformità

Per ulteriori informazioni, fare riferimento a [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

**Nota:** i Supplementi informativi completano gli standard PCI DSS e individuano ulteriori considerazioni e raccomandazioni per soddisfare i requisiti PCI DSS, senza però modificare, eliminare o sostituirsi agli standard PCI DSS o ad alcuno dei suoi requisiti.

## Scelta del questionario di autovalutazione e dell'attestato più appropriati per la propria azienda

In base alle regole del marchio di pagamento, tutti gli esercenti e i provider di servizi devono garantire la conformità a tutti gli standard PCI DSS. Esistono cinque categorie SAQ, illustrate brevemente nella tabella seguente e descritte in maggior dettaglio nei paragrafi successivi. Utilizzare la tabella per valutare quale questionario SAQ è più appropriato per la propria azienda ed esaminare le descrizioni dettagliate per accertarsi di soddisfare tutti i requisiti previsti nel questionario scelto.

SAQ	Descrizione
A	Esercenti con carta non presente (e-commerce o via posta/telefono), tutte le funzioni per i dati di titolari di carta sono fornite dall'esterno. <i>Non applicabile mai ad esercenti con contatto diretto con il cliente.</i>
B	Esercenti che utilizzano solo macchinetta stampigliatrice senza alcuna memorizzazione elettronica dei dati di titolari di carta, oppure esercenti con terminali per connessione in uscita indipendenti senza alcuna memorizzazione elettronica dei dati di titolari di carta
C-VT	Esercenti che utilizzano solo terminali virtuali basati su Web, senza alcuna memorizzazione elettronica dei dati di titolari di carta
C	Esercenti con sistemi di pagamento connessi a Internet, nessuna memorizzazione dei dati di titolari di carta
D	Tutti gli altri esercenti non inclusi nelle descrizioni dei questionari SAQ A-C precedenti e <b>tutti i provider di servizi</b> definiti da un marchio di pagamento come idonei alla compilazione di un questionario SAQ.

### SAQ A – Esercenti con carta non presente, tutte le funzioni per i dati di titolari di carta sono fornite dall'esterno

*Il questionario SAQ A è stato sviluppato per rispondere ai requisiti applicabili ad esercenti che conservano solo resoconti o ricevute cartacee con i dati di titolari di carta e non i dati stessi in formato elettronico e che non elaborano o trasmettono tali dati nei loro sistemi o in sede.*

*Per una guida grafica per la scelta del tipo di SAQ, vedere "Quale SAQ si adatta meglio al proprio ambiente?" a pagina 17.*

Gli esercenti SAQ A non memorizzano i dati di titolari di carta in formato elettronico, non elaborano o trasmettono tali dati nei loro sistemi o in sede e convalidano la propria conformità completando il questionario SAQ A e l'attestato di conformità ad esso associato, confermando che:

- La società accetta solo transazioni con carta non presente (e-commerce o via posta/telefono).
- La società non memorizza, elabora o trasmette dati di titolari di carta nei sistemi o in sede, ma si affida interamente a provider di servizi di terze parti per tutte queste operazioni.
- La società ha confermato che la terza parte che si occupa della memorizzazione, dell'elaborazione e/o della trasmissione dei dati di titolari di carta è conforme agli standard PCI DSS.

- La società conserva solo resoconti o ricevute cartacee con i dati di titolari di carta e questi documenti non sono in formato elettronico.
- La società non memorizza i dati di titolari di carta in formato elettronico.

**Questa opzione non è mai applicabile ad esercenti con un ambiente POS che prevede il contatto diretto con i clienti.**

## **SAQ B - Esercenti che utilizzano solo macchinette stampigliatrici oppure solo terminali per connessione in uscita indipendenti. Nessuna memorizzazione elettronica dei dati dei titolari di carta.**

*Il questionario SAQ B è stato sviluppato per rispondere ai requisiti applicabili ad esercenti che elaborano i dati di titolari di carta solo tramite macchinette stampigliatrici o terminali per connessione in uscita indipendenti.*

Gli esercenti SAQ B elaborano i dati dei titolari di carta solo tramite macchinette stampigliatrici oppure mediante terminali per connessione in uscita indipendenti e possono essere società con punti vendita reali (carta presente) oppure società di e-commerce o vendita tramite posta elettronica/telefono (carta non presente). Tali esercenti devono convalidare la propria conformità completando il questionario SAQ B e l'attestato di conformità ad esso associato, confermando che:

- La società utilizza solo una macchinetta stampigliatrice e/o terminali per connessione in uscita indipendenti (connessi tramite la linea telefonica al processore) per acquisire i dati della carta di pagamento dei clienti.
- I terminali per connessione in uscita indipendenti non sono connessi ad altri sistemi all'interno dell'ambiente.
- I terminali per connessione in uscita indipendenti non sono connessi a Internet.
- La società non trasmette dati dei titolari di carta di tramite una rete (rete interna o Internet).
- La società conserva solo resoconti o ricevute cartacee con i dati di titolari di carta e questi documenti non sono ricevuti in formato elettronico.
- La società non memorizza i dati di titolari di carta in formato elettronico.

*Per una guida grafica per la scelta del tipo di SAQ, vedere "Quale SAQ si adatta meglio al proprio ambiente?" a pagina 17.*

## **SAQ C-VT – Esercenti con terminali virtuali basati su Web, Nessuna memorizzazione elettronica dei dati dei titolari di carta**

*Il questionario SAQ C-VT è stato sviluppato per rispondere ai requisiti applicabili a tutti gli esercenti che elaborano i dati dei titolari di carta solo mediante terminali virtuali isolati su computer connessi a Internet.*

Un terminale virtuale è un accesso basato su browser Web al sito Web di un acquirente, elaboratore o provider di servizi di terzi per autorizzare le transazioni della carta di pagamento, in cui l'esercente inserisce manualmente i dati della carta mediante un browser Web connesso in modo sicuro. A differenza dei terminali fisici, quelli virtuali non leggono i dati direttamente da una carta di pagamento. Dal momento che le transazioni della carta di pagamento sono inserite manualmente, i terminali virtuali sono in genere usati al posto dei terminali fisici in ambienti di esercenti con un volume limitato di transazioni.

Questi esercenti elaborano i dati dei titolari di carta solo tramite un terminale virtuale e non memorizzano tali dati su alcun computer. Questi terminali virtuali sono connessi a Internet per accedere

*Per una guida grafica per la scelta del tipo di SAQ, vedere "Quale SAQ si adatta meglio al proprio ambiente?" a pagina 17.*

a terze parti che ospitano la funzione di elaborazione del pagamento del terminale virtuale. Questa terza parte può essere un elaboratore, un acquirente o un altro provider di servizi di terzi che memorizza, elabora e/o trasmette i dati dei titolari di carta per autorizzare e/o contabilizzare le transazioni di pagamento del terminale virtuale dell'esercente.

L'applicazione di questa opzione SAQ riguarda solo gli esercenti che inseriscono manualmente una singola transazione per volta con una tastiera in una soluzione di terminale virtuale basato su Web.

Gli esercenti SAQ C-VT elaborano i dati dei titolari di carta utilizzando terminali virtuali connessi a Internet, non memorizzano dati dei titolari di carta su alcun computer, e possono essere società con punti vendita reali (carta presente) oppure società con vendita per posta/telefono (carta non presente). Tali esercenti devono convalidare la propria conformità completando il questionario SAQ C-VT e l'attestato di conformità ad esso associato, confermando che:

- L'unica elaborazione di pagamenti della società viene effettuata mediante un terminale virtuale a cui si accede mediante un browser Web collegato ad Internet.
- La soluzione di terminale virtuale della società è fornita ed ospitata da un provider di servizi di terze parti convalidato PCI DSS.
- La società accede alla soluzione di terminale virtuale conforme PCI DSS via computer ed è isolata in un'unica posizione e non è collegata ad altre posizioni o sistemi nell'ambito del suo ambiente (ciò si può ottenere mediante segmentazione di rete o firewall per isolare il computer dagli altri sistemi).
- Il computer della società non ha software installato che determina la memorizzazione dei dati dei titolari di carta (ad esempio, non vi è alcun software per elaborazione batch o store-and-forward);
- Il computer della società non dispone di alcun dispositivo hardware collegato che viene usato per acquisire o memorizzare i dati dei titolari di carta (ad esempio non è collegato alcun lettore di carte);
- La società non riceve o trasmette in altro modo i dati dei titolari di carta elettronicamente tramite alcun canale (ad esempio mediante una rete interna o Internet);
- La società conserva solo resoconti o copie cartacee delle ricevute.
- La società non memorizza i dati di titolari di carta in formato elettronico.

**Questa opzione non si applica mai alle società di e-commerce.**

## **SAQ C – Esercenti con sistemi di pagamento connessi a Internet, nessuna memorizzazione elettronica dei dati dei titolari di carta**

*Il questionario SAQ C è stato sviluppato per rispondere ai requisiti applicabili ad esercenti i cui sistemi di pagamento (ad esempio, sistemi POS) sono connessi a Internet (ad esempio tramite DSL, modem via cavo, ecc.) per uno dei due seguenti motivi:*

1. *Il sistema di pagamento si trova su un computer connesso a Internet (ad esempio, per operazioni e-mail o esplorazione Web), oppure*
2. *Il sistema di pagamento è connesso a Internet per trasmettere i dati di titolari di carta.*

*Per una guida grafica per la scelta del tipo di SAQ, vedere "Quale SAQ si adatta meglio al proprio ambiente?" a pagina 17.*

Gli esercenti SAQ C elaborano i dati di titolari di carta mediante sistemi POS o altri sistemi di pagamento connessi a Internet, non memorizzano tali dati su un computer e possono essere società di e-commerce con punti vendita reali (carta presente) o società di e-commerce o vendita tramite posta

elettronica/telefono (carta non presente). Gli esercenti SAQ C devono convalidare la propria conformità completando il questionario SAQ C e l'attestato di conformità ad esso associato, confermando che:

- La società dispone di un sistema di applicazione di pagamento e di una connessione Internet sul medesimo dispositivo e/o sulla stessa rete locale (LAN).
- L'applicazione di pagamento/dispositivo Internet non è collegato ad altri sistemi all'interno dell'ambiente (ciò può essere ottenuto mediante la segmentazione di rete per isolare l'applicazione di pagamento/dispositivo Internet da tutti gli altri sistemi).
- Il negozio della società non è collegato ad alcun'altra sede di negozio ed ogni LAN è solo per un unico negozio.
- La società conserva solo resoconti o copie cartacee delle ricevute.
- La società non memorizza i dati di titolari di carta in formato elettronico.
- Il fornitore del software del sistema di pagamento della società utilizza tecniche sicure per fornire supporto in remoto al sistema di pagamento.

## **SAQ D – Tutti gli altri esercenti e provider di servizi definiti da un marchio di pagamento come idonei alla compilazione del questionario SAQ**

*Il questionario SAQ D è stato sviluppato per tutti i provider di servizi definiti da un marchio di pagamento come idonei alla compilazione di un questionario SAQ, nonché per gli esercenti idonei al SAQ che non rientrano nelle descrizioni dei tipi di SAQ da A a C sopra descritti.*

Gli esercenti ed i provider di servizi SAQ D convalidano la propria conformità completando il questionario SAQ D e l'attestato di conformità ad esso associato.

Sebbene molte aziende che completano il questionario SAQ D debbano convalidare la propria conformità con 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. Fare riferimento alla guida seguente per informazioni sull'esclusione dei requisiti relativi alla tecnologia wireless e di determinati altri requisiti specifici.

## Guida per la non applicabilità di determinati requisiti specifici

---

**Esclusione:** Se per convalidare la propria conformità agli standard PCI DSS occorre completare il questionario SAQ C o D, è possibile considerare le seguenti eccezioni: Vedere “Non applicabilità” di seguito per la risposta appropriata al questionario SAQ.

- Requisiti 1.2.3, 2.1.1 e 4.1.1 (SAQ C e D): Fornire una risposta a queste domande specifiche della tecnologia wireless solo se tale tecnologia è disponibile nella propria rete. Tenere presente che occorre comunque fornire una risposta al requisito 11.1 (uso di un processo 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.
- Requisiti 6.3 e 6.5 (SAQ D): Queste domande riguardano in modo specifico applicazioni e codice personalizzati, e si è tenuti a rispondere solo se la società sviluppa applicazioni personalizzate.
- Requisiti da 9.1 a 9.4 (SAQ D): Fornire una risposta a queste domande solo per strutture con “aree sensibili” come definite nel presente documento. Per “aree sensibili” si intende centri dati, aree server e aree che ospitano sistemi di memorizzazione, elaborazione o trasmissione dei dati di titolari di carta. Ciò esclude le aree in cui 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.

**Non applicabilità:** Per tutti i questionari SAQ, questi ed eventuali altri requisiti considerati non applicabili al proprio ambiente devono essere indicati con “N/A” nella colonna “Speciale” del questionario SAQ. Di conseguenza, completare il foglio di lavoro “Spiegazione di non applicabilità” nell’appendice SAQ per ogni voce “N/A”.

## Istruzioni per il completamento del questionario SAQ

---

1. Utilizzare le presenti linee guida per determinare il questionario SAQ appropriato per la propria azienda.
2. Utilizzare *il documento Navigazione in PCI DSS: Comprensione dello scopo dei requisiti* per comprendere come e perché i requisiti sono rilevanti per la propria azienda.
3. Valutare il proprio ambiente per la conformità agli standard PCI DSS.
4. Utilizzare il questionario SAQ appropriato come strumento per convalidare la conformità agli standard PCI DSS.
5. Seguire le istruzioni disponibili nella sezione “Conformità agli standard PCI DSS - Operazioni” del questionario SAQ appropriato e fornire tutta la documentazione richiesta al proprio acquirente o marchio di pagamento, come necessario.

## Qual è il questionario più adatto all'ambiente della propria azienda?

