Settore delle carte di pagamento (PCI)
Standard di protezione dei dati

Questionario di autovalutazione A-EP e Attestato di conformità

Esercenti di e-commerce parzialmente in outsourcing che utilizzano un sito Web di terze parti per l'elaborazione dei pagamenti

Per l'uso con PCI DSS versione 3.2

Aprile 2016

Modifiche del documento

Data	Versione PCI DSS	Revisione SAQ	Descrizione
N/A	1.0		Non utilizzata.
N/A	2.0		Non utilizzata.
Febbraio 2014	3.0		È stato sviluppato un nuovo questionario SAQ per rispondere ai requisiti applicabili agli esercenti di e-commerce con siti Web che non ricevono direttamente i dati dei titolari di carta ma che incidono sulla sicurezza della transazione di pagamento e/o sull'integrità della pagina che accetta i dati dei titolari di carta del consumatore. Il contenuto è allineato ai nuovi requisiti e procedure di test PCI DSS v3.0.
Aprile 2015	3.1		Aggiornato per allinearlo a PCI DSS v3.1. Per informazioni dettagliate sulle modifiche di PCI DSS, fare riferimento a *PCI DSS - Riepilogo delle modifiche di PCI DSS dalla versione 3.0 alla 3.1*.
Giugno 2015	3.1		Requisito 11.3 aggiornato per correggere l'errore.
Luglio 2015	3.1	1.1	Aggiornato per rimuovere i riferimenti alle "migliori 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 *PCI DSS - Riepilogo delle modifiche di PCI DSS dalla versione 3.1 alla 3.2.*

Sommario

Operazioni preliminari

È stato sviluppato un nuovo questionario SAQ A-EP per rispondere ai requisiti applicabili agli esercenti di e-commerce con siti web che non ricevono direttamente i dati dei titolari di carta ma che incidono sulla sicurezza della transazione di pagamento e/o sull'integrità della pagina che accetta i dati dei titolari di carta.

Gli esercenti SAQ A-EP sono esercenti di e-commerce che si avvalgono parzialmente di terzi convalidati PCI DSS per la gestione del proprio canale di pagamento di e-commerce e che non memorizzano, elaborano né trasmettono in formato elettronico i dati dei titolari di carta nei propri sistemi o sedi.

Gli esercenti SAQ A-EP confermano che, per questo canale di pagamento:

- La società accetta solo le transazioni di e-commerce.
- Tutte le operazioni di elaborazione dei dati dei titolari di carta, con l'eccezione della pagina di pagamento, vengono interamente esternalizzate a un elaboratore pagamenti di terzi convalidato PCI DSS.
- Il sito web non riceve direttamente i dati dei titolari di carta ma verifica in che modo i consumatori, o i relativi dati dei titolari di carta, vengono indirizzati a un elaboratore di pagamenti di terzi convalidato PCI DSS.
- Il sito web dell'esercente è ospitato da un provider di terzi convalidato in base a tutti i requisiti PCI DSS applicabili (ad es., inclusa l'Appendice A PCI DSS se il provider è un provider di hosting condiviso);
- Tutti gli elementi delle pagine di pagamento che vengono inviati al browser del consumatore provengono dal sito Web dell'esercente o da un provider di servizi conformi agli standard PCI DSS.
- La società non memorizza, elabora o trasmette in formato elettronico i 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 eventuali dati dei titolari di carta su carta (ad esempio, resoconti o ricevute cartacei) e questi documenti non sono in formato elettronico.

Questo SAQ è applicabile solo per canali di e-commerce.

Questa versione più breve del questionario di autovalutazione comprende domande che riguardano un tipo specifico di ambiente di esercenti di dimensioni ridotte, secondo quando definito nei criteri di idoneità esposti in precedenza. Qualora siano presenti requisiti PCI DSS applicabili al proprio ambiente che non sono coperti dal presente questionario di autovalutazione, ciò potrebbe indicare che questo questionario non è adatto al proprio ambiente. Inoltre, è comunque necessario soddisfare tutti i requisiti PCI DSS applicabili per garantire la conformità agli standard PCI DSS.

Nota: *ai fini di questo questionario SAQ, i requisiti PCI DSS che fanno riferimento all'"ambiente dei dati dei titolari di carta" sono applicabili ai siti Web dell'esercente. Questo si verifica perché il sito Web dell'esercente influisce direttamente sulla modalità di trasmissione dei dati dei titolari di carta, anche se il sito Web stesso non riceve alcun dato.*

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 (come definito alla sezione 2g dell'Attestato di conformità).
3. Valutare il proprio ambiente per la conformità ai requisiti PCI DSS applicabili.
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 A-EP)
   - 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 *(Requisiti PCI DSS e procedure di valutazione della sicurezza)*	• Istruzioni sulla determinazione dell'ambito • Istruzioni sullo scopo di tutti i requisiti PCI DSS • Dettagli delle procedure di test • Istruzioni sui controlli compensativi
Documenti relativi a istruzioni e linee guida SAQ	• Informazioni su tutti i questionari SAQ e sui relativi criteri di idoneità • Come determinare quale questionario SAQ è adatto alla propria azienda
Glossario, abbreviazioni e acronimi PCI DSS e PA-DSS	• Descrizioni e definizioni dei termini utilizzati in PCI DSS e nei questionari di autovalutazione

Queste e altre risorse sono disponibili sul sito Web PCI SSC *(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:
Sì	Il test previsto è stato eseguito e tutti gli elementi del requisito sono stati soddisfatti come indicato.
Sì con CCW (Foglio di lavoro - Controllo compensativo)	Il test previsto è stato eseguito e il requisito risulta soddisfatto grazie all'ausilio di un controllo compensativo. Tutte le risposte di questa colonna richiedono il completamento di un Foglio di lavoro - Controllo compensativo (CCW) presente nell'Appendice B del questionario SAQ. 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.
No	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.
N/A (non applicabile)	Il requisito non si applica all'ambiente dell'azienda. (Per consultare alcuni esempi, vedere la *Guida per la non applicabilità di determinati requisiti specifici* riportata di seguito.) Tutte le risposte di questa colonna richiedono una spiegazione di supporto disponibile nell'Appendice C del questionario SAQ.

Guida per la non applicabilità di determinati requisiti specifici

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".

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?	Quali sono i canali di pagamento coperti dal presente questionario SAQ?
☐ Ordini via posta/telefono (MOTO)	☐ Ordini via posta/telefono (MOTO)
☐ E-Commerce	☐ E-Commerce
☐ Con carta presente (contatto diretto)	☐ 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)
Esempio: punti vendita	*3*	*Boston, MA, Stati Uniti*

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)
			☐ Sì ☐ No	
			☐ Sì ☐ No	
			☐ Sì ☐ No	
			☐ Sì ☐ No	
			☐ Sì ☐ 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 DSS? *(Consultare la sezione "Segmentazione di rete" di PCI DSS per indicazioni sulla segmentazione di rete.)*	☐ Sì ☐ No

Parte 2f. Provider di servizi di terzi

L'azienda utilizza un responsabile dell'integrazione e rivenditore qualificati (QIR)? Se sì: Nome dell'azienda QIR: Singolo nome QIR: Descrizione dei servizi forniti dal QIR:	☐ Sì ☐ No
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.)?	☐ Sì ☐ No

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.*

Parte 2g. Idoneità al completamento del modulo SAQ A-EP

L'esercente dichiara la propria idoneità per il completamento di questa versione più breve del questionario di autovalutazione perché, per questo canale:

☐	L'esercente accetta solo le transazioni di e-commerce.
☐	Tutte le operazioni di elaborazione dei dati dei titolari di carta, con l'eccezione della pagina di pagamento, vengono interamente esternalizzate a un elaboratore pagamenti di terzi convalidato PCI DSS.
☐	Il sito web dell'esercente non riceve direttamente i dati dei titolari di carta ma verifica in che modo i consumatori, o i relativi dati dei titolari di carta, vengono indirizzati a un elaboratore di pagamenti di terzi convalidato PCI DSS.
☐	Il sito web dell'esercente è ospitato da un provider di terzi convalidato in base a tutti i requisiti PCI DSS applicabili (ad es., inclusa l'Appendice A PCI DSS se il provider è un provider di hosting condiviso);
☐	Tutti gli elementi delle pagine di pagamento che vengono inviati al browser del consumatore provengono dal sito Web dell'esercente o da un provider di servizi conformi agli standard PCI DSS.
☐	L'esercente non memorizza, elabora o trasmette dati dei titolari di carta nei propri sistemi o in sede, ma si affida interamente a provider di servizi di terzi per tali operazioni.
☐	L'esercente 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.
☐	L'esercente conserva eventuali dati dei titolari di carta su carta (ad esempio, resoconti o ricevute cartacei) e questi documenti non sono in formato elettronico.

Sezione 2 - Questionario di autovalutazione A-EP

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 una rete sicura

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.)*			
			Sì	Sì con CCW	No	N/A
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?	▪ Analizzare il processo documentato ▪ Consultare il personale ▪ Esaminare le configurazioni di rete	☐	☐	☐	☐
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?	▪ Analizzare il diagramma di rete aggiornato ▪ Esaminare le configurazioni di rete	☐	☐	☐	☐
	(b) È presente un processo volto a garantire il costante aggiornamento del diagramma?	▪ Consultare il personale responsabile	☐	☐	☐	☐
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?	▪ Analizzare il diagramma del flusso di dati attuale ▪ Esaminare le configurazioni di rete.	☐	☐	☐	☐
	(b) È presente un processo volto a garantire il costante aggiornamento del diagramma?	▪ Consultare il personale	☐	☐	☐	☐
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?	▪ Analizzare gli standard di configurazione del firewall ▪ Osservare le configurazioni di rete per verificare che sia presente un firewall	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
	(b) Il diagramma di rete attuale è coerente con gli standard di configurazione del firewall?	▪ Confrontare gli standard di configurazione del firewall per diagramma di rete attuale	☐	☐	☐	☐
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?	▪ Analizzare gli standard di configurazione di firewall e router	☐	☐	☐	☐
	(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?	▪ Analizzare gli standard di configurazione di firewall e router ▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐
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?	▪ Analizzare gli standard di configurazione di firewall e router	☐	☐	☐	☐
	(b) La revisione dei set di regole di firewall e router viene effettuata almeno ogni sei mesi?	▪ Esaminare la documentazione prodotta dalle revisioni dei firewall	☐	☐	☐	☐
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: ***Nota:*** *una "rete non attendibile" è una qualsiasi rete esterna alle reti che appartengono all'entità sottoposta a revisione e/o che l'entità non è in grado di controllare o gestire.*					
1.2.1	(a) Il traffico in entrata e in uscita è limitato a quello indispensabile per l'ambiente dei dati dei titolari di carta?	▪ Analizzare gli standard di configurazione di firewall e router ▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐
	(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".	▪ Analizzare gli standard di configurazione di firewall e router ▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
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)?	▪ Analizzare gli standard di configurazione di firewall e router ▪ Esaminare i file di configurazione del router e le configurazioni del router	☐	☐	☐	☐
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?	▪ Analizzare gli standard di configurazione di firewall e router ▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐
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?	▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐
1.3.2	Il traffico Internet in entrata è stato limitato agli indirizzi IP all'interno della zona DMZ?	▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐
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.)	▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐
1.3.4	Viene autorizzato in modo esplicito il traffico in uscita dall'ambiente dei dati di titolari di carta ad Internet?	▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐
1.3.5	Sono consentite nella rete solo le connessioni già stabilite?	▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
1.3.7	(a) Sono in atto misure volte a impedire la divulgazione di indirizzi IP privati e informazioni di routing ad Internet? ***Nota:*** *i metodi per oscurare l'indirizzamento IP possono includere, senza limitazioni:* • *NAT (Network Address Translation);* • *posizionamento di server contenenti dati dei titolari di carta dietro server/firewall proxy;* • *rimozione o filtraggio di annunci di instradamento per reti private che utilizzano indirizzamento registrato;* *uso interno di spazio indirizzi RFC1918 invece degli indirizzi registrati*.	▪ Esaminare le configurazioni di firewall e router	☐	☐	☐	☐
	(b) Sono autorizzate eventuali divulgazioni ad entità esterne di indirizzi IP privati e di informazioni di routing?	▪ Esaminare le configurazioni di firewall e router ▪ Consultare il personale	☐	☐	☐	☐
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?	▪ Analizzare le politiche e gli standard di configurazione ▪ Esaminare i dispositivi mobili e/o di proprietà dei dipendenti	☐	☐	☐	☐
	(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?	▪ Analizzare le politiche e gli standard di configurazione ▪ Esaminare i dispositivi mobili e/o di proprietà dei dipendenti	☐	☐	☐	☐
1.5	Le politiche di sicurezza e le procedure operative per la gestione dei firewall sono: ▪ documentate; ▪ in uso; ▪ note a tutte le parti coinvolte?	▪ Analizzare le politiche di sicurezza e le procedure operative ▪ Consultare il personale	☐	☐	☐	☐

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
2.1	(a) I valori predefiniti del fornitore vengono sempre modificati prima di installare un sistema in rete? *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.*	▪ Analizzare le politiche e le procedure ▪ Esaminare la documentazione del fornitore ▪ Osservare le configurazioni di sistema e le impostazioni account ▪ Consultare il personale	☐	☐	☐	☐
	(b) Gli account predefiniti non necessari vengono rimossi o disattivati prima dell'installazione di un sistema sulla rete?	▪ Analizzare le politiche e le procedure ▪ Analizzare la documentazione del fornitore ▪ Esaminare le configurazioni di sistema e le impostazioni account ▪ Consultare il personale	☐	☐	☐	☐
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? *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).*	▪ Analizzare gli standard di configurazione del sistema ▪ Analizzare gli standard di hardening accettati dal settore ▪ Analizzare le politiche e le procedure ▪ Consultare il personale	☐	☐	☐	☐
	(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?	▪ Analizzare le politiche e le procedure ▪ Consultare il personale	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
	(c) Quando si configurano nuovi sistemi, vengono applicati gli standard di configurazione del sistema?	▪ Analizzare le politiche e le procedure ▪ Consultare il personale	☐	☐	☐	☐
	(d) Gli standard di configurazione del sistema comprendono quanto segue: • Modifica di tutti i valori predefiniti del fornitore ed eliminazione di account predefiniti non necessari? • Implementazione di una sola funzione principale per server per impedire la coesistenza sullo stesso server di funzioni che richiedono livelli di sicurezza diversi? • Abilitazione di servizi, protocolli, daemon, ecc. necessari, come richiesto per la funzione del sistema? • Implementazione di funzioni di sicurezza aggiuntive per servizi, protocolli o daemon necessari considerati non sicuro? • Configurazione di parametri di sicurezza del sistema per evitare un uso improprio? • Rimozione di tutta la funzionalità non necessaria, ad esempio script, driver, funzioni, sottosistemi, file system e server Web non utilizzati?	▪ Analizzare gli standard di configurazione del sistema	☐	☐	☐	☐
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? *Ad esempio, server Web, database server e DNS devono essere implementati su server separati.*	▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
	(b) In caso di utilizzo di tecnologie di virtualizzazione, viene implementata una sola funzione primaria per dispositivo o componente di sistema virtuale?	▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
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)?	▪ Analizzare gli standard di configurazione ▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
	(b) Tutti i servizi, i daemon o i protocolli non sicuri attivi sono giustificati a fronte di standard di configurazione documentati?	▪ Analizzare gli standard di configurazione ▪ Consultare il personale ▪ Esaminare le impostazioni di configurazione ▪ Confrontare i servizi attivati ecc. in base alle giustificazioni documentate	☐	☐	☐	☐
2.2.3	Sono state documentate e implementate le funzioni di sicurezza aggiuntive per servizi, protocolli o daemon necessari considerati non sicuri? ***Nota:*** *laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.*	▪ Analizzare gli standard di configurazione ▪ Esaminare le impostazioni di configurazione ▪ Esaminare le impostazioni di configurazione	☐	☐	☐	☐
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	☐	☐	☐	☐
	(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	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
	(c) Le impostazioni dei parametri di sicurezza sono impostate correttamente sui componenti di sistema?	▪ Esaminare i componenti di sistema ▪ Esaminare le impostazioni dei parametri di sicurezza ▪ Confrontare le impostazioni degli standard di configurazione del sistema	☐	☐	☐	☐
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	☐	☐	☐	☐
	(b) Tutte le funzioni abilitate sono documentate e supportano una configurazione sicura?	▪ Analizzare la documentazione ▪ Esaminare i parametri di sicurezza sui componenti di sistema	☐	☐	☐	☐
	(c) Sui componenti di sistema sono presenti solo funzionalità documentate?	▪ Analizzare la documentazione ▪ Esaminare i parametri di sicurezza sui componenti di sistema	☐	☐	☐	☐
2.3	È stata eseguita la cifratura dell'accesso amministrativo non da console come segue: ***Nota*: *laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.***					
	(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?	▪ Esaminare i componenti di sistema ▪ Esaminare le configurazioni del sistema ▪ Osservare un accesso amministratore	☐	☐	☐	☐
	(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?	▪ Esaminare i componenti di sistema ▪ Esaminare servizi e file	☐	☐	☐	☐

Domanda PCI DSS	Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
		Sì	**Sì con CCW**	**No**	**N/A**
(c) L'accesso amministratore alle interfacce di gestione basate su Web è cifrato con un metodo di crittografia avanzata?	▪ Esaminare i componenti di sistema ▪ Osservare un accesso amministratore	☐	☐	☐	☐
(d) Per la tecnologia in uso, viene implementata una crittografia avanzata in conformità alle migliori pratiche di settore e/o alle raccomandazioni del fornitore?	▪ Esaminare i componenti di sistema ▪ Analizzare la documentazione del fornitore ▪ Consultare il personale	☐	☐	☐	☐

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	Sì con CCW	No	N/A
3.2	(c) I dati sensibili di autenticazione vengono eliminati o resi non recuperabili dopo il completamento del processo di autorizzazione?	▪ Analizzare le politiche e le procedure ▪ Esaminare le configurazioni del sistema ▪ Esaminare i processi di eliminazione	☐	☐	☐	☐
	(d) Tutti i sistemi aderiscono ai seguenti requisiti relativi alla non memorizzazione di dati sensibili di autenticazione dopo l'autorizzazione (anche se cifrati)?					
3.2.2	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?	▪ Esaminare le origini dei dati tra cui: • Dati di transazioni in entrata • Tutti i registri • File di cronologia • File di traccia • Schema del database • Contenuto del database	☐	☐	☐	☐
3.2.3	Il numero di identificazione personale (PIN) o il blocco PIN cifrato non viene memorizzato dopo l'autorizzazione?	▪ Esaminare le origini dei dati tra cui: • Dati di transazioni in entrata • Tutti i registri • File di cronologia • File di traccia • Schema del database • Contenuto del database	☐	☐	☐	☐

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.)*			
			Sì	Sì con CCW	No	N/A
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? ***Nota:*** *laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.* *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).*	▪ Analizzare gli standard documentati ▪ Analizzare le politiche e le procedure ▪ Analizzare tutte località in cui si trasmettono o ricevono i dati dei titolari di carta ▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
	(b) Vengono accettati solo certificati e/o chiavi affidabili?	▪ Osservare le trasmissioni in ingresso e in uscita ▪ Esaminare le chiavi e i certificati	☐	☐	☐	☐
	(c) Sono implementati protocolli di sicurezza per usare solo configurazioni sicure e non supportare versioni o configurazioni non sicure?	▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
	(d) Viene implementato il livello di crittografia corretto per la metodologia in uso (controllare i suggerimenti, le pratiche consigliate del fornitore)?	▪ Analizzare la documentazione del fornitore ▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
	(e) Per le implementazioni TLS, è abilitato TLS durante la trasmissione o la ricezione dei dati dei titolari di carta? *Ad esempio, per le implementazioni basate su browser:* • *"HTTPS" viene visualizzato come protocollo dell'URL del browser;* • *i dati dei titolari di carta vengono richiesti solo se "HTTPS" viene visualizzato come parte dell'URL.*	▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
4.2	(b) Sono presenti politiche in cui si indica che i PAN non protetti non devono essere inviati mediante tecnologie di messaggistica degli utenti finali?	▪ Analizzare le politiche e le procedure	☐	☐	☐	☐
4.3	Le politiche di sicurezza e le procedure operative per la cifratura delle trasmissioni dei dati dei titolari di carta sono: ▪ documentate; ▪ in uso; ▪ note a tutte le parti coinvolte?	▪ Analizzare le politiche di sicurezza e le procedure operative ▪ Consultare il personale	☐	☐	☐	☐

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.)*			
			Sì	Sì con CCW	No	N/A
5.1	È stato installato un software antivirus su tutti i sistemi comunemente colpiti da software dannoso?	▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
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)?	▪ Analizzare la documentazione del fornitore ▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
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?	▪ Consultare il personale	☐	☐	☐	☐
5.2	Tutti i meccanismi antivirus sono mantenuti come segue:					
	(a) Il software antivirus e le definizioni sono aggiornati?	▪ Esaminare le politiche e le procedure ▪ Esaminare le configurazioni antivirus, inclusa l'installazione principale ▪ Esaminare i componenti di sistema	☐	☐	☐	☐
	(b) Sono attivati e vengono eseguiti aggiornamenti automatici e scansioni periodiche?	▪ Esaminare le configurazioni antivirus, inclusa l'installazione principale ▪ Esaminare i componenti di sistema	☐	☐	☐	☐
	(c) Tutti i meccanismi antivirus generano log di audit e, questi log sono conservati in base al Requisito 10.7 PCI DSS?	▪ Esaminare le configurazioni antivirus ▪ Analizzare i processi di conservazione dei log	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
5.3	Tutti i meccanismi antivirus sono: ▪ Attivamente in esecuzione? ▪ Non disattivabili o modificabili dagli utenti? ***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.*	▪ Esaminare le configurazioni antivirus ▪ Esaminare i componenti di sistema ▪ Osservare i processi ▪ Consultare il personale	☐	☐	☐	☐
5.4	Le politiche di sicurezza e le procedure operative per la protezione dei sistemi contro il malware sono: ▪ documentate; ▪ in uso; ▪ note a tutte le parti coinvolte?	▪ Analizzare le politiche di sicurezza e le procedure operative ▪ Consultare il personale	☐	☐	☐	☐

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
6.1	È presente un processo per individuare vulnerabilità alla sicurezza, incluso quanto segue: ▪ Utilizzo di fonti esterne attendibili di informazioni sulle vulnerabilità? ▪ Assegnazione di una classificazione dei rischi alle vulnerabilità che include l'identificazione di tutte le vulnerabilità ad "alto rischio" e "critiche"? ***Nota**: 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.* *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.*	▪ Analizzare le politiche e le procedure ▪ Consultare il personale ▪ Osservare i processi	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
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?	▪ Analizzare le politiche e le procedure	☐	☐	☐	☐
	(b) Sono state installate patch di protezione critiche entro un mese dal relativo rilascio? ***Nota**: le patch di sicurezza critiche vanno identificate in conformità al processo di classificazione dei rischi definito nel Requisito 6.1.*	▪ Analizzare le politiche e le procedure ▪ Esaminare i componenti di sistema ▪ Confrontare elenco delle patch di sicurezza installate con gli elenchi delle ultime patch del fornitore	☐	☐	☐	☐
6.4.5	(a) Le procedure di controllo delle modifiche sono documentate e richiedono quanto segue? • documentazione dell'impatto; • approvazione documentata del controllo delle modifiche prodotta da parti autorizzate; • test della funzionalità per verificare che la modifica non influisca negativamente sulla sicurezza del sistema; • procedure di back-out.	▪ Analizzare i processi e le procedure di controllo delle modifiche	☐	☐	☐	☐
	(b) I seguenti fattori vengono richiesti e documentati per tutte le modifiche:					
6.4.5.1	Documentazione dell'impatto?	▪ Tenere traccia delle modifiche per aggiornare la documentazione di controllo ▪ Esaminare la documentazione di controllo delle modifiche	☐	☐	☐	☐
6.4.5.2	Approvazione documentata delle parti autorizzate?	▪ Tenere traccia delle modifiche per aggiornare la documentazione di controllo ▪ Esaminare la documentazione di controllo delle modifiche	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
6.4.5.3	(a) Test della funzionalità per verificare che la modifica non influisca negativamente sulla sicurezza del sistema?	▪ Tenere traccia delle modifiche per aggiornare la documentazione di controllo ▪ Esaminare la documentazione di controllo delle modifiche	☐	☐	☐	☐
	(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?	▪ Tenere traccia delle modifiche per aggiornare la documentazione di controllo ▪ Esaminare la documentazione di controllo delle modifiche	☐	☐	☐	☐
6.4.5.4	Procedure di back-out?	▪ Tenere traccia delle modifiche per aggiornare la documentazione di controllo ▪ Esaminare la documentazione di controllo delle modifiche	☐	☐	☐	☐
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? ***Nota:*** *questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.*	▪ Tenere traccia delle modifiche per aggiornare la documentazione di controllo ▪ Esaminare la documentazione di controllo delle modifiche ▪ Consultare il personale ▪ Osservare le reti o i sistemi interessati	☐	☐	☐	☐
6.5	I processi di sviluppo software si occupano delle vulnerabilità di codifica comuni?	▪ Analizzare le politiche e le procedure di sviluppo software	☐	☐	☐	☐
	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?	▪ Esaminare le policy e le procedure di sviluppo software ▪ Esaminare i record della formazione	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
	(c) Le applicazioni vengono sviluppate in base a linee guida di codifica sicura per proteggere le applicazioni quanto meno dalle seguenti vulnerabilità:					
6.5.1	Le tecniche di codifica si occupano degli injection flaw, in particolare di SQL injection? ***Nota:*** *Considerare, inoltre, OS Command Injection, LDAP e XPath injection flaw, nonché altri tipi di injection flaw.*	▪ Esaminare le policy e le procedure di sviluppo software ▪ Consultare il personale responsabile	☐	☐	☐	☐
6.5.2	Le tecniche di codifica si occupano delle vulnerabilità di buffer overflow?	▪ Esaminare le policy e le procedure di sviluppo software ▪ Consultare il personale responsabile	☐	☐	☐	☐
6.5.4	Le tecniche di codifica si occupano delle comunicazioni non sicure?	▪ Esaminare le policy e le procedure di sviluppo software ▪ Consultare il personale responsabile	☐	☐	☐	☐
6.5.5	Le tecniche di codifica si occupano della gestione degli errori non corretta?	▪ Esaminare le policy e le procedure di sviluppo software ▪ Consultare il personale responsabile	☐	☐	☐	☐
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)?	▪ Esaminare le policy e le procedure di sviluppo software ▪ Consultare il personale responsabile	☐	☐	☐	☐
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)?	▪ Esaminare le policy e le procedure di sviluppo software ▪ Consultare il personale responsabile	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
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?	▪ Esaminare le policy e le procedure di sviluppo software ▪ Consultare il personale responsabile	☐	☐	☐	☐
6.5.9	Le tecniche di codifica si occupano del cross-site request forgery (CSRF)?	▪ Esaminare le policy e le procedure di sviluppo software ▪ Consultare il personale responsabile	☐	☐	☐	☐
6.5.10	Le tecniche di codifica si occupano di violazione dell'autenticazione e gestione delle sessioni?	▪ Esaminare le policy e le procedure di sviluppo software ▪ Consultare il personale responsabile	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
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 *uno* dei seguenti metodi? ▪ Analisi delle applicazioni Web rivolte al pubblico tramite strumenti o metodi manuali o automatici di valutazione della sicurezza della vulnerabilità delle applicazioni, come segue: – Almeno una volta all'anno – dopo ogni modifica; – da un'organizzazione specializzata in sicurezza delle applicazioni; – che almeno tutte le vulnerabilità elencate nel Requisito 6.5 vengano incluse nella valutazione; – che tutte le vulnerabilità vengano corrette; – Che l'applicazione venga nuovamente valutata dopo le correzioni ***Nota**: la valutazione non corrisponde alle scansioni delle vulnerabilità eseguite in base al Requisito 11.2.* - **O** - ▪ 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: – posta davanti alle applicazioni Web rivolte al pubblico per rilevare ed evitare attacchi basati su Web; – in esecuzione e aggiornata secondo necessità; – in grado di generare log di audit; – configurata in modo da bloccare gli attacchi basati sul Web o da generare un avviso investigato immediatamente.	▪ Analizzare i processi documentati ▪ Consultare il personale ▪ Esaminare i record di valutazioni di sicurezza delle applicazioni ▪ Esaminare le impostazioni di configurazione del sistema	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
6.7	Le politiche di sicurezza e le procedure operative per lo sviluppo e la manutenzione di applicazioni e sistemi sicuri sono: ▪ documentate; ▪ in uso; ▪ note a tutte le parti coinvolte?	▪ Analizzare le politiche di sicurezza e le procedure operative ▪ Consultare il personale	☐	☐	☐	☐

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
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:					
7.1.2	L'accesso agli ID utente con privilegi è limitato come segue: ▪ Alla quantità minima necessaria per le responsabilità di ruolo? ▪ Assegnato solo a ruoli che necessitano specificatamente tale accesso privilegiato?	▪ Esaminare la politica scritta di controllo dell'accesso ▪ Consultare il personale ▪ Consultare i membri del management ▪ Analizzare gli ID utente con privilegi	☐	☐	☐	☐
7.1.3	L'accesso viene assegnato in base alla classificazione e alla funzione del singolo ruolo del personale?	▪ Esaminare la politica scritta di controllo dell'accesso ▪ Consultare i membri del management ▪ Analizzare gli ID utente	☐	☐	☐	☐
7.1.4	L'approvazione documentata delle parti autorizzate viene richiesta specificando i privilegi necessari?	▪ Analizzare gli ID utente ▪ Confrontare con le approvazioni documentate ▪ Confrontare i privilegi assegnati con le approvazioni documentate	☐	☐	☐	☐

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
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?	▪ Analizzare le procedure delle password ▪ Consultare il personale	☐	☐	☐	☐
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)?	▪ Analizzare le procedure delle password ▪ Esaminare gli ID utente con privilegi e generali e le autorizzazioni associate ▪ Osservare le impostazioni di sistema				
8.1.3	L'accesso per gli utenti non attivi viene disattivato o rimosso immediatamente?	▪ Analizzare le procedure delle password ▪ Esaminare gli utenti account non attivi ▪ Analizzare gli elenchi di accesso attuali ▪ Osservare i dispositivi di autenticazione fisici	☐	☐	☐	☐
8.1.4	Gli account utente non attivi vengono rimossi o disabilitati entro 90 giorni?	▪ Analizzare le procedure delle password ▪ Osservare gli account utente	☐	☐	☐	☐
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?	▪ Analizzare le procedure delle password ▪ Consultare il personale ▪ Osservare i processi	☐	☐	☐	☐
	(b) Gli account per l'accesso in remoto di terzi vengono monitorati durante l'uso?	▪ Consultare il personale ▪ Osservare i processi	☐	☐	☐	☐
8.1.6	(a) I tentativi di accesso ripetuti sono limitati bloccando l'ID utente dopo un massimo di sei tentativi?	▪ Analizzare le procedure delle password ▪ Esaminare le impostazioni di configurazione del sistema	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
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?	▪ Analizzare le procedure delle password ▪ Esaminare le impostazioni di configurazione del sistema	☐	☐	☐	☐
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?	▪ Analizzare le procedure delle password ▪ Esaminare le impostazioni di configurazione del sistema	☐	☐	☐	☐
8.2	Oltre ad assegnare un ID univoco, viene adottato uno o più dei seguenti metodi per autenticare tutti gli utenti? ▪ qualcosa che l'utente conosce, come una password o una passphrase; ▪ Qualcosa in possesso dell'utente, come un dispositivo token o una smart card ▪ qualcosa che l'utente è, come un elemento biometrico.	▪ Analizzare le procedure delle password ▪ Osservare i processi di autenticazione	☐	☐	☐	☐
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?	▪ Analizzare le procedure delle password ▪ Analizzare la documentazione del fornitore ▪ Esaminare le impostazioni di configurazione del sistema ▪ Osservare i file delle password ▪ Osservare le trasmissioni di dati	☐	☐	☐	☐
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?	▪ Analizzare le procedure di autenticazione ▪ Osservare il personale	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
8.2.3	(a) I parametri delle password utente vengono configurati per richiedere che password/passphrase soddisfino i seguenti requisiti? • Lunghezza minima della password di 7 caratteri • Presenza di caratteri numerici e alfabetici In alternativa, le password/passphrase devono presentare una complessità e solidità pari almeno ai parametri indicati sopra.	▪ Esaminare le impostazioni di configurazione del sistema per verificare i parametri delle password	☐	☐	☐	☐
8.2.4	(a) Le password/passphrase degli utenti vengono modificate almeno una volta ogni 90 giorni?	▪ Analizzare le procedure delle password ▪ Esaminare le impostazioni di configurazione del sistema	☐	☐	☐	☐
8.2.5	(a) La nuova password/passphrase specificata deve essere diversa dalle ultime quattro password/passphrase utilizzate?	▪ Analizzare le procedure delle password ▪ Componente di sistema campione ▪ Esaminare le impostazioni di configurazione del sistema	☐	☐	☐	☐
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?	▪ Analizzare le procedure delle password ▪ Esaminare le impostazioni di configurazione del sistema ▪ Osservare il personale di sicurezza	☐	☐	☐	☐
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: ***Nota:*** *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.*						

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
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? ***Nota:*** *questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.*	▪ Esaminare le configurazioni del sistema ▪ Osservare l'accesso al CDE da parte dell'amministratore	☐	☐	☐	☐
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?	▪ Esaminare le configurazioni del sistema ▪ Osservare la connessione del personale in remoto	☐	☐	☐	☐
8.4	(a) Le procedure e le politiche di autenticazione vengono documentate e comunicate a tutti gli utenti?	▪ Analizzare le politiche e le procedure ▪ Analizzare il metodo di distribuzione ▪ Consultare il personale ▪ Consultare gli utenti	☐	☐	☐	☐
	(b) Le procedure e le politiche di autenticazione includono quanto segue? • Istruzioni sulla selezione di credenziali di autenticazione avanzata • Istruzioni su come gli utenti dovrebbero proteggere le proprie credenziali di autenticazione • Istruzioni per non riutilizzare le password utilizzate precedentemente • Istruzioni su come gli utenti devono modificare le password in caso di sospetta compromissione delle password	▪ Analizzare le politiche e le procedure ▪ Analizzare la documentazione fornita agli utenti	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
8.5	Account e password di gruppo, condivisi o generici o altri metodi di autenticazione sono vietati come segue: ▪ Gli ID e gli account utente generici sono disabilitati o rimossi. ▪ Non esistono ID utente condivisi per le attività di amministrazione del sistema e per altre funzioni critiche. ▪ Gli ID utente condivisi e generici non vengono utilizzati per gestire i componenti di sistema.	▪ Analizzare le politiche e le procedure ▪ Esaminare gli elenchi di ID utente ▪ Consultare il personale	☐	☐	☐	☐
8.6	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? ▪ I meccanismi di autenticazione devono essere assegnati a un singolo account e non vanno condivisi tra più account. ▪ Vanno adottati controlli fisici e/o logici per assicurare che solo un account determinato possa utilizzare tale meccanismo di accesso.	▪ Analizzare le politiche e le procedure ▪ Consultare il personale ▪ Esaminare le impostazioni di configurazione del sistema e/o i controlli fisici	☐	☐	☐	☐
8.8	Le politiche di sicurezza e le procedure operative per l'identificazione e l'autenticazione sono: ▪ documentate; ▪ in uso; ▪ note a tutte le parti coinvolte?	▪ Esaminare le politiche di sicurezza e le procedure operative ▪ Consultare il personale	☐	☐	☐	☐

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
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?	▪ Osservare i controlli di accesso fisici ▪ Osservare il personale	☐	☐	☐	☐
9.5	Tutti i supporti sono protetti fisicamente (inclusi, senza limitazione, computer, supporti elettronici rimovibili, ricevute cartacee, resoconti cartacei e fax)? *Ai fini del Requisito 9, per "supporti" si intendono tutti i supporti elettronici e cartacei contenenti dati di titolari di carta.*	▪ Analizzare le politiche e le procedure per proteggere fisicamente i supporti ▪ Consultare il personale	☐	☐	☐	☐
9.6	(a) La distribuzione interna ed esterna di qualsiasi tipo di supporto è rigorosamente controllata?	▪ Analizzare le politiche e le procedure per la distribuzione dei supporti	☐	☐	☐	☐
	(b) I controlli devono includere quanto segue:					
9.6.1	Il supporto è classificato in modo da poter determinare la sensibilità dei dati?	▪ Analizzare le politiche e le procedure per la classificazione dei supporti ▪ Consultare il personale di sicurezza	☐	☐	☐	☐
9.6.2	Il supporto viene inviato tramite un corriere affidabile o un altro metodo di consegna che può essere adeguatamente monitorato?	▪ Consultare il personale ▪ Esaminare i registri di controllo e la documentazione della distribuzione dei supporti	☐	☐	☐	☐
9.6.3	L'approvazione del management viene concessa prima dello spostamento dei supporti (soprattutto quando i supporti vengono distribuiti agli individui)?	▪ Consultare il personale ▪ Esaminare i registri di controllo e la documentazione della distribuzione dei supporti	☐	☐	☐	☐
9.7	Sono in atto controlli adeguati per la memorizzazione e l'accesso ai supporti?	▪ Analizzare le politiche e le procedure	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	**Sì con CCW**	**No**	**N/A**
9.8	(a) Tutti i supporti vengono distrutti quando non sono più necessari per scopi aziendali o legali?	▪ Analizzare le politiche e le procedure di distruzione periodica dei supporti	☐	☐	☐	☐
	(c) La distruzione dei supporti 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?	▪ Analizzare le politiche e le procedure di distruzione periodica dei supporti ▪ Consultare il personale ▪ Osservare i processi	☐	☐	☐	☐
	(b) I contenitori usati per conservare i materiali che contengono le informazioni da distruggere sono protetti per impedire l'accesso al contenuto?	▪ Esaminare la sicurezza dei contenitori di conservazione	☐	☐	☐	☐

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
10.1	Gli audit trail sono attivi e funzionanti per i componenti di sistema?	▪ Osservare i processi ▪ Consultare l'amministratore di sistema	☐	☐	☐	☐
	L'accesso ai componenti di sistema è collegato ad ogni singolo utente?	▪ Osservare i processi ▪ Consultare l'amministratore di sistema	☐	☐	☐	☐
10.2	Sono stati implementati audit trail automatizzati per tutti i componenti del sistema per ricostruire i seguenti eventi:					
10.2.2	Tutte le azioni intraprese da un utente con privilegi di utente root o amministratore?	▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit	☐	☐	☐	☐
10.2.3	Accesso a tutti gli audit trail?	▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit	☐	☐	☐	☐
10.2.4	Tentativi di accesso logico non validi?	▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit	☐	☐	☐	☐
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?	▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
10.2.6	Inizializzazione, arresto o pausa dei log di audit?	▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit	☐	☐	☐	☐
10.2.7	Creazione ed eliminazione di oggetti a livello di sistema?	▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit	☐	☐	☐	☐
10.3	Vengono registrate le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento:					
10.3.1	Identificazione utente?	▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit	☐	☐	☐	☐
10.3.2	Tipo di evento?	▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit	☐	☐	☐	☐
10.3.3	Data e ora?	▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit	☐	☐	☐	☐
10.3.4	Indicazione di successo o fallimento?	▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
10.3.5	Origine dell'evento?	▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit	☐	☐	☐	☐
10.3.6	Identità o nome del dato interessato, componente di sistema o risorsa?	▪ Consultare il personale ▪ Osservare i log di audit ▪ Esaminare le impostazioni dei relativi log di audit	☐	☐	☐	☐
10.4	Tutti gli orologi e gli orari critici del sistema sono sincronizzati utilizzando la tecnologia per la sincronizzazione dell'ora? Tale tecnologia viene aggiornata? ***Nota:*** *NTP (Network Time Protocol) è un esempio di tecnologia per la sincronizzazione dell'ora.*	▪ Analizzare gli standard e i processi di configurazione dell'ora	☐	☐	☐	☐
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?	▪ Analizzare gli standard e i processi di configurazione dell'ora ▪ Esaminare i parametri di sistema relativi all'ora	☐	☐	☐	☐
	(b) Laddove esiste più di un server di riferimento orario designato, i server comunicano tra loro per mantenere un orario esatto?	▪ Analizzare gli standard e i processi di configurazione dell'ora ▪ Esaminare i parametri di sistema relativi all'ora	☐	☐	☐	☐
	(c) I sistemi ricevono le informazioni orarie soltanto dai server centrali designati.	▪ Analizzare gli standard e i processi di configurazione dell'ora ▪ Esaminare i parametri di sistema relativi all'ora	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
10.4.2	I dati dell'ora sono protetti come segue: (a) L'accesso ai dati dell'ora è limitato solo al personale con un'esigenza aziendale di accedere a tali dati?	▪ Esaminare le configurazioni di sistema e le impostazioni per la sincronizzazione dell'ora	☐	☐	☐	☐
	(b) Le modifiche alle impostazioni dell'ora su sistemi critici sono registrate, monitorate ed esaminate?	▪ Esaminare le configurazioni di sistema e le impostazioni e i log per la sincronizzazione dell'ora	☐	☐	☐	☐
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.) *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).*	▪ Esaminare le configurazioni del sistema	☐	☐	☐	☐
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?	▪ Consultare gli amministratori di sistema ▪ Esaminare le configurazioni di sistema e le autorizzazioni	☐	☐	☐	☐
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?	▪ Consultare gli amministratori di sistema ▪ Esaminare le configurazioni di sistema e le autorizzazioni	☐	☐	☐	☐
10.5.3	Viene eseguito il backup dei file di audit trail su un server dei log o un supporto centralizzato difficile da modificare?	▪ Consultare gli amministratori di sistema ▪ Esaminare le configurazioni di sistema e le autorizzazioni	☐	☐	☐	☐
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?	▪ Consultare gli amministratori di sistema ▪ Esaminare le configurazioni di sistema e le autorizzazioni	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
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)?	▪ Esaminare le impostazioni, i file monitorati e i risultati delle attività di monitoraggio	☐	☐	☐	☐
10.6	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? ***Nota:*** *gli strumenti di raccolta, analisi e generazione di avvisi per i log possono essere utilizzati ai fini della conformità al requisito 10.6.*					
10.6.1	(b) I seguenti registri ed eventi di sicurezza vengono analizzati almeno una volta al giorno, sia manualmente che attraverso strumenti di registro? • Tutti gli eventi di sicurezza. • Registri di tutti i componenti di sistema che memorizzano, elaborano o trasmettono CHD e/o SAD. • Registri di tutti i componenti di sistema critici. • 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).	▪ Analizzare le politiche e le procedure di sicurezza ▪ Osservare i processi ▪ Consultare il personale	☐	☐	☐	☐
10.6.2	(b) I registri e tutti gli altri componenti di sistema vengono rivisti periodicamente, manualmente o tramite strumenti di registro, in base alle politiche e alla strategia di gestione del rischio dell'azienda?	▪ Analizzare le politiche e le procedure di sicurezza ▪ Analizzare la documentazione di valutazione dei rischi ▪ Consultare il personale	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
10.6.3	(b) Viene eseguito il follow-up di eccezioni e anomalie individuate durante il processo di revisione?	▪ Analizzare le politiche e le procedure di sicurezza ▪ Osservare i processi ▪ Consultare il personale	☐	☐	☐	☐
10.7	(b) I log di audit vengono conservati per almeno un anno?	▪ Analizzare le politiche e le procedure di sicurezza ▪ Consultare il personale ▪ Esaminare i log di audit	☐	☐	☐	☐
	(c) Sono immediatamente disponibili per l'analisi almeno i log degli ultimi tre mesi?	▪ Consultare il personale ▪ Osservare i processi	☐	☐	☐	☐

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

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
11.2.2	(a) Vengono eseguite scansioni esterne di vulnerabilità trimestrali? ***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.*	▪ Analizzare i risultati dai quattro trimestri più recenti di scansioni delle vulnerabilità esterne	☐	☐	☐	☐
	(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)?	▪ Analizzare i risultati di ogni scansione trimestrale esterna e ripetere la scansione	☐	☐	☐	☐
	(c) Le scansioni esterne di vulnerabilità trimestrali vengono eseguite dal fornitore di prodotti di scansione approvato (ASV) PCI SSC?	▪ Analizzare i risultati di ogni scansione trimestrale esterna e ripetere la scansione	☐	☐	☐	☐
11.2.3	(a) Le scansioni interne ed esterne vengono eseguite, e ripetute se necessario, dopo ogni modifica significativa? ***Nota:*** *le scansioni devono essere eseguite da personale qualificato.*	▪ Esaminare e associare la documentazione di controllo delle modifiche e i report di scansione	☐	☐	☐	☐
	(b) Il processo di scansione comprende nuove scansioni fino a quando: • Per le scansioni esterne, non esistano vulnerabilità a cui sia assegnato un punteggio superiore a 4.0 da parte del CVSS. • 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?	▪ Analizzare i rapporti delle scansioni	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
	(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)?	▪ Consultare il personale	☐	☐	☐	☐
11.3	La metodologia dei test di penetrazione include quanto segue? ▪ È basata sugli approcci ai test di penetrazione accettati dal settore (ad esempio, NIST SP800-115). ▪ Include la copertura dell'intero perimetro dell'ambiente dei dati dei titolari di carta e i dei sistemi critici. ▪ Include i test dall'interno e dall'esterno della rete. ▪ Comprende i test per convalidare eventuali controlli di segmentazione e riduzione della portata. ▪ Definisce i test di penetrazione a livello di applicazione affinché includano almeno le vulnerabilità elencate nel Requisito 6.5. ▪ Definisce i test di penetrazione a livello di rete affinché includano componenti che supportano le funzioni di rete nonché i sistemi operativi. ▪ Include la revisione e la valutazione delle minacce e delle vulnerabilità verificatesi negli ultimi 12 mesi. ▪ Specifica la conservazione dei risultati dei test di penetrazione e dei risultati delle attività di correzione.	▪ Esaminare la metodologia dei test di penetrazione ▪ Consultare il personale responsabile	☐	☐	☐	☐
11.3.1	(a) I test di penetrazione *esterna* 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)?	▪ Esaminare la portata del lavoro ▪ Esaminare i risultati dai test di penetrazione esterna più recenti	☐	☐	☐	☐
	(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)?	▪ Consultare il personale responsabile	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
11.3.3	Le vulnerabilità sfruttabili individuate durante il test di penetrazione vengono corrette e il test viene ripetuto per verificare le correzioni?	▪ Esaminare i risultati dei test di penetrazione	☐	☐	☐	☐
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?	▪ Esaminare i controlli di segmentazione ▪ Analizzare la metodologia dei test di penetrazione	☐	☐	☐	☐
	(b) I test di penetrazione volti a verificare i controlli di segmentazione rispondono ai seguenti criteri? • Vengono eseguiti almeno una volta all'anno e dopo eventuali modifiche ai controlli/metodi di segmentazione. • Coprono tutti i controlli/metodi di segmentazione in uso. • 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.	▪ Esaminare i risultati dai test di penetrazione più recenti	☐	☐	☐	☐
	(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)?	▪ Consultare il personale responsabile	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
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: • in corrispondenza del perimetro dell'ambiente dei dati dei titolari di carta; • in corrispondenza dei punti critici nell'ambiente dei dati dei titolari di carta.	▪ Esaminare le configurazioni del sistema ▪ Esaminare i diagrammi di rete	☐	☐	☐	☐
	(b) Le tecniche di rilevamento delle intrusioni e/o di prevenzione delle intrusioni sono state configurate per avvertire il personale di violazioni sospette?	▪ Esaminare le configurazioni del sistema ▪ Consultare il personale responsabile	☐	☐	☐	☐
	(c) Vengono tenuti aggiornati tutti i sistemi, le basi e le firme di rilevamento e prevenzione delle intrusioni?	▪ Esaminare le configurazioni IDS/IPS ▪ Esaminare la documentazione del fornitore	☐	☐	☐	☐
11.5	(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? *Tra gli esempi di file che devono essere monitorati:* • *Eseguibili di sistema* • *eseguibili di applicazioni* • *File di configurazione e parametri* • *File memorizzati centralmente, di cronologia o archiviazione, di registro e audit* • *File critici ulteriori determinati dall'entità (ad esempio, tramite la valutazione dei rischi o altri mezzi)*	▪ Osservare le impostazioni di sistema e i file monitorati ▪ Esaminare le impostazioni di configurazione del sistema	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
	(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? ***Nota:*** *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).*	▪ Osservare le impostazioni di sistema e i file monitorati ▪ Analizzare i risultati delle attività di monitoraggio	☐	☐	☐	☐
11.5.1	È stato adottato un processo per rispondere a eventuali avvisi generati dalla soluzione di rilevamento delle modifiche?	▪ Esaminare le impostazioni di configurazione del sistema	☐	☐	☐	☐

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
12.1	È stata definita, pubblicata, gestita e diffusa una politica per la sicurezza tra tutto il personale interessato?	▪ Analizzare la politica di sicurezza delle informazioni	☐	☐	☐	☐
12.1.1	La politica di sicurezza viene rivista almeno una volta all'anno e aggiornata quando l'ambiente cambia?	▪ Analizzare la politica di sicurezza delle informazioni ▪ Consultare il personale responsabile	☐	☐	☐	☐
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?	▪ Analizzare le politiche e le procedure di sicurezza delle informazioni ▪ Consultare un campione di personale responsabile	☐	☐	☐	☐
12.5	(b) Le seguenti responsabilità per la gestione della sicurezza delle informazioni sono state assegnate a una singola persona o a un team?					
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?	▪ Analizzare le politiche e le procedure di sicurezza delle informazioni	☐	☐	☐	☐
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?	▪ Analizzare il programma di consapevolezza della sicurezza	☐	☐	☐	☐
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:					

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
12.8.1	È stato conservato un elenco di provider di servizi, inclusa una descrizione dei servizi forniti?	▪ Analizzare le politiche e le procedure ▪ Osservare i processi ▪ Analizzare un elenco dei provider di servizi	☐	☐	☐	☐
12.8.2	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? ***Nota:*** *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.*	▪ Osservare i contratti scritti ▪ Analizzare le politiche e le procedure	☐	☐	☐	☐
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?	▪ Osservare i processi ▪ Analizzare le politiche e le procedure e la documentazione di supporto	☐	☐	☐	☐
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?	▪ Osservare i processi ▪ Analizzare le politiche e le procedure e la documentazione di supporto	☐	☐	☐	☐
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?	▪ Osservare i processi ▪ Analizzare le politiche e le procedure e la documentazione di supporto	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
12.10.1	(a) È stato creato un piano di risposta da implementare in caso di violazione del sistema?	▪ Analizzare il piano di risposta agli incidenti ▪ Analizzare le procedure per il piano di risposta agli incidenti	☐	☐	☐	☐
	(b) Il piano include almeno i seguenti elementi?					
	• Ruoli, responsabilità e strategie di comunicazione e contatto in caso di violazione, nonché notifiche ai marchi di pagamento	▪ Analizzare le procedure per il piano di risposta agli incidenti	☐	☐	☐	☐
	• Procedure specifiche di risposta agli incidenti	▪ Analizzare le procedure per il piano di risposta agli incidenti	☐	☐	☐	☐
	• Procedure di ripristino e continuità delle attività aziendali	▪ Analizzare le procedure per il piano di risposta agli incidenti	☐	☐	☐	☐
	• Processi di backup dei dati	▪ Analizzare le procedure per il piano di risposta agli incidenti	☐	☐	☐	☐
	• Analisi dei requisiti legali per la segnalazione di violazioni	▪ Analizzare le procedure per il piano di risposta agli incidenti	☐	☐	☐	☐
	• Copertura e risposte per tutti i componenti di sistema critici	▪ Analizzare le procedure per il piano di risposta agli incidenti	☐	☐	☐	☐
	• Riferimenti e descrizioni delle procedure di risposta agli incidenti adottate dai marchi di pagamento	▪ Analizzare le procedure per il piano di risposta agli incidenti	☐	☐	☐	☐

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
A2.1	*Per i terminali POS POI (e i punti di terminazione SSL/TLS a cui si connettono) che utilizzano SSL e/o TLS iniziale:* • È confermato che i dispositivi non sono soggetti a eventuali exploit noti per SSL/TLS iniziale *O:* • È in atto un piano formale di migrazione e riduzione dei rischi in base al Requisito A2.2?	▪ 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	☐	☐	☐	☐

Domanda PCI DSS		Test previsti	Risposta *(Selezionare una risposta per ogni domanda.)*			
			Sì	Sì con CCW	No	N/A
A2.2	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: ▪ 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; ▪ risultati della valutazione dei rischi e controlli per la riduzione dei rischi in atto; ▪ descrizione dei processi per ricercare eventuali nuove vulnerabilità associate a SSL/TLS iniziale; ▪ descrizione dei processi di controllo delle modifiche implementati per accertarsi che SSL/TLS iniziale non venga implementato nei nuovi ambienti; ▪ panoramica del piano del progetto di migrazione inclusa la data di completamento della migrazione prevista non oltre il 30 giugno 2018?	▪ Analizzare il piano documentato di migrazione e di riduzione dei rischi	☐	☐	☐	☐

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

Appendice C - Spiegazione di non applicabilità

Se è stata selezionata la colonna "N/A" (Non applicabile) del questionario, utilizzare questo foglio di lavoro per spiegare il motivo per cui il requisito descritto non è applicabile alla propria azienda.

Requisito	Motivo per cui il requisito non è applicabile
Esempio:	
3.4	I dati dei titolari di carta non vengono mai archiviati in formato elettronico

Sezione 3 - Dettagli su convalida e attestato

Parte 3. Convalida PCI DSS

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

In base ai risultati documentati nel SAQ A-EP 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):***

☐	**Conforme:** 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 **CONFORMITÀ** globale; pertanto *(Ragione sociale esercente)* ha dimostrato la massima conformità agli standard PCI DSS.
☐	**Non conforme:** 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 **NON CONFORME** globale; pertanto *(Ragione sociale esercente)* non ha dimostrato la massima conformità agli standard PCI DSS. **Data di destinazione** per conformità: è possibile che a un'entità che invia questo modulo con lo stato "Non conforme" venga richiesto di completare il Piano d'azione presente nella Parte 4 del presente documento. *Consultare il proprio acquirente o il marchio di pagamento prima di completare la Parte 4.*
☐	**Conforme ma con eccezione legale:** 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. *Se selezionata, completare quanto segue:*

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)

☐	Il questionario di autovalutazione A-EP PCI DSS, versione *(n. versione SAQ)*, è stato completato in base alle istruzioni qui fornite.
☐	Tutte le informazioni contenute nel questionario SAQ e in questo attestato rappresentano in modo onesto i risultati della mia valutazione sotto tutti gli aspetti.
☐	Ho verificato con il fornitore dell'applicazione di pagamento che il mio sistema di pagamento non memorizza dati sensibili di autenticazione dopo l'autorizzazione.
☐	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.
☐	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)	
☐	Nessuna prova della memorizzazione dei dati della traccia completa[1], dei dati CAV2, CVC2, CID o CVV2[2] oppure dei dati PIN[3] dopo che l'autorizzazione alla transazione è stata individuata su QUALSIASI sistema esaminato durante questa valutazione.
☐	Le scansioni ASV vengono completate dal Fornitore di prodotti di scansione approvato (ASV) PCI SSC *(Nome ASV)*

Parte 3b. Attestato esercente	
Firma del funzionario esecutivo dell'esercente ↑	*Data:*
Nome del funzionario esecutivo dell'esercente:	*Mansione:*

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:	

Firma del funzionario espressamente autorizzato dell'azienda QSA ↑	*Data:*
Nome del funzionario espressamente autorizzato*:*	*Azienda QSA:*

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:	

[1] 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.

[2] 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.

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

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

Selezionare la risposta appropriata per "Conforme ai requisiti PCI DSS" per ogni requisito. In caso di 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	☐	☐	
2	Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione	☐	☐	
3	Proteggere i dati dei titolari di carta memorizzati	☐	☐	
4	Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche	☐	☐	
5	Proteggere tutti i sistemi dal malware e aggiornare regolarmente i programmi o il software antivirus	☐	☐	
6	Sviluppare e gestire sistemi e applicazioni protette	☐	☐	
7	Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario	☐	☐	
8	Individuare e autenticare l'accesso ai componenti di sistema	☐	☐	
9	Limitare l'accesso fisico ai dati dei titolari di carta	☐	☐	
10	Registrare e monitorare tutti gli accessi a risorse di rete e dati dei titolari di carta	☐	☐	
11	Eseguire regolarmente test dei sistemi e processi di protezione	☐	☐	
12	Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale	☐	☐	
Appendice A2	Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale	☐	☐	

** I requisiti PCI DSS indicati qui fanno riferimento alle domande della Sezione 2 del questionario SAQ.*