L’ Approccio prioritario per il rispetto della conformità PCI DSS

Lo standard Settore delle carte di pagamento Standard di protezione dei dati (PCI DSS) fornisce una struttura dettagliata composta da 12 requisiti per la protezione dei dati dei titolari di carta memorizzati, elaborati e/o trasmessi da esercenti e altre organizzazioni. Per la sua natura onnicomprensiva, lo standard fornisce una quantità così grande di informazioni sulla sicurezza che alcune persone che sono responsabili della sicurezza dei dati dei titolari di carta potrebbero chiedersi dove iniziare il percorso continuo verso la conformità. A tale scopo, PCI Security Standards Council fornisce il seguente Approccio prioritario per consentire agli interessati di capire dove possono agire per ridurre il rischio anticipatamente nel processo di conformità. Nessuna singola pietra miliare dell’Approccio prioritario fornirà conformità PCI DSS o sicurezza completa, ma seguendone le linee guida gli interessati potranno accelerare il processo di protezione dei dati dei titolari di carta.

CARATTERISTICHE PRINCIPALI

Possibilità per gli esercenti di identificare gli obiettivi a più alto rischio

Creazione di un linguaggio comune in relazione alle iniziative di implementazione e valutazione PCI DSS

Dimostrazione agli esercenti dei progressi nel processo di conformità tramite le pietre miliari

Cos’è l’Approccio prioritario?

L’Approccio prioritario fornisce sei pietre miliari della sicurezza che consentiranno a esercenti e altre organizzazioni di proteggersi in modo incrementale dai fattori di rischio più alto e minacce in crescita nel raggiungimento della conformità PCI DSS. L’Approccio prioritario e le relative pietre miliari (descritte a pagina 2) sono destinati a fornire i seguenti vantaggi:

- roadmap che un’organizzazione può utilizzare per eliminare i suoi rischi in ordine di priorità;
- approccio pragmatico che consente “rapide vittorie”;
- supporto per la pianificazione finanziaria e operativa;
- promozione di indicatori dei progressi misurabili e oggettivi;
- promozione della coerenza tra i valutatori.

Obiettivi dell’Approccio prioritario

L’Approccio prioritario fornisce una roadmap delle attività di conformità in base al rischio associato alla memorizzazione, all’elaborazione e/o alla trasmissione dei dati dei titolari di carta. La roadmap consente di assegnare priorità alle iniziative per raggiungere la conformità, stabilire le pietre miliari, ridurre il rischio di violazioni dei dati dei titolari di carta anticipatamente nel processo di conformità e permette agli acquirenti di misurare in modo oggettivo attività di conformità e riduzione del rischio da parte di esercenti, provider di servizi e altri. L’Approccio prioritario è stato progettato in base all’analisi dei dati derivanti da violazioni effettive e al feedback di Qualified Security Assessor (QSA), di investigatori forensi e del Consiglio consultivo di PCI Security Standards Council. Non è stato concepito come un approccio sostitutivo, scorciatoia o provvisorio alla conformità PCI DSS e non è una struttura unica obbligatoria applicabile a ogni organizzazione. L’Approccio prioritario è idoneo per gli esercenti che subiscono una valutazione in sede o utilizzano il questionario SAQ D.

LA CONFORMITÀ PCI DSS È UN PROCESSO CONTINUO

FONDATORI PCI SSC

ORGANIZZAZIONI PARTECIPANTI

Esercenti, banche, elaboratori, sviluppatori e venditori al punto vendita

Esclusione di responsabilità

Per raggiungere la confirmità PCI DSS, un'organizzazione deve soddisfare tutti i requisiti PCI DSS, indipendentemente dall'ordine in cui sono stati soddisfatti o dal fatto che l'organizzazione che desidera perseguire tale conformità segua l'Approccio prioritario PCI DSS. Il presente documento non modifica o manipola PCI DSS o alcuno dei relativi requisiti e può essere modificato senza avviso. PCI SSC non è responsabile di eventuali errori o danni di alcun tipo derivanti dall'uso delle informazioni ivi contenute. PCI SSC non rilascia alcuna garanzia o dichiarazione in merito ad accuratezza o sufficienza delle informazioni fornite come parte dell'Approccio prioritario e PCI SSC non si assume alcun obbligo o responsabilità in relazione all'uso o all'abuso di tali informazioni.

Pietre miliari per assegnare priorità alle iniziative di conformità PCI DSS

L'Approccio prioritario include sei pietre miliari. La matrice riportata di seguito fornisce un riepilogo degli obiettivi e degli scopi ad alto livello di ciascuna pietra miliare. Il resto del presente documento associa le pietre miliari a ciascuno di tutti i dodici requisiti PCI DSS e dei relativi sottorequisiti.

Pietra miliare	Obiettivi
1	**Rimuovere dati sensibili di autenticazione e limitare la conservazione dei dati.** Questa pietra miliare riguarda un'area di rischio chiave per le entità che sono state compromesse. Tenere presente che, se non vengono memorizzati i dati sensibili di autenticazione e altri dati dei titolari di carta, gli effetti di una compromissione saranno notevolemente ridotti. Se non sono necessari, non memorizzarli.
2	**Proteggere sistemi e reti ed essere preparati a rispondere a una violazione del sistema.** Questa pietra miliare riguarda i controlli per i punti di accesso alla maggior parte delle compromissioni e i processi di risposta.
3	**Proteggere le applicazioni delle carte di pagamento.** Questa pietra miliare riguarda i controlli per applicazioni, processi di applicazioni e server di applicazioni. I punti deboli presenti in queste aree rappresentano una facile preda di utenti non autorizzati che cercano di compromettere i sistemi e ottenere l'accesso ai dati dei titolari di carta.
4	**Monitorare e controllare l'accesso ai sistemi.** I controlli per questa pietra miliare consentono di rilevare chi, cosa, quando e come relativamente a chi sta accedendo alla rete e all'ambiente dei dati dei titolari di carta.
5	**Proteggere i dati di titolari di carta memorizzati.** Per le organizzazioni che hanno analizzati i loro processi aziendali e determinato che devono memorizzare i PAN (Primary Account Number), la pietra miliare 5 riguarda meccanismi di protezione chiave per i dati memorizzati.
6	**Finalizzare le iniziative di conformità restanti e accertarsi che siano in atto tutti i controlli.** Lo scopo della pietra miliare 6 è completare i requisiti PCI DSS e finalizzare tutte le politiche, le procedure e i processi correlati restanti necessari per proteggere l'ambiente dei dati dei titolari di carta.

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
Requisito 1: Installare e gestire una configurazione firewall per proteggere i dati dei titolari di carta						
1.1 Stabilire e implementare standard di configurazione del firewall e del router che includano:						
1.1.1 Un processo formale per l'approvazione e il test di tutte le connessioni di rete e le modifiche apportate alla configurazione del firewall e del router						6
1.1.2 Diagramma di rete aggiornato che identifica tutte le connessioni tra ambiente dei dati dei titolari di carta e altre reti, comprese eventuali reti wireless	1					
1.1.3 Diagramma aggiornato che mostra tutti i flussi dei dati dei titolari di carta sui sistemi e sulle reti	1					
1.1.4 Requisiti per un firewall per ogni connessione Internet e tra tutte le zone demilitarizzate (DMZ) e la zona della rete interna		2				
1.1.5 Descrizione di gruppi, ruoli e responsabilità per la gestione dei componenti di rete						6
1.1.6 Documentazione della giustificazione e dell'approvazione aziendali per l'uso di tutti i servizi, i protocolli e le porte consentiti, inclusa la documentazione delle funzioni di sicurezza implementate per i protocolli considerati non sicuri.		2				
1.1.7 Una revisione dei set di regole del firewall e del router almeno ogni sei mesi						6
1.2 Creazione di configurazioni di firewall e router che limitino le connessioni tra le reti non attendibili e qualsiasi componente di sistema nell'ambiente dei dati dei titolari di carta. *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 Limitazione del traffico in entrata e in uscita a quello indispensabile per l'ambiente dati dei titolari di carta e, specificatamente, rifiutare tutto l'altro traffico.		2				
1.2.2 Protezione e sincronizzazione dei file di configurazione del router.		2				
1.2.3 Installazione di firewall perimetrali tra le reti wireless e l'ambiente dei dati dei titolari di carta e configurazione di tali firewall per 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.		2				
1.3 Vietare l'accesso pubblico diretto tra Internet e i componenti di sistema nell'ambiente dei dati di titolari di carta.						
1.3.1 Implementazione di una zona DMZ per limitare il traffico in entrata ai soli componenti di sistema che forniscono servizi, protocolli e porte autorizzati accessibili pubblicamente.		2				
1.3.2 Limitazione del traffico Internet in entrata agli indirizzi IP all'interno della zona DMZ.		2				
1.3.3 Implementare 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 di origine interno.)		2				
1.3.4 Non consentire il traffico in uscita non autorizzato dall'ambiente dei dati dei titolari di carta a Internet.		2				
1.3.5 Consentire nella rete solo le connessioni già "stabilite".		2				

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
1.3.6 Posizionare i componenti di sistema che memorizzano i dati dei titolari di carta (come un database) in una zona di rete interna, separata dalla zona DMZ e da altre reti non attendibili.		2				
1.3.7 Non divulgare indirizzi IP privati e informazioni di routing a parti non autorizzate. *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.*		2				
1.4 Installare 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 che vengono utilizzati anche per accedere al CDE. Le configurazioni del firewall (o funzionalità equivalente) includono quanto segue: • vengono definite impostazioni di configurazione specifiche; • il firewall personale (o funzionalità equivalente) sia attivamente in esecuzione; • il firewall personale (o funzionalità equivalente) non sia modificabile dagli utenti di dispositivi mobili.		2				
1.5 Verificare che le politiche di sicurezza e le procedure operative per la gestione dei firewall siano documentate, in uso e note a tutte le parti coinvolte.		2				
Requisito 2: Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione						
2.1 Modificare sempre i valori predefiniti del fornitore e rimuovere o disabilitare account predefiniti non necessari prima di installare un sistema sulla 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.		2				
2.1.1 Per gli ambienti wireless connessi all'ambiente dei dati dei titolari di carta o che trasmettono tali dati, modificare TUTTE le impostazioni predefinite del fornitore wireless, incluse, senza limitazioni, chiavi di cifratura wireless predefinite, password e stringhe di comunità SNMP.		2				
2.2. Sviluppare standard di configurazione per tutti i componenti di sistema. Accertarsi che questi standard risolvano tutte le vulnerabilità della sicurezza note e siano coerenti con gli standard di hardening accettati dal settore. Le fonti di standard di hardening accettati dal settore possono includere, senza limitazioni: • CIS (Center for Internet Security) • ISO (International Organization for Standardization) • Istituto SANS (SysAdmin Audit Network Security) • NIST (National Institute of Standards Technology)			3			

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
2.2.1 Implementare solo una funzione principale per server per impedire la coesistenza sullo stesso server di funzioni che richiedono livelli di sicurezza diversi. Ad esempio, server Web, database server e DNS devono essere implementati su server separati. *Nota: dove si utilizzano tecnologie di virtualizzazione, implementare solo una funzione principale per componente di sistema virtuale.*			3			
2.2.2 Abilitazione di servizi, protocolli, daemon, ecc. necessari, come richiesto per la funzione del sistema.			3			
2.2.3 Implementare funzioni di sicurezza aggiuntive per eventuali servizi, protocolli o daemon richiesti considerati non sicuri. *Nota: laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.*		2				
2.2.4 Configurazione dei parametri di sicurezza del sistema per evitare un uso improprio.			3			
2.2.5 Rimozione di tutta la funzionalità non necessaria, ad esempio script, driver, funzioni, sottosistemi, file system e server Web non utilizzati.			3			
2.3 Eseguire la cifratura di tutto l'accesso amministrativo non da console, tramite crittografia avanzata. *Nota: laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.*		2				
2.4 Realizzazione di un inventario dei componenti di sistema nell'ambito dello standard PCI DSS.		2				
2.5 Verificare che i criteri di protezione e le procedure operative per la gestione delle impostazioni predefinite del fornitore e di altri parametri di sicurezza siano documentati, in uso e noti a tutte le parti coinvolte.		2				
2.6 I provider di hosting condiviso devono proteggere l'ambiente ospitato e i dati dei titolari di carta di ciascuna entità. Questi provider devono soddisfare specifici requisiti come descritto nell'Appendice A1: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso.			3			
Requisito 3 - Proteggere i dati dei titolari di carta memorizzati						
3.1 Mantenere al minimo la memorizzazione dei dati dei titolari di carta implementando politiche, procedure e processi per la conservazione e l'eliminazione dei dati che includano per tutta la memorizzazione dei dati dei titolari di carta almeno quanto riportato di seguito: • limitazione della quantità dei dati memorizzati e del tempo di conservazione in base alle esigenze aziendali, legali e/o legislative; • requisiti specifici di conservazione dei dati dei titolari di carta; • processi per la rimozione sicura dei dati quando non sono più necessari; • processo trimestrale per identificare ed eliminare in modo sicuro i dati dei titolari di carta memorizzati che superano i requisiti di conservazione definiti.	1					
3.2 Non memorizzare dati sensibili di autenticazione dopo l'autorizzazione (anche se cifrati). Se si ricevono dati sensibili di autenticazione, dopo il completamento del processo di autorizzazione rendere tutti i dati non recuperabili. Gli emittenti e le società che supportano servizi di emissione sono autorizzati a memorizzare i dati sensibili di autenticazione in presenza di: • una giustificazione aziendale • memorizzazione sicura dei dati I dati sensibili di autenticazione includono i dati citati nei seguenti Requisiti da 3.2.1 a 3.2.3:	1					

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
3.2.1 Non memorizzare l'intero contenuto di qualsiasi traccia (dalla striscia magnetica presente sul retro della carta, dati equivalenti contenuti in un chip o in altro luogo) dopo l'autorizzazione. Questi dati sono denominati anche traccia completa, traccia, traccia 1, traccia 2 e dati della striscia magnetica. Nota: nel normale svolgimento delle attività, è possibile che sia necessario conservare i seguenti elementi di dati della striscia magnetica: • Nome del titolare della carta • PAN (Primary Account Number) • data di scadenza • Codice di servizio Per ridurre al minimo il rischio, memorizzare solo gli elementi di dati necessari per l'azienda.	1					
3.2.2 Non memorizzare il Card Validation Code or Value (numero a tre o quattro cifre impresso sulla parte anteriore o posteriore di una carta di pagamento utilizzato per verificare le transazioni con carta non presente) dopo l'autorizzazione.	1					
3.2.3 Dopo l'autorizzazione, non memorizzare il numero di identificazione personale (PIN) o il blocco PIN cifrato.	1					
3.3 Mascherare il PAN completo quando visualizzato (non devono essere visibili più di sei cifre all'inizio e quattro cifre alla fine) per renderlo visibile solo al personale con un'esigenza aziendale legittima. *Nota: questo requisito non sostituisce i requisiti più rigorosi per la visualizzazione dei dati dei titolari di carta, ad esempio requisiti legali o del marchio di carta di pagamento per ricevute di punti di vendita (POS).*					5	
3.4 Rendere illeggibile il PAN ovunque sia memorizzato (inclusi i supporti digitali portatili, supporti di backup e i log) utilizzando uno dei seguenti approcci: • hash one-way basati su crittografia avanzata (l'hash deve essere dell'intero PAN); • Troncatura (non si può usare l'hashing per sostituire la parte troncata del PAN) • Token e pad indicizzati (i pad devono essere custoditi in un luogo sicuro) • crittografia avanzata con relativi processi e procedure di gestione delle chiavi. *Nota: per un utente non autorizzato è relativamente facile ricostruire i dati PAN originali se ha accesso alla versione troncata e hash del PAN. Nel caso in cui la versione troncata e hash dello stesso PAN siano presenti nell'ambiente di un'entità, devono essere predisposti ulteriori controlli per verificare che non sia possibile correlare la versione troncata e hash per ricostruire il PAN originale.*					5	
3.4.1 Se si utilizza la cifratura del disco (anziché la cifratura del database a livello di file o colonna), l'accesso logico deve essere gestito in modo distinto e indipendente dai meccanismi di controllo dell'accesso e di autenticazione del sistema operativo nativo (ad esempio, non utilizzando database di account utente locali o credenziali di accesso alla rete generiche). Le chiavi di decifratura non devono essere associate agli account utente. *Nota: questo requisito si applica in aggiunta a tutti gli altri requisiti di gestione delle chiavi e di cifratura PCI DSS.*					5	
3.5 Documentare e implementare procedure per proteggere le chiavi utilizzate per tutelare i dati dei titolari di carta contro divulgazione e uso improprio: *Nota: questo requisito si applica alle chiavi utilizzate per cifrare i dati dei titolari di carta memorizzati e alle chiavi di cifratura delle chiavi (KEK) utilizzate per proteggere le chiavi di cifratura dei dati. Tali KEK devono essere avanzate almeno quanto la chiave di cifratura dei dati.*						

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
3.5.1 Requisito aggiuntivo solo per provider di servizi: conservare una descrizione documentata dell'architettura crittografica che includa: • dettagli di tutti gli algoritmi, i protocolli e le chiavi utilizzati per la protezione dei dati dei titolari di carta, incluse la data di scadenza e l'attendibilità della chiave; • descrizione dell'utilizzo per ciascuna chiave; • inventario di eventuali HSM e altri SCD utilizzati per la gestione delle chiavi. *Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.*					5	
3.5.2 Limitare l'accesso alle chiavi di crittografia al minor numero possibile di custodi necessari.					5	
3.5.3 Memorizzare sempre le chiavi segrete e private utilizzate per cifrare/ decifrare costantemente i dati dei titolari di carta in una (o più) delle seguenti forme: • cifrate con chiave KEK avanzata almeno quanto la chiave di cifratura dei dati che viene memorizzata separatamente dalla chiave di cifratura dei dati; • interne a un dispositivo crittografico protetto (come un modulo di sicurezza (host) hardware (HSM) o un dispositivo di punto di interazione approvato PTS); • come almeno due componenti o condivisioni di chiavi a lunghezza integrale, in conformità a un metodo accettato nel settore. *Nota: non è necessario memorizzare le chiavi pubbliche in uno di questi moduli.*					5	
3.5.4 Memorizzare le chiavi di crittografia nel minor numero possibile di posizioni.					5	
3.6 Documentare e implementare completamente tutti i processi e le procedure di gestione delle chiavi di crittografia utilizzate per la cifratura dei dati di titolari di carta, incluso quanto segue: *Nota: sono disponibili numerosi standard di settore per la gestione delle chiavi in diverse risorse, tra cui il sito del NIST all'indirizzo http://csrc.nist.gov.*						
3.6.1 Generazione di chiavi di crittografia avanzata					5	
3.6.2 Distribuzione di chiavi di crittografia sicure					5	
3.6.3 Memorizzazione di chiavi di crittografia sicure					5	
3.6.4 Modifiche delle chiavi di crittografia per le chiavi giunte al termine del loro periodo di validità (ad esempio, una volta trascorso un periodo di tempo definito e/o dopo la produzione da parte di una determinata chiave di una quantità definita di testo di cifratura), come specificato dal fornitore dell'applicazione associato o dal proprietario delle chiavi, ed in base alle linee guida ed alle migliori pratiche di settore (ad esempio, NIST Special Publication 800-57).					5	
3.6.5 Ritiro o sostituzione delle chiavi (ad esempio, archiviazione, distruzione e/o revoca) come ritenuto necessario in caso di indebolimento dell'integrità della chiave (ad esempio, partenza di un dipendente a conoscenza di chiavi con testo in chiaro) o chiavi per le quali esista il sospetto che siano state compromesse. Nota: se ritirate o sostituite le chiavi di crittografia devono essere conservate, queste chiavi devono essere archiviate in modo sicuro (ad esempio usando una KEK). Le chiavi di crittografia archiviate dovrebbero essere usate solo per scopi di decifratura/verifica.					5	

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
3.6.6 Se vengono utilizzate le operazioni manuali di gestione delle chiavi di crittografia con testo in chiaro, tali operazioni vanno gestite utilizzando i principi di "split knowledge" e controllo duale. Nota: esempi di operazioni manuali di gestione delle chiavi includono, senza limitazioni, la generazione, la trasmissione, il caricamento, la memorizzazione e la distruzione delle chiavi.					5	
3.6.7 Prevenzione di tentativi di sostituzione non autorizzata delle chiavi di crittografia.					5	
3.6.8 Obbligo per i custodi delle chiavi di crittografia di riconoscere in modo formale che accettano e confermano di conoscere le proprie responsabilità.					5	
3.7 Verificare che i criteri di protezione e le procedure operative per la protezione dei dati dei titolari di carta memorizzati siano documentati, in uso e noti a tutte le parti coinvolte.					5	
Requisito 4 - Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche						
4.1 Utilizzare la crittografia avanzata e i protocolli di sicurezza per proteggere i dati sensibili dei titolari di carta quando vengono trasmessi su reti pubbliche aperte, incluso quando: • vengono accettati solo certificati e chiavi affidabili; • il protocollo utilizzato supporta soltanto versioni o configurazioni sicure; • il livello di cifratura è corretto per la metodologia di cifratura in uso. *Nota: laddove si utilizza SSL/TLS iniziale, devono essere completati i requisiti dell'Appendice A2.* *Esempi di reti pubbliche aperte includono, senza limitazioni:* • *Internet* • *tecnologie wireless, incluso 802.11 e Bluetooth* • *tecnologie mobili, ad esempio, comunicazioni GSM (Global System for Mobile), CDMA (code division multiple access)* • *GPRS (General Packet Radio Service)* • *comunicazioni satellitari*		2				
4.1.1 Garantire che le reti wireless che trasmettono i dati dei titolari di carta o connesse all'ambiente dei dati dei titolari di carta utilizzino le migliori pratiche di settore per implementare la cifratura avanzata per l'autenticazione e la trasmissione.		2				
4.2 Non inviare mai PAN non protetti mediante tecnologie di messaggistica degli utenti finali (ad esempio, e-mail, messaggistica istantanea, SMS, chat, ecc.).		2				
4.3 Verificare che i criteri di protezione e le procedure operative per la cifratura delle trasmissioni dei dati dei titolari di carta siano documentati, in uso e noti a tutte le parti coinvolte.		2				
Requisito 5: Utilizzare e aggiornare regolarmente il software o i programmi antivirus						
5.1 Distribuire il software antivirus su tutti i sistemi solitamente interessati da malware (in particolare PC e server).		2				
5.1.1 Garantire che tutti i programmi antivirus siano in grado di rilevare, rimuovere e proteggere contro tutti i tipi di malware noto.		2				
5.1.2 Effettuare valutazioni periodiche dei sistemi che non vengono comunemente interessati da malware per individuare e valutare l'evoluzione delle minacce malware e confermare o meno la necessità di software antivirus per tali sistemi.		2				

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
5.2 Verificare che tutti i meccanismi antivirus siano: • aggiornati • inclusi in scansioni periodiche • in grado di generare log di audit da conservare in base al Requisito 10.7 PCI DSS		2				
5.3 Garantire che i meccanismi antivirus siano in esecuzione in modo attivo e che non possono essere disabilitati o alterati dagli utenti a meno che non siano stati specificatamente autorizzati dalla direzione per ogni singolo caso e per un periodo di tempo limitato. *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.*		2				
5.4 Verificare che i criteri di protezione e le procedure operative per la protezione dei sistemi contro il malware siano documentati, in uso e noti a tutte le parti coinvolte.		2				
Requisito 6: Sviluppare e gestire sistemi e applicazioni protette						
6.1 Stabilire un processo per identificare le vulnerabilità della sicurezza, utilizzando fonti esterne attendibili per le informazioni sulle vulnerabilità della sicurezza e assegnare una classificazione dei rischi (ad esempio, "alta", "media" o "bassa") alle vulnerabilità della sicurezza recentemente rilevate. *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 delle organizzazioni 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.*			3			
6.2 Assicurare che tutti i componenti di sistema ed il software siano protetti dalle vulnerabilità note mediante l'installazione delle patch di sicurezza dei fornitori. Installare patch di sicurezza critiche entro un mese dalla release. *Nota: le patch di sicurezza critiche vanno identificate in conformità al processo di classificazione dei rischi definito nel Requisito 6.1.*			3			
6.3 Sviluppare applicazioni software interne ed esterne (incluso l'accesso amministrativo basato su Web alle applicazioni) in maniera sicura, come segue: • in conformità allo standard PCI DSS (ad esempio autenticazione e registrazione sicure); • sulla base di standard e/o migliori pratiche di settore; • integrazione della sicurezza delle informazioni per l'intera durata del ciclo di sviluppo del software. *Nota: valido per tutto il software sviluppato internamente, nonché per il software su misura o personalizzato, sviluppato da terzi.*			3			
6.3.1 Rimozione di sviluppo, test e/o account, ID utente e password di applicazioni personalizzate prima dell'attivazione o della release di tali applicazioni ai clienti.			3			

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
6.3.2 Analizzare il codice personalizzato prima della release in produzione o della distribuzione ai clienti per individuare eventuali vulnerabilità del codice (mediante processi manuali o automatici) e accertarsi almeno che: • le modifiche del codice siano analizzate da utenti singoli diversi dall'autore del codice originario e da utenti esperti di tecniche di analisi del codice e pratiche di codifica sicure; • le analisi del codice garantiscano che il codice venga sviluppato in base a linee guida di codifica sicure; • le correzioni appropriate vengono implementate prima della release; • i risultati dell'analisi del codice vengono esaminati e approvati dalla direzione prima della release; *Nota: questo requisito per le analisi del codice si applica a tutto il codice personalizzato (interno ed esterno), come parte della durata del ciclo di sviluppo del sistema. Le analisi del codice possono essere condotte da personale interno preparato o da terze parti. Le applicazioni Web rivolte al pubblico sono anche soggette a controlli aggiuntivi, per risolvere le minacce costanti e le vulnerabilità dopo l'implementazione, secondo quanto definito nel Requisito 6.6 PCI DSS.*			**3**			
6.4 Seguire i processi e le procedure di controllo delle modifiche per tutte le modifiche apportate ai componenti di sistema. I processi devono includere quanto segue:			**3**			
6.4.1 Separare gli ambienti di sviluppo/test dagli ambienti di produzione e garantire tale separazione con i controlli di accesso.			**3**			
6.4.2 Separare le responsabilità tra ambienti di sviluppo/test e ambienti di produzione			**3**			
6.4.3 I dati di produzione (PAN attivi) sono esclusi dalle attività di test o sviluppo			**3**			
6.4.4 Rimuovere dai componenti di sistema dati e account di test prima che il sistema diventi attivo/entri in produzione.			**3**			
6.4.5 Le procedure di controllo delle modifiche devono includere quanto segue:						**6**
6.4.5.1 Documentazione dell'impatto.						**6**
6.4.5.2 Approvazione documentata delle modifiche da parte di parti autorizzate.						**6**
6.4.5.3 Esecuzione del test della funzionalità per verificare che la modifica non influisca negativamente sulla sicurezza del sistema.						**6**
6.4.5.4 Procedure di back-out.						**6**
6.4.6 Al completamento di una modifica significativa, tutti i requisiti PCI DSS pertinenti devono essere implementati su tutte le reti e tutti i sistemi nuovi o modificati e la documentazione deve essere aggiornata come applicabile. *Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.*						**6**
6.5 Risoluzione delle vulnerabilità di codifica comuni nei processi di sviluppo software come segue: • formare gli sviluppatori almeno una volta all'anno sulle tecniche di codifica sicura aggiornate, inclusi i metodi per evitare le vulnerabilità di codifica comuni; • sviluppare applicazioni in base a linee guida di codifica sicura. *Nota: le vulnerabilità elencate dal punto 6.5.1 al punto 6.5.10 erano presenti nelle migliori pratiche di settore al momento della pubblicazione di questa versione dello standard PCI DSS. Tuttavia, poiché le migliori pratiche di settore per la gestione delle vulnerabilità sono state aggiornate (ad esempio, la OWASP Guide, SANS CWE Top 25, CERT Secure Coding, ecc.), per questi requisiti è necessario utilizzare le migliori pratiche più recenti.*			**3**			
Nota: i requisiti da 6.5.1 a 6.5.6, riportati di seguito, si riferiscono a tutte le applicazioni (interne o esterne).						

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
6.5.1 Injection flaw, in particolare SQL injection. Considerare, inoltre, OS Command Injection, LDAP e XPath injection flaw, nonché altri tipi di injection flaw.			3			
6.5.2 Buffer overflow			3			
6.5.3 Memorizzazione di dati crittografici non sicura			3			
6.5.4 Comunicazioni non sicure			3			
6.5.5 Gestione degli errori non corretta			3			
6.5.6 Tutte le vulnerabilità ad "alto rischio" identificate nel processo di identificazione delle vulnerabilità (come definito nel Requisito 6.1 PCI DSS).			3			
Nota: i requisiti da 6.5.7 a 6.5.10, riportati di seguito, si riferiscono ad applicazioni Web e interfacce di applicazioni (interne o esterne):						
6.5.7 XSS (Cross-Site Scripting)			3			
6.5.8 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).			3			
6.5.9 Cross-site request forgery (CSRF)			3			
6.5.10 Violazione dell'autenticazione e gestione delle sessioni			3			
6.6 Per le applicazioni Web esterne, risolvere costantemente le nuove minacce e vulnerabilità e garantire che queste applicazioni siano protette da attacchi noti mediante uno dei seguenti metodi: • analisi delle applicazioni Web rivolte al pubblico tramite strumenti o metodi di valutazione della sicurezza delle applicazioni manuali o automatici, almeno una volta all'anno e dopo ogni modifica; *Nota: la valutazione non corrisponde alle scansioni delle vulnerabilità eseguite in base al Requisito 11.2.* • installazione di una soluzione tecnica automatica che rileva e impedisce gli attacchi basati sul Web (ad esempio, un firewall per applicazioni Web) davanti alle applicazioni Web rivolte al pubblico per monitorare costantemente tutto il traffico.			3			
6.7 Verificare che i criteri di protezione e le procedure operative per lo sviluppo e la manutenzione di applicazioni e sistemi sicuri siano documentati, in uso e noti a tutte le parti coinvolte.			3			
Requisito 7: Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario						
7.1 Limitare l'accesso ai componenti di sistema e ai dati di titolari di carta solo alle persone per le cui mansioni è realmente necessario.						
7.1.1 Definizione delle esigenze di accesso per ogni ruolo, incluso: • componenti di sistema e risorse dati di cui ogni ruolo ha bisogno per accedere alla relativa funzione; • Livello di privilegio necessario (ad esempio, utente, amministratore, ecc.) per accedere alle risorse.				4		
7.1.2 Limitazione dell'accesso a ID utente privilegiati alla quantità minima necessaria per le responsabilità di ruolo.				4		
7.1.3 Assegnazione dell'accesso basata sulla classificazione e sulla funzione del ruolo del personale.				4		

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
7.1.4 Richiedere l'approvazione documentata delle parti autorizzate specificando i privilegi necessari.				4		
7.2 Stabilire un sistema di controllo dell'accesso per i componenti di sistema che limiti l'accesso in base all'effettiva esigenza di un utente e che sia impostato su "deny all" a meno che non sia specificatamente consentito. Il sistema di controllo dell'accesso deve includere quanto segue:						
7.2.1 Copertura di tutti i componenti di sistema				4		
7.2.2 Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale.				4		
7.2.3 Impostazione predefinita "deny all".				4		
7.3 Verificare che i criteri di protezione e le procedure operative per la limitazione dell'accesso ai dati dei titolari di carta siano documentati, in uso e noti a tutte le parti coinvolte.				4		
Requisito 8: Assegnare un ID univoco a chiunque abbia accesso a un computer						
8.1 Definizione e implementazione di politiche e procedure per garantire una corretta gestione dell'identificazione degli utenti non consumatori e amministratori su tutti i componenti di sistema nel seguente modo:						
8.1.1 Assegnare a tutti gli utenti un ID univoco prima di consentire l'accesso ai componenti di sistema o ai dati dei titolari di carta.		2				
8.1.2 Controllare le operazioni di aggiunta, eliminazione e modifica di ID utente, credenziali e altri oggetti identificativi.		2				
8.1.3 Revocare immediatamente l'accesso per gli utenti non attivi.		2				
8.1.4 Rimuovere/disabilitare gli account utente non attivi entro 90 giorni.		2				
8.1.5 Gestire gli ID utilizzati da terzi per accedere, fornire supporto o manutenzione dei componenti di sistema tramite accesso remoto come segue: • abilitati solo durante il periodo di tempo necessario e disabilitati se non in uso; • monitorati quando in uso.		2				
8.1.6 Limitare i tentativi di accesso ripetuti bloccando l'ID utente dopo un massimo di sei tentativi.		2				
8.1.7 Impostare la durata del blocco a un minimo di 30 minuti o finché l'amministratore non abilita l'ID utente.		2				
8.1.8 Se una sessione è inattiva per più di 15 minuti, è necessario che l'utente effettui di nuovo l'autenticazione per riattivare il terminale o la sessione.		2				
8.2 Oltre ad assegnare un ID univoco, garantire la corretta gestione dell'autenticazione degli utenti non cliente e amministratori su tutti i componenti di sistema adottando almeno uno 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.		2				
8.2.1 Utilizzando la crittografia avanzata, rendere illeggibili tutte le credenziali di autenticazione (quali password/passphrase) durante la trasmissione e la memorizzazione su tutti i componenti di sistema.		2				
8.2.2 Verificare l'identità dell'utente prima di modificare le credenziali di autenticazione, ad esempio ripristinando la password, fornendo nuovi token o generando nuove chiavi.		2				

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
8.2.3 Le password/passphrase devono soddisfare i seguenti parametri: • Lunghezza minima di almeno 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.		2				
8.2.4 Modificare le password/passphrase dell'utente almeno una volta ogni 90 giorni.		2				
8.2.5 Non consentire l'invio di una nuova password/passphrase uguale a una delle ultime quattro password/passphrase utilizzate.		2				
8.2.6 Impostare le password/passphrase per il primo accesso e il ripristino su un valore univoco per ogni utente e modificarlo immediatamente dopo il primo uso.		2				
8.3 Proteggere tutto il singolo accesso amministrativo non da console e tutto l'accesso remoto al CDE utilizzando l'autenticazione a più fattori. *Nota: l'autenticazione a più fattori richiede l'utilizzo di almeno due dei tre metodi di autenticazione (fare riferimento al Requisito 8.2 per le descrizioni dei metodi di autenticazione). Utilizzare due volte un fattore (ad esempio, l'uso di due password separate) non viene considerato come un'autenticazione a più fattori.*						
8.3.1 Incorporare l'autenticazione a più fattori per tutto l'accesso non da console al CDE per il personale con accesso amministrativo. *Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.*		2				
8.3.2 Incorporare 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 dell'entità.		2				
8.4 Documentare e comunicare le procedure e le politiche di autenticazione a tutti gli utenti inclusi: • 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 per modificare le password in caso di sospetta compromissione delle password.				4		
8.5 Non utilizzare ID e password di gruppo, condivisi o generici né altri metodi di autenticazione, come segue: • gli ID utente generici sono disabilitati o rimossi; • non esistono ID utente condivisi per le attività di amministrazione del sistema e altre funzioni critiche; • gli ID utente condivisi e generici non vengono utilizzati per gestire i componenti di sistema.				4		
8.5.1 Requisito aggiuntivo solo per provider di servizi: i provider di servizi con accesso remoto alle sedi dei clienti (ad esempio, per fornire assistenza a sistemi o server POS) devono utilizzare credenziali di autenticazione univoche (quali password/passphrase) per ogni cliente. *Nota: questo requisito non è valido per i provider di hosting condiviso che accedono al proprio ambiente di hosting in cui sono ospitati più ambienti dei clienti.*		2				

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
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 deve essere 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.				4		
8.7 Tutto l'accesso a eventuali database contenenti dati dei titolari di carta (incluso l'accesso da parte di applicazioni, amministratori e tutti gli altri utenti) è limitato come segue: • Tutti gli accessi, le query e le azioni dell'utente sul database si verificano tramite metodi programmatici. • Solo gli amministratori del database hanno la possibilità di accedere o eseguire query direttamente sui database. • Gli ID di applicazione per le applicazioni del database possono essere utilizzati esclusivamente dalle applicazioni e non da utenti singoli o altri processi non relativi alle applicazioni.				4		
8.8 Verificare che i criteri di protezione e le procedure operative per l'identificazione e l'autenticazione siano documentati, in uso e noti a tutte le parti coinvolte.				4		
Requisito 9: Limitare l'accesso fisico ai dati dei titolari di carta						
9.1 Utilizzare i controlli dell'accesso alle strutture appropriati per limitare e monitorare gli accessi fisici ai sistemi nell'ambiente dei dati dei titolari di carta.		2				
9.1.1 Utilizzare videocamere o meccanismi di controllo dell'accesso per monitorare il singolo accesso fisico ad aree sensibili. Esaminare i dati raccolti e correlarli con altri. Conservare i dati per almeno tre mesi, se non diversamente richiesto dalle leggi in vigore. *Nota: per "aree sensibili" si intendono centri dati, aree server e aree che ospitano sistemi di memorizzazione, elaborazione o trasmissione dei dati dei titolari di carta. Ciò esclude le aree rivolte al pubblico in cui vi sono i terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio.*		2				
9.1.2 Implementare controlli fisici e/o logici per limitare l'accesso ai connettori di rete pubblicamente accessibili. Ad esempio, i connettori di rete che si trovano nelle aree pubbliche e nelle aree accessibili ai visitatori potrebbero essere disattivati e attivati solo quando l'accesso alla rete è autorizzato esplicitamente. In alternativa, è possibile implementare i processi per garantire che i visitatori siano scortati costantemente nelle aree con connettori di rete attivi.		2				
9.1.3 Limitare l'accesso fisico a punti di accesso wireless, gateway, dispositivi portatili, hardware di rete e comunicazione e linee di telecomunicazione.		2				
9.2 Sviluppare procedure per consentire di distinguere facilmente tra personale in sede e visitatori e includere: • individuazione di personale in sede e visitatori (ad esempio, assegnando tessere magnetiche); • modifiche ai requisiti di accesso; • revoca o disattivazione dell'identificazione scaduta del personale in sede e dei visitatori (quali tessere magnetiche).					5	
9.3 Controllare l'accesso fisico per il personale in sede alle aree sensibili come segue: • l'accesso deve essere autorizzato e basato sulla mansione dell'utente; • l'accesso viene revocato immediatamente al termine del rapporto di lavoro e tutti i meccanismi di accesso fisici, quali chiavi, schede di accesso, ecc., vengono restituiti o disattivati.		2				

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
9.4 Implementare le procedure per identificare e autorizzare i visitatori. Le procedure devono includere quanto segue:						
9.4.1 I visitatori ricevono l'autorizzazione prima di accedere e devono essere sempre scortati nelle aree in cui i dati dei titolari di carta sono elaborati o custoditi.					5	
9.4.2 I visitatori vengono identificati e ricevono una tessera magnetica o altro strumento di identificazione che scade e che consente di distinguere visivamente i visitatori dal personale in sede.					5	
9.4.3 Ai visitatori viene chiesto di restituire la tessera magnetica o altro strumento di identificazione prima di lasciare la struttura o in corrispondenza della data di scadenza.					5	
9.4.4 Il registro dei visitatori viene utilizzato per mantenere un audit trail fisico dell'attività dei visitatori nella struttura nonché nelle aree computer e nei centri dati in cui vengono memorizzati o trasmessi i dati dei titolari di carta. Documentare il nome del visitatore, l'azienda rappresentata e il personale in sede che autorizza l'accesso fisico sul registro. Conservare questo registro per almeno tre mesi, se non diversamente richiesto dalla legge.					5	
9.5 Proteggere fisicamente tutti i supporti.					5	
9.5.1 Conservare i backup dei supporti in un luogo sicuro, preferibilmente in una struttura esterna, come un luogo alternativo o di backup oppure un magazzino. Controllare la sicurezza del luogo almeno una volta all'anno.					5	
9.6 Mantenere un rigido controllo sulla distribuzione interna o esterna di qualsiasi tipo di supporto, incluso quanto segue:						
9.6.1 Classificare i supporti in modo che si possa determinare la sensibilità dei dati.					5	
9.6.2 Inviare i supporti tramite un corriere affidabile o un altro metodo di consegna che possa essere monitorato in modo appropriato.					5	
9.6.3 Accertarsi che il management approvi tutti i supporti che vengono spostati da un'area protetta (in particolare quando i supporti vengono distribuiti a singoli utenti).					5	
9.7 Mantenere un rigido controllo sulla conservazione e sull'accessibilità dei supporti.						
9.7.1 Conservare in modo appropriato i registri di inventario per tutti i supporti ed eseguire tali inventari almeno una volta all'anno.					5	
9.8 Distruggere i supporti quando non sono più necessari per scopi aziendali o legali, come segue:						
9.8.1 Stracciare, bruciare o mandare al macero i materiali cartacei in modo che i dati dei titolari di carta non possano essere ricostruiti. Proteggere i contenitori utilizzati per il materiale da distruggere.	1					
9.8.2 Rendere i dati dei titolari di carta su supporti elettronici non recuperabili, in modo che non sia possibile ricostruirli.	1					
9.9 Proteggere contro manomissioni e sostituzioni i dispositivi che acquisiscono i dati delle carte di pagamento attraverso un'interazione fisica diretta con la carta. *Nota: questi requisiti si applicano ai dispositivi che leggono le carte utilizzati nelle transazioni con carta presente (ossia, tessera magnetica o dip) nel punto vendita. Questo requisito non si applica ai componenti per l'immissione manuale, quali tastiere di computer o tastierini di POS.*						
9.9.1 Conservare un elenco aggiornato di dispositivi. L'elenco deve includere quanto segue: • Marca, modello del dispositivo • Posizione del dispositivo (ad esempio, l'indirizzo della sede o della struttura in cui si trova il dispositivo) • numero di serie del dispositivo o altro metodo di identificazione univoca.		2				

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
9.9.2 Ispezionare periodicamente le superfici del dispositivo per rilevare manomissioni (ad esempio, aggiunta di skimmer di carte ai dispositivi) o sostituzioni (ad esempio, controllando il numero di serie o le caratteristiche del dispositivo per verificare che non sia stato sostituito con un dispositivo fraudolento). *Nota: esempi di indicazioni che un dispositivo potrebbe essere stato alterato o sostituito includono raccordi o cavi innestati nel dispositivo, etichette di sicurezza mancanti o modificate, involucri rotti o di colori diversi o modifiche al numero di serie o altri contrassegni esterni.*		2				
9.9.3 Garantire la formazione del personale che deve essere a conoscenza dei tentativi di alterazione o sostituzione dei dispositivi. La formazione deve comprendere quanto segue: • Verifica dell'identità di eventuali terzi che sostengono di essere addetti alle riparazioni o alla manutenzione, prima di consentire loro l'autorizzazione a modificare o risolvere i problemi dei dispositivi. • Divieto di installare, sostituire o restituire dispositivi in assenza di verifica. • Massima attenzione al comportamento sospetto in prossimità dei dispositivi (ad esempio, tentativi di persone sconosciute di disconnettere o aprire i dispositivi). • Segnalazione di comportamento sospetto e indicazioni di alterazione o sostituzione del dispositivo al personale appropriato (ad esempio, un manager o un addetto alla sicurezza).		2				
9.10 Verificare che i criteri di protezione e le procedure operative per la limitazione dell'accesso fisico ai dati dei titolari di carta siano documentati, in uso e noti a tutte le parti coinvolte.					5	
Requisito 10: Registrare e monitorare tutto l'accesso a risorse di rete e dati dei titolari di carta						
10.1 Implementare audit trail per collegare l'accesso ai componenti di sistema a ogni singolo utente.				4		
10.2 Implementare audit trail automatizzati per tutti i componenti del sistema per ricostruire i seguenti eventi:						
10.2.1 Tutti gli accessi utente ai dati dei titolari di carta				4		
10.2.2 Tutte le azioni intraprese da un utente con privilegi di utente root o amministratore				4		
10.2.3 Accesso a tutti gli audit trail				4		
10.2.4 Tentativi di accesso logico non validi				4		
10.2.5 Uso e modifiche dei meccanismi di identificazione e autenticazione (compresi, a titolo esemplificativo, creazione di nuovi account, incremento dei privilegi) e tutte le modifiche, le aggiunte o le eliminazioni agli account con privilegi root o di amministratore				4		
10.2.6 Inizializzazione, arresto o pausa dei log di audit				4		
10.2.7 Creazione ed eliminazione di oggetti a livello di sistema				4		
10.3 Registrare almeno le seguenti voci di audit trail per tutti i componenti di sistema per ciascun evento:						
10.3.1 Identificazione utente				4		
10.3.2 Tipo di evento				4		
10.3.3 Data e ora				4		
10.3.4 Indicazione di successo o fallimento				4		
10.3.5 Origine dell'evento				4		
10.3.6 Identità o nome dell'elemento interessato (dati, componente di sistema o risorsa).				4		

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
10.4 Utilizzando la tecnologia per la sincronizzazione dell'ora, sincronizzare tutti gli orologi e gli orari critici del sistema ed assicurare che sia implementato quanto segue per l'acquisizione, la distribuzione e la memorizzazione dell'ora. *Nota: NTP (Network Time Protocol) è un esempio di tecnologia per la sincronizzazione dell'ora.*				4		
10.4.1 I sistemi critici hanno l'ora esatta e uniforme.				4		
10.4.2 I dati dell'ora sono protetti.				4		
10.4.3 Le impostazioni dell'ora sono ricevute da sorgenti per l'orario accettate dal settore.				4		
10.5 Proteggere gli audit trail in modo che non possano essere modificati.						
10.5.1 Limitare la visualizzazione degli audit trail a coloro che realmente necessitano di tali informazioni per scopi aziendali.				4		
10.5.2 Proteggere i file di audit trail da modifiche non autorizzate.				4		
10.5.3 Eseguire immediatamente il backup dei file di audit trail su un server di registro centralizzato o un supporto difficile da modificare.				4		
10.5.4 Scrivere registri per tecnologie rivolte al pubblico su un server di registro o un dispositivo per supporti sicuro, centralizzato e interno.				4		
10.5.5 Utilizzare un meccanismo di monitoraggio dell'integrità dei file o un software di rilevamento delle modifiche sui registri per accertarsi che i dati di registro esistenti non possano essere modificati senza generare avvisi (sebbene l'aggiunta di nuovi dati non dovrebbe generare avvisi).				4		
10.6 Esaminare i log e gli eventi di sicurezza per tutti i componenti di sistema al fine di identificare anomalie o attività sospette. *Nota: strumenti di raccolta, analisi e generazione di avvisi per i log possono essere utilizzati ai fini della conformità a questo requisito.*						
10.6.1 Rivedere i seguenti elementi almeno quotidianamente: • 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. • Log 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 reindirizzamento e-commerce).				4		
10.6.2 Rivedere periodicamente i registri di tutti gli altri componenti di sistema in base alle politiche e alla strategia di gestione del rischio dell'azienda, secondo quanto stabilito dalla valutazione annuale dei rischi dell'azienda.				4		
10.6.3 Eseguire il follow-up di eccezioni e anomalie individuate durante il processo di revisione.				4		
10.7 Conservare la cronologia dell'audit trail per almeno un anno, con un minimo di tre mesi di disponibilità immediata per l'analisi (ad esempio, online, archiviazione o recuperabile da backup).				4		

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
10.8 Requisito aggiuntivo solo per provider di servizi: implementare un processo per il rilevamento tempestivo e il reporting di errori dei sistemi di controllo di sicurezza critici, inclusi, senza limitazione, errori di: • Firewall • IDS/IPS • FIM • Antivirus • Controlli dell'accesso fisico • Controlli dell'accesso logico • Meccanismi di log di audit • Controlli di segmentazione (se utilizzati) *Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.*				4		
10.8.1 Requisito aggiuntivo solo per provider di servizi: risolvere gli errori di eventuali controlli di sicurezza critici in maniera tempestiva. I processi di risoluzione degli errori presenti nei controlli di sicurezza devono includere: • ripristino delle funzioni di sicurezza; • identificazione e documentazione della durata (data e ora dell'inizio e della fine) dell'errore della sicurezza; • identificazione e documentazione delle cause dell'errore, inclusa la causa principale, e documentazione delle attività di correzione richieste per identificare ed eliminare la causa principale; • identificazione e risoluzione di eventuali problemi di sicurezza che insorgono durante l'errore; • esecuzione di una valutazione dei rischi per determinare se sono richieste ulteriori azioni come conseguenza dell'errore della sicurezza; • implementazione di controlli per impedire il ripetersi della causa dell'errore; • ripresa del monitoraggio dei controlli di sicurezza. *Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.*				4		
10.9 Verificare che i criteri di protezione e le procedure operative per il monitoraggio di tutto l'accesso alle risorse di rete e ai dati dei titolari di carta siano documentati, in uso e noti a tutte le parti coinvolte.				4		
Requisito 11: Eseguire regolarmente test dei sistemi e processi di sicurezza						
11.1 Implementare i processi per accertare la presenza di punti di accesso wireless (802.11) e rilevare e identificare tutti i punti di accesso wireless autorizzati e non autorizzati almeno a cadenza trimestrale. *Nota: i metodi che si possono utilizzare nel processo comprendono, senza limitazioni, scansioni della rete wireless, controlli di tipo fisico e logico di infrastrutture e componenti di sistema, NAC (Network Access Control) o IDS/IPS wireless. Qualunque sia il metodo adottato, questo deve essere in grado di rilevare e identificare sia i dispositivi autorizzati che quelli non autorizzati.*				4		
11.1.1 Mantenere un inventario dei punti di accesso wireless autorizzati, compresa una giustificazione aziendale documentata.				4		
11.1.2 Implementare le procedure di risposta agli incidenti in caso di rilevamento di punti di accesso wireless non autorizzati.		2				

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
11.2 Eseguire scansioni di vulnerabilità della rete interne ed esterne almeno una volta ogni tre mesi e dopo ogni cambiamento significativo apportato alla rete (ad esempio, l'installazione di nuovi componenti di sistema, la modifica della topologia della rete, la modifica delle regole del firewall, gli aggiornamenti dei prodotti). *Nota: è possibile unire più rapporti delle scansioni per il processo di scansione trimestrale per accertarsi che sia stata eseguita la scansione di tutti i sistemi e siano state risolte tutte le vulnerabilità applicabili. Potrebbe essere necessaria una documentazione ulteriore per verificare che le vulnerabilità non corrette siano in fase di correzione.* *Per la conformità iniziale a PCI DSS, non è necessario che vengano completati quattro scansioni trimestrali positive se il valutatore verifica che 1) il risultato della scansione più recente era positivo, 2) l'entità dispone di politiche e procedure documentate che richiedono l'esecuzione di scansioni trimestrali e 3) le vulnerabilità rilevate nei risultati della scansione sono state corrette nel modo dimostrato da una nuova scansione. Per gli anni successivi alla revisione PCI DSS iniziale, è necessario eseguire quattro scansioni trimestrali con esito positivo.*		2				
11.2.1 Eseguire scansioni delle vulnerabilità interne trimestrali. Identificare le vulnerabilità ed eseguire nuove scansioni per verificare che tutte le vulnerabilità "ad alto rischio" siano risolte in base alla classificazione di vulnerabilità dell'entità (secondo il Requisito 6.1). le scansioni devono essere eseguite da personale qualificato.		2				
11.2.2 Eseguire scansioni esterne della vulnerabilità trimestrali tramite un fornitore di prodotti di scansione approvato (ASV) autorizzato dall'Ente responsabile degli standard di protezione PCI (PCI SSC). Ripetere le scansioni secondo esigenza, fino a che non si ottengono scansioni positive. *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.*		2				
11.2.3 Eseguire scansioni interne ed esterne e ripeterle, se necessario, dopo ogni modifica significativa. le scansioni devono essere eseguite da personale qualificato.		2				
11.3 Implementare una metodologia per il test di penetrazione che preveda 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. • specifichi la conservazione dei risultati dei test di penetrazione e dei risultati delle attività di correzione.		2				
11.3.1 Eseguire test di penetrazione esterna almeno una volta all'anno e dopo ogni aggiornamento o modifica significativa dell'infrastruttura o dell'applicazione (quale un aggiornamento del sistema operativo, l'aggiunta all'ambiente di una subnet o di un server Web).		2				

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
11.3.2 Eseguire test di penetrazione interna almeno una volta all'anno e dopo ogni aggiornamento o modifica significativa dell'infrastruttura o dell'applicazione (quale un aggiornamento del sistema operativo, l'aggiunta all'ambiente di una subnet o di un server Web).		2				
11.3.3 Le vulnerabilità sfruttabili individuate durante il test di penetrazione vengono corrette e il test viene ripetuto per verificare le correzioni.		2				
11.3.4 Se si utilizza la segmentazione per isolare il CDE dalle altre reti, eseguire i test di penetrazione almeno una volta all'anno e dopo eventuali modifiche ai controlli/metodi di segmentazione per verificare che i metodi di segmentazione siano funzionali ed efficaci e isolare tutti i sistemi che non rientrano nell'ambito dai sistemi che rientrano nel CDE.		2				
11.3.4.1 Requisito aggiuntivo solo per provider di servizi: se si utilizza la segmentazione, confermare l'ambito PCI DSS eseguendo test di penetrazione nei controlli di segmentazione almeno ogni sei mesi e dopo eventuali modifiche ai controlli/metodi di segmentazione. *Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.*		2				
11.4 Utilizzare tecniche di rilevamento intrusioni e/o prevenzione delle intrusioni per rilevare e/o prevenire le intrusioni nella rete. Monitorare tutto il traffico in corrispondenza del perimetro dell'ambiente dei dati dei titolari di carta nonché dei punti critici all'interno dell'ambiente stesso e segnalare possibili compromissioni al personale addetto. Mantenere aggiornati tutti i motori, basi e firme di rilevamento e prevenzione delle intrusioni.		2				
11.5 Distribuire un meccanismo di rilevamento della modifiche (ad esempio, gli strumenti di monitoraggio dell'integrità dei file) per segnalare al personale modifiche non autorizzate (incluse modifiche, aggiunte ed eliminazioni) di file system, file di configurazione o file di contenuto critici e per configurare il software in modo che esegua confronti di file critici almeno una volta alla settimana. *Nota: ai fini del meccanismo di rilevamento 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 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).*				4		
11.5.1 Implementare una procedura per rispondere a eventuali avvisi generati dalla soluzione di rilevamento modifiche.				4		
11.6 Garantire che i criteri di protezione e le procedure operative per il monitoraggio e i test della sicurezza siano documentati, in uso e noti a tutte le parti coinvolte.				4		
Requisito 12 - Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale						
12.1 Stabilire, pubblicare, conservare e rendere disponibile una politica di sicurezza.						6
12.1.1 Rivedere la politica di sicurezza almeno una volta all'anno e aggiornarla quando l'ambiente cambia.						6

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
12.2 Implementare un processo di valutazione dei rischi che: • venga eseguito almeno una volta all'anno e in occasione di modifiche significative all'ambiente (ad esempio, acquisizione, fusione, trasferimento, ecc.); • identifichi risorse critiche, minacce e vulnerabilità; • consenta di ottenere una formale analisi dei rischi documentata. Esempi di metodologie per la valutazione dei rischi includono, senza limitazioni, OCTAVE, ISO 27005 e NIST SP 800-30.	1					
12.3 Sviluppare politiche che regolano l'uso per tecnologie critiche e definire l'uso corretto di queste tecnologie. *Nota: esempi di tecnologie critiche comprendono, senza limitazioni, accesso remoto e tecnologie wireless, laptop, tablet, supporti elettronici rimovibili, uso della posta elettronica e di Internet.* Accertarsi che tali politiche richiedano quanto segue:						6
12.3.1 Approvazione esplicita delle parti autorizzate						6
12.3.2 Autenticazione per l'uso della tecnologia						6
12.3.3 Un elenco di tutti i dispositivi di questo tipo e del personale autorizzato all'accesso						6
12.3.4 Un metodo per determinare accuratamente e rapidamente proprietario, informazioni di contatto e scopo (ad esempio, etichettatura, codifica e/o inventariazione dei dispositivi)						6
12.3.5 Usi accettabili della tecnologia						6
12.3.6 Posizioni di rete accettabili per le tecnologie						6
12.3.7 Elenco di prodotti approvati dalla società						6
12.3.8 Disconnessione automatica delle sessioni per tecnologie di accesso remoto dopo un periodo di tempo specifico di inattività						6
12.3.9 Attivazione di tecnologie di accesso remoto per fornitori e partner aziendali solo quando necessario, con disattivazione immediata dopo l'uso						6
12.3.10 Per il personale che accede ai dati dei titolari di carta utilizzando tecnologie di accesso remoto, proibire la copia, lo spostamento o la memorizzazione dei dati dei titolari di carta su dischi rigidi locali e supporti elettronici rimovibili, a meno che ciò non sia stato espressamente autorizzato per un'esigenza aziendale specifica. Laddove è presente un'esigenza aziendale autorizzata, le politiche che regolano l'uso devono richiedere la protezione dei dati in conformità a tutti i requisiti PCI DSS applicabili.						6
12.4 Accertarsi che nelle procedure e nella politica di sicurezza siano definite in modo chiaro le responsabilità in termini di protezione delle informazioni per tutto il personale.						6
12.4.1 Requisito aggiuntivo solo per provider di servizi: ai dirigenti verrà assegnata la responsabilità della protezione dei dati dei titolari di carta e di un programma di conformità PCI DSS per includere: • responsabilità generale del rispetto della conformità PCI DSS; • definizione di un documento di dichiarazione di intenti per un programma di conformità PCI DSS e comunicazione tra di loro. *Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.*						6

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
12.5 Assegnare a un utente singolo o a un team le seguenti responsabilità di gestione della sicurezza delle informazioni:						6
12.5.1 Stabilire, documentare e distribuire le politiche e le procedure di sicurezza.						6
12.5.2 Monitoraggio e analisi degli avvisi e delle informazioni sulla sicurezza e distribuzione al personale appropriato.						6
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.		2				
12.5.4 Amministrare gli account utente, incluse aggiunte, eliminazioni e modifiche.						6
12.5.5 Monitorare e controllare tutti gli accessi ai dati.						6
12.6 Implementare 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.						6
12.6.1 Formare il personale al momento dell'assunzione e almeno una volta all'anno. Nota: i metodi possono essere diversi in funzione del ruolo svolto dal personale e del suo livello di accesso ai dati dei titolari di carta.						6
12.6.2 Richiedere al personale di certificare almeno una volta all'anno di aver letto e compreso la politica e le procedure di sicurezza.						6
12.7 Sottoporre il personale potenziale a screening prima dell'assunzione per ridurre al minimo il rischio di attacchi da fonti interne. Esempi di indagini sulla storia personale sono informazioni su impieghi precedenti, precedenti penali, storico del credito e controlli delle referenze. *Nota: per quel personale potenziale da assumere per determinate posizioni come cassieri di negozi, che hanno accesso a un solo numero di carta alla volta durante una transazione, questo requisito è solo consigliato.*						6
12.8 Gestire e implementare le politiche e le 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.		2				
12.8.1 Conservare un elenco di provider di servizi inclusa una descrizione del servizio fornito.		2				
12.8.2 Conservare 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 oppure memorizzare, elaborare o trasmettere 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.*		2				
12.8.3 Accertarsi che esista un processo definito per incaricare i provider di servizi, che includa tutte le attività di due diligence appropriate prima dell'incarico.		2				
12.8.4 Conservare un programma per monitorare lo stato di conformità allo standard PCI DSS dei provider di servizi con cadenza almeno annuale.		2				
12.8.5 Mantenere le informazioni su quali requisiti PCI DSS vengono gestiti da ogni provider di servizi e quali vengono gestiti dall'entità.		2				

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
12.9 Requisito aggiuntivo solo per provider di servizi: i provider di servizi riconoscono per iscritto nei confronti dei clienti di essere responsabili della protezione dei dati dei titolari di carta di cui entrano in possesso oppure di memorizzare, elaborare o trasmettere 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.*		2				
12.10 Implementare un piano di risposta agli incidenti. Prepararsi a rispondere immediatamente a una violazione del sistema.						
12.10.1 Creare il piano di risposta agli incidenti da attuare in caso di violazione del sistema. Accertarsi che il piano includa almeno i seguenti elementi: • ruoli, responsabilità e strategie di comunicazione e contatto in caso di compromissione, nonché notifiche ai marchi di pagamento; • procedure specifiche di risposta agli incidenti; • procedure di ripristino e continuità delle attività aziendali; • processi di backup dei dati; • analisi dei requisiti legali per la segnalazione delle compromissioni; • copertura e risposte per tutti i componenti di sistema critici; • riferimenti e descrizioni delle procedure di risposta agli incidenti adottate dai marchi di pagamento.		2				
12.10.2 Analizzare e testare il piano, inclusi tutti gli elementi elencati nel Requisito 12.10.1, almeno un volta all'anno.		2				
12.10.3 Nominare personale specifico disponibile 24 ore al giorno, 7 giorni su 7 in caso di emergenza.		2				
12.10.4 Formare in modo appropriato il personale addetto al controllo delle violazioni della sicurezza.		2				
12.10.5 Includere allarmi provenienti dai sistemi di monitoraggio della sicurezza incluso, senza limitazioni, dai firewall di rilevamento e prevenzione delle intrusioni e dai sistemi di monitoraggio dell'integrità dei file.		2				
12.10.6 Sviluppare un processo che consenta di correggere e migliorare il piano di risposta agli incidenti tenendo conto delle lezioni apprese e degli ultimi sviluppi nel settore.		2				
12.11 Requisito aggiuntivo solo per provider di servizi: eseguire analisi almeno una volta all'anno per confermare che il personale sta seguendo i criteri di protezione e le procedure operative. Le analisi devono coprire i seguenti processi: • analisi dei log giornaliere; • analisi dei set di regole dei firewall; • applicazione di standard di configurazione a nuovi sistemi; • risposta ad avvisi di sicurezza; • processi di gestione delle modifiche. *Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; dopo tale data, diventerà un requisito.*						6

Requisiti v3.2 PCI DSS	Pietra miliare					
	1	2	3	4	5	6
12.11.1 Requisito aggiuntivo solo per provider di servizi: conservare la documentazione del processo di analisi trimestrale per includere: • documentazione dei risultati delle analisi; • analisi e approvazione dei risultati da parte del personale a cui è stata assegnata la responsabilità del programma di conformità PCI DSS. *Nota: questo requisito è considerato una delle migliori pratiche fino al 31 gennaio 2018; xdopo tale data, diventerà un requisito.*						6
Appendice A1: Requisiti PCI DSS aggiuntivi per provider di hosting condiviso						
A.1 Proteggere l'ambiente e i dati ospitati di ogni entità (ossia, esercente, provider di servizi o altra entità), nei modi previsti dal punto A.1.1 al punto A.1.4: Il provider di hosting è tenuto a soddisfare questi requisiti, oltre a tutte le altre sezioni rilevanti dello standard PCI DSS. *Nota: anche se un provider di hosting soddisfa tutti questi requisiti, la conformità dell'entità che utilizza tale provider di hosting non è automaticamente garantita. Ogni entità deve soddisfare i requisiti e ottenere la convalida della conformità allo standard PCI DSS, come applicabile.*			3			
A.1.1 Garantire che ogni entità esegua solo processi con accesso esclusivo al proprio ambiente dei dati dei titolari di carta.			3			
A.1.2 Limitare l'accesso e i privilegi di ciascuna entità esclusivamente al relativo ambiente di dati dei titolari di carta.			3			
A.1.3 Accertarsi che le funzioni di audit trail e di generazione dei log siano abilitate e siano univoche per l'ambiente dei dati dei titolari di carta di ciascuna entità e che siano coerenti con il Requisito 10 PCI DSS.			3			
A.1.4 Abilitare processi per fornire tutte le informazioni necessarie per un'indagine legale tempestiva in caso di una compromissione nei confronti di un esercente o un provider di servizi ospitato.			3			
Appendice A2: Requisiti PCI DSS aggiuntivi per entità che utilizzano SSL/TLS iniziale *Nota: questa appendice si applica alle entità che utilizzano SSL/TLS iniziale come controllo di sicurezza per proteggere il CDE e/o CHD.*						
A2.1 Laddove i terminali POI POS (e i punti di terminazione SSL/TLS a cui si connettono) utilizzano SSL e/o TLS iniziale, l'entità deve: • confermare che i dispositivi non sono soggetti a eventuali exploit noti per tali protocolli. O: • disporre di un piano formale di migrazione e di riduzione dei rischi.		2				
A2.2 Le entità con implementazioni esistenti (diverse da quelle consentite in A2.1) che utilizzano SSL e/o TLS iniziale devono avere adottato un piano formale di migrazione e riduzione dei rischi.		2				
A2.3 Requisito aggiuntivo solo per provider di servizi: tutti i provider di servizi devono fornire un'offerta sicura entro il 30 giugno 2016. *Nota: prima del 30 giugno 2016, il provider di servizi deve disporre di un'opzione di protocollo sicuro inclusa nella sua offerta di servizi o di un piano documentato di migrazione e riduzione dei rischi (secondo A2.2) che includa una data di destinazione per la fornitura di un'opzione di protocollo sicuro entro il 30 giugno 2016. Dopo questa data, tutti i provider di servizi devono offrire un'opzione di protocollo sicuro per questo servizio.*		2				