

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

Riepilogo delle modifiche di PCI DSS dalla versione 2.0 alla 3.0

Novembre 2013

Introduzione

Il presente documento contiene un riepilogo delle modifiche apportate da PCI DSS v2.0 a PCI DSS v3.0. La tabella 1 fornisce una panoramica dei tipi di modifiche incluse in PCI DSS v3.0. La tabella 2 fornisce un riepilogo delle modifiche materiali presenti in PCI DSS v3.0.

Tabella 1 - Tipi di modifiche

Tipo di modifica	Definizione
Chiarimento	Maggiori informazioni sullo scopo del requisito. Assicura che la formulazione sintetica nello standard presenti lo scopo desiderato dei requisiti.
Ulteriori istruzioni	Spiegazioni, definizioni e/o istruzioni per favorire la comprensione di o fornire ulteriori informazioni o istruzioni su un determinato argomento.
Requisito in evoluzione	Modifiche per assicurare che gli standard siano aggiornati alle minacce emergenti ed ai cambiamenti del mercato.

Tabella 2 - Riepilogo delle modifiche

Sezione		Modifica	Tipo
PCI DSS v2.0	PCI DSS v3.0		
Informazioni sull'applicabilità dello standard PCI DSS	Informazioni sull'applicabilità dello standard PCI DSS	Chiarito che i dati sensibili di autenticazione non devono essere memorizzati dopo l'autorizzazione, anche se non è presente un numero PAN nell'ambiente.	Chiarimento
Relazione tra PCI DSS e PA-DSS	Relazione tra PCI DSS e PA-DSS	Chiarito che tutte le applicazioni che memorizzano, elaborano o trasmettono i dati dei titolari di carta rientrano nella valutazione PCI DSS di un'entità, anche se conforme allo standard PA-DSS. Chiarita l'applicabilità di PCI DSS ai fornitori di applicazioni di pagamento.	Chiarimento
Ambito della valutazione per la conformità ai requisiti PCI DSS	Ambito dei requisiti PCI DSS	Aggiunti esempi di componenti di sistema; aggiunte istruzioni su come determinare in modo accurato l'ambito della valutazione. Chiarito lo scopo della segmentazione. Chiarite le responsabilità sia di terzi che dei rispettivi clienti in relazione alla definizione dell'ambito e alla copertura dei requisiti PCI DSS; dimostrato anche che le terze parti sono tenute a mettere i propri clienti nella condizione di verificare l'ambito della valutazione PCI DSS delle terze parti stesse.	Ulteriori istruzioni
	Implementazione di PCI DSS nei processi business-as-usual	Nuova sezione per fornire istruzioni "business-as-usual" per l'implementazione della sicurezza nelle attività BAU (business-as-usual) e garantire la costante conformità allo standard PCI DSS. Questa sezione include solo raccomandazioni e istruzioni, non nuovi requisiti PCI DSS.	Ulteriori istruzioni
	Procedure di valutazione	Aggiunta nuova intestazione per separare la sezione sull'ambito dello PCI DSS dalla sezione di campionamento.	Chiarimento
Campionamento di strutture aziendali/componenti di sistema	Per valutatori: campionamento delle strutture aziendali e dei componenti di sistema.	Istruzioni per il campionamento avanzato destinate ai valutatori.	Ulteriori istruzioni
Istruzioni e contenuto per il rapporto sulla conformità	Istruzioni e contenuto per il rapporto sulla conformità	Contenuto precedente trasferito in documenti separati - Modello rapporto sulla conformità a PCI DSS e Istruzioni per il reporting del rapporto sulla conformità a PCI DSS.	Chiarimento
Conformità allo standard PCI DSS - Passaggi per il completamento	Processo di valutazione PCI DSS	Sezione aggiornata per mettere in evidenza il processo di valutazione più che la documentazione.	Chiarimento

Requisiti PCI DSS e procedure di valutazione della sicurezza dettagliate	Requisiti PCI DSS e procedure di valutazione della sicurezza dettagliate	All'inizio di questa sezione, termini aggiunti per definire le intestazioni delle colonne in questa sezione e rimossi i riferimenti alle colonne "Presente", "Non presente" e "Data di destinazione/Commenti".	Chiarimento
--	--	--	-------------

Modifiche generali implementate per tutti i requisiti PCI DSS		Tipo
Nuova colonna per descrivere lo scopo di ogni requisito, con contenuto derivato dal precedente documento di istruzioni Navigazione in PCI DSS. Le istruzioni in questa colonna servono a comprendere i requisiti e non sostituiscono né estendono i requisiti PCI DSS e le procedure di test.		Ulteriori istruzioni
Per le politiche di sicurezza e le procedure operative giornaliere (ex Requisiti 12.1.1 e 12.2), assegnato un nuovo numero di requisito e spostati requisiti e procedure di test in ciascuno dei Requisiti 1-11.		Chiarimento
Termini aggiornati nei requisiti e/o nelle procedure di test corrispondenti per motivi di allineamento e uniformità.		Chiarimento
Sono stati separati requisiti/procedure di test complessi per maggiore chiarezza e sono state rimosse le procedure di test ridondanti o sovrapposte.		Chiarimento
Sono state migliorate le procedure di test per chiarire il livello di convalida previsto per ogni requisito.		Chiarimento
Altre modifiche generali apportate includono: <ul style="list-style-type: none"> sono state rimosse le seguenti colonne: "Presente", "Non presente" e "Data di destinazione/Commenti"; requisiti e procedure di test sono stati rinumerati in base alle modifiche; requisiti e procedure di test sono stati riformattati per migliorarne la leggibilità, ad esempio contenuto di un paragrafo riformattato in elenco puntato, ecc.; sono state portate ovunque modifiche di formulazione minori per migliorare la leggibilità; sono stati corretti i refusi. 		

Requisito		Modifica	Tipo
PCI DSS v2.0	PCI DSS v3.0		
Requisito 1			
1.1.x	1.1.x	Chiarito che gli standard di firewall e router devono essere entrambi documentati e implementati.	Chiarimento
1.1.2	1.1.2 1.1.3	Chiarito che cosa deve includere il diagramma di rete e aggiunto un nuovo Requisito in 1.1.3 per un diagramma attuale che mostri i flussi di dati dei titolari di carta.	Requisito in evoluzione
1.1.5	1.1.6	Chiariti gli esempi di servizi, protocolli e porte non sicuri per specificare SNMP v1 e v2.	Chiarimento
1.2.2	1.2.2	Chiarito che lo scopo di proteggere i file di configurazione del router è tutelarli dall'accesso non autorizzato.	Chiarimento
1.2.3	1.2.3	Chiarito che lo scopo di controllare il traffico tra reti wireless e l'ambiente dei dati dei titolari di carta è consentire solo il traffico autorizzato.	Chiarimento

Requisito		Modifica	Tipo
PCI DSS v2.0	PCI DSS v3.0		
1.3.4	1.3.4	Chiarito che lo scopo del requisito è implementare le misure anti-spoofing per rilevare e bloccare gli indirizzi IP sorgente contraffatti impedendo loro di accedere alla rete.	Chiarimento
1.4	1.4	Termini allineati tra requisito e procedure di test per garantire l'uniformità.	Chiarimento
Requisito 2			
2.1	2.1	Chiarito che il requisito per la modifica delle password predefinite dei fornitori è valido per tutte le password predefinite, compresi sistemi, applicazioni, software di sicurezza, terminali, ecc. e che gli account predefiniti non necessari verranno rimossi o disabilitati.	Chiarimento
2.1.1	2.1.1	Chiarito che lo scopo del requisito è che tutte le impostazioni predefinite wireless dei fornitori vengano modificate al momento dell'installazione.	Chiarimento
2.2	2.2	Chiarito che gli standard di configurazione del sistema comprendono procedure per la modifica di tutte le impostazioni predefinite dei fornitori e gli account predefiniti non necessari.	Chiarimento
2.2.2	2.2.2 2.2.3	Requisito 2.2.2 suddiviso in due requisiti per mettere in evidenza separatamente servizi, protocolli e porte <i>necessari</i> (2.2.2) e servizi, protocolli e porte <i>sicuri</i> (2.2.3).	Chiarimento
	2.4	Nuovo requisito per mantenere un inventario dei componenti di sistema inclusi nell'ambito dello standard PCI DSS per favorire lo sviluppo degli standard di configurazione.	Requisito in evoluzione
Requisito 3			
3.1 3.1.1	3.1	Uniti il Requisito 3.1.1 e le procedure di test nel Requisito 3.1 per chiarire e ridurre la ridondanza.	Chiarimento
3.2	3.2	Chiarito che, se si ricevono dati sensibili di autenticazione dopo il completamento del processo di autorizzazione, i dati dovranno essere resi non recuperabili. Chiarite le procedure di test per le società che supportano servizi di emissione e memorizzano dati sensibili di autenticazione.	Chiarimento
3.3	3.3	Chiarito lo scopo del requisito per il mascheramento dei numeri PAN consolidando la nota precedente nel testo del requisito e potenziando le procedure di test.	Chiarimento

Requisito		Modifica	Tipo
PCI DSS v2.0	PCI DSS v3.0		
3.4.1	3.4.1	Chiarito che l'accesso logico alla cifratura del disco deve essere gestito <i>separatamente</i> e indipendentemente dai meccanismi di controllo dell' <i>autenticazione</i> e dell'accesso del sistema operativo nativo e che le chiavi di decifratura non devono essere <i>associate agli</i> account utente.	Chiarimento
3.5	3.5	Chiarito che le procedure di gestione delle chiavi devono essere sia implementate che documentate.	Chiarimento
3.5.2	3.5.2 3.5.3	Requisito 3.5.2 suddiviso in due requisiti per mettere in evidenza separatamente la memorizzazione delle chiavi di crittografia in una forma sicura (3.5.2) e nel minor numero di posizioni possibile (3.5.3). Il Requisito 3.5.2 fornisce inoltre flessibilità grazie a più opzioni per la memorizzazione sicura delle chiavi di crittografia.	Chiarimento
3.6.x	3.6.x	Aggiunte procedure di test per verificare l'implementazione delle procedure di gestione delle chiavi di crittografia.	Chiarimento
3.6.6	3.6.6	Chiariti i principi di "split knowledge" e controllo duale.	Chiarimento
Requisito 4			
4.1	4.1	Termini allineati tra requisito e procedure di test per garantire l'uniformità. Sono stati inoltre ampliati gli esempi di reti aperte e pubbliche.	Chiarimento
Requisito 5			
Requisito 5 - Generale		Titolo aggiornato per riflettere lo scopo del requisito (ossia <i>proteggere tutti i sistemi contro il malware</i>).	Chiarimento
	5.1.2	Nuovo requisito per valutare le minacce malware in evoluzione per qualsiasi sistema non considerato comunemente colpito dal software dannoso.	Requisito in evoluzione
5.2	5.2	Termini allineati tra requisito e procedure di test per garantire l'uniformità.	Chiarimento
	5.3	Nuovo requisito per garantire che le soluzioni antivirus siano in esecuzione in modo attivo (in precedenza in 5.2) e che non possono essere disabilitate o alterate dagli utenti a meno che non siano stati specificatamente autorizzati dalla direzione per ogni singolo caso.	Requisito in evoluzione
Requisito 6			

Requisito		Modifica	Tipo
PCI DSS v2.0	PCI DSS v3.0		
6.2	6.1	Invertito l'ordine dei requisiti 6.1 e 6.2. Il Requisito 6.1 riguarda ora l'identificazione e la classificazione dei rischi delle nuove vulnerabilità e il 6.2 riguarda l'applicazione di patch alle vulnerabilità critiche. Chiarito come il processo di classificazione dei rischi (6.1) si allinea al processo di applicazione di patch (6.2).	Chiarimento
6.1	6.2	Vedere spiegazione sopra per 6.1. Inoltre, è stato chiarito che questo requisito è valido per le patch "applicabili".	Chiarimento
6.3	6.3	Aggiunta una nota per chiarire che il requisito per i processi di sviluppo software scritti sono validi per tutto il software sviluppato all'interno e il software "su misura".	Chiarimento
6.3.1	6.3.1	"Pre-produzione" modificato in "sviluppo/test" per chiarire lo scopo del requisito.	Chiarimento
6.4	6.4	Procedure di test migliorate per includere le revisioni dei documenti per tutti i requisiti da 6.4.1 a 6.4.4.	Chiarimento
6.4.1	6.4.1	Termini allineati tra requisito e procedura di test per chiarire che la separazione degli ambienti di produzione/sviluppo viene messa in atto con i controlli di accesso.	Chiarimento
6.5	6.5	Aggiornata la formazione degli sviluppatori per includere come evitare le vulnerabilità di codifica comuni e comprendere come i dati sensibili vengono gestiti nella memoria.	Chiarimento
6.5.x	6.5.x	Requisiti aggiornati per riflettere le vulnerabilità di codifica attuali ed emergenti e le linee guida di codifica sicura. Aggiornate le procedure di test per chiarire come le tecniche di codifica affrontano le vulnerabilità.	Chiarimento
	6.5.10	Nuovo requisito per le pratiche di codifica per proteggere contro la violazione dell'autenticazione e la gestione delle sessioni. <i>Valido dal 1° luglio 2015</i>	Requisito in evoluzione
6.6	6.6	Maggiore flessibilità grazie alla specificazione della <i>soluzione tecnica automatica che rileva e previene gli attacchi basati sul Web</i> piuttosto che il "firewall di applicazioni Web". Aggiunta una nota per chiarire che la valutazione non corrisponde alle scansioni delle vulnerabilità richieste al punto 11.2.	Chiarimento
Requisito 7			
7.1	7.1	Procedura di test riformulata per chiarire che cosa include la politica in base alle modifiche ai requisiti da 7.1.1 a 7.1.4.	Chiarimento

Requisito		Modifica	Tipo
PCI DSS v2.0	PCI DSS v3.0		
	7.1.1	Nuovo 7.1.1 per coprire la definizione delle esigenze di accesso per ogni ruolo, per supportare i requisiti da 7.1.2 a 7.1.4.	Chiarimento
7.1.1	7.1.2	Requisito incentrato sulla restrizione degli ID utente privilegiati al numero minimo di privilegi necessari e procedure di test migliorate.	Chiarimento
7.1.2	7.1.3	Requisito incentrato sull'assegnazione dell'accesso in base alla classificazione e alla funzione del ruolo dell'individuo.	Chiarimento
7.1.4		Rimosso il precedente Requisito 7.1.4 (coperto dal Requisito 7.2).	Chiarimento
Requisito 8			
Requisito 8 - Generale		<p>Titolo aggiornato per riflettere lo scopo del requisito (ossia identificare e autenticare ogni accesso ai componenti di sistema).</p> <p>Requisiti aggiornati e riorganizzati per fornire un approccio più olistico all'autenticazione e all'identificazione utente:</p> <ul style="list-style-type: none"> • 8.1 incentrato sull'identificazione utente; • 8.2 incentrato sull'autenticazione utente; • requisiti aggiornati per prendere in considerazione i metodi di autenticazione diversi dalle password; • termine "password" modificato in "password/frasi" dove il requisito si applica solo a password/frasi; • termine "password" modificato in "credenziali di autenticazione" dove il requisito è valido per qualsiasi tipo di credenziale di autenticazione; • chiarito che i requisiti di sicurezza delle password sono validi per gli account utilizzati da fornitori terzi. 	Chiarimento
8.5.6	8.1.5	Chiarito che il requisito per l'accesso remoto del fornitore è valido per i fornitori che accedono, supportano o mantengono i componenti di sistema e che deve essere disabilitato quando non in uso.	Chiarimento
8.4.2	8.2.1	Chiarito che è necessario utilizzare la crittografia avanzata per rendere le credenziali di autenticazione non leggibili durante la trasmissione e la memorizzazione.	Chiarimento
8.5.2	8.2.2	Chiarito che l'identificazione utente deve essere verificata prima di modificare le credenziali di autenticazione; sono state aggiunte la fornitura di nuovi token e la generazione di nuove chiavi come esempi di modifica.	Chiarimento

Requisito		Modifica	Tipo
PCI DSS v2.0	PCI DSS v3.0		
8.5.10 8.5.11	8.2.3	Uniti i requisiti minimi di complessità e solidità delle password in un unico requisito; incrementata la flessibilità per alternative che rispondono a complessità e solidità equivalente.	Requisito in evoluzione
8.3	8.3	Chiarito che il requisito per l'autenticazione a due fattori è valido per utenti, amministratori e tutte le terze parti, compreso l'accesso dei fornitori per supporto o manutenzione.	Chiarimento
8.5.7	8.4	Migliorato il requisito per includere istruzioni di documentazione e comunicazione su come gli utenti devono proteggere le proprie credenziali di autenticazione, compreso il riutilizzo di password/frasi e la modifica di password/frasi in caso di sospetta compromissione.	Chiarimento
	8.5.1	Nuovo requisito per i provider di servizi con accesso remoto alle sedi dei clienti, per utilizzare credenziali di autenticazione univoche per ogni cliente. <i>Valido dal 1° luglio 2015</i>	Requisito in evoluzione
	8.6	Nuovo requisito dove vengono utilizzati altri meccanismi di autenticazione (ad esempio, token fisici o logici, smart card, certificati, ecc.) che chiarisce che i meccanismi devono essere collegati ad account individuali e che si deve assicurare che solo l'utente previsto può accedere a quel meccanismo.	Requisito in evoluzione
8.5.16	8.7	Termini allineati tra requisito e procedure di test per garantire l'uniformità.	Chiarimento
Requisito 9			
9.1.2	9.1.2	Chiarito che lo scopo del requisito è implementare i controlli di accesso fisico e/o logico per proteggere connettori di rete accessibili pubblicamente.	Chiarimento
9.2.x	9.2.x	Chiarito che lo scopo del requisito è identificare, fare una distinzione tra e concedere l'accesso a personale in sede e visitatori e che i badge sono solo un'opzione (e non obbligatori).	Chiarimento
	9.3	Nuovo requisito per controllare l'accesso fisico alle aree sensibili per il personale in sede, incluso un processo per autorizzare l'accesso e revocare l'accesso immediatamente alla risoluzione del rapporto di lavoro.	Requisito in evoluzione
9.3.x	9.4.x	Termini allineati tra il requisito e le procedure di test per garantire l'uniformità e per chiarire che i visitatori devono essere sempre scortati e che l'audit trail per l'attività dei visitatori deve includere sempre l'accesso alla struttura, alla sala computer e/o al centro dati.	Chiarimento

Requisito		Modifica	Tipo
PCI DSS v2.0	PCI DSS v3.0		
9.5-9.10	9.5-9.8	<p>Precedente Requisito 9.6 spostato e rinumerato in 9.5 e precedente Requisito 9.5 rinumerato come Requisito secondario 9.5.1.</p> <p>Precedente Requisito 9.7 rinumerato in 9.6 e precedente Requisito 9.8 rinumerato come Requisito secondario 9.6.3.</p> <p>Precedente Requisito 9.9 rinumerato in 9.7 e precedente Requisito 9.10 rinumerato come Requisito secondario 9.8.</p>	Chiarimento
	9.9.x	<p>Nuovi requisiti per proteggere contro manomissioni e sostituzioni i dispositivi che acquisiscono i dati della carta di pagamento attraverso un'interazione fisica con la carta.</p> <p><i>Valido dal 1° luglio 2015</i></p>	Requisito in evoluzione
Requisito 10			
10.1	10.1	Chiarito che gli audit trail devono essere implementati per collegare l'accesso ai componenti di sistema a ogni singolo utente, più che stabilire un processo.	Chiarimento
10.2.1	10.2.1	Chiarito che lo scopo è includere l'accesso di ogni singolo <i>utente</i> ai dati dei titolari di carta negli audit trail.	Chiarimento
10.2.5	10.2.5	Requisito migliorato per includere le modifiche ai meccanismi di identificazione e autenticazione (tra cui creazione di nuovi account e aumento dei privilegi) e tutte le modifiche, aggiunte ed eliminazioni relative agli account con accesso root o amministrativo.	Requisito in evoluzione
10.2.6	10.2.6	Requisito migliorato per includere l'arresto o la sospensione dei log di audit.	Requisito in evoluzione
10.6	10.6.x	Chiarito che lo scopo delle revisioni di log è identificare le anomalie o l'attività sospetta e fornire maggiori istruzioni sull'ambito delle revisioni di log giornaliere. Consentita inoltre maggiore flessibilità per la revisione degli eventi di sicurezza e i log di sistema critici a cadenza giornaliera e altri eventi log a cadenza periodica, come definito nella strategia di gestione dei rischi dell'entità.	Chiarimento
Requisito 11			
11.1.x	11.1.x	Requisito migliorato per includere un inventario dei punti di accesso wireless autorizzati e una giustificazione aziendale (11.1.1) per supportare la scansione di dispositivi wireless non autorizzati; aggiunto nuovo Requisito 11.1.2 per allinearsi a una procedura di test già esistente, per le procedure di risposta agli incidenti se vengono rilevati i punti di accesso wireless non autorizzati.	Requisito in evoluzione

Requisito		Modifica	Tipo
PCI DSS v2.0	PCI DSS v3.0		
11.2	11.2	Aggiunte istruzioni sulla combinazione di più rapporti delle scansioni al fine di ottenere e documentare un risultato positivo.	Ulteriori istruzioni
11.2.1	11.2.1	Chiarito che le scansioni delle vulnerabilità includono le scansioni ulteriori necessarie per risolvere tutte le vulnerabilità “alte” (come identificato dal Requisito 6.1 di PCI DSS) e che tali operazioni devono essere eseguite da personale qualificato.	Chiarimento
11.2.2	11.2.2	Chiarito che le scansioni di vulnerabilità esterne comprendono le scansioni ulteriori necessarie fino a che non si ottengono scansioni positive; aggiunta una nota con riferimento alla Guida del programma ASV.	Chiarimento
11.2.3	11.2.3	Chiarito che le scansioni interne ed esterne eseguite dopo modifiche significative includono le scansioni ulteriori necessarie per risolvere tutte le vulnerabilità “alte” (come identificato dal Requisito 6.1 di PCI DSS) e che tali operazioni devono essere eseguite da personale qualificato.	Chiarimento
	11.3	Nuovo requisito per implementare una metodologia per il test di penetrazione. <i>Valido dal 1° luglio 2015 Sarà necessario attenersi ai requisiti di PCI DSS v2.0 per il test di penetrazione fino a che non entra in vigore PCI DSS v3.0.</i>	Requisito in evoluzione
11.3	11.3.1 11.3.2	Ex Requisito 11.3 suddiviso in 11.3.1 per i requisiti del test di penetrazione <i>esterni</i> e in 11.3.2 per i requisiti del test di penetrazione <i>interni</i> .	Chiarimento
11.3	11.3.3	Nuovo requisito creato dalla procedura di test precedente (11.3.b) per correggere le vulnerabilità sfruttabili individuate durante il test di penetrazione e per ripetere il test al fine di verificare le correzioni.	Chiarimento
	11.3.4	Nuovo requisito, se si utilizza la segmentazione per isolare l'ambiente dei dati dei titolari di carta da altre reti, per eseguire il test di penetrazione per verificare che i metodi di segmentazione siano funzionali ed efficaci.	Requisito in evoluzione
11.4	11.4	Flessibilità incrementata specificando <i>le tecniche di rilevamento intrusioni e/o prevenzione delle intrusioni per rilevare e/o prevenire le intrusioni nella rete</i> più che “i sistemi di rilevamento intrusioni e/o i sistemi di prevenzione intrusioni”.	Chiarimento
11.5	11.5	Flessibilità incrementata specificando il <i>meccanismo di rilevamento dei cambiamenti</i> più che il “monitoraggio dell'integrità file”.	Chiarimento

Requisito		Modifica	Tipo
PCI DSS v2.0	PCI DSS v3.0		
	11.5.1	Nuovo requisito per implementare una procedura per rispondere a eventuali avvisi generati dal meccanismo di rilevamento modifiche (supporta 11.5).	Requisito in evoluzione
Requisito 12			
12.1.1 12.2	1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6	Uniti gli ex requisiti al punto 12.1.1 (per la politica di sicurezza delle informazioni per rispondere a tutti i requisiti PCI DSS) e al punto 12.2 (per le procedure di sicurezza operativa); spostati nei requisiti da 1 a 11, come requisito singolo in ciascuno.	Chiarimento
12.1.3	12.1.1	Spostato ex Requisito 12.1.3 in 12.1.1.	Chiarimento
12.1.2	12.2	Spostato ex Requisito 12.1.2 per un processo di valutazione dei rischi annuale in 12.2; chiarito che la valutazione dei rischi deve essere eseguita almeno una volta all'anno e <i>dopo modifiche significative all'ambiente</i> .	Requisito in evoluzione
12.3.4	12.3.4	Chiarito che l'etichettatura è solo un esempio di metodo da utilizzare.	Chiarimento
12.3.8	12.3.8	Nuova procedura di test per verificare che la politica sia implementata per la disconnessione delle sessioni di accesso remoto dopo un periodo specifico di inattività.	Chiarimento
12.3.10	12.3.10	Termini allineati tra il requisito e le procedure di test per chiarire che, dove è presente un'esigenza aziendale autorizzata che richiede al personale di accedere ai dati dei titolari di carta mediante tecnologie di accesso remoto, i dati devono essere protetti in conformità a tutti i requisiti PCI DSS applicabili.	Chiarimento
12.8	12.8	Chiarito lo scopo di implementare e gestire 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.	Chiarimento
12.8.2	12.8.2	Chiarite le responsabilità applicabili per accordo/conferma scritti del provider di servizi.	Chiarimento
	12.8.5	Nuovo requisito per mantenere le informazioni su quali requisiti PCI DSS vengono gestiti da ogni provider di servizi e quali vengono gestiti dall'entità.	Requisito in evoluzione
	12.9	Nuovo requisito per i provider di servizi per fornire accordo/conferma scritti ai loro clienti come specificato al Requisito 12.8. <i>Valido dal 1° luglio 2015</i>	Requisito in evoluzione

Requisito		Modifica	Tipo
PCI DSS v2.0	PCI DSS v3.0		
12.9.x	12.10.x	Requisito rinumerato e aggiornato 12.10.5 per chiarire che lo scopo è includere gli avvisi provenienti dai <i>sistemi di monitoraggio della sicurezza</i> nel piano di risposta agli incidenti.	Chiarimento