

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

**Riepilogo delle modifiche di
PCI DSS dalla versione 3.1 alla 3.2**

Aprile 2016

Introduzione

Il presente documento contiene un riepilogo delle modifiche apportate da PCI DSS v3.1 a PCI DSS v3.2. La Tabella 1 fornisce una panoramica dei tipi di modifiche. La Tabella 2 fornisce un riepilogo delle modifiche effettive rilevate in PCI DSS v3.2.

Tabella 1 - Tipi di modifiche

¹ 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 ¹
PCI DSS v3.1	PCI DSS v3.2		
Tutte	Tutte	Corretti errori tipografici minori (grammatica, punteggiatura, formattazione, ecc.) e integrati aggiornamenti minimi per una migliore leggibilità del documento.	Chiarimento
Relazione tra PCI DSS e PA-DSS	Relazione tra PCI DSS e PA-DSS	Aggiunta l'indicazione che le minacce alla sicurezza sono in costante evoluzione e che le applicazioni di pagamento non supportate dal fornitore potrebbero non offrire lo stesso livello di sicurezza della versione supportata.	Ulteriori istruzioni
Ambito dei requisiti PCI DSS	Ambito dei requisiti PCI DSS	Chiarito che devono essere presi in considerazione i siti di backup/ripristino quando si conferma l'ambito PCI DSS.	Chiarimento
Migliori pratiche per implementare lo standard PCI DSS nei processi business-as-usual	Migliori pratiche per implementare lo standard PCI DSS nei processi business-as-usual	Aggiornata nota per chiarire che alcuni principi business-as-usual potrebbero essere requisiti per alcune entità, come quelle definite in Convalida aggiuntiva delle entità designate (Appendice A3).	Chiarimento
	Versioni PCI DSS	Nuova sezione per descrivere come questa versione di PCI DSS influisce sulla versione precedente.	Ulteriori istruzioni
Requisiti			
Aspetti generali	Aspetti generali	Eliminati gli esempi di protocolli "avanzati" o "sicuri" da numerosi requisiti, poiché questi possono cambiare in qualsiasi momento.	Chiarimento
Aspetti generali	Aspetti generali	Spostati gli esempi da numerosi requisiti e/o procedure di test nella colonna Istruzioni e aggiunte istruzioni laddove appropriato.	Chiarimento
Aspetti generali	Aspetti generali	Modificata l'espressione "password/frasi" in "password/passphrase" in numerosi requisiti per coerenza.	Chiarimento
Aspetti generali	Aspetti generali	Chiarito che il termine corretto è autenticazione a più fattori, anziché autenticazione a due fattori, poiché possono essere utilizzati due o più fattori.	Chiarimento
Aspetti generali	Aspetti generali	Eliminate le note dai requisiti che fanno riferimento alla data di validità 1 luglio 2015, poiché questi sono validi adesso. I requisiti interessati sono 6.5.10, 8.5.1, 9.9, 11.3 e 12.9.	Chiarimento

Sezione		Modifica	Tipo ¹
PCI DSS v3.1	PCI DSS v3.2		
1.1.6	1.1.6	Chiarito che l'approvazione dell'uso aziendale è inclusa nella giustificazione. Eliminati gli esempi di protocolli "insicuri" poiché questi possono cambiare in base agli standard del settore.	Chiarimento
1.2.1	1.2.1	Aggiunte istruzioni per chiarire lo scopo del requisito.	Chiarimento
1.3	1.3	Aggiunte istruzioni per chiarire lo scopo del requisito.	Chiarimento
1.3.3		Rimosso il requisito poiché lo scopo viene soddisfatto tramite altri requisiti in 1.2 e 1.3.	Chiarimento
1.3.4-1.3.8	1.3.3-1.3.7	Rinumerati a causa dell'eliminazione del precedente Requisito 1.3.3.	Chiarimento
1.3.6	1.3.5	Aggiornato per chiarire lo scopo del requisito anziché l'uso di un determinato tipo di tecnologia.	Chiarimento
1.4	1.4	Maggiore flessibilità includendo <i>o funzionalità equivalente</i> come alternativa al firewall personale. Chiarito che il requisito si applica a tutti dispositivi mobili che si connettono a Internet se all'esterno della rete e che accedono anche al CDE.	Chiarimento
2.1	2.1	Chiarito che il requisito si applica alle applicazioni di pagamento.	Chiarimento
2.2.3	2.2.3	Eliminate la nota e le procedure di test relative alla rimozione di SSL/TLS iniziale e spostate nella nuova Appendice A2.	Chiarimento
2.3	2.3	Eliminate la nota e le procedure di test relative alla rimozione di SSL/TLS iniziale e spostate nella nuova Appendice A2. Eliminato il riferimento a "gestione basata su Web" poiché il requisito già specifica "tutto l'accesso amministrativo non da console", che per definizione include qualsiasi accesso basato sul Web.	Chiarimento
3.3	3.3	Aggiornato il requisito per chiarire che eventuali visualizzazioni del PAN per più di sei cifre all'inizio/quattro cifre alla fine richiede un'esigenza aziendale legittima. Aggiunte istruzioni su comuni scenari di mascheratura.	Requisito in evoluzione

Sezione		Modifica	Tipo ¹
PCI DSS v3.1	PCI DSS v3.2		
3.4.d	3.4.d	Aggiornata la procedura di test per chiarire che l'esame di log di audit include i log delle applicazioni di pagamento.	Chiarimento
3.4.1	3.4.1	Aggiunta la nota al requisito per chiarire che il requisito si applica in aggiunta a tutti gli altri requisiti di gestione delle chiavi e di cifratura PCI DSS.	Chiarimento
	3.5.1	Nuovo requisito per i provider di servizi per conservare una descrizione documentata dell'architettura crittografica. <i>Data di validità 1 febbraio 2018</i>	Requisito in evoluzione
3.5.1-3.5.3	3.5.2 – 3.5.4	Rinumerati a causa dell'aggiunta del nuovo Requisito 3.5.1.	Chiarimento
3.6.1.b	3.6.1.b	Aggiornata la sezione della procedura di test per chiarire che il test implica l'osservazione di procedure anziché il metodo stesso di generazione di chiavi, poiché questo non dovrebbe essere osservabile. Aggiunte le istruzioni relative alla definizione del Glossario di "Generazione di chiavi di crittografia".	Chiarimento
4.1	4.1	Eliminate la nota e le procedure di test relative alla rimozione di SSL/TLS iniziale e spostate nella nuova Appendice A2.	Chiarimento
6.2	6.2	Aggiunto il chiarimento alla colonna Istruzioni che il requisito per l'installazione di patch per tutto il software include le applicazione di pagamento.	Chiarimento
6.4.4	6.4.4	Aggiornato requisito per allinearli alla procedura di test.	Chiarimento
6.4.5	6.4.5	Chiarito che i processi di controllo delle modifiche non sono limitati alle patch e alle modifiche al software.	Chiarimento
	6.4.6	Nuovo requisito per i processi di controllo delle modifiche per includere la verifica dei requisiti PCI DSS interessati da una modifica. <i>Data di validità 1 febbraio 2018</i>	Requisito in evoluzione
6.5	6.5	Chiarito che la formazione per gli sviluppatori deve essere aggiornata e svolgersi almeno annualmente.	Chiarimento
6.5.a-6.5.d	6.5.a-6.5.c	Eliminata la procedura di test 6.5.b e rinumerate le procedure di test restanti di conseguenza.	Chiarimento

Sezione		Modifica	Tipo ¹
PCI DSS v3.1	PCI DSS v3.2		
7.2	7.2	Aggiornati il requisito, le procedure di test e la colonna Istruzioni per chiarire che possono essere utilizzati uno o più sistemi di controllo dell'accesso.	Chiarimento
Requisito 8	Requisito 8	Aggiunta nota al Requisito 8 che indica che i requisiti di autenticazione non si applicano agli account utilizzati dai consumatori (ad es. titolari di carta).	Chiarimento
8.1.5	8.1.5	Chiarito che il requisito è destinato a tutti i terzi con accesso remoto, anziché solo ai fornitori.	Chiarimento
8.2.3	8.2.3	Aggiornata la colonna Istruzioni per tenere conto delle modifiche agli standard di settore.	Chiarimento
8.3	8.3	Chiarito che il termine corretto è autenticazione a più fattori, anziché autenticazione a due fattori, poiché possono essere utilizzati due o più fattori.	Chiarimento
8.3	8.3, 8.3.1, 8.3.2	<p>Ampliato il Requisito 8.3 in sottorequisiti, per richiedere l'autenticazione a più fattori per tutto il personale con accesso amministrativo non da console e per tutto il personale con accesso remoto al CDE.</p> <p>Il nuovo Requisito 8.3.2 riguarda l'autenticazione a più fattori per tutto il personale con accesso remoto al CDE (incorpora il precedente Requisito 8.3).</p> <p>Il nuovo Requisito 8.3.1 riguarda l'autenticazione a più fattori per tutto il personale con accesso amministrativo non da console al CDE.</p> <p><i>Requisito 8.3.1 valido dal 1 febbraio 2018</i></p>	Requisito in evoluzione
9.1.1	9.1.1	Chiarito che possono essere utilizzati sia videocamere che meccanismi di controllo dell'accesso.	Chiarimento
9.5.1.a-9.5.1.b	9.5.1	Unite le procedure di test per chiarire che il valutatore verifica che la posizione di memorizzazione venga analizzata almeno annualmente.	Chiarimento
	10.8, 10.8.1	<p>Nuovo requisito per i provider di servizi per rilevare e segnalare eventuali errori dei sistemi di controllo della sicurezza critici.</p> <p><i>Data di validità 1 febbraio 2018</i></p>	Requisito in evoluzione
10.8	10.9	Rinumerato a causa dell'aggiunta del nuovo Requisito 10.8.	Chiarimento

Sezione		Modifica	Tipo ¹
PCI DSS v3.1	PCI DSS v3.2		
11.2.1	11.2.1	Chiarito che le vulnerabilità ad “Elevate” devono essere risolte in base alla classificazione di vulnerabilità dell’entità (come definito nel Requisito 6.1) e verificate mediante scansioni ripetute.	Chiarimento
11.3.4	11.3.4	Aggiunta la procedura di test 11.3.4.c per verificare che il test di penetrazione venga eseguito da una risorsa interna o da una terza parte qualificata.	Chiarimento
	11.3.4.1	Nuovo requisito per i provider di servizi per eseguire test di penetrazione nei controlli di segmentazione almeno ogni sei mesi. <i>Data di validità 1 febbraio 2018</i>	Requisito in evoluzione
11.5.a	11.5.a	Rimossa l’espressione “all’interno dell’ambiente dei dati dei titolari di carta” dalla procedura di test per coerenza con il requisito, poiché il requisito può applicarsi a sistemi critici collocati all’esterno del CDE designato.	Chiarimento
12.3.3	12.3.3	Riformattata la procedura di test per maggiore chiarezza.	Chiarimento
	12.4	Nuovo requisito per i dirigenti dei provider di servizi per stabilire responsabilità per la protezione dei Dati dei titolari di carta e per il programma di conformità PCI DSS. <i>Data di validità 1 febbraio 2018</i>	Requisito in evoluzione
12.4	12.4.1	Rinumerato a causa dell’aggiunta del nuovo Requisito 12.4.	Chiarimento
12.6	12.6	Chiarito che lo scopo del programma di consapevolezza della sicurezza è accertarsi che il personale sia consapevole delle procedure e dei criteri di protezione dei dati dei titolari di carta.	Chiarimento
12.8.1	12.8.1	Chiarito che l’elenco di provider di servizi include una descrizione del servizio fornito.	Chiarimento
12.8.2	12.8.2	Aggiunte istruzioni che la responsabilità dei provider di servizi dipenderà dal servizio specifico fornito e dal contratto tra le due parti.	Ulteriori istruzioni
12.10.2	12.10.2	Chiarito che l’analisi del piano di risposta agli incidenti comprende tutti gli elementi elencati nel Requisito 12.10.1.	Chiarimento

Sezione		Modifica	Tipo ¹
PCI DSS v3.1	PCI DSS v3.2		
	12.11, 12.11.1	Nuovo requisito per i provider di servizi per eseguire analisi almeno ogni tre mesi e per verificare che il personale stia seguendo i criteri di protezione e le procedure operative. <i>Data di validità 1 febbraio 2018</i>	Requisito in evoluzione
Appendice A	Appendice A1	Rinumerata l'Appendice " <i>Requisiti PCI DSS aggiuntivi per provider di hosting condiviso</i> " per includere nuove appendici.	Chiarimento
	Appendice A2	Nuova Appendice con requisiti aggiuntivi per entità che utilizzano SSL/TLS iniziale, che incorpora nuove scadenze di migrazione per la rimozione di SSL/TLS iniziale.	Chiarimento
	Appendice A3	Nuova Appendice per incorporare la sezione "Convalida aggiuntiva delle entità designate" (DESV), che era in precedenza un documento separato.	Chiarimento