



# Lo Standard PCI DSS

L'ambito di applicazione, i requisiti,  
le esigenze di mercato



Ing. Vittorio Torre  
ISO 27001 LA, CISA, CISSP  
Nexsoft S.p.A.



# INDICE DELLA PRESENTAZIONE :

1. Overview e ambito di applicazione
2. La struttura dello standard
3. I requisiti in dettaglio
4. Le esigenze di mercato
5. Riferimenti bibliografici e sitografici



## Il PCI Council

Il PCI Security Standards Council è l'organo internazionale per lo sviluppo, il miglioramento, la memorizzazione, la diffusione e l'implementazione degli standard di sicurezza per la protezione dei dati afferenti una carta di credito/debito.

La missione del PCI Security Standards Council è di migliorare la sicurezza dei dati di pagamento guidando l'educazione e la consapevolezza (awareness) degli standard da esso emessi.





## **Gli standard PCI**

Gli standard PCI racchiudono i requisiti di sicurezza rivolti alle istituzioni e aziende che archiviano, elaborano e/o trasmettono dati relativi a carte di credito o debito dei card brand costituenti lo stesso PCI.

Tali requisiti sono suddivisi principalmente in:

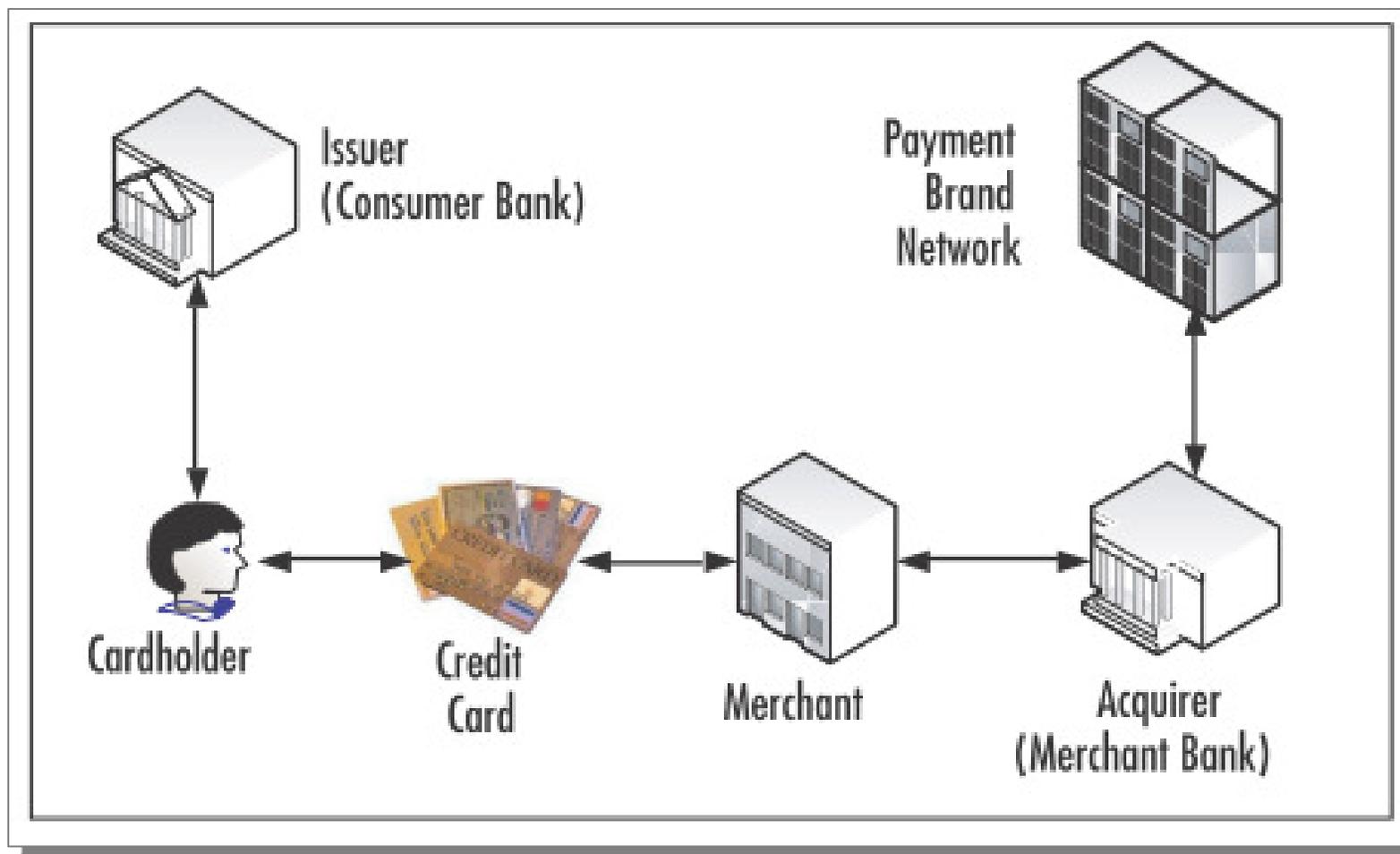
- PCI Data Security Standard (PCI DSS)
- PCI Personal Identification Number (PCI PIN)
- PCI PIN Entry Devices (PCI PED)
- Payment Application DSS (PA-DSS)

### **PCI Data Security Standard**

Lo standard PCI DSS rappresenta una comune serie di prassi di *due diligence* di sicurezza che aiuta a garantire la gestione sicura dei dati relativi a carte di pagamento. Esso include requisiti per la gestione della sicurezza, le policy, le procedure.

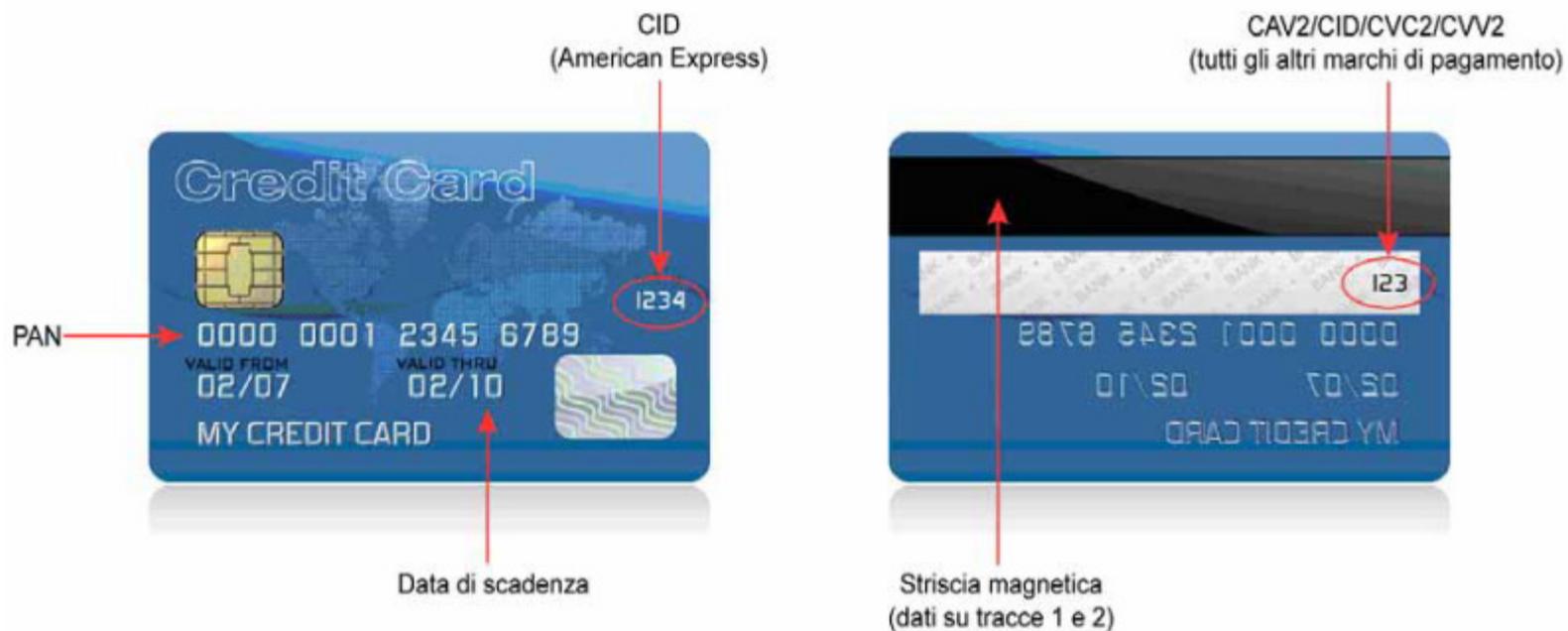


## Lo schema generale di pagamento





## La struttura della carta di credito

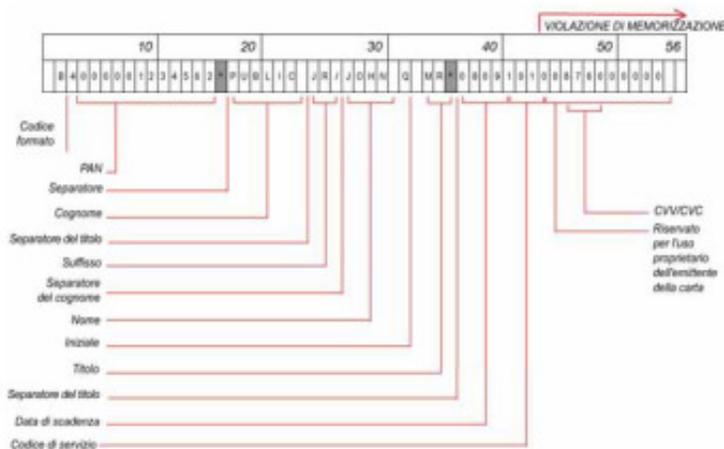




## La struttura della carta di credito

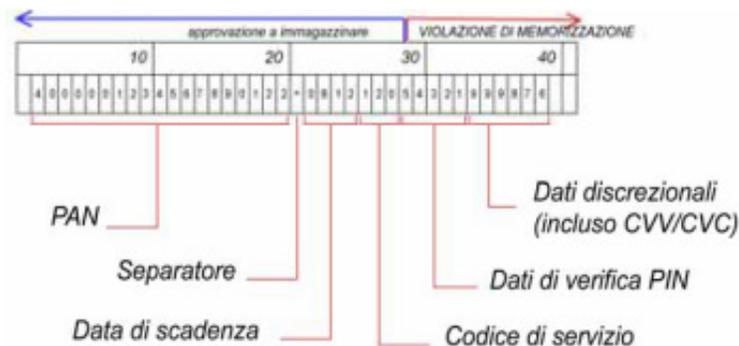
### Traccia 1

- Contiene tutti i campi delle tracce 1 e 2
- Lunghezza massima di 79 caratteri



### Traccia 2

- Tempo di elaborazione inferiore per le vecchie trasmissioni su connessione remota
- Lunghezza massima di 40 caratteri





## L'applicabilità del PCI DSS

	Elemento di dati	Memorizzazione consentita	Protezione richiesta
Dati di titolari di carta	PAN	Si	Si
	Nome titolare di carta <sup>1</sup>	Si	Si <sup>1</sup>
	Codice di servizio <sup>1</sup>	Si	Si <sup>1</sup>
	Data di scadenza <sup>1</sup>	Si	Si <sup>1</sup>
Dati sensibili di autenticazione <sup>2</sup>	Dati completi della striscia magnetica <sup>3</sup>	No	N/A
	CAV2/CVC2/CVV2/CID	No	N/A
	PIN/Blocco PIN	No	N/A

Il PAN (Primary Account Number) è il fattore determinante nell'applicabilità dei requisiti PCI DSS (e degli standard PA-DSS).

**Se il PAN non viene memorizzato, elaborato o trasmesso, lo standard PCI DSS (e PA-DSS) non è applicabile.**



## L'applicabilità del PCI DSS

I requisiti di PCI DSS devono essere applicati a tutti i componenti di sistema inclusi nell'ambiente dei dati di titolari dei carta o collegati ad esso.

### **Componenti di rete**

Firewall  
Switch  
Router  
Punti di accesso wireless  
Dispositivi di rete  
Altri dispositivi di sicurezza

### **Server**

Web  
Database  
Autenticazione  
e-mail  
Proxy  
NTP (Network Time Protocol)  
DNS (Domain Name Server)

### **Applicazioni**

Tutte le applicazioni acquistate e personalizzate,  
comprese applicazioni interne ed esterne (Internet).

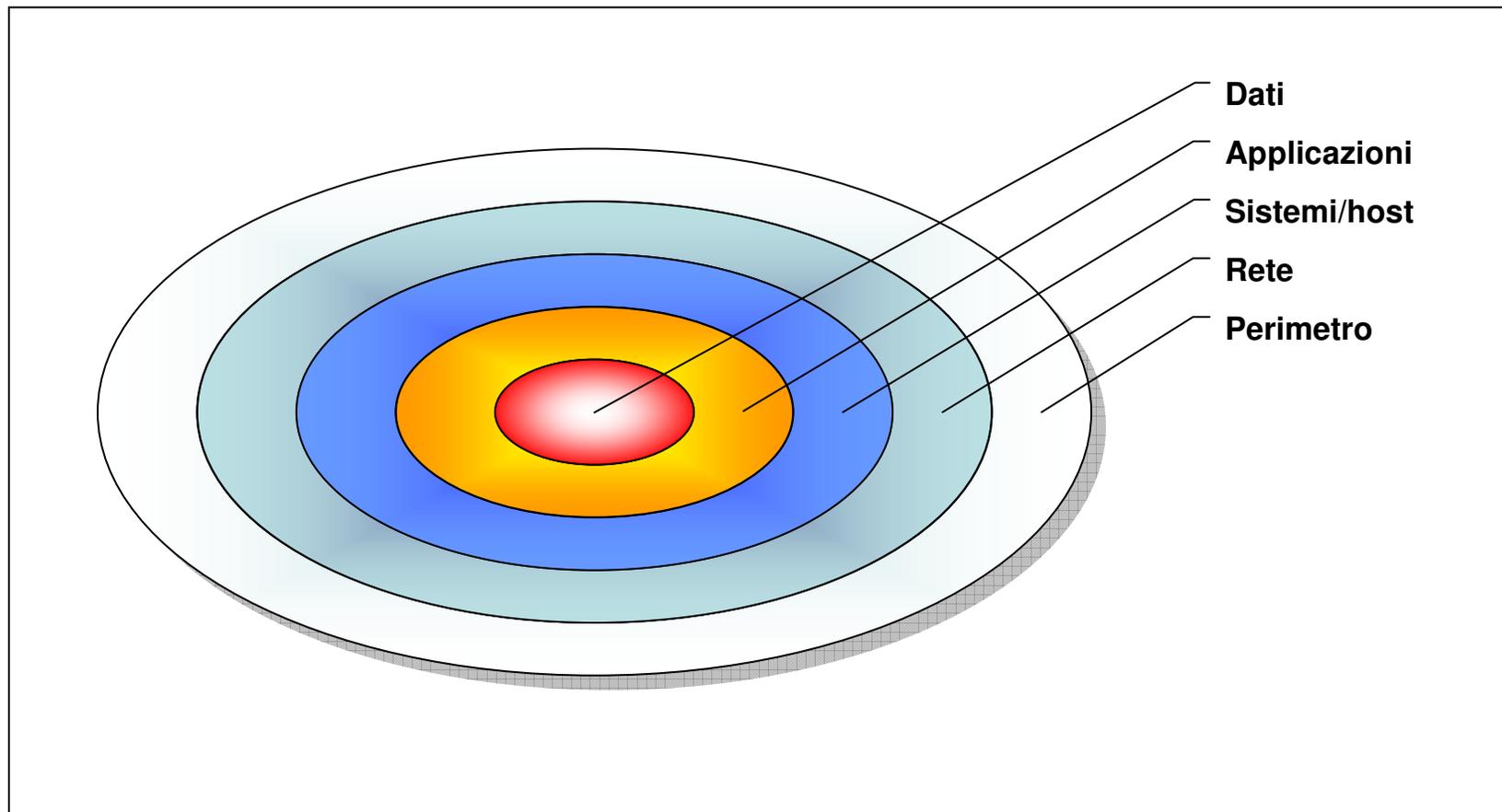


## **INDICE DELLA PRESENTAZIONE :**

1. Overview e ambito di applicazione
2. **La struttura dello standard**
3. I requisiti in dettaglio
4. Le esigenze di mercato
5. Riferimenti bibliografici e sitografici



## L'approccio dello standard: la "layered security"





## La struttura dello standard

### **Sviluppo e gestione di una rete sicura**

- **Requisito 1:** Installare e gestire una configurazione firewall per proteggere i dati di titolari di carta
- **Requisito 2:** Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione

### **Protezione dei dati di titolari di carta**

- **Requisito 3:** Proteggere i dati di titolari di carta memorizzati
- **Requisito 4:** Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche

### **Manutenzione di un programma per la gestione delle vulnerabilità**

- **Requisito 5:** Utilizzare e aggiornare regolarmente il software antivirus
- **Requisito 6:** Sviluppare e gestire sistemi e applicazioni protette

### **Implementazione di rigide misure di controllo dell'accesso**

- **Requisito 7:** Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario
- **Requisito 8:** Assegnare un ID univoco a chiunque abbia accesso a un computer
- **Requisito 9:** Limitare l'accesso fisico ai dati di titolari di carta

### **Monitoraggio e test delle reti regolari**

- **Requisito 10:** Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta
- **Requisito 11:** Eseguire regolarmente test di sistemi e processi di protezione

### **Gestione di una politica di sicurezza delle informazioni**

- **Requisito 12:** Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori



## **INDICE DELLA PRESENTAZIONE :**

1. Overview e ambito di applicazione
2. La struttura dello standard
3. **I requisiti in dettaglio**
4. Le esigenze di mercato
5. Riferimenti bibliografici e sitografici



## COSTRUIRE E MANTENERE UNA RETE SICURA



## Costruire e mantenere una rete sicura

### I Firewall - Principali tipologie

- PACKET FILTERING

Pros	Cons
Low cost	Rules are sometimes hard to configure
Fast and efficient	Router performance affected
Technology is widely available	Bugs and vulnerabilities are more prone in this technology

- PROXIES

Pros	Cons
"Intelligent" filtering	May require modification of servers/clients
Includes user-level authentication	Much slower than packet filtering
Normally provides good logging	Extensive configurations and management

- STATEFUL INSPECTION

Pros	Cons
Fast	Expensive
Transparent to the user	Complex configurations
Multiple inspection points at different layers of the OSI	UDP is stateless and requires additional configurations



## Costruire e mantenere una rete sicura

### I Firewall - Le architetture

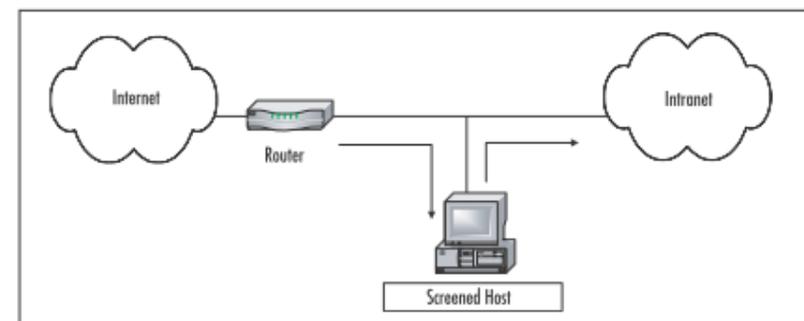
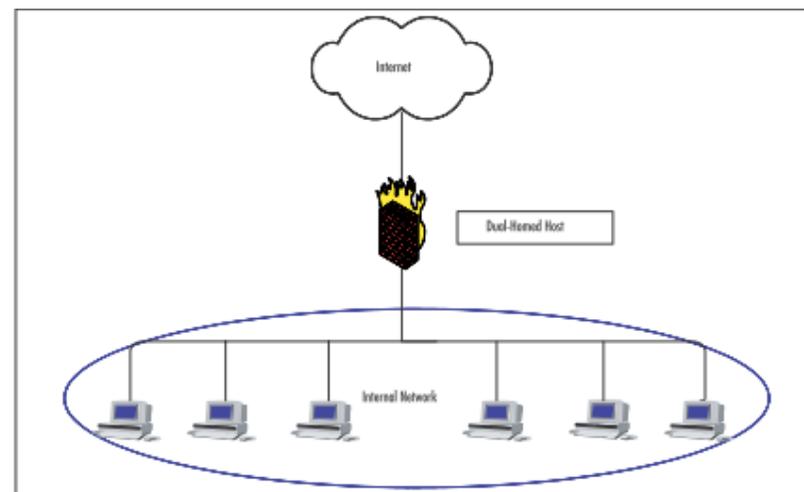
#### Dual-homed host (Bastion host)

Una singola macchina connessa a due reti e funzionante da gateway.

**Ogni tipo di traffico deve essere analizzato e richiede specifica configurazione del firewall (ad esempio come proxy).**

#### Screened host

Il router filtra il traffico non voluto; lo screened host aggiunge sicurezza ispezionando tutto il traffico e permettendo o negando il traffico in base alle definite policy di sicurezza.



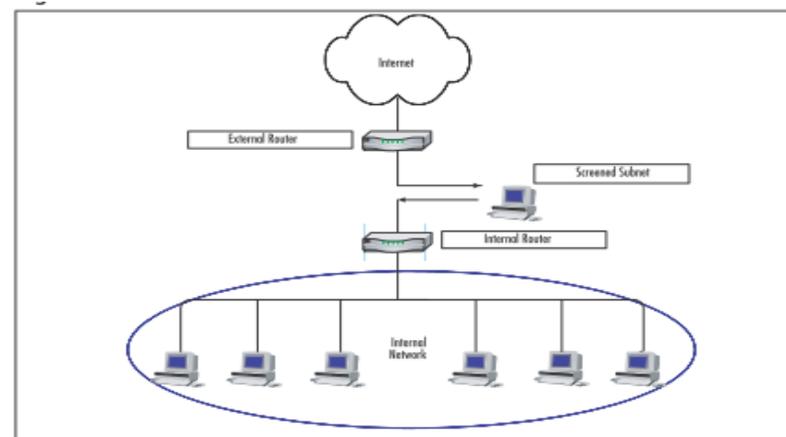


## Costruire e mantenere una rete sicura

### I Firewall - Le architetture

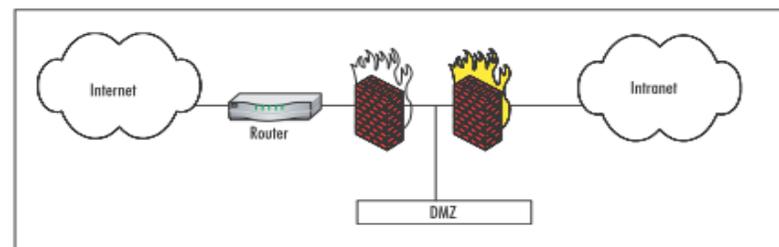
#### Screened subnet

Combinazione delle architetture dual-homed e screened-host.



#### Dual firewall configuration

Il router fornisce il primo layer di sicurezza e il primo firewall fornisce stateful inspection per il traffico della DMZ. Il secondo firewall previene che qualsiasi traffico originato da Interne o dalla DMZ acceda alla rete interna.





## **Costruire e mantenere una rete sicura**

La sezione 1.1 del PCI DSS fornisce una **guida per il processo di configurazione e mantenimento dei firewall e dei router.**

- 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
- 1.1.2 Un diagramma aggiornato della rete con tutte le connessioni ai dati di titolari di carta, comprese eventuali reti wireless
- 1.1.3 I requisiti per un firewall per ogni connessione Internet e tra tutte le zone demilitarizzate (DMZ) e la zona della rete interna
- 1.1.4 Una descrizione di gruppi, ruoli e responsabilità per la gestione logica dei componenti della rete
- 1.1.5 La documentazione e la giustificazione aziendale per l'uso di tutti i servizi, i protocolli e le porte consentite, inclusa la documentazione delle funzioni di sicurezza implementate per i protocolli considerati non sicuri
- 1.1.6 Una revisione dei set di regole del firewall e del router almeno ogni sei mesi



## **Costruire e mantenere una rete sicura**

Le sezioni 1.2, 1.3, 1.4 contengono requisiti strettamente legati tra loro.

L'obiettivo è di **filtrare il traffico proveniente o destinato ad una "rete non attendibile"**, cioè a 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.

- La sezione 1.2 determina i requisiti per la creazione di una configurazione del firewall che limiti le connessioni tra le reti non attendibili e qualsiasi componente di sistema nell'ambiente dei dati di titolari di carta.
- La sezione 1.3 è focalizzata ad impedire l'accesso pubblico diretto tra Internet e i componenti di sistema nell'ambiente dei dati di titolari di carta.
- La sezione 1.4 determina i requisiti orientati all'installazione di personal firewall (software) su tutti i computer portatili e i computer di proprietà dei dipendenti con connettività diretta a Internet (ad esempio, laptop utilizzati dai dipendenti), che vengono utilizzati per accedere alla rete aziendale.



## **Costruire e mantenere una rete sicura**

### **Negare il traffico proveniente da reti e host non fidati**

La riservatezza, l'integrità e la disponibilità sono il cuore della sezione 1.2.

Il principio utilizzato è **negare tutto quello che non è assolutamente necessario al business.**

- 1.2.1 Limitare il traffico in entrata e in uscita a quello indispensabile per l'ambiente dei dati dei titolari di carta.
- 1.2.2 Proteggere e sincronizzare i file di configurazione del router.
- 1.2.3 Installare firewall perimetrali tra le reti wireless e l'ambiente dei dati dei titolari di carta e configurare tali firewall per negare o controllare il traffico (se necessario per gli scopi aziendali) dall'ambiente wireless all'ambiente dei dati dei titolari di carta.

Un buon diagramma dei flussi logici, accoppiato con un'accurata lista di servizi, porte e protocolli, risulta essere uno strumento fondamentale.

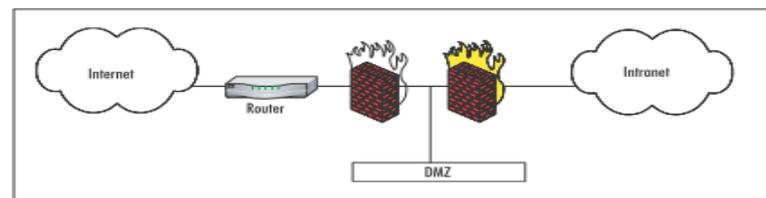


## Costruire e mantenere una rete sicura

**Vietare l'accesso pubblico diretto tra Internet e i componenti di sistema nell'ambiente dei dati di titolari di carta.**

La sezione 1.3 richiede che siano esaminate le configurazioni del firewall e del router per **determinare che non vi sia accesso diretto tra i sistemi pubblici e i sistemi interni** (in particolare quelli che memorizzano i dati dei titolari di carte).

- 1.3.1 Implementare una zona DMZ per limitare il traffico in entrata e in uscita ai soli protocolli necessari per l'ambiente dei dati di titolari di carta.
- 1.3.2 Limitare il traffico Internet in entrata agli indirizzi IP all'interno della zona DMZ.
- 1.3.3 Non consentire nessun percorso diretto per il traffico in entrata o in uscita tra Internet e l'ambiente dei dati di titolari di carta.
- 1.3.4 Non consentire agli indirizzi interni di passare da Internet alla zona DMZ.

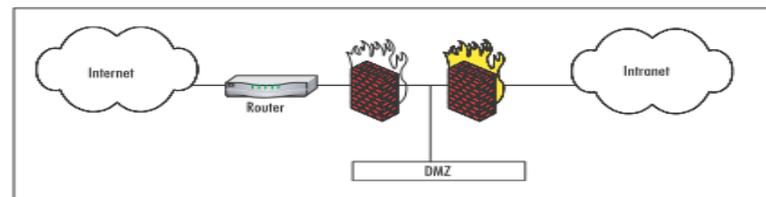




## **Costruire e mantenere una rete sicura**

**Vietare l'accesso pubblico diretto tra Internet e i componenti di sistema nell'ambiente dei dati di titolari di carta.**

- 1.3.5 Limitare il traffico in uscita dall'ambiente dei dati di titolari di carta a Internet in modo che il traffico in uscita possa accedere solo agli indirizzi IP all'interno della zona DMZ.
- 1.3.6 Implementare un controllo efficiente, anche noto come "dynamic packet filtering" (ossia che consente solo alle connessioni già "stabilite" di accedere alla rete).
- 1.3.7 Posizionare il database in una zona di rete interna, separata dalla zona DMZ.
- 1.3.8 Implementare un IP-masquerading per evitare che gli indirizzi interni vengano tradotti e resi noti su Internet, tramite lo spazio indirizzi RFC 1918. Utilizzare tecnologie NAT (Network Address Translation), ad esempio PAT.





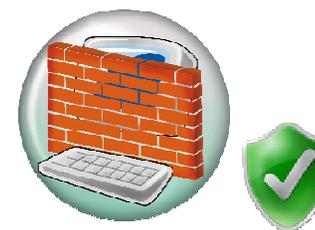
## **Costruire e mantenere una rete sicura**

Se un computer non dispone di un firewall o di un programma antivirus installato, spyware, cavalli di Troia, virus, worm e rootkit (malware) possono essere scaricati e/o installati inconsapevolmente. Il computer è ancora più vulnerabile se è connesso direttamente a Internet e non è protetto da un firewall aziendale.

La sezione 1.4 richiede **l'installazione dei personal firewall per computer connessi direttamente ad Internet.**

In generale, le unità potrebbero non sempre avere le patch critiche in modo tempestivo e i personal firewall forniscono maggiore garanzia.

- 1.4 Installare firewall personali (software) su tutti i computer portatili e i computer di proprietà dei dipendenti con connettività diretta a Internet (ad esempio, laptop utilizzati dai dipendenti), che vengono utilizzati per accedere alla rete aziendale.





## **Costruire e mantenere una rete sicura**

### **Default di sistema e altri parametri di configurazione**

La securizzazione di una rete richiede, tra l'altro, la gestione del default di sistema, l'attenzione nella configurazione dei parametri di configurazione, la gestione delle stesse, la protezione degli accessi amministrativi.

E' fondamentale che sia considerato:

- il non utilizzo delle password di default;
- la cancellazione degli account non necessari;
- lo sviluppo di configurazioni standard;
- l'implementazione di server dedicati;
- la configurazione dei parametri di sicurezza del sistema;
- la disabilitazione e/o rimozione dei servizi, protocolli e funzionalità non necessari;
- la cifratura degli accessi amministrativi da remoto;
- la protezione dell'ambiente ospitato, per i provider che offrono hosting.



## **Costruire e mantenere una rete sicura**

### **Password di default**

Le password di default esistono per quasi tutti i sistemi operativi e applicazioni; esse sono spesso utilizzate dagli utenti non autorizzati (all'interno o all'esterno dell'azienda) per compromettere i sistemi.

2.1 Modificare sempre le impostazioni predefinite del fornitore prima di installare un sistema su una rete, ad esempio, password, stringhe di comunità SNMP (Simple Network Management Protocol) ed eliminazione di account non necessari.

2.1.1 Per gli ambienti wireless connessi all'ambiente dei dati di titolari di carta o che trasmettono tali dati, modificare le impostazioni predefinite del fornitore wireless, incluse, senza limitazione, chiavi di cifratura wireless predefinite, password e stringhe di comunità SNMP.

Accertarsi che le impostazioni di sicurezza dei dispositivi wireless consentano l'uso della tecnologia di cifratura avanzata per l'autenticazione e la trasmissione.



## **Costruire e mantenere una rete sicura**

### **Password di default**

Sebbene ci siano diverse alternative per poter effettuare l'autenticazione, come l'utilizzo della biometria, Smart Cards e token, il maggior utilizzo è quello dei tradizionali ID e password.

In considerazione di ciò, è buona pratica che le policy e le procedure:

- Determinino il cambio di password almeno trimestralmente.
- Gestiscano le password assegnate ai nuovi utenti alla rete.
- Vietino l'utilizzo della stessa password iniziale.

Una robusta policy relativa alle password aumenterà la protezione de sistema contro potenziali compromissioni.



## **Costruire e mantenere una rete sicura**

Alcune semplici regole per le password, prima e dopo aver cambiato la password di default, sono le seguenti:

- Le password di utenze non amministrative devono essere cambiate almeno ogni 60-90 giorni.
- Gli account di un utente che hanno privilegi amministrativi devono avere una password distinta e diversa da tutti gli altri account tenuti dallo stesso utente
- Le password non devono essere trasmesse su internet tramite e-mail o ogni altra forma di comunicazione, senza essere cifrate.
- Le password devono essere lunghe almeno 6-8 caratteri, con una combinazione di maiuscole, minuscole, caratteri alfanumerici e speciali (ad es.: !%@\$)
- Le password non devono essere scritte né condivise con alcuno.



## **Costruire e mantenere una rete sicura** **Rafforzamento dei sistemi - Hardening**

La sezione 2.2 richiede che siano sviluppati standard di configurazione per tutti i componenti di sistema al fine di **risolvere tutte le vulnerabilità della sicurezza note**. (rif.: [www.nist.gov](http://www.nist.gov), [www.sans.org](http://www.sans.org), [www.cisecurity.org](http://www.cisecurity.org)).

- 2.2.1 Implementare una sola funzione principale per server.
- 2.2.2 Disattivare tutti i servizi e i protocolli non necessari e non protetti (che non sono strettamente necessari per eseguire la funzione specifica del dispositivo).
- 2.2.3 Configurare i parametri di sicurezza del sistema per evitare un uso improprio.
- 2.2.4 Rimuovere tutta la funzionalità non necessaria, ad esempio script, driver, funzioni, sottosistemi, file system e server Web non utilizzati.



## **Costruire e mantenere una rete sicura** **Cifrare gli accessi amministrativi da remoto**

La sezione 2.3 richiede che l'amministrazione remota sia eseguita con l'autenticazione sicura e comunicazioni cifrate. In particolare:

- sia invocato l'SSH (o altro metodo di cifratura) prima che la password amministrativa sia richiesta;
- siano controllati i servizi e i file di parametri di sistema per assicurarsi che Telnet o un altro comando di log-in remoto (per es.: i comandi "r" in Unix - cioè rlogin, rsh, ruptime, rcp, rwho) non sia disponibile;
- sia cifrato l'accesso amministrativo ad ogni interfaccia di gestione wireless con Secure Socket Layer/Transport Layer Security (SSL/TLS).

### **2.3 Eseguire la cifratura di tutto l'accesso amministrativo non da console.**

Utilizzare tecnologie quali SSH, VPN o SSL/TLS per la gestione basata su Web e altre attività amministrative non da console.



## **Costruire e mantenere una rete sicura**

### **Gli Hosting Provider devono proteggere l'ambiente offerto**

Quando tutti i dati si trovano sullo stesso server e sono sotto il controllo di un singolo ambiente, spesso le impostazioni di questi server condivisi non sono gestite dai singoli client, pertanto i client possono aggiungere funzioni non sicure e script che influiscono sulla sicurezza di tutti gli altri ambienti client.

Diventa più facile che un utente non autorizzato comprometta i dati di un client e ottenga così l'accesso ai dati di tutti gli altri client.

La sezione 2.4 richiede che **l'hosting provider protegga l'ambiente e i dati dell'entità ospitate.**

2.4 I provider di hosting condiviso devono proteggere l'ambiente ospitato e i dati di titolari di carta di ciascuna entità. Questi provider devono soddisfare specifici requisiti descritti nell'Appendice A dello standard.



## PROTEZIONE DEI DATI DI TITOLARI DI CARTA



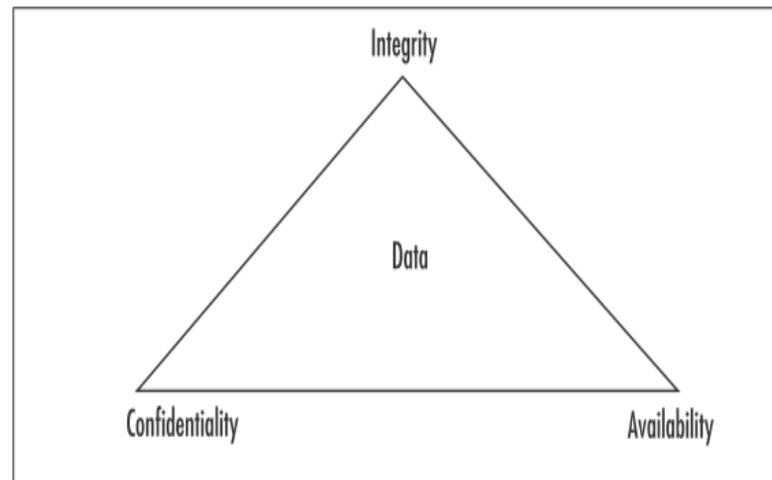
## Protezione dei dati di titolari di carta

Il requisito del Payment Card Industry Data Security Standard (PCI-DSS) a protezione dei dati dei titolari di carta si compone di due elementi fondamentali:

- Protezione dei dati di titolari di carta memorizzati
- Cifratura della trasmissione dei dati di titolari di carta su reti aperte e pubbliche

I tre principi alla base della valutazione dell'efficacia dei controlli impiegati a protezione del patrimonio informativo sono:

- Riservatezza;
- Integrità;
- Disponibilità (RID).





## **Protezione dei dati di titolari di carta**

### **Proteggere i dati di titolari di carta memorizzati**

La cifratura, troncatura, mascheratura e hashing sono metodi di protezione dei dati di titolari di carta determinanti se un utente non autorizzato elude altri controlli di sicurezza della rete e ottiene l'accesso ai dati.

Lo strumento maggiormente efficace per assicurare che i dati di titolari di carta non siano esposti a utenti non autorizzati (riservatezza) è la cifratura.

I relativi software possono essere suddivisi in due grandi categorie:

- la cifratura a livello di file o cartelle;
- la cifratura dell'intero disco.

Oltre a questi è da evidenziare anche la cifratura a livello di database.

Al fine di limitare i rischi possibili, è comunque consigliato di:

- non memorizzare i dati di carta a meno che non sia assolutamente necessario;
- eseguire la troncatura.



## **Protezione dei dati di titolari di carta**

### **Proteggere i dati di titolari di carta memorizzati**

#### **Cifratura a livello di file o cartella**

La cifratura a livello di file o cartella (o a livello di file system) è un sistema di cifratura dove specifiche cartelle, file o volumi sono cifrati da un pacchetto software di terze parti o da una stessa funzionalità del sistema operativo.

<b>Vantaggi</b>	<b>Svantaggi</b>
<ul style="list-style-type: none"><li>- Buon livello di granularità</li><li>- Integrazione del livello di restrizioni di accesso.</li><li>- Conservazione della cifratura anche a seguito di uno spostamento del file (es.: nastri di backup).</li><li>- Basso livello di invasività sulla struttura del DB</li><li>- Performance di sistema</li><li>- Capacità di logging e auditing.</li></ul>	<ul style="list-style-type: none"><li>- Possibili problemi di performance, specialmente con database relazionali.</li><li>- Risorse extra per la gestione delle chiavi.</li><li>- Livello di granularità non sufficiente se in un DB alcuni campi devono essere protetti a differenza di altri.</li><li>- Possibilità di cifrare più di quanto effettivamente richiesto dalla conformità PCI.</li></ul>



## **Protezione dei dati di titolari di carta**

### **Proteggere i dati di titolari di carta memorizzati**

#### **Cifratura a livello di disco completo (Full Disk Encryption - FDE)**

Il metodo di cifratura FDE cifra ogni file contenuto nel drive, includendo il sistema operativo/i file di sistema. Questo è usualmente effettuato sulla base dei settori.

<b>Vantaggi</b>	<b>Svantaggi</b>
<ul style="list-style-type: none"><li>- Ogni elemento sul disco è cifrato, incluso i file temporanei e i file di sistema.</li><li>- L'utente finale non ha discrezionalità.</li><li>- Le operazioni di cifratura/decifratura sono trasparenti.</li><li>- Autenticazione di pre-boot.</li><li>- Inutilizzo dei dati in caso di boot da altri dispositivi.</li></ul>	<ul style="list-style-type: none"><li>- Incremento nei tempi di scrittura e lettura.</li><li>- Per i sistemi che cifrano sulla base dei settori, la frammentazione può essere un problema.</li><li>- Il recupero dei dati e la gestione delle chiavi richiede estrema cura anche in osservanza alla disponibilità.</li><li>- L'autenticazione al sistema implica l'accesso ai dati.</li><li>- La corruzione del software di cifratura può avere gravi ripercussioni.</li></ul>



## **Protezione dei dati di titolari di carta**

### **Proteggere i dati di titolari di carta memorizzati**

#### **Cifratura a livello di database**

La cifratura a livello di campo permette un approccio più granulare per rendere la chiave del titolare di carta illegibile, focalizzandosi sullo specifico dato che necessita essere protetto.

<b>Vantaggi</b>	<b>Svantaggi</b>
<ul style="list-style-type: none"><li>- In caso di query su colonne non cifrate, nessun impatto sulle performance.</li><li>- In caso di ricerca su campi cifrati l'overhead è minimo.</li><li>- Può essere utilizzato dagli amministratori in congiunzione con altri controlli di sicurezza.</li></ul> <p>Nota: Attenzione alla separazione dei compiti tra gli amministratori di sicurezza e gli amministratori del database.</p>	<ul style="list-style-type: none"><li>- Richiede l'integrazione con il DB.</li><li>- Altamente invasivo al progetto del database (tipi, riferimenti, query,..)</li><li>- La gestione delle chiavi deve essere ben pianificata.</li><li>- Può determinare un falso senso di sicurezza: le elaborazioni batch degli esercenti e dei provider di servizio comunemente utilizzano flat file.</li><li>- Inefficace per i dati che non risiedono in DB.</li></ul>



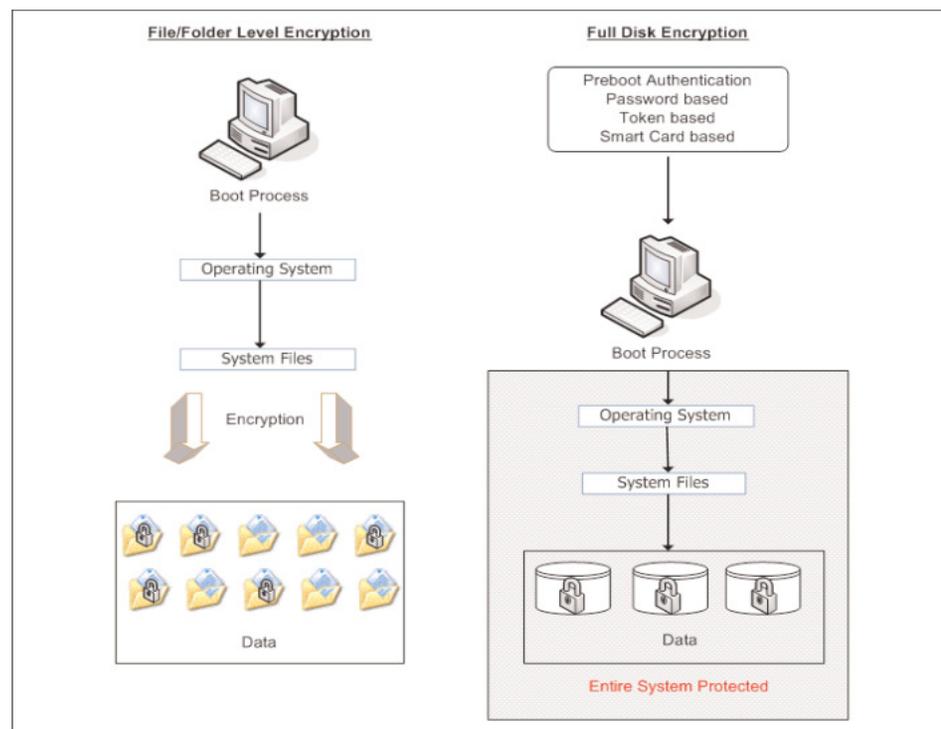
## Protezione dei dati di titolari di carta

### Proteggere i dati di titolari di carta memorizzati

Al fine di proteggere i dati memorizzati dei titolari di carta, può essere necessario utilizzare sia la cifratura al livello di file che l'FDE.

In aggiunta possono essere necessari i controlli di accesso al database e la cifratura del database a livello di campo. Ogni ambiente è differente.

L'**FDE** è molto utilizzato per proteggere i dati sulle workstation e i dispositivi mobili, mentre la **cifratura al livello di file** è molto più utile sui dispositivi di storage.



Un programma di sicurezza ben progettato deve proibire la memorizzazione e il trasferimento di dati a un laptop o desktop di un impiegato.



## **Protezione dei dati di titolari di carta**

### **Limitare la memorizzazione dei dati di titolari di carta.**

Le sezioni 3.1 e 3.2 richiedono di **limitare al massimo la memorizzazione dei dati di titolari di carta**. Sviluppare una politica per la conservazione e l'eliminazione dei dati. Limitare la quantità di dati memorizzati e il tempo di conservazione in base alle esigenze aziendali, legali e/o legislative.

Ad ogni modo **non memorizzare mai i dati sensibili di autenticazione dopo l'autorizzazione (anche se crittografati)**.

- 3.2.1 Non memorizzare l'intero contenuto delle tracce della striscia magnetica (presente sul retro della carta, contenuto in un chip o in altro luogo). Questi dati sono denominati anche traccia completa, traccia, traccia 1, traccia 2 e dati di striscia magnetica.
- 3.2.2 Non memorizzare il codice o il valore di validazione della carta utilizzato per verificare le transazioni con carta non presente.
- 3.2.3 Non memorizzare il numero di identificazione personale (PIN) o il blocco PIN cifrato.



## **Protezione dei dati di titolari di carta**

### **Rendere illeggibile, al minimo, il PAN.**

*Il PAN è l'informazione MINIMA sull'account che deve essere resa illeggibile.*

Le sezioni 3.3 e 3.4 richiedono di **mascherare il PAN quando visualizzato** se non vi è l'esigenza aziendale legittima di visualizzare (es.: copia per l'esercente) il numero PAN intero. Non devono essere visibili più di sei cifre all'inizio e quattro cifre alla fine.

In ogni caso è necessario **rendere illeggibile almeno il numero PAN ovunque sia memorizzato** (inclusi i dati su supporti digitali portatili, supporti di backup, registri) utilizzando:

- Hash one-way basati su crittografia avanzata
- Troncatura
- Token e pad indicizzati (i pad devono essere custoditi in un luogo sicuro)
- Crittografia avanzata con relativi processi e procedure di gestione delle chiavi



## **Protezione dei dati di titolari di carta**

### **Rendere illegibile, al minimo, il PAN.**

I danni derivanti dal furto o dalla perdita dei nastri di backup durante il trasporto possono essere limitati garantendo l'illeggibilità dei numeri PAN mediante operazioni di cifratura, troncatura o hashing.

I numeri PAN conservati nella memoria principale (database o file flat, ad esempio fogli elettronici su file di testo) e nella memoria non principale (backup, log di audit, log di eccezioni o risoluzione dei problemi) devono essere protetti.

### **L'accesso al sistema operativo non deve garantire l'accesso ai dati cifrati.**

- 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 indipendente dai meccanismi di controllo dell'accesso al sistema operativo nativo (ad esempio, non utilizzando database di account utente locali). Le chiavi di decifratura non devono essere associate agli account utente.



## **Protezione dei dati di titolari di carta**

### **Proteggere le chiavi di crittografia**

Le sezioni 3.5 e 3.6 sono volte alla protezione delle chiavi di crittografia utilizzate per la cifratura dei dati di titolari di carta, documentandone ed implementando completamente tutti i processi e le procedure di gestione al fine di:

- 3.5.1 Limitare l'accesso alle chiavi di crittografia al minor numero possibile di persone necessarie.
- 3.5.2 Memorizzare le chiavi di crittografia in modo sicuro nel minor numero possibile di posizioni e moduli.

Nei processi da documentare e implementare, si richiede che sia almeno incluso quanto segue:

- 3.6.1 Generazione di chiavi di “crittografia avanzata”
- 3.6.2 Distribuzione sicura delle chiavi di crittografia
- 3.6.3 Memorizzazione sicura delle chiavi di crittografia

(segue)



## **Protezione dei dati di titolari di carta**

### **Proteggere le chiavi di crittografia**

#### 3.6.4 Modifica periodica di chiavi di crittografia

- In base a quanto richiesto e consigliato dall'applicazione associata (ad esempio, re-keying), preferibilmente in modo automatico
- Almeno una volta all'anno

#### 3.6.5 Ritiro o sostituzione di chiavi di crittografia precedentemente o potenzialmente compromesse

#### 3.6.6 Uso della procedura "split knowledge" e definizione del controllo duale delle chiavi

#### 3.6.7 Prevenzione di tentativi di sostituzione non autorizzata delle chiavi di crittografia

#### 3.6.8 Obbligo per i custodi delle chiavi di crittografia di firmare una dichiarazione in cui accettano e confermano di conoscere le proprie responsabilità.



## **Protezione dei dati di titolari di carta**

### **Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche**

Le informazioni sensibili devono essere cifrate durante la trasmissione su reti a cui utenti non autorizzati possono accedere facilmente, reti con connettività ad Internet, reti ritenute insicure.

Esempi di rete pubbliche e aperte nell'ambito della valutazione PCI DSS sono:

- Internet
- Tecnologie wireless
- Comunicazioni GSM (Global System for Mobile)
- GPRS (General Packet Radio Service)

Reti wireless configurate in modo errato e vulnerabilità in protocolli di cifratura e autenticazione precedenti sono obiettivi continui di utenti non autorizzati che sfruttano tali vulnerabilità per ottenere privilegi di accesso per ambienti di dati di titolari di carta.





## **Protezione dei dati di titolari di carta**

### **Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche**

La sezione 4.1 richiede l'**utilizzo di protocolli di crittografia e sicurezza avanzati**, quali SSL/TLS o IPSEC, per proteggere i dati sensibili di titolari di carta **durante la trasmissione su reti pubbliche e aperte**.

Essi sono necessari per impedire agli utenti non autorizzati di ottenere accesso alla rete wireless (e ai dati sulla rete) o di utilizzare la rete wireless per raggiungere le reti interne o i dati.

Per tali reti non dovrebbe essere utilizzata la cifratura WEP in quando un aggressore può utilizzare strumenti di cracking basati sulla forza bruta, facilmente disponibili. (Implementazioni già effettuate prima del 31/03/09 devono essere convertite prima del 30/06/10).

- 4.1.1 Garantire che le reti wireless che trasmettono i dati di titolari di carta o connesse all'ambiente dei dati di titolari di carta utilizzino le pratiche di settore consigliate (ad esempio, IEEE 802.11i) per implementare la cifratura avanzata per l'autenticazione e la trasmissione.



## Protezione dei dati di titolari di carta

### **Cifrare i dati di titolari di carta trasmessi su reti aperte e pubbliche**

L'e-mail, la messaggistica istantanea e la chat possono essere facilmente intercettati mediante packet-sniffing durante il recapito attraverso reti interne e pubbliche.

La sezione 4.2 richiede che **non** siano utilizzati questi strumenti di messaggistica per **inviare numeri PAN**, a meno che non dispongano di funzioni di cifratura.

E' necessario che:

- - sia eseguita la crittografia avanzata sui dati di titolari di carta quando inviati tramite tecnologie di messaggistica dell'utente finale;
  - esista una politica in cui viene stabilito che i numeri PAN non cifrati non devono essere inviati tramite tecnologie di messaggistica dell'utente finale.





## MANUTENZIONE DI UN PROGRAMMA PER LA GESTIONE DELLE VULNERABILITA'



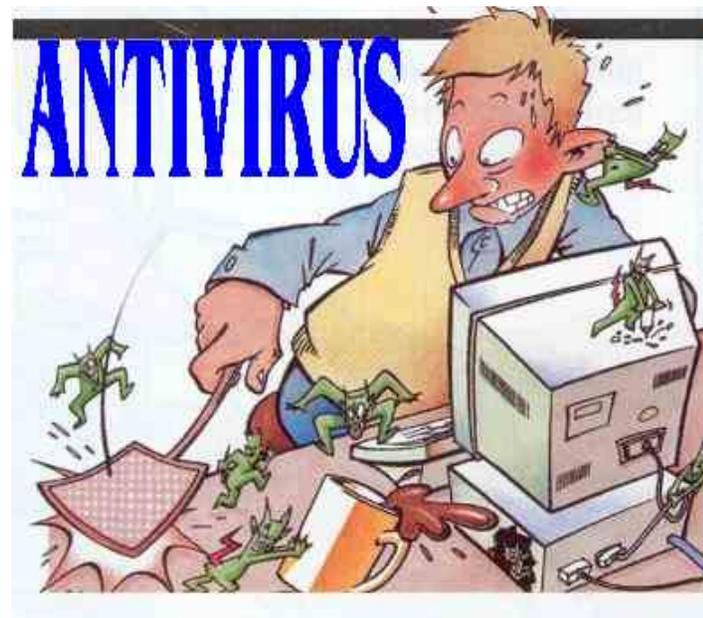
## Manutenzione di un programma per la gestione delle vulnerabilità

### Utilizzare e aggiornare regolarmente il software antivirus

Le vulnerabilità del sistema permettono ai software dannosi, comunemente noti come "malware", inclusi virus, worm e cavalli di Troia, di accedere alla rete durante molte attività aziendali approvate, quali la posta elettronica dei dipendenti e l'uso di Internet, computer portatili e dispositivi di memorizzazione.

La sezione 5.1 richiede che venga distribuito il **software antivirus su tutti i sistemi comunemente colpiti da malware** (in particolare PC e server).

- 5.1.1 Garantire che tutti i programmi antivirus siano in grado di rilevare e rimuovere tutti i tipi di malware nonché garantire una protezione sicura.





## Manutenzione di un programma per la gestione delle vulnerabilità

### Utilizzare e aggiornare regolarmente il software antivirus

È importante proteggersi da TUTTI i tipi e le forme di software dannoso.

La sezione 5.2 richiede di **garantire che tutti i meccanismi antivirus siano aggiornati, in esecuzione e in grado di generare log di audit.**

Il miglior software antivirus presenta un'efficacia limitata se non dispone delle definizioni dei virus correnti o se non è attivo nella rete o in un singolo computer.

I log di audit consentono di monitorare l'attività dei virus e le reazioni dell'antivirus.





## **Manutenzione di un programma per la gestione delle vulnerabilità**

### **Sviluppare e gestire sistemi e applicazioni protette**

L'identificazione delle vulnerabilità e l'aggiornamento delle configurazioni devono essere effettuate attraverso un processo strutturato. Gli utenti non autorizzati sfruttano tali vulnerabilità per ottenere l'accesso privilegiato ai sistemi.

Per proteggere i dati dei titolari di carta da uso non autorizzato e malware, **tutti i sistemi critici devono disporre delle patch di software corrette più recenti.**

Nota: Le patch software corrette sono le patch valutate e testate in modo soddisfacente per garantire che non siano in conflitto con le configurazioni di sicurezza esistenti.

Per le applicazioni sviluppate in-house, è possibile evitare numerose vulnerabilità utilizzando processi di sviluppo del sistema standard e tecniche di codifica sicure.





## Manutenzione di un programma per la gestione delle vulnerabilità

### Sviluppare e gestire sistemi e applicazioni protette

La sezione 6.1 richiede la **garanzia che su tutti i componenti di sistema e il software siano installate le patch di sicurezza più recenti** (quelle critiche entro un mese dal rilascio).

**Nota:** Per garantire che le patch necessarie vengano installate sui sistemi e sui dispositivi ad alta priorità entro un mese e su altri dispositivi e sistemi meno importanti entro tre mesi, è possibile adottare un approccio basato sulla priorità assegnata in base al rischio.

La sezione 6.2 richiede che sia stabilito un **processo per identificare le vulnerabilità della sicurezza recentemente rilevate** (ad esempio, attraverso un abbonamento a servizi di notifica gratuiti disponibili in Internet).





## **Manutenzione di un programma per la gestione delle vulnerabilità**

### **Sviluppare e gestire sistemi e applicazioni protette**

La sezione 6.3 richiede di incorporare la protezione delle informazioni nell'intero ciclo di sviluppo del software. In particolare:

- 6.3.1 Tutte le patch di sicurezza e le modifiche di configurazione del sistema e del software devono essere sottoposte a test prima di essere distribuite, incluso, senza limitazione la convalida di tutto l'input, del processo di gestione degli errori, del processo di memorizzazione di dati crittografici sicuro, la convalida di comunicazioni sicure, la convalida di un processo di controllo dell'accesso basato su ruolo (RBAC, Role-Based Access Control) appropriato.

(segue)

Senza l'inclusione della sicurezza durante le fasi di definizione dei requisiti, progettazione, analisi e test dello sviluppo del software, le vulnerabilità di protezione possono essere introdotte, inavvertitamente o con cattive intenzioni, nell'ambiente di produzione.



## **Manutenzione di un programma per la gestione delle vulnerabilità**

### **Sviluppare e gestire sistemi e applicazioni protette**

- 6.3.2 Ambienti di sviluppo, test e produzione separati.
- 6.3.3 Responsabilità assegnate agli ambienti di sviluppo, test e produzione separate.
- 6.3.4 I dati di produzione (PAN attivi) devono essere esclusi dalle attività di test o sviluppo.
- 6.3.5 Dati e account di test devono essere rimossi prima dell'attivazione dei sistemi di produzione.
- 6.3.6 Account, ID utente e password di applicazioni personalizzate vengono rimossi prima dell'attivazione o della distribuzione di tali applicazioni ai clienti.
- 6.3.7 Il codice personalizzato viene analizzato prima del rilascio in produzione o della distribuzione ai clienti per identificare eventuali vulnerabilità.



## Manutenzione di un programma per la gestione delle vulnerabilità

### Sviluppare e gestire sistemi e applicazioni protette

Senza controlli di modifica del software appropriati, le funzionalità di protezione possono essere inavvertitamente o deliberatamente omesse o rese inattive, possono verificarsi problemi di elaborazione o è possibile che venga introdotto del codice dannoso.

La sezione 6.4 richiede che siano seguite le **procedure di controllo delle modifiche** per tutte quelle da apportare ai componenti di sistema.

Le procedure devono includere quanto segue:

- 6.4.1 Documentazione dell'impatto
- 6.4.2 Approvazione del management delle parti interessate
- 6.4.3 Test della funzionalità operativa
- 6.4.4 Procedure di back-out





## Manutenzione di un programma per la gestione delle vulnerabilità

### Sviluppare e gestire sistemi e applicazioni protette

Lo strato applicazione è ad alto rischio e può divenire bersaglio di minacce interne ed esterne. Senza la corretta protezione, i dati dei titolari di carte e altre informazioni riservate dell'azienda possono essere esposte, causando danni all'azienda, ai suoi clienti e alla sua reputazione.

La sezione 6.5 richiede che **tutte le applicazioni Web** (interne, esterne e con accesso amministrativo all'applicazione tramite Web) **siano sviluppate in base alle linee guida di codifica sicura, quali le linee guida Open Web Application Security Project** prevenendo possibili vulnerabilità del codice comuni nei processi di sviluppo del software, incluso:

- 6.5.1 XSS (Cross-Site Scripting)
- 6.5.2 Injection flaw, in particolare SQL injection.
- 6.5.3 Esecuzione di file pericolosi

(segue)





## Manutenzione di un programma per la gestione delle vulnerabilità

### Sviluppare e gestire sistemi e applicazioni protette

- 6.5.4 Riferimenti a oggetti diretti non sicuri
- 6.5.5 Cross-site request forgery (CSRF)
- 6.5.6 Perdita di informazioni e gestione degli errori non appropriata
- 6.5.7 Violazione dell'autenticazione e gestione delle sessioni
- 6.5.8 Memorizzazione di dati crittografici non sicura
- 6.5.9 Comunicazioni non sicure
- 6.5.10 Mancata limitazione dell'accesso URL





## **Manutenzione di un programma per la gestione delle vulnerabilità**

### **Sviluppare e gestire sistemi e applicazioni protette**

Gli attacchi alle applicazioni con interfaccia Web sono comuni e spesso riusciti. Essi sono permessi da **pratiche di codifica poco attente**.

La sezione 6.6 mira a **ridurre il numero di compromissioni sulle applicazioni Web** per il pubblico, che danno luogo a violazioni dei dati dei titolari di carte.

Essa richiede di assicurare una protezione costante da nuove minacce e vulnerabilità e garantire che queste applicazioni siano protette da attacchi noti mediante almeno 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.
- Installazione di un firewall per applicazioni Web a protezione delle applicazioni Web rivolte al pubblico.



## IMPLEMENTARE RIGIDE MISURE DI CONTROLLO DELL'ACCESSO



## **Implementazione di rigide misure di controllo dell'accesso**

### **Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario**

Allo scopo di garantire che solo il personale autorizzato possa accedere a dati critici, la sezione 7.1 richiede di **limitare l'accesso ai componenti di sistema e ai dati di titolari di carta** solo alle persone per le cui mansioni è realmente necessario, in base alle esigenze e alle responsabilità del ruolo.

Le limitazioni di accesso devono includere quanto segue:

- 7.1.1 Limitazione dei diritti di accesso a ID utente privilegiati alla quantità minima necessaria per le responsabilità di ruolo.
- 7.1.2 Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale.
- 7.1.3 Richiesta di un modulo di autorizzazione firmato dal management che specifica i privilegi necessari.
- 7.1.4 Implementazione di un sistema di controllo dell'accesso automatico.



## **Implementazione di rigide misure di controllo dell'accesso**

**Limitare l'accesso ai dati di titolari di carta solo se effettivamente necessario**

E' fondamentale l'implementazione di **un meccanismo che limiti l'accesso in base all'effettiva esigenza**. La sezione 7.2 richiede che sia stabilito tale meccanismo per i componenti di sistemi con più utenti al fine di limitare l'accesso in base alla reale necessità di un utente e impostare "deny all" per impedire ogni accesso se non specificatamente consentito.

Il sistema di controllo dell'accesso deve includere quanto segue:

- 7.2.1 Copertura di tutti i componenti di sistema.
- 7.2.2 Assegnazione dei privilegi basata sulla classificazione e sulla funzione del ruolo del personale.
- 7.2.3 Impostazione predefinita "deny-all".





## Implementazione di rigide misure di controllo dell'accesso

### **Assegnare un ID univoco a chiunque abbia accesso a un computer**

Garantendo l'identificazione univoca di ogni utente, un'organizzazione può mantenere la responsabilità delle azioni e disporre di un effettivo audit trail per ogni dipendente. In questo modo i problemi vengono risolti più velocemente ed è possibile attuare un contenimento quando si rilevano abusi o cattive intenzioni.

Le sezioni 8.1 e 8.2 richiedono di **assegnare a tutti gli utenti un ID univoco** prima di consentire l'accesso ai componenti di sistema o ai dati di titolari di carta e adottare almeno uno dei seguenti metodi per autenticare tutti gli utenti:

- Password o passphrase
- Autenticazione a due fattori  
(ad esempio, dispositivi token, smart card, biometrica o chiavi pubbliche)





## **Implementazione di rigide misure di controllo dell'accesso**

### **Assegnare un ID univoco a chiunque abbia accesso a un computer**

La sezione 8.3 richiede di **incorporare l'autenticazione a due fattori per l'accesso remoto alla rete** (accesso a livello di rete dall'esterno) da parte di dipendenti, amministratori e terze parti.

Per una maggiore sicurezza, l'organizzazione può prendere in considerazione l'uso dell'autenticazione a due fattori anche per l'accesso a reti con protezione maggiore da reti con protezione minore, ad esempio dai desktop aziendali (minore protezione) ai server/database di produzione con i dati dei titolari di carte (maggiore protezione).

Possibili tecnologie sono:

- RADIUS (Remote Authentication and Dial-In Service)
- TACACS (Terminal Access Controller Access Control System) con token
- VPN (basata su SSL/TLS o IPSEC) con certificati singoli.



## Implementazione di rigide misure di controllo dell'accesso

### **Assegnare un ID univoco a chiunque abbia accesso a un computer**

Molti dispositivi e applicazioni di rete trasmettono l'ID utente e la password non cifrata sulla rete e/o memorizzano le password senza cifratura. Un utente non autorizzato potrebbe facilmente intercettare tali informazioni utilizzando uno "sniffer" durante la trasmissione o accedendo al file in cui esse sono memorizzate.

La sezione 8.4 richiede di **rendere tutte le password illeggibili durante la trasmissione e la memorizzazione** su tutti i componenti di sistema tramite la "crittografia avanzata".





## **Implementazione di rigide misure di controllo dell'accesso**

### **Assegnare un ID univoco a chiunque abbia accesso a un computer**

La sezione 8.5 è volta a **garantire una corretta autenticazione utente e gestione delle password per amministratori e utenti non consumatori** su tutti i componenti di sistema. In dettaglio si richiede di:

- 8.5.1 Controllare le operazioni di aggiunta, eliminazione e modifica di ID utente, credenziali e altri oggetti identificativi.
- 8.5.2 Verificare l'identità dell'utente prima di eseguire il ripristino delle password.
- 8.5.3 Impostare la password per il primo accesso su un valore univoco per ogni utente e modificarla immediatamente dopo il primo uso.
- 8.5.4 Revocare immediatamente l'accesso per gli utenti non attivi.
- 8.5.5 Rimuovere/disabilitare gli account utente non attivi almeno ogni 90 giorni.
- 8.5.6 Abilitare gli account utilizzati dai fornitori per la gestione in remoto solo durante il periodo di tempo necessario.

(segue)



## **Implementazione di rigide misure di controllo dell'accesso**

### **Assegnare un ID univoco a chiunque abbia accesso a un computer**

- 8.5.7 Comunicare le procedure e le politiche relative alle password a tutti gli utenti con accesso ai dati di titolari di carta.
- 8.5.8 Non utilizzare account e password di gruppo, condivisi o generici.
- 8.5.9 Modificare le password utente almeno ogni 90 giorni.
- 8.5.10 Richiedere una lunghezza minima della password di 7 caratteri.
- 8.5.11 Utilizzare password contenenti valori numerici e alfabetici.
- 8.5.12 Non consentire l'invio di una nuova password uguale a una delle ultime quattro password utilizzate.
- 8.5.13 Limitare i tentativi di accesso ripetuti bloccando l'ID utente dopo un massimo di sei tentativi.
- 8.5.14 Impostare la durata del blocco a un minimo di 30 minuti o finché l'amministratore non abilita l'ID utente.

(segue)



## **Implementazione di rigide misure di controllo dell'accesso**

### **Assegnare un ID univoco a chiunque abbia accesso a un computer**

- 8.5.15 Se una sessione è inattiva per oltre 15 minuti, l'utente deve immettere nuovamente la password per riattivare il terminale.
- 8.5.16 Autenticare tutti gli accessi al database contenente i dati di titolari di carta. Sono compresi gli accessi da applicazioni, amministratori e tutti gli altri utenti.



## **Implementazione di rigide misure di controllo dell'accesso**

### **Limitare l'accesso fisico ai dati di titolari di carta**

Gli accessi fisici ai dati o ai sistemi offrono la possibilità di accedere ai dispositivi o ai dati con impatto sia sui sistemi elettronici che sulle copie cartacee.

La sezione 9.1 richiede di **utilizzare i controlli dell'accesso alle strutture, appropriati per limitare e monitorare gli accessi fisici ai sistemi nell'ambiente dei dati di titolari di carta.**

9.1.1 Utilizzare videocamere o altri meccanismi di controllo dell'accesso per monitorare gli accessi fisici 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.

9.1.2 Limitare l'accesso fisico a connettori di rete accessibili pubblicamente.

9.1.3 Limitare l'accesso fisico a punti di accesso wireless, gateway e dispositivi portatili.





## Implementazione di rigide misure di controllo dell'accesso

### Limitare l'accesso fisico ai dati di titolari di carta

Senza l'uso di sistemi badge e controlli all'ingresso, gli utenti non autorizzati possono facilmente accedere all'edificio per rubare, disattivare, interrompere o distruggere sistemi critici e dati dei titolari di carte.

La sezione 9.2 richiede lo **sviluppo di procedure che consentano a tutto il personale di distinguere facilmente tra dipendenti e visitatori**, in particolare in aree che permettono l'accesso ai dati di titolari di carta.

**Nota:** Per "dipendente" si intende un qualsiasi dipendente a prescindere dal contratto, un collaboratore o consulente che svolge le sue prestazioni in sede.

Per "visitatore" si intende chiunque abbia necessità di accedere alla struttura per un breve periodo di tempo, solitamente non più di un giorno.





## **Implementazione di rigide misure di controllo dell'accesso**

### **Limitare l'accesso fisico ai dati di titolari di carta**

I visitatori devono accedere solo alle aree a cui sono autorizzati e devono essere identificabili come tali (in modo che i dipendenti possano controllarne le attività) e che il loro accesso sia limitato solo alla durata della visita legittima.

La sezione 9.3 richiede la **garanzia e la verifica della corretta gestione di tutti i visitatori**, includendo le seguenti attenzioni:

- 9.3.1 Ricevono l'autorizzazione appropriata prima di accedere alle aree in cui i dati di titolari di carta sono elaborati o custoditi.
- 9.3.2 Ricevono un token fisico (ad esempio, una tessera magnetica o un dispositivo di accesso) che scade e che identifica i visitatori come non dipendenti.
- 9.3.3 Restituiscono il token fisico prima di lasciare la struttura o in corrispondenza della data di scadenza.



## **Implementazione di rigide misure di controllo dell'accesso**

### **Limitare l'accesso fisico ai dati di titolari di carta**

Soprattutto nelle zone in cui sono presenti i dati dei titolari di carte, è necessario inoltre prendere in considerazione l'implementazione di registri all'ingresso degli edifici.

Tale registro documenta informazioni minime sul visitatore e può offrire assistenza, in caso di un'indagine su una violazione dei dati, nell'identificazione dell'accesso fisico a un edificio o un locale e potenzialmente ai dati dei titolari di carte.

La sezione 9.4 richiede di **utilizzare un registro visitatori per conservare un audit trail fisico** dell'attività dei visitatori e di documentare su di esso il nome del visitatore, l'azienda rappresentata e il dipendente che autorizza l'accesso fisico.

La conservazione del registro è, se non diversamente richiesto dalla legge, di almeno tre mesi.





## Implementazione di rigide misure di controllo dell'accesso

### Limitare l'accesso fisico ai dati di titolari di carta

Le sezioni 9.5 e 9.6 sono volte a **proteggere fisicamente i dati dei titolari di carta compreso se conservati in backup**. In particolare:

- La sezione 9.5 richiede che **i supporti dei backup siano conservati in un luogo sicuro**, preferibilmente in una struttura esterna o un magazzino e di controllare la sicurezza del luogo almeno una volta all'anno.
- La sezione 9.6 richiede che **tutti i supporti cartacei ed elettronici contenenti dati di titolari di carta siano protetti fisicamente**.

Essi possono essere soggetti a visualizzazione, copia o scansione non autorizzate se sono trasferiti senza protezione su supporti portatili, stampati o lasciati sulla scrivania.





## **Implementazione di rigide misure di controllo dell'accesso**

### **Limitare l'accesso fisico ai dati di titolari di carta**

La sezione 9.7 richiede che sia mantenuto **un rigido controllo sulla distribuzione interna o esterna dei supporti utilizzati**, incluso quanto segue:

- 9.7.1 Classificare il supporto in modo che possa essere identificato come riservato.
- 9.7.2 Inviare il supporto tramite un corriere affidabile o un altro metodo di consegna che possa essere monitorato in modo appropriato.

**L'approvazione da parte del management ha prioritaria importanza.**

La sezione 9.8 richiede che esso approvi tutti i supporti contenenti i dati di titolari di carta che vengono spostati da un'area protetta (in particolare quando i supporti vengono distribuiti a singoli utenti).





## **Implementazione di rigide misure di controllo dell'accesso**

### **Limitare l'accesso fisico ai dati di titolari di carta**

Nelle procedure consigliate (requisito 9.6) è necessario includere lo sviluppo di un processo per limitare l'accesso ai supporti contenenti dati dei titolari di carte.

La sezione 9.9 richiede che siano mantenuti **rigidi controlli sulla memorizzazione e sull'accesso a supporti contenenti dati di titolari di carta.**

A tal proposito è doveroso:

- 9.9.1 Conservare in modo appropriato i registri di inventario per tutti i supporti ed eseguire tali inventari almeno una volta all'anno.

Senza metodi di inventario attenti e controlli di storage potrebbe non essere possibile accorgersi del furto o della mancanza di supporti per diverso tempo.



## **Implementazione di rigide misure di controllo dell'accesso**

### **Limitare l'accesso fisico ai dati di titolari di carta**

La sezione 9.10 richiede che siano distrutti i supporti contenenti dati di titolari di carta quando non sono più necessari per scopi aziendali o legali, come segue:

- 9.10.1 Stracciare, bruciare o mandare al macero i materiali cartacei in modo che i dati di titolari di carta non possano essere ricostruiti.
- 9.10.2 Rendere i dati di titolari di carta su supporti elettronici non recuperabili, in modo che non sia possibile ricostruirli.

Lo sviluppo di un processo per la corretta distruzione dei supporti contenenti dati dei titolari di carte, comprendendo la corretta conservazione di tali supporti prima della distruzione, permette di ridurre il rischio che lo smaltimento delle informazioni possa dare luogo a compromissioni e comportare perdite finanziarie o di reputazione.



## MONITORAGGIO E TEST REGOLARI DELLE RETI



## Monitoraggio e test delle reti regolari

### **Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta**

I meccanismi di accesso e la possibilità di tenere traccia delle attività degli utenti sono di fondamentale importanza per impedire, rilevare o ridurre al minimo l'impatto di una compromissione di dati.

La presenza dei registri in tutti gli ambienti consente di tenere traccia, dare l'allarme ed eseguire un'analisi quando si verifica un problema.

Senza registri di attività del sistema, è molto difficile determinare la causa che ha generato l'eventuale compromissione.

La sezione 10.1 richiede che sia **stabilito un processo per collegare a ciascun utente tutti gli accessi ai componenti di sistema** (in particolare l'accesso eseguito con privilegi di amministratore, ad esempio come utente root).



## **Monitoraggio e test delle reti regolari**

### **Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta**

Al fine di implementare un controllo per il monitoraggio preventivo e l'analisi post-incidente, la sezione 10.2 richiede che **siano implementati audit trail automatizzati su tutti i componenti del sistema per ricostruire i seguenti eventi:**

- 10.2.1 Tutti i singoli accessi di utenti a dati di titolari di carta
- 10.2.2 Tutte le azioni intraprese da un utente con privilegi di utente root o amministratore
- 10.2.3 Accesso a tutti gli audit trail
- 10.2.4 Tentativi di accesso logico non validi
- 10.2.5 Uso di meccanismi di identificazione e autenticazione
- 10.2.6 Inizializzazione di log di audit
- 10.2.7 Creazione ed eliminazione di oggetti a livello di sistema



## Monitoraggio e test delle reti regolari

### **Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta**

Al fine di poter identificare rapidamente una potenziale compromissione e disporre di dettagli sufficienti per sapere chi, cosa, dove, come e quando, la sezione 10.3 richiede di **registrare per ciascun evento e per tutti i componenti di sistema almeno le seguenti voci di audit trail** :

- 10.3.1 Identificazione utente
- 10.3.2 Tipo di evento
- 10.3.3 Data e ora
- 10.3.4 Indicazione di successo o fallimento
- 10.3.5 Origine dell'evento
- 10.3.6 Identità o nome dell'elemento interessato  
(dati, componente di sistema o risorsa)



*Chi ?  
Cosa ?  
Dove ?  
Quando ?*



## **Monitoraggio e test delle reti regolari**

### **Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta**

Per i team legali attivati dopo un incidente, l'ora di ciascuna attività è fondamentale per determinare come sono stati compromessi i sistemi

Se un utente non autorizzato ha accesso alla rete, potrebbe cambiare gli indicatori di data/ora delle sue azioni all'interno dei log di audit per impedire il rilevamento delle sue attività o, se le limitazioni di accesso non sono adeguate, modificare direttamente l'ora su un server di riferimento orario.

La sezione 10.4 richiede di **sincronizzare tutti gli orologi e gli orari critici del sistema.**



## **Monitoraggio e test delle reti regolari**

### **Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta**

La sezione 10.5 richiede di **proteggere gli audit trail in modo che possa esserne garantita la completezza, la precisione e l'integrità**. Allo scopo:

- 10.5.1 Limitare la visualizzazione degli audit trail a coloro che realmente necessitano di tali informazioni per scopi aziendali.
- 10.5.2 Proteggere i file di audit trail da modifiche non autorizzate.
- 10.5.3 Eseguire immediatamente il backup dei file di audit trail su un server di registro centralizzato o un supporto difficile da modificare.
- 10.5.4 Scrivere registri per tecnologie rivolte al pubblico su un server di registro sulla LAN interna.
- 10.5.5 Utilizzare un meccanismo di monitoraggio dell'integrità dei file e un software di rilevamento delle modifiche di log per accertarsi che i dati di log esistenti non possano essere modificati senza generare avvisi (non per l'aggiunta di nuovi dati)



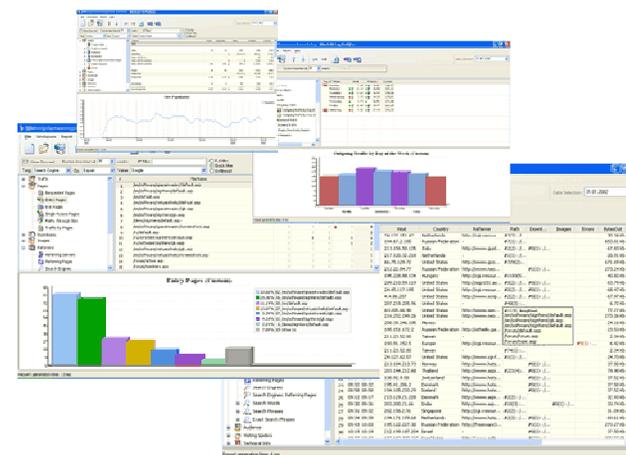
## Monitoraggio e test delle reti regolari

### **Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta**

Molte violazioni avvengono per giorni o mesi prima di essere rilevate. Il controllo quotidiano dei registri riduce al minimo la durata e l'esposizione di una potenziale violazione.

La sezione 10.6 richiede che siano **esaminati i registri per tutti i componenti di sistema almeno una volta al giorno.**

Le analisi dei log devono includere i server che eseguono funzioni di sicurezza, quali i servizi anti-intrusione IDS (Intrusion Detection System), i server di autenticazione, autorizzazione e accounting (AAA), ad esempio RADIUS.





## **Monitoraggio e test delle reti regolari**

### **Registrare e monitorare tutti gli accessi a risorse di rete e dati di titolari di carta**

Con la disponibilità immediata di registri afferenti a tre mesi di attività, un'entità può identificare rapidamente e ridurre al minimo l'impatto di una violazione dei dati. Può però essere necessaria una cronologia maggiore per consentire agli investigatori di determinare il periodo e i sistemi interessati da una potenziale violazione avvenuta o in corso.

La sezione 10.7 richiede di **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).

Nota: La conservazione dei nastri di backup fuori sede può richiedere tempi superiori per il ripristino, l'analisi e l'identificazione dei sistemi interessati o dei dati.



## Monitoraggio e test delle reti regolari

### Eeguire regolarmente test dei sistemi e processi di protezione

L'implementazione e/o lo sfruttamento della tecnologia wireless all'interno di una rete rappresentano uno dei percorsi più noti agli utenti non autorizzati per ottenere l'accesso alla rete e ai dati dei titolari di carte.

Se viene installato un dispositivo o una rete wireless senza che l'azienda ne sia a conoscenza, un aggressore potrebbe accedere alla rete con facilità e in modo "invisibile". Inoltre, possono essere utilizzati analizzatori wireless, scanner di porte e altri strumenti di rete che rilevano i dispositivi wireless.

La sezione 11.1 richiede di **verificare la presenza di punti di accesso wireless utilizzando un analizzatore wireless almeno una volta ogni tre mesi oppure distribuendo un IDS/IPS wireless** per identificare tutti i dispositivi wireless in uso.

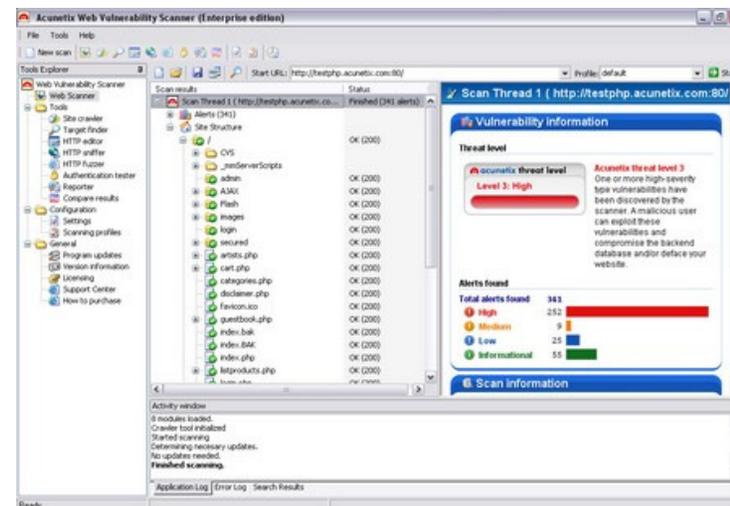


## Monitoraggio e test delle reti regolari

### Eeguire regolarmente test dei sistemi e processi di protezione

Un vulnerability scanner è uno strumento automatico eseguito su server e dispositivi di rete interni ed esterni, studiato per esporre le potenziali vulnerabilità e identificare le porte nelle reti che possono essere individuate e sfruttate da utenti non autorizzati. Una volta identificati questi punti deboli, l'entità li corregge e ripete la scansione per verificare che le vulnerabilità siano state corrette.

La sezione 11.2 richiede **l'esecuzione di scansioni interne ed esterne della rete almeno una volta ogni tre mesi e dopo ogni cambiamento significativo apportato alla rete** (ad es.: l'installazione di nuovi componenti di sistema, la modifica della topologia della rete, la modifica delle regole o l'aggiornamento di un firewall).





## Monitoraggio e test delle reti regolari

### **Eeguire regolarmente test dei sistemi e processi di protezione**

I test di penetrazione a livello di rete e di applicazione, a differenza delle scansioni delle vulnerabilità, sono manuali e tentano di sfruttare alcune delle vulnerabilità identificate nelle scansioni.

La sezione 11.3 richiede di eseguire **test di penetrazione esterna ed 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).

Questi test di penetrazione devono includere quanto segue:

11.3.1 Test di penetrazione a livello di rete

11.3.2 Test di penetrazione a livello di applicazione





## Monitoraggio e test delle reti regolari

### **Eeguire regolarmente test dei sistemi e processi di protezione**

Gli avvisi di protezione generati dovrebbero essere monitorati, al fine di fermare i tentativi di intrusione. La sezione 11.4 richiede di **utilizzare sistemi di rilevamento e/o di prevenzione delle intrusioni** per monitorare tutto il traffico nell'ambiente dei dati di titolari di carta e segnalare possibili rischi al personale addetto. Inoltre richiede di **mantenere tutti i sistemi di rilevamento e prevenzione delle intrusioni aggiornati**.

Versioni obsolete di sistemi di rilevamento non dispongono di definizioni correnti e non identificano le nuove vulnerabilità, portando così ad una mancata rilevazione delle violazioni.

Senza un approccio proattivo al rilevamento di attività non autorizzate, gli attacchi alle risorse del computer (o l'abuso di tali risorse) potrebbero non essere rilevati in tempo reale.



## Monitoraggio e test delle reti regolari

### **Eeguire regolarmente test dei sistemi e processi di protezione**

I sistemi di monitoraggio dell'integrità dei file (FIM) controllano e segnalano le modifiche ai file critici.

La sezione 11.5 richiede che sia **distribuito il software di monitoraggio dell'integrità dei file** per segnalare al personale modifiche non autorizzate di file system, file di configurazione o file di contenuto critici; inoltre, è necessario **configurare il software in modo che esegua confronti di file critici almeno una volta alla settimana.**

**Nota:** Ai fini del monitoraggio dell'integrità dei file, i file critici sono solitamente file che non cambiano frequentemente ma la cui modifica può indicare la compromissione, effettiva o potenziale, del sistema. In genere i file critici, oltre quelli di sistema, devono essere valutati e definiti dall'entità (ossia dall'esercente o dal provider di servizi).





## GESTIRE UNA POLITICA DI SICUREZZA DELLE INFORMAZIONI



## Gestire una politica di sicurezza delle informazioni

### Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori

Una politica di sicurezza rigida definisce il livello di sicurezza per l'intera società e spiega ai dipendenti quali sono le aspettative nei loro confronti in termini di sicurezza. Tutti i dipendenti devono essere a conoscenza della sensibilità dei dati e delle proprie responsabilità in termini di protezione.

La sezione 12.1 richiede che sia **stabilita, pubblicata, conservata e resa disponibile una politica di sicurezza** conforme a quanto indicato di seguito:

- 12.1.1 Risponde a tutti i requisiti PCI DSS.
- 12.1.2 Include un processo annuale che identifica minacce e vulnerabilità e che consente di ottenere una valutazione dei rischi formale.
- 12.1.3 Include una revisione almeno una volta l'anno e aggiornamenti in caso di cambiamenti dell'ambiente



## Gestire una politica di sicurezza delle informazioni

### Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori

Le procedure di sicurezza operativa giornaliere fungono da "istruzioni alla scrivania" che i dipendenti possono utilizzare nelle loro attività di manutenzione e amministrazione del sistema quotidiane.

Le procedure di sicurezza operativa non documentate possono determinare:

- insufficienza comprensione dello scopo delle attività;
- difficile o impropria ripetizione per i nuovi dipendenti;
- potenziali lacune nei processi con conseguenti vulnerabilità.

La sezione 12.2 richiede che siano **sviluppate procedure di sicurezza operativa giornaliere coerenti con i requisiti** di questa specifica (ad esempio, procedure per la manutenzione degli account utente e procedure di revisione dei registri).



## Gestire una politica di sicurezza delle informazioni

### Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori

In base alla politica dell'azienda, le istruzioni al personale possono sia vietare l'uso di determinati dispositivi e altre tecnologie, sia fornire una guida ad un corretto uso e implementazione. In assenza di esse, i dipendenti possono utilizzare le tecnologie in violazione delle politiche dell'azienda, consentendo agli utenti non autorizzati di accedere ai sistemi critici e ai dati dei titolari di carte.

Un esempio può essere l'impostazione inconsapevole di reti wireless prive di protezione.

La sezione 12.3 richiede che siano **sviluppate politiche per l'uso da parte dei dipendenti di tecnologie critiche** (ad esempio, tecnologie di accesso remoto, wireless, supporti elettronici rimovibili, laptop, PDA, uso della posta elettronica e di Internet) per definire l'uso corretto di queste tecnologie per tutti i dipendenti e i collaboratori esterni.



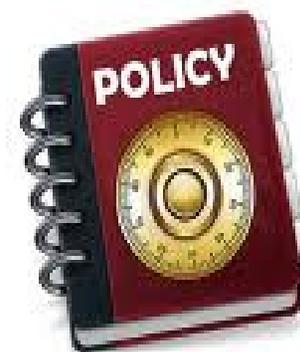
## Gestire una politica di sicurezza delle informazioni

### Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori

Nella definizione delle politiche, **la sezione 12.3 richiede che siano compresi i seguenti item:**

- 12.3.1 Approvazione esplicita del management
- 12.3.2 Autenticazione per l'uso della tecnologia
- 12.3.3 Elenco di tutti i dispositivi di questo tipo e del personale autorizzato all'accesso
- 12.3.4 Etichettatura di dispositivi con proprietario, informazioni di contatto e scopo
- 12.3.5 Usi accettabili delle tecnologie
- 12.3.6 Posizioni di rete accettabili per le tecnologie
- 12.3.7 Elenco di prodotti approvati dalla società

(segue)





## **Gestire una politica di sicurezza delle informazioni**

### **Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori**

- 12.3.8 Disconnessione automatica delle sessioni per tecnologie di accesso remoto dopo un periodo di tempo specifico di inattività
- 12.3.9 Attivazione di tecnologie di accesso remoto per fornitori solo quando necessario, con disattivazione immediata dopo l'uso
- 12.3.10 Durante l'accesso ai dati di titolari di carta tramite tecnologie di accesso remoto, vietare la copia, lo spostamento e la memorizzazione dei dati di titolari di carta su dischi rigidi locali e supporti elettronici rimovibili.



## Gestire una politica di sicurezza delle informazioni

### Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori

Senza l'assegnazione di ruoli e responsabilità di protezione chiaramente definiti, potrebbero verificarsi interazioni incoerenti con il gruppo di protezione, generando un'implementazione delle tecnologie non sicura o l'uso di tecnologie non aggiornate.

La sezione 12.4 richiede che **la politica e le procedure di sicurezza definiscano chiaramente le responsabilità in termini di protezione delle informazioni** per tutti i dipendenti e i collaboratori.





## **Gestire una politica di sicurezza delle informazioni**

### **Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori**

Ogni persona o team di gestione della sicurezza delle informazioni deve essere chiaramente consapevole delle responsabilità e delle attività correlate.

La sezione 12.5 richiede che siano considerati i seguenti item:

- 12.5.1 Definizione, documentazione e distribuzione delle politiche e delle procedure di sicurezza
- 12.5.2 Monitoraggio e analisi degli avvisi e delle informazioni sulla sicurezza e distribuzione al personale appropriato
- 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
- 12.5.4 Amministrazione di account utente, incluse aggiunte, eliminazione e modifiche
- 12.5.5 Monitoraggio e controllo di tutti gli accessi ai dati



## Gestire una politica di sicurezza delle informazioni

### Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori

Se gli utenti non sono istruiti sulle loro responsabilità di sicurezza, le misure di protezione e i processi implementati potrebbero divenire inefficaci a causa di errori o azioni intenzionali dei dipendenti.

La sezione 12.6 richiede che sia **implementato un programma formale di security awareness** per rendere tutti i dipendenti consapevoli dell'importanza della sicurezza dei dati di titolari di carta.

- 12.6.1 Formare i dipendenti al momento dell'assunzione e almeno una volta all'anno.
- 12.6.2 Richiedere ai dipendenti di certificare almeno una volta all'anno che hanno letto e compreso la politica e le procedure di sicurezza della società.





## Gestire una politica di sicurezza delle informazioni

### Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori

L'esecuzione di approfondite indagini di base prima dell'assunzione dei dipendenti che dovranno accedere ai dati dei titolari di carte riduce il rischio di uso non autorizzato dei numeri PAN e di altri dati dei titolari di carte da parte di individui con precedenti penali o discutibili.

La sezione 12.7 richiede che i **potenziali dipendenti siano sottoposti a screening prima di assumerli** per ridurre al minimo il rischio di attacchi da fonti interne.

**Nota:** Per i dipendenti che hanno accesso a un solo numero di carta alla volta, quali i cassieri di un negozio, questo requisito è solo consigliato.





## **Gestire una politica di sicurezza delle informazioni**

### **Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori**

La sezione 12.8 si applica **se un esercente o un provider di servizi condivide i dati dei titolari di carte con un provider di servizi**. In tal caso si dovranno gestire e implementare politiche e procedure che richiedano di:

- 12.8.1 Conservare un elenco dei provider di servizi.
- 12.8.2 Conservare un accordo scritto in base al quale il provider di servizi si assume la responsabilità della protezione dei dati di titolari di carta di cui entra in possesso.
- 12.8.3 Accertarsi che esista un processo definito per incaricare i provider di servizi, che includa tutte le attività di dovuta diligenza appropriate prima dell'incarico.
- 12.8.4 Conservare un programma per monitorare lo stato di conformità agli standard PCI DSS dei provider di servizi.



## Gestire una politica di sicurezza delle informazioni

### Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori

La sezione 12.9 richiede che **sia implementato un piano di risposta agli incidenti.**

E' necessario che esso sia completo e contenere tutti gli elementi importanti in modo da consentire all'azienda di rispondere in modo efficace nel caso di una violazione che influisca sui dati dei titolari di carte.

E' doveroso che tale programma sia correttamente divulgato, letto e compreso dalle parti responsabili.

(segue)





## **Gestire una politica di sicurezza delle informazioni**

### **Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori**

- 12.9.1 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 violazione, 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 violazioni
  - Copertura e risposte per tutti i componenti di sistema critici
  - Riferimenti e descrizioni delle procedure di risposta agli incidenti adottate dai marchi di pagamento



## **Gestire una politica di sicurezza delle informazioni**

### **Gestire una politica che garantisca la sicurezza delle informazioni per dipendenti e collaboratori**

- 12.9.2 Eseguire un test del piano almeno una volta all'anno.
- 12.9.3 Nominare personale specifico disponibile 24 ore al giorno, 7 giorni su 7 in caso di emergenza.
- 12.9.4 Formare in modo appropriato il personale addetto al controllo delle violazioni della sicurezza.
- 12.9.5 Includere allarmi dai sistemi di rilevamento e prevenzione delle intrusioni e dai sistemi di monitoraggio dell'integrità dei file.
- 12.9.6 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.



## **INDICE DELLA PRESENTAZIONE :**

1. Overview e ambito di applicazione
2. La struttura dello standard
3. I requisiti in dettaglio
4. **Le esigenze di mercato**
5. Riferimenti bibliografici e sitografici



## Le esigenze di mercato

**Qualsiasi persona fisica o giuridica, sia essa operatore commerciale o fornitore di servizi**, che archivi, elabori e/o trasmetta dati di titolari di carte di credito/debito, indipendentemente dalle dimensioni e dal volume di operazioni effettuate, è tenuta alla conformità ai requisiti PCI DSS.

- Tutti gli operatori commerciali che effettuano operazioni con carte di pagamento sono classificati in 4 livelli distinti, determinati dal numero delle loro operazioni annue.
- Le procedure di convalida che l'operatore commerciale è tenuto ad osservare per ottenere e mantenere la conformità sono determinate dal livello di appartenenza.





## Le esigenze di mercato

### Suddivisione in livelli degli operatori commerciali

- **Livello 1:** operatori commerciali con oltre 6 milioni di operazioni con carte di credito/debito e operatori commerciali di cui siano stati compromessi i dati dei titolari di carte di credito/debito.
- **Livello 2:** operatori commerciali con un numero di transazioni con carte di credito/debito compreso tra 1 e 6 milioni.
- **Livello 3:** operatori commerciali con un numero di transazioni con carte di credito/debito compreso tra 20.000 e 1 milione.
- **Livello 4:** tutti gli altri operatori commerciali.



## Le esigenze di mercato

Allo stesso modo, sempre al fine di determinare le procedure di convalida per l'ottenimento e il mantenimento della conformità, **tutte le aziende fornitrici di servizi** che elaborano operazioni con carte di credito sono classificate nei seguenti 3 livelli.

- **Livello 1:** tutti gli incaricati del trattamento di dati e tutti i servizi di pagamento virtuali.
- **Livello 2:** tutti i fornitori di servizi non contemplati nel Livello 1, ma con oltre 1 milione di conti o operazioni con carte di credito all'anno.
- **Livello 3:** i fornitori di servizi, non compresi nel Livello 1, con meno di 1 milione di conti od operazioni con carte di credito all'anno.



## **Le esigenze di mercato**

Per ottemperare alle norme PCI DSS, le aziende sono tenute a rispettare e dimostrare l'applicazione di tutti i requisiti indicati nelle stesse norme.

A questo scopo:

### **Operatori commerciali:**

- Per gli operatori commerciali di livello 1: controllo di sicurezza annuale in sito e scansioni trimestrali della rete. I controlli di sicurezza in sito sono eseguiti da consulenti di sicurezza qualificati (QSA - Qualified Security Assessor).
- Per gli operatori di livello 2, 3 e 4: questionario di auto-accertamento annuale e scansioni trimestrali della rete. I questionari di auto-accertamento sono compilati internamente dall'operatore commerciale. Le scansioni di rete sono eseguite da un fornitore approvato (ASV - Approved Scanning Vendor).



## Le esigenze di mercato

### Fornitori di servizi:

- Per i fornitori di servizi di livello 1 e 2: controllo di sicurezza annuale in sito e scansioni trimestrali della rete. I controlli di sicurezza in sito sono eseguiti da consulenti di sicurezza qualificati (QSA).
- Per i fornitori di servizi di livello 3: questionario di auto-accertamento annuale e scansioni trimestrali della rete. I questionari di auto-accertamento sono compilati internamente dal fornitore di servizi. Le scansioni di rete sono eseguite da un fornitore Approved Scanning Vendor (ASV).



## Le esigenze di mercato

Gli **acquirer** non sono attualmente tenuti a eseguire procedure specifiche di convalida o certificazione PCI DSS. Tuttavia, devono comunque ottemperare alle norme relative garantendo la conformità attraverso controlli interni (seguendo i criteri forniti nel questionario di auto-accertamento) oppure affidando il processo a consulenti di sicurezza qualificati (QSA).

Inoltre, tali istituzioni sono responsabili di garantire:

- la conformità alle norme PCI DSS da parte dei loro operatori commerciali;
- la conformità alle norme PCI DSS da parte di tutti i fornitori di servizi tramite i quali esse, o i loro operatori commerciali, archiviano, trasmettono o elaborano dati di carte di pagamento.



## Le esigenze di mercato

Tutti gli *acquirer* devono garantire che gli operatori commerciali e i fornitori di servizi, agli opportuni livelli, effettuino la convalida di conformità alla normativa. Nel caso di operatori commerciali con oltre 20.000 operazioni l'anno la documentazione deve essere direttamente richiesta.

Dopo la ricezione delle relazioni di conformità, gli *acquirer* sono tenuti a compilare e inviare report mensili sulla conformità alle maggiori associazioni di carte di credito/debito. Tutta la documentazione di convalida della conformità va conservata e messa a disposizione su richiesta delle suddette associazioni.



## **Le esigenze di mercato**

L'inosservanza delle norme PCI DSS comporta delle conseguenze. **Le aziende rischiano multe fino a 500.000 dollari USA e costose spese legali.** Da un punto di vista operativo, gli operatori commerciali e fornitori di servizi di livello 2, 3 o 4 che hanno subito violazioni di sicurezza della rete **possono vedere il loro livello portato al livello 1, con conseguenti effetti negativi in termini di costi**, poiché la conformità al livello 1 è più impegnativa. Inoltre, l'inosservanza produce effetti negativi sulla reputazione del marchio ed espone le società ad una forte pubblicità negativa che indebolisce la fiducia dei consumatori.

**Per ritornare al proprio livello originale, dopo lo spostamento al livello 1 a causa di una violazione di sicurezza, sono richiesti due anni:**

- il primo anno è assegnato alla correzione degli eventuali errori procedurali che hanno causato la violazione;
- il secondo anno è un periodo di transizione per assicurarsi che non siano accadute nuove violazioni di sicurezza.



## **INDICE DELLA PRESENTAZIONE :**

1. Overview e ambito di applicazione
2. La struttura dello standard
3. I requisiti in dettaglio
4. Le esigenze di mercato
5. **Riferimenti bibliografici e sitografici**



## **Bibliografia e sitografia :**

### **Risorse on line:**

Il sito del Consiglio degli standard Payment Card Industry

<https://www.pcisecuritystandards.org>

Documentazione di supporto

[https://www.pcisecuritystandards.org/tech/supporting\\_documents.htm](https://www.pcisecuritystandards.org/tech/supporting_documents.htm)

Domande sulle norme PCI DSS

<http://pcianswers.com>

Elenco esaustivo delle risorse PCI DSS

<http://pcianswers.com/resources/>

### **Altre risorse on line di interesse:**

Informazioni generali relative al Programma Account Information Security

[http://www.visaeurope.ch/it/visa\\_per\\_gli\\_esercenti/ais.jsp](http://www.visaeurope.ch/it/visa_per_gli_esercenti/ais.jsp)

Sito di riferimento per Visa

<https://partnernetwork.visa.com/>



## Altri riferimenti:

---

Card Brand

Additional Program Information

---

American Express Web:

[www.americanexpress.com/datasecurity](http://www.americanexpress.com/datasecurity)

e-mail: [American.Express.Data.Security@aexp.com](mailto:American.Express.Data.Security@aexp.com)

Discover Web:

[www.discovernetwork.com/resources/data/data\\_security.html](http://www.discovernetwork.com/resources/data/data_security.html)

e-mail: [askdatasecurity@discoverfinancial.com](mailto:askdatasecurity@discoverfinancial.com)

JCB Web:

[www.jcb-global.com/english/pci/index.html](http://www.jcb-global.com/english/pci/index.html)

e-mail: [riskmanagement@jcbati.com](mailto:riskmanagement@jcbati.com)

MasterCard Web:

[www.mastercard.com/sdp](http://www.mastercard.com/sdp)

e-mail: [sdp@mastercard.com](mailto:sdp@mastercard.com)

Visa USA Web:

[www.visa.com/cisp](http://www.visa.com/cisp)

e-mail: [cisp@visa.com](mailto:cisp@visa.com)

Visa Canada Web:

[www.visa.ca/ais](http://www.visa.ca/ais)

---



**Grazie**

Vittorio Torre  
v.torre@nexsoft.it