STANDARD DI SICUREZZA SUI DATI PREVISTI DAI CIRCUITI INTERNAZIONALI

Payment Card Industry Data Security Standard

Costruire e mantenere una "rete" sicura
Requisito 1. Installare e mantenere aggiornata la configurazione di un firewall per proteggere i dati.
Requisito 2. Non utilizzare le configurazioni standard predisposte dal fornitore relativamente al set-up delle password o di altri parametri di sicurezza.

Proteggere i dati dei Titolari di carte di credito
Requisito 3. Utilizzare meccanismi di restrizione degli accessi ai dati dei titolari memorizzati.
Requisito 4. Trattare con sistemi di cifratura (crittografia) i dati dei Titolari e le altre informazioni critiche quando queste sono trasmesse attraverso network di pubblico dominio.

Adottare e mantenere un sistema strutturato di rilevazione e gestione delle vulnerabilità informatiche
Requisito 5. Utilizzare e aggiornare regolarmente software anti-virus.
Requisito 6. Sviluppare e mantenere sistemi e applicazioni sicuri.

Implementare procedure di controllo per l'accesso ai dati
Requisito 7. Restringere l'accesso ai dati al personale autorizzato normalmente alla sua gestione.
Requisito 8. Assegnare un ID unico e personale a ciascun soggetto che abbia accesso al sistema.
Requisito 9. Garantire che l'accesso fisico ai dati dei Titolari sia limitato ai soli soggetti autorizzati nelle modalità previste.

Monitorare e testare regolarmente i Network
Requisito 10. Tracciare e monitorare tutti gli accessi alle risorse di rete ed ai dati dei Titolari.
Requisito 11. Testare regolarmente i sistemi e i processi di sicurezza.

Mantenere una politica di informazione sulla sicurezza
Requisito 12. Mantenere una politica che diffonda informazioni sulla sicurezza.

Si noti che il "Payment Card Industry (PCI) Data Security Requirement" si applica a tutti i membri, gli esercenti e i fornitori di servizi che conservano, processano o trasmettono dati dei Titolari di carta di credito. In aggiunta, tali requisiti sulla sicurezza si applicano a tutte le componenti del sistema, definite come tutte le componenti di rete, server o applicazioni che contengono o sono in connessione con i dati dei Titolari. Le componenti di rete includono, anche se non limitatamente, firewall, switches, Router, punti di accesso wireless, strumenti di rete e altri strumenti sulla sicurezza. I server includono, ma non limitatamente, web, database, autenticazione, DNS, mail, proxy e NTP. Le applicazioni includono sia quelle acquistate esternamente, sia quelle sviluppate internamente, incluse le applicazioni web sia ad uso interno sia perimetrali (ad accesso esterno).

STANDARD DI SICUREZZA SUI DATI PREVISTI DAI CIRCUITI INTERNAZIONALI

Costruire e mantenere una "rete" sicura

Requisito 1: Installare e mantenere un firewall per proteggere i dati

I firewall sono dispositivi installati nei computer per controllare sia il traffico di dati indirizzati dall'esterno verso l'interno di un network aziendale, sia il traffico di dati indirizzati dall'interno verso le aree più sensibili del network aziendale. Tutti i sistemi, siano sistemi per il commercio elettronico o per l'accesso ai dati sul desktop o nelle e-mail del personale, necessitano di essere protetti da accessi non autorizzati provenienti da Internet. Spesso, scambi apparentemente insignificanti a/da Internet, possono creare passaggi non protetti in sistemi chiave. I firewall sono meccanismi di protezione fondamentali per qualsiasi rete di computer.

1.1. Costruire una **configurazione standard del firewall** che includa:

1.1.1. Un processo formale per approvare e testare tutte le connessioni a network esterni al sistema e i cambiamenti alla struttura del firewall.

1.1.2. Un diagramma aggiornato del network con tutte le connessioni ai dati dei titolari di carta di credito, comprese tutte le connessioni wireless.

1.1.3. Requisiti per un controllo effettuato dal firewall su ogni connessione a Internet e tra ogni DMZ e la Intranet.

1.1.4. Descrizione dei gruppi, dei ruoli e delle responsabilità per la gestione logica delle componenti del network.

1.1.5. Liste formali dei servizi e delle porte necessari per il business.

1.1.6. Giustificazione e documentazione per ogni protocollo disponibile oltre a HTTP e SSL, SSH e VPN.

1.1.7. Giustificazione e documentazione per ogni protocollo di rischio consentito (FTP, ecc.), che includa i motivi dell'utilizzo del protocollo e le funzioni di sicurezza implementate.

1.1.8. Periodica revisione dell'insieme di regole del firewall/router.

1.1.9. Configurazione degli standard per i router.

1.2. Costruire un **firewall che rifiuti tutti i messaggi provenienti da network/host non sicuri**, ad eccezione per:

1.2.1. Protocolli web - HTTP (porta 80) e Secure Sockets Layer (SSL) (tipicamente porta 443).

1.2.2. Protocolli di amministrazione di sistema - Secure Shell (SSH) o Virtual Private network (VPN).

1.2.3. Altri protocolli richiesti dal business (ISO 8583).

1.3. Configurare il firewall in modo da **limitare le connessioni tra server accessibili pubblicamente e le componenti del sistema che conservano i dati dei Titolari**, incluse tutte le connessioni con reti wireless.
Tale configurazione dovrebbe includere:

1.3.1. Restrizione del traffico Internet in entrata agli indirizzi IP con il DMZ (filtri di ingresso).

1.3.2. Restrizione del traffico Internet in entrata e in uscita alle porte 80 e 443.

1.3.3. Negazione della possibilità per gli indirizzi interni di passare da Internet nel DMZ (filtri di uscita).

1.3.4. Nella rete devono essere consentite unicamente connessioni autorizzate. Si consigliano le tecniche firewalling di tipo Statefull inspection o dynamic packed filtering.

1.3.5. Posizionamento del database in una zona interna del network, separata dal DMZ.

1.3.6. Restrizione del traffico in uscita esclusivamente a ciò che è necessario per il pagamento con carta.

1.3.7. Rendere sicura e sincronizzata la gestione dei diversi file di configurazione del router (e.g. i files di configurazione di funzionamento running - configuration files - e i file di configurazione di start-up-rebooting files - devono avere le stesse configurazioni di sicurezza).

1.3.8. Rifiuto di tutto il restante traffico in entrata e in uscita non specificatamente consentito.

1.3.9. Installazione di firewall perimetrali tra tutte le reti wireless e l'ambiente di pagamento e loro configurazione per rifiutare o controllare (se tale traffico è necessario per gli scopi del business) tutte le connessioni da ambiente wireless.

1.3.10. Installazione di software wireless personali su tutti i computer portatili e/o di proprietà del personale con connessione diretta a Internet (es. laptop usati dai dipendenti) e utilizzati per accedere alla rete aziendale.

1.4. **Proibire accessi pubblici diretti** tra i network esterni e le componenti del sistema che conservano informazioni sui Titolari di carta (es. database).

1.4.1. Implementare un DMZ per filtrare e monitorare il traffico al fine di proibire collegamenti diretti per il traffico Internet in entrata e in uscita.

1.4.2. Restringere agli indirizzi IP con DMZ il traffico in uscita proveniente dalle applicazioni per il pagamento con carta.

1.5. **Implementare protocolli Internet (IP) finalizzati a mascherare gli indirizzi interni** in modo che non vengano visualizzati sulla rete Internet. Utilizzare tecnologie che implementino uno spazio RFC 1918, come Port Address Translation (PAT) o Network Address Translation (NAT).

Requisito 2: Non utilizzare sistemi di password o altri parametri di sicurezza definiti di default dal fornitore

Gli hacker (interni o esterni a un'azienda) spesso utilizzano password o altri elementi definiti di default dal fornitore per compromettere il sistema. Tali elementi sono ben conosciuti dagli hacker e facilmente determinabili attraverso informazioni di dominio pubblico.

2.1. **Cambiare sempre le opzioni predefinite dal fornitore** prima di installare un sistema in rete (ad esempio password, SNMP community string ed eliminazione di account non necessari).

2.1.1. Per gli ambienti wireless, cambiare le configurazioni di default del fornitore, includendo chiavi WEP, opzioni predefinite SSID, password e SNMP community string e disattivando le trasmissioni SSID. Attivare la tecnologia Wi-Fi Protected access (WPA) per la criptatura e l'autenticazione nel caso di WPA attivo

2.2. Sviluppare **configurazioni standard** per tutte le componenti di sistema. Assicurarsi che tali standard gestiscano tutte le vulnerabilità conosciute e seguano le best practice del sistema.

2.2.1. Implementare solamente una funzione base per server (web server, database server e DNS dovrebbero essere implementati su server separati)

2.2.2. Disattivare tutti i servizi e i protocolli non necessari e non sicuri (servizi e protocolli non direttamente necessari per gestire la specifica funzione del dispositivo)

2.2.3. Configurare parametri di sicurezza per impedire abusi

2.2.4. Eliminare tutte le funzioni non necessarie, come script, driver, feature, sottosistemi, file di sistema (ad esempio server web non necessari)

2.3. Gli accessi da remoto devono avvenire su **connessioni cifrate**. Utilizzare tecnologie di tipo SSH, VPN o SSL/TLS per la gestione tramite applicazione web-based e tutte le altre forme di accesso di tipo amministrativo non da consolle.

Proteggere i dati dei Titolari di carta di credito

Requisito 3: Proteggere i dati memorizzati

La criptatura è l'ultimo meccanismo di protezione, in quanto anche se qualcuno riuscisse a penetrare attraverso tutti gli altri dispositivi di difesa e ad accedere ai dati criptati, non sarebbe in grado di leggerli se non decifrando la chiave di criptatura. Di seguito si illustrano i principi fondamentali di tale meccanismo di protezione.

3.1. Minimizzare il numero di informazioni memorizzate relative ai Titolari di carta. Sviluppare una politica di **mantenimento e smaltimento dei dati**. Limitare l'ampiezza della memoria ed il periodo di conservazione dei dati sulla base dei tempi necessari per gli scopi di business, legali e/o di regolamento, come formalizzato nella politica di mantenimento dei dati.

3.2. **Non conservare dati che consentano di autenticare il Titolare** successivamente alla richiesta di autorizzazione (nemmeno se criptati).

3.2.1. Non conservare l'intero contenuto di qualunque dato presente sulla banda magnetica (sul retro della carta o nel chip).

3.2.2. Non conservare il codice di validazione della carta (codice a tre o quattro cifre stampato sul fronte o sul retro della carta di pagamento (CVV2 e CVC2).

3.2.3. Non conservare il PIN (PVV).

3.2.3. Configurare parametri di sicurezza per impedire abusi.

3.2.4. Eliminare tutte le funzioni non necessarie, come script, driver, feature, sottosistemi, file di sistema (ad esempio server web non necessari).

3.3. **Mascherare i numeri** digitati quando visualizzati su display (sono visualizzabili al massimo le prime 6 e le ultime 4 cifre della carta). Si noti che ciò non si applica per i dipendenti che necessitano di vedere tutti i numeri di carta di credito.

3.4. Rendere **illeggibili i dati sensibili** dei Titolari ovunque siano conservati (compresi i dati su supporti mobili, su supporti di riserva e in logs e i dati ricevuti o conservati da reti wireless) utilizzando uno dei seguenti sistemi:

- Hashe unidirezionale, come SHA-1.
- Troncamento.
- Indice token e PADs, con il PADs conservato in modo sicuro.
- Criptografia avanzata, come Triple-DES 128-bit o AES 256-bit associata a processi e procedure chiave di gestione Come minimo deve essere reso illeggibile il numero della carta di credito.

3.5. Proteggere le **chiavi di criptatura** da tentativi di decifrazione e abusi.

3.5.1. Restringere l'accesso alle chiavi al minor numero di persone necessario.

3.5.2. Conservare le chiavi in modo sicuro nel minor numero di forme e luoghi.

3.6. **Documentare e implementare** tutti i processi e le procedure chiave di gestione, compreso:

3.6.1. Generazione di chiavi forti (eg. 3D).

3.6.2. Distribuzione delle chiavi in modo sicuro.

3.6.3. Conservazione delle chiavi in modo sicuro.

3.6.4. Modifica periodica delle chiavi.

3.6.5. Distruzione delle vecchie chiavi.

3.6.6. Suddivisione della conoscenza e doppio controllo delle chiavi (in questo modo, per ricostruire l'intera chiave sono necessarie 2 o 3 persone, ciascuna a conoscenza solamente della propria parte).

STANDARD DI SICUREZZA SUI DATI PREVISTI DAI CIRCUITI INTERNAZIONALI

3.6.7 Prevenzione da sostituzioni non autorizzate delle chiavi.
3.6.8 Sostituzione di chiavi conosciute o che si sospetta compromesse.
3.6.9 Revoca di chiavi vecchie o non valide (principalmente per le chiavi RSA).
3.6.10 Firma di un format da parte delle persone che custodiscono le chiavi in cui vengono accettate le proprie responsabilità.

Requisito 4: Criptare i dati dei Titolari e le informazioni sensibili quando trasmessi attraverso network di pubblico dominio
Le informazioni sensibili devono essere criptate durante la trasmissione in Internet, in quanto è semplice per un hacker intercettare i dati durante il transito.

4.1. Usare **tecniche di criptografia** (almeno 128 bit), come Secure Socket Layer (SSL), Point-to-point Tunnelling Protocol (PPTP), Internet Protocol Security (IPSEC) per salvaguardare i dati sensibili dei Titolari durante la trasmissione attraverso network di pubblico dominio.
4.1.1. Per i network wireless che trasmettono i dati dei Titolari, criptare la trasmissione utilizzando la tecnologia Wi-Fi Protected Access (WPA) in caso di WPA attivo, o VPN o SSL a 128 bit. Non contare mai esclusivamente sul WEP per proteggere dati confidenziali e accessi a una wireless LAN. Utilizzare una delle suddette tecnologie insieme a WEP a 128 bit, e alternare le chiavi WEP condivise trimestralmente e ogniqualvolta vi è un cambio del personale.
4.2. Non inviare mai informazioni sui Titolari attraverso **e-mail non criptate**.

Mantenere un programma di gestione della sicurezza

Requisito 5: Utilizzare e aggiornare regolarmente i software anti-virus
Molti virus entrano nella rete attraverso le e-mail del personale. I software anti-virus devono essere utilizzati in tutti i sistemi di e-mail al fine di proteggere la rete da software che potrebbero danneggiarla.

5.1. Utilizzare meccanismi anti-virus su tutti i sistemi comunemente attaccati (PC e server).
5.2. Assicurarsi che tutti i meccanismi anti-virus siano aggiornati, correttamente funzionanti e in grado di generare una verifica dei log.

Requisito 6: Sviluppare e mantenere sistemi e applicazioni sicuri
La presenza di vulnerabilità nei sistemi di sicurezza può essere sfruttata in modo illegale. Molte di queste vulnerabilità sono eliminate attraverso specifiche componenti (patches) aggiuntive che possono essere richieste ai fornitori (in alcuni casi tali aggiornamenti sono automatici). Tutti i sistemi dovrebbero avere software aggiornati per proteggersi contro abusi da parte del personale, di hacker esterni e di virus. Relativamente alle applicazioni sviluppate internamente, molte vulnerabilità possono essere eliminate attraverso la standardizzazione dei processi di sviluppo dei sistemi e mediante l'uso di tecniche di scrittura che garantiscano la generazione di un codice sicuro.

6.1. Assicurarsi che tutte le componenti e i software di sistema abbiano l'**ultima versione dei programmi** (con aggiornamenti dei patches di sicurezza).
6.1.1. Installare le patches non più tardi di un mese dalla data del loro rilascio da parte del fornitore.
6.2 Implementare un processo per **aggiornare il catalogo delle vulnerabilità** (iscriversi ai servizi di allerting disponibili gratuitamente su Internet). Aggiornare i propri standard per gestire le vulnerabilità emergenti.
6.3. Sviluppare programmi basati sulle **best practices del sistema** ed includere la sicurezza delle informazioni in tutto il ciclo di vita di **sviluppo del software**. Includere i seguenti elementi:
6.3.1. Test di tutte le modifiche di programmi, patches, sistemi e software prima del passaggio all'ambiente di produzione.
6.3.2. Separazione degli ambienti di sviluppo e test da quelli di produzione.
6.3.3. Differenziazione dei diritti di accesso ai dati negli ambienti di sviluppo e produzione.
6.3.4. Divieto di utilizzo di dati di produzione nell'ambiente di sviluppo (i numeri reali di carte di credito non devono essere utilizzati per testare o sviluppare il sistema).
6.3.5. Rimozione dei dati di test prima che i sistemi di produzione diventino attivi.
6.3.6. Rimozione dei dati, delle username e delle password personalizzate prima che le applicazioni diventino attive e vengano rilasciate ai clienti.
6.3.7. Revisione del codice personalizzato prima del rilascio in produzione o ai clienti, al fine di individuare ogni possibile vulnerabilità.
6.4. Seguire delle **procedure di controllo** per tutte le modifiche effettuate a sistemi o software. Le procedure dovrebbero includere:
6.4.1. Documentazione dell'impatto.
6.4.2. Gestione del processo di rilascio delle autorizzazioni a procedere da parte dei soggetti autorizzati.
6.4.3. Test per verificare le funzioni operative.
6.4.4. Procedure di back out.
6.5. Sviluppare applicazioni e software basati su linee guida di **codifica sicura**, come le linee guida "Open Web Application Security Project". Verificare il codice personalizzato per **identificare eventuali vulnerabilità** generatisi nel processo di programmazione. Fare riferimento, sul sito www.owasp.org , alle "Ten Most Critical Web Application Security Vulnerabilietes". Prevenire le più comuni vulnerabilità nei processi di sviluppo del software, inclusi:
6.5.1. Mancata validazione dell'input.
6.5.2. Malfunzionamento del controllo accessi (utilizzo malevolo di una utenza accreditata).
6.5.3. Broken authentication/session management (utilizzo di credenziali e cookies di sessione).
6.5.4. Cross site scripting (XSS).
6.5.5. Buffer overflows.
6.5.6. Injection flows (e.g. SQL injection).
6.5.7. Inadeguata gestione degli errori.
6.5.8. Mancata protezione della base dati.
6.5.9. Denial of service.
6.5.10. Configurazione dell'ambiente non sicura.

Implementare meccanismi "forti" di restrizione e controllo degli accessi

Requisito 7: Restringere l'accesso ai dati al personale sulla base del privilegio minimo (need-to-know)
In questo modo si può accedere ai dati critici solamente in una modalità autorizzata.

7.1. **Limitare l'accesso alle informazioni sui Titolari** solamente al personale le cui mansioni lo richiedono.
7.2. Adottare meccanismi che restringano l'accesso ai dati sulla base del principio del **need to know**, in tal modo ciascun operatore dovrà avere la possibilità di vedere solo i dati sui quali è autorizzato ad operare in funzione delle sue mansioni. Sui medesimi dati, i soggetti non autorizzati, in quanto la loro mansione non richiede l'uso del dato in oggetto, non potranno accedere.

Requisito 8: Restringere l'accesso ai dati al personale sulla base del privilegio minimo (need-to-know)
Questo assicura che le operazioni sui dati sensibili siano effettuate da utilizzatori conosciuti e autorizzati, di cui è possibile tenere una traccia.

8.1. Identificare tutti gli utenti attraverso una **username personale** prima di consentire l'accesso alle componenti di sistema o ai dati dei Titolari.
8.2. Utilizzare **almeno uno** dei seguenti sistemi, in aggiunta all'identificazione personale, per autenticare tutti gli utenti:
- Password.
- Token (ad esempio SecureID, certificati, o chiavi pubbliche).
- Metodi biometrici.

8.3. Implementare **due elementi di autenticazione** per gli accessi remoti al network da parte del personale, degli amministratori e di terze parti. Utilizzare tecnologie come RADIUS o TACACS con token, o VPN con certificati individuali.
8.4. **Criptare tutte le password** durante la trasmissione e l'autenticazione, su tutte le componenti del sistema.
8.5. Assicurare un'**appropriata autenticazione dell'utente** e la gestione delle password per gli utenti non utilizzatori dei dati e per gli amministratori su tutte le componenti del sistema.
8.5.1 Controllare l'aggiunta, la cancellazione, e la modifica degli user IDs, delle credenziali e di altri elementi identificativi.
8.5.2 Verificare l'identità dell'utente prima di resettare le password.
8.5.3 Per il primo accesso stabilire una password specifica per ogni utente e chiedere di cambiarla immediatamente dopo il primo utilizzo.
8.5.4 Revocare immediatamente l'accesso agli utenti che hanno concluso il rapporto di lavoro.
8.5.5 Rimuovere i contatti degli utenti inattivi almeno ogni 90 giorni.
8.5.6 Attivare i contatti utilizzati dai venditori per la manutenzione remota solamente per il tempo necessario.
8.5.7 Distribuire le procedure per le password a tutti gli utenti che hanno accesso alle informazioni sui Titolari.
8.5.8 Non utilizzare gruppi, condivisioni o password generiche.
8.5.9 Cambiare password almeno ogni 90 giorni.
8.5.10 Richiedere una lunghezza minima della password di almeno 7 caratteri.
8.5.11 Utilizzare password contenenti sia caratteri alfabetici che numerici.
8.5.12 Non permettere all'utente di inserire una nuova password che sia uguale ad una delle ultime quattro password utilizzate.
8.5.13 Limitare i tentativi ripetuti di accesso bloccando l'user ID dopo non più di sei tentativi.
8.5.14 Fissare la lunghezza del blocco a 30 minuti o fino a quando un addetto riattivi la user ID.
8.5.15 Se una sessione è inattiva per più di 15 minuti, chiedere all'utente di reinserire la password e riattivare il terminale.

STANDARD DI SICUREZZA SUI DATI PREVISTI DAI CIRCUITI INTERNAZIONALI

8.5.16 Autenticare tutti gli accessi ad ogni database contenente informazioni sui Titolari. Questo include gli accessi applicativi da tools di amministrazione e da qualunque punto di accesso disponibile.

Requisito 9: Restringere l'accesso fisico ai dati del titolare

Ogni accesso fisico ai sistemi che contengono i dati dei Titolari dà l'opportunità di accedere ai dati e rimuovere sistemi o copie fisiche e dovrebbe essere adeguatamente ristretto.

9.1. Effettuare adeguati controlli per limitare e **monitorare l'accesso fisico** ai sistemi che conservano, processano o trasmettono dati dei Titolari.

9.1.1. Utilizzare videocamere per monitorare le aree sensibili. Controllare i dati così raccolti e compararli con altre aree di accesso.

9.1.2. Restringere l'accesso fisico alle prese\connessioni di rete accessibili pubblicamente.

9.1.3. Restringere l'accesso fisico ai punti di accesso wireless, ai gateway ed ai dispositivi manuali.

9.1.4. Revocare immediatamente l'accesso agli utenti che hanno concluso il rapporto di lavoro.

9.2. Sviluppare procedure che aiutino tutto il personale a **distinguere tra dipendenti e visitatori**, specialmente nelle aree dove i dati sui Titolari sono accessibili.
Per dipendenti si intendono il personale full time, part time e temporaneo e i consulenti che lavorano permanentemente nell'organizzazione. Per visitatori si intendono invece i fornitori, gli ospiti dei dipendenti, il personale di servizio o chiunque abbia bisogno di entrare nell'area di conservazione dei dati per una breve durata, generalmente non più di un giorno.

9.3. Assicurarsi che tutti i visitatori:

9.3.1. Siano autorizzati prima di entrate nelle aree dove i dati dei titolari sono processati o conservati.

9.3.2. Abbiano ricevuto un supporto fisico (ad esempio un badge o un dispositivo di accesso) che scada e che li identifichi come non dipendenti.

9.3.3. Restituiscano il supporto fisico prima di lasciare l'area o alla data di scadenza.

9.4. Utilizzare un log per **tracciare l'attività dei visitatori**. Tenere tale log per un minimo di tre mesi, a meno di diverse indicazioni stabilite dalla legge.

9.5. Conservare i **supporti che contengono i back-up** in un sito diverso da quello in cui si trova il sistema di produzione, ad esempio usando dei servizi di housing messi a disposizione dalle società specializzate in gestione dei siti alternativi.

9.6. Rendere fisicamente **sicuri tutti i supporti cartacei ed elettronici** (computer, supporti elettronici, hardware, linee di telecomunicazione, fatture cartacee, report cartacei e fax) che contengono informazioni sui Titolari.

9.7. Mantenere uno stretto **controllo sulla distribuzione** interna o esterna di ogni genere di supporto contenente informazioni sui Titolari.

9.7.1. Etichettare il supporto in modo che possa essere identificato come riservato.

9.7.2. Inviare il supporto attraverso corrieri sicuri o un meccanismo di spedizione che possa essere accuratamente tracciato.

9.8. Assicurarsi che il management approvi tutti gli **spostamenti dei supporti** da un'area sicura (soprattutto quando i supporti sono consegnati a persone).

9.9. Mantenere uno stretto **controllo sulla conservazione e l'accessibilità** dei supporti che contengono informazioni sui Titolari:

9.9.1. Tenere un inventario di tutti i supporti ed assicurarsi che sia conservato in modo sicuro.

9.10. Distruggere i supporti contenenti informazioni sui Titolari quando non sono più necessarie per il business o per motivi legali:

9.10.1. Stracciare o incenerire le copie materiali.

9.10.2. Smagnetizzare, fare a pezzi o distruggere in altri modi i supporti elettronici in modo che i dati dei titolari non possano essere ricostruiti.

Monitorare e testare regolarmente i Network

Requisito 10: Tracciare e monitorare tutti gli accessi alle risorse di rete e ai dati dei Titolari

I meccanismi di riconoscimento e di monitoraggio delle attività degli utenti sono fondamentali. La presenza di elementi di riconoscimento in tutte le aree permette di tracciare e analizzare gli eventuali problemi. Determinare la causa di una disfunzione è molto difficile senza sistemi di riconoscimento.

10.1. Tracciare gli accessi in modo tale che tutti gli accessi ai componenti del sistema siano **riconducibili alle utenze** riconosciute e assegnate individualmente al personale autorizzato.

10.2. Implementare **meccanismi automatici di Audit trails** in modo tale che, per ogni componente del sistema, i seguenti eventi siano ricostruibili:

10.2.1. Tutti gli accessi di un utente ai dati dei titolari.

10.2.2. Tutte le azioni effettuate da utenze con privilegi di amministratore o di root.

10.2.3. Accesso a tutti i tracciati di controllo e di audit.

10.2.4 Tentativi di accesso non validi

10.2.5 Utilizzo di meccanismi di identificazione e autenticazione

10.2.6 Cancellazione o reimpostazione dei parametri e dei files di log

10.2.7 Creazione e cancellazione di elementi a livello di sistema

10.3 Per ogni evento, su ogni componente del sistema, **registrare almeno i seguenti elementi**:

10.3.1 Identificazione dell'utente

10.3.2 Tipo dell'operazione/evento

10.3.3 Data e ora

10.3.4 Indicazione dell'esito dell'operazione (eseguita, interrotta, non avviata, fallita ecc..)

10.3.5 Origine dell'operazione (causa dell'evenento es: nome del programma che ha richiesto l'accesso, codice dell'abend ecc..)

10.3.6 Codice identificativo della componente del sistema che è stata oggetto dell'evento (dato, applicazione, utente, ambiente ecc..)

10.4 Sincronizzare tutte le clocks dei sistemi.

10.5 Proteggere i file di log e di audit in modo che non possano essere alterati.

10.5.1 Limitare l'accesso ai tracciati di controllo a coloro le cui mansioni lo richiedono

10.5.2 Proteggere i file contenenti i tracciati di controllo da modifiche non autorizzate

10.5.3 Effettuare immediatamente una copia di riserva dei file contenenti i tracciati di controllo su un server centralizzato o su supporti difficili da alterare

10.5.4 Copiare gli elementi di riconoscimento per una rete wireless su un server nella LAN interna

10.5.5 Utilizzare software di rilevamento di modifiche non autorizzate (es.Tripwire) effettuate sui file di log e di audit, in modo tale che qualunque intervento su questi file origini un segnale di allarme.

10.6 Analizzare almeno giornalmente **i log per tutte le componenti del sistema**. La revisione dei log dovrebbe includere quei server che svolgono funzioni di sicurezza come IDS e server di autenticazione (AAA) (ad esempio RADIUS).

10.7 Tenere la **memoria dei tracciati di controllo** per un periodo coerente con le necessità di utilizzo e le regole imposte dalla legge.
Una memoria dei tracciati di controllo generalmente copre un periodo di almeno un anno,con un minimo di tre mesi di disponibilità on line.

Requisito 11: Testare regolarmente i sistemi e i processi di sicurezza

Nuove vulnerabilità sono continuamente scoperte da hacker e ricercatori e introdotte da nuovi software. I sistemi, i processi e i software personali dovrebbero essere testati frequentemente per assicurarsi che sia mantenuta la sicurezza nel tempo e successivamente a eventuali modifiche.

11.1. Testare i sistemi di **controllo della sicurezza**, le limitazioni, le connessioni di rete e le restrizioni periodicamente, in modo da assicurarsi che siano in grado di **identificare e bloccare adeguatamente qualsiasi tentativo di accesso non autorizzato**. Quando è utilizzata una tecnologia wireless, utilizzare periodicamente un analizzatore wireless, in modo da identificare tutti i dispositivi wireless in uso.

11.2. Effettuare una scansione delle **vulnerabilità dei network interni ed esterni** almeno trimestralmente e dopo ogni significativo cambiamento nella rete (ad esempio installazione di nuove componenti di sistema, modifiche nella topologia del network, modifiche nelle regole del firewall, upgrade di prodotto). Si noti che la scansione di vulnerabilità esterne deve essere effettuata da un fornitore abilitato dal settore delle carte di pagamento.

11.3. Effettuare **test approfonditi sulle infrastrutture e le applicazioni del network** almeno una volta all'anno e dopo ogni significativo miglioramento o modifica dell'infrastruttura o delle applicazioni (ad esempio upgrade dei sistemi operativi, aggiunta di sottonetwork, aggiunta di web server).

11.4. Utilizzare **sistemi di rilevamento** di intrusioni nel network, sistemi di rilevamento di intrusioni sul server e/o sistemi di rilevamento di intrusioni per monitorare tutto il traffico della rete e avvisare il personale in caso di sospette intromissioni. Conservare tutti i meccanismi di rilevamento e prevenzione delle intrusioni aggiornati.

11.5. Implementare un monitoraggio dell'**integrità dei file** per avvisare il personale di modifiche non autorizzate dei sistemi critici o del contenuto dei file ed effettuare confronti dei file critici almeno giornalmente (o più frequentemente se il processo può essere automatizzato).
I file critici non sono necessariamente quelli contenenti dati dei Titolari. Per gli scopi di monitoraggio dell'integrità dei file, i file critici sono quelli che non vengono regolarmente modificati ma la cui modifica potrebbe indicare un **danneggiamento del sistema o il rischio di un danneggiamento**. I prodotti di monitoraggio dell'integrità dei file generalmente vengono preconfigurati con file critici per il relativo sistema operativo. Altri file critici, come quelli per le applicazioni personali, devono essere valutate e definite dall'esercente o dal fornitore del server.

STANDARD DI SICUREZZA SUI DATI PREVISTI DAI CIRCUITI INTERNAZIONALI

Mantenere una politica di informazione sulla sicurezza

Requisito 12: Adottare una politica che diffonda informazioni sulla sicurezza

Un'adeguata politica sulla sicurezza diffonde i propri principi all'interno dell'intera azienda e si preoccupa di far sapere ai dipendenti che cosa ci si aspetta da loro. Tutto il personale dovrebbe essere consapevole della sensibilità dei dati e delle loro responsabilità per proteggerli.

12.1. Costruire, pubblicizzare, mantenere e diffondere una **politica sulla sicurezza.**

12.1.1. Diffondere tutte le regole contenute in questo documento.

12.1.2. Implementare un processo su base annuale che identifichi minacce, vulnerabilità e risultati in un documento formale sulla valutazione del rischio.

12.1.3. Stabilire una revisione del documento almeno una volta all'anno e aggiornarlo quando vi sono dei cambiamenti.

12.2. Sviluppare **procedure operative** giornaliere sulla sicurezza in base alle regole contenute in questo documento (ad esempio procedure di manutenzione sull'account dell'utente, procedure di revisione dei log).

12.3. Sviluppare politiche di utilizzo per particolari tecnologie di interfaccia utente, come modem e wireless, in modo da definirne un **utilizzo appropriato** per tutto il personale. Assicurarsi che queste politiche richiedano:

12.3.1. Approvazione esplicita del management.

12.3.2. Autenticazione per l'utilizzo della tecnologia.

12.3.3. Una lista di tutti i dispositivi e del personale con accesso.

12.3.4. Etichettatura dei dispositivi con l'indicazione del proprietario e dei suoi riferimenti.

12.3.5. Utilizzi consentiti per tipo di tecnologia (es. uso del pc portatile).

12.3.6. Limitazioni logistiche all'uso della tecnologia mobile e regole di networking e accessibilità (es. uso del pc portatile in connessione wireless fuori sede)

12.3.7. Una lista dei prodotti accettati dall'azienda.

12.3.8. Disconnessione automatica dei modem dopo un determinato periodo di inattività.

12.3.9. Attivazione dei modem per gli esercenti solamente quando ne hanno bisogno, con immediata disattivazione dopo l'utilizzo.

12.3.10. Durante l'accesso remoto via modem ai dati dei Titolari, disattivare la memoria contenente i dati sui drive locali, sui floppy disk o su altri supporti esterni. Disattivare anche le funzioni di stampa e di taglia, copia e incolla durante gli accessi remoti.

12.4. Assicurarsi che le procedure e le **politiche di sicurezza** definiscano chiaramente le **responsabilità in merito alla sicurezza** delle informazioni per tutto il personale.

12.5. Assegnare a una persona o a un gruppo le seguenti responsabilità in merito **alla gestione della sicurezza** delle informazioni:

12.5.1. Definire, formalizzare e diffondere procedure e politiche sulla sicurezza.

12.5.2. Monitorare e analizzare informazioni e allarmi sulla sicurezza e comunicarli al personale competente.

12.5.3. Definire, formalizzare e diffondere procedure di reazione ad incidenti sulla sicurezza per assicurare una puntuale ed efficace gestione di tutte le situazioni.

12.5.4. Amministrare gli account degli utenti, incluse aggiunte, cancellazioni e modifiche.

12.5.5. Monitorare e controllare tutti gli accessi ai dati.

12.6. Rendere tutto il personale consapevole dell'**importanza della sicurezza** delle informazioni sui Titolari.

12.6.1. Educare il personale (ad esempio con poster, lettere, memo, riunioni e promozioni).

12.6.2. Chiedere ai dipendenti di sottoscrivere una dichiarazione in cui dichiarano di aver letto e compreso le procedure e le politiche dell'azienda sulla sicurezza.

12.7. Controllare i dipendenti con accesso ai dati per **minimizzare il rischio di abusi** da parte delle risorse interne. Per quei dipendenti che hanno accesso ai dati di una carta solo per il tempo di effettuare la transazione, come i commessi dei negozi, è solamente una raccomandazione.

12.8. Chiedere contrattualmente ai soggetti esterni con accesso ai dati dei Titolari di aderire ai **"Payment card industry security requirements"**. Come minimo, il contratto dovrebbe contenere le seguenti indicazioni:

12.8.1. Consapevolezza che il soggetto esterno è responsabile per la sicurezza dei dati dei Titolari in suo possesso.

12.8.2. Possesso da parte di ciascun brand di carte di pagamento, Acquirer ed esercente dei dati dei Titolari e consapevolezza che tali dati possono essere utilizzati esclusivamente per completare una transazione, supportare un programma di fedeltà, aiutare i servizi di controllo delle frodi o per altri usi specificatamente richiesti dalla legge.

12.8.3. Continuazione del business in caso di grandi distruzioni, disastri e fallimenti.

12.8.4. Condizioni legali che assicurino che a un rappresentante del "Payment Card Industry" o a un soggetto esterno da esso approvato, vengano forniti piena collaborazione e libero accesso per effettuare una revisione sulla sicurezza dopo un'eventuale intrusione. La revisione convaliderà l'adesione al "Payment Card Industry Data Security Standard" per proteggere i dati dei Titolari.

12.8.5. Condizioni relative al termine del contratto che assicurino che la terza parte continuerà a trattare i dati sui Titolari come confidenziali.

12.9. Definire un piano di **reazione agli ad eventuali incidenti**. Essere preparati a rispondere immediatamente ad un'eventuale violazione del sistema.

12.9.1. Creare un piano di reazione da usare nel caso in cui il sistema di sicurezza venga compromesso. Assicurarsi che il piano includa, come minimo, specifiche procedure di reazione, procedure di protezione e continuazione del business, processi di copia dei dati, ruoli e responsabilità, strategie di comunicazione (ad esempio informare gli acquirer e le associazioni sulle carte di credito).

12.9.2. Testare il piano almeno annualmente.

12.9.3. Designare determinati dipendenti ad essere disponibili in ogni momento per rispondere agli allarmi.

12.9.4. Garantire un'adeguata formazione ai dipendenti con responsabilità di risposta alle violazioni sulla sicurezza.

12.9.5. Includere allarmi per il rilevamento e la prevenzione delle intrusioni e sistemi di monitoraggio dell'integrità dei file.

12.9.6. Disporre di un processo che consenta di adeguare il modello di reazione\ gestione degli incidenti informatici in base alla storia registrata in azienda e acquisendo le best practices di settore.