




METODOLOGIA DEL SERVIZIO PCI DSS

**Standard di sicurezza dei dati del settore
delle carte di pagamento.**

INTRODUZIONE PCI DSS



TOPCertifier presenta una lista di controllo semplificata per l'analisi delle lacune PCI DSS per aiutarti a identificare aree in cui la tua organizzazione potrebbe aver bisogno di miglioramenti per conformarsi allo standard PCI DSS (Payment requisiti dello standard di sicurezza dei dati del settore delle carte). Questa lista di controllo offre un fondamentale framework per valutare l'allineamento con PCI DSS e funge da passo iniziale valutare la tua conformità.

SEZIONE 1: SICUREZZA DEI DATI

- i dati delle carte di pagamento sono adeguatamente crittografati durante la trasmissione e l'archiviazione
- I dati sensibili di autenticazione, come i numeri CVV, non vengono archiviati dopo l'autorizzazione
- esiste una politica per la protezione dei dati dei titolari di carta e dei dati sensibili di autenticazione

SEZIONE 2: SICUREZZA DELLA RETE E DEL FIREWALL

- Le configurazioni di rete e le regole del firewall vengono regolarmente riviste e aggiornate
- esiste un diagramma di rete che illustri il flusso dei dati dei titolari di carta
- Sono in atto politiche e procedure di sicurezza per proteggere l'infrastruttura di rete

SEZIONE 3: CONTROLLO DEGLI ACCESSI

- I privilegi di accesso degli utenti sono limitati in base alle esigenze aziendali
- è implementata l'autenticazione a più fattori per l'accesso remoto alla rete
- Gli account utente vengono prontamente disattivati in caso di cessazione o cambio di ruolo

SEZIONE 4: GESTIONE DELLA VULNERABILITÀ

- Le patch di sicurezza vengono applicate tempestivamente per risolvere le vulnerabilità
- esiste un processo per la scansione delle vulnerabilità e i test di penetrazione
- Le patch di sicurezza critiche vengono esaminate e assegnate la priorità in base al rischio

SEZIONE 5: POLITICHE E PROCEDURE DI SICUREZZA

- Le politiche e le procedure di sicurezza complete sono documentate e diffuse?
- esiste un programma di formazione sulla sensibilizzazione alla sicurezza per i dipendenti
- Le politiche di sicurezza vengono riviste e aggiornate secondo necessità

SEZIONE 6: MONITORAGGIO E REGISTRAZIONE

- Gli eventi e i registri di sicurezza vengono regolarmente esaminati e monitorati
- esiste un processo per condurre avvisi in tempo reale per attività sospette
- Sono state stabilite procedure di risposta e segnalazione degli incidenti

SEZIONE 7: RISPOSTA ALL'INCIDENTE

- esiste un piano di risposta agli incidenti che delinea le fasi per affrontare gli incidenti di sicurezza
- I dipendenti sono formati su come riconoscere e segnalare incidenti di sicurezza
- esiste un processo documentato per l'analisi e il miglioramento post-incidente

SEZIONE 8: SICUREZZA FISICA

- Sono in atto controlli sull'accesso fisico per impedire l'accesso non autorizzato ai dati dei titolari di carta
- l'accesso alle aree sicure è limitato e monitorato
- Sono conservati sistemi di videosorveglianza e registri dei visitatori per le aree sensibili

SEZIONE 9: FORNITORI DI SERVIZI DI TERZE PARTI

- I fornitori di terze parti vengono valutati per la conformità PCI DSS
- Sono in atto accordi scritti con i fornitori di servizi per garantire la protezione dei dati dei titolari di carta
- Esiste un processo per monitorare e valutare le pratiche di sicurezza di terze parti

Tieni presente che questa lista di controllo fornisce una panoramica di alto livello ed è essenziale eseguire a analisi approfondita specifica per i processi e il contesto della vostra organizzazione. Inoltre, lo è si consiglia di collaborare con esperti o consulenti PCI DSS per condurre un'indagine completa Gap Analysis per la tua organizzazione.