

Cosa sono i requisiti per la sicurezza dei dati?

Si tratta di un insieme di norme che IWBank chiede di rispettare a tutti gli Esercenti che trasmettono, elaborano o memorizzano informazioni sui Titolari di Carta.

Perche sono stati introdotti tali requisiti?

Per assicurare la conformità del trattamento dei dati di carta ai vigenti standard di sicurezza dei dati: PCI Data Security Standard (PCI DSS).

Cos'è il PCI DSS?

Il PCI Data Security Standard definisce per l'intero settore delle carte di pagamento un insieme di requisiti tecnici atti a proteggere i dati di una transazione. Il PCI-DSS costituisce la base tecnica delle Norme operative per la sicurezza dei dati e consente agli Esercenti e ai Fornitori di servizi di ottemperare a un insieme di standard tecnici di sicurezza dei dati

A cosa serve rispettare tali requisiti per la mia attività?

L'eventuale utilizzo fraudolento dei dati di carta comporta ripercussioni negative per la tua azienda, per gli altri Esercenti, per gli Emittenti di Carte. Anche un singolo episodio può danneggiare gravemente la reputazione di un'azienda e la sua efficienza operativa. Evitare questo rischio attraverso l'adozione di procedure per la protezione dei dati contribuisce a rafforzare la fiducia dei clienti e a migliorare la reputazione della vostra azienda.

Tale adeguamento è obbligatorio?

La conformità agli standard PCI-DSS consente di adottare procedure aziendali ottimali in materia di protezione dei dati ed è inoltre obbligatoria per collaborare con IWBank - in qualità di banca acquirer delle carte Visa e Mastercard. L'Esercente aderendo al servizio POS S2S si impegna a rispettare i termini e le condizioni ivi previsti, che includono i requisiti di sicurezza dei dati e la conformità alle normative PCI DSS.

Entro quale data devo adeguarmi?

Gli obblighi di cui sopra sono in vigore dal gennaio 2007 per tutti gli Esercenti. Queste norme introducono ulteriori obblighi (a seconda del numero di transazioni) nel fornire a IWBank la documentazione che convalida la conformità al PCI-DSS.

Devo rispettare gli standard anche se non memorizzo le informazioni dei Titolari?

Sì, le norme si applicano a tutte le attrezzature, i sistemi e le reti utilizzati per trasmettere o elaborare le informazioni relative ai Titolari di Carta.

Sono previsti particolari obblighi di certificazione?

Se e in quale misura è necessario certificarsi, dipende dalla quantità di transazioni effettuate dall'Esercente. Le attività da compiere si distinguono tra questi tre tipi di certificazione:

Self Assessment Questionnaire (SAQ)

È necessario compilare un dettagliato formulario di sicurezza.

Network Scan Un'azienda addetta alla sicurezza (Approved Scanning Vendors), accreditata da Visa e/o MasterCard, esegue periodicamente e d'accordo con il partner contrattuale un attacco simulato al sistema per individuarne eventuali punti deboli.

On-Site Security Audit:

I partner contrattuali di grandi dimensioni o la cui sicurezza è particolarmente critica vengono ispezionati in loco.

Chi sostiene i costi della certificazione?

I costi della certificazione sono interamente a carico dell'esercente e lo stesso vale per i costi sostenuti per la rimozione dei difetti accertati nei controlli di certificazione.

Con quale frequenza occorre rinnovare la certificazione?

La certificazione va rinnovata a intervalli regolari, ossia:

- o Network Scan: 4 volte all'anno;
- o On-Site Security Audit: 1 volta all'anno;
- o Self Assessment Questionnaire: 1 volta all'anno;

Eventuali modifiche del partner contrattuale, quali l'installazione di nuove componenti hardware o software, la creazione di un nuovo sito web oppure il cambiamento del provider dei servizi di pagamento, devono essere immediatamente comunicate a IWBANK.

Un Esercente può ritenersi conforme se ha problemi di non conformità irrisolti, ma fornisce un piano di riparazione?

IWBANK invita gli Esercenti a eseguire una revisione iniziale, sviluppare un piano di riparazione, risolvere le non conformità come previsto dal piano ed eseguire una nuova convalida della conformità degli aspetti oggetto di riparazione. L'Esercente potrà, comunque, essere considerato responsabile per le frodi derivanti dalla mancata sicurezza.

Per ulteriori dettagli:

- o www.visaeurope.com
- o www.pcisecuritystandards.org
- o www.mastercard.com