**LISTA CONTROLLI CARD PAYMENT INDUSTRY DATA SECURITY STANDARD**

1. Installare e mantenere una **firewall configuration** to protect cardholder data:

Questo requisito impone di utilizzare firewall e altre misure di sicurezza per proteggere i dati dei titolari di carte. - Funzionecheck\_firewall\_status-

1. Non usare **password di default** fornite dai fornitori:

Le password predefinite di sistemi e applicazioni devono essere cambiate per ridurre il rischio di accessi non autorizzati. - Funzione check\_default\_passwords-

1. **Proteggere i dati di titolari di carte memorizzati (crittografia)** :

I dati sensibili dei titolari di carte memorizzati devono essere crittografati per impedire l'accesso non autorizzato.

1. Crittografare la trasmissione dei dati dei titolari di carte su reti pubbliche:

Le informazioni sensibili devono essere protette durante la trasmissione attraverso internet o altre reti pubbliche. -Funzione: check\_encryption\_on\_ports

check\_encryption\_usage

check\_non\_encrypted\_connections

check\_non\_encrypted\_connection

1. Sviluppare e mantenere le applicazioni sicure:

Le applicazioni che gestiscono dati di titolari di carte devono essere sviluppate e mantenute con adeguati standard di sicurezza. (con OpenSSL)  
Vedere di aggiungere anche controlli quali firme digitali, backup

Funzione:test\_encryption

1. **Limitare l'accesso ai dati** dei titolari di carte solo a chi ne ha bisogno:

L'accesso ai dati sensibili dei titolari di carte deve essere limitato solo alle persone autorizzate e necessarie per svolgere le loro mansioni.

Funzione limit\_acces\_to\_authorized\_users

1. Assegnare un ID unico a ciascuna persona con accesso al sistema:

Ogni utente che accede ai dati dei titolari di carte deve avere un identificatore univoco per tracciare le attività degli utenti.

1. Limitare l'accesso fisico ai dati dei titolari di carte:

Le strutture fisiche e le risorse contenenti dati sensibili devono essere protette da accessi non autorizzati.

1. **Monitorare e tracciare tutti gli accessi ai dati** dei titolari di carte:

Devono essere implementati sistemi di monitoraggio per registrare e tracciare l'accesso ai dati sensibili dei titolari di carte.

1. **Testare regolarmente le proprie reti e i sistemi:**

È necessario condurre regolarmente test di sicurezza e vulnerabilità per identificare e correggere eventuali debolezze nella sicurezza.

1. Mantenere una policy di sicurezza dell'informazione:

Deve essere sviluppata e mantenuta una politica di sicurezza dell'informazione che definisca le regole e le procedure per proteggere i dati dei titolari di carte.