



# PCI DSS e GFI LANguard N.S.S. 8

Requisiti PCI DSS	Controllo di verifica	Monitoraggio e creazione di rapporti	Avvisi	Applicazione	Note
<b>Requisito 1: Installazione e manutenzione di una configurazione firewall per proteggere i dati dei titolari di carte di credito/debito (bancomat)</b>					
1.3 Creazione di una configurazione firewall per limitare le connessioni ai dati dei titolari di carte					
1.3.9 Installazione di software firewall sui computer portatili e quelli di proprietà dei dipendenti con connessione diretta a internet, adoperati per accedere alla rete dell'azienda	✓	✓	●	✓	Profili di scansione e rapporti predefiniti
<b>Requisito 2: Non utilizzo delle password predefinite fornite dal produttore</b>					
2.1 Modifica dei valori predefiniti forniti dal produttore ogni volta che si installa un sistema sulla rete					
2.1	●	✓	●		Profili di scansione e rapporti predefiniti
2.2 Sviluppo di standard di configurazione validi per tutti i componenti di sistemi; gestione di tutte le vulnerabilità note					
2.2.2 Disabilitazione di tutti i servizi e protocolli non necessari (cioè dei servizi e protocolli non direttamente necessari per eseguire la funzionalità specificata dei dispositivi)	✓	✓	●		Profili di scansione e rapporti predefiniti
2.2.3 Configurazione di parametri di protezione del sistema per impedire abusi	✓	✓	●		Profili di scansione e rapporti predefiniti
2.2.4 Rimozione di tutte le funzionalità non necessarie, quali script, driver e server web	✓	✓	●		Profili di scansione e rapporti predefiniti
<b>Requisito 5: Utilizzo e aggiornamento regolari di software o programmi antivirus</b>					
5.1 Distribuzione di software antivirus su tutti i sistemi comunemente attaccati da virus					
5.1	✓	✓	●	✓	Profili di scansione e rapporti predefiniti
5.2 Garanzia che tutti i meccanismi siano attivamente in esecuzione					
5.2	✓	✓	●	✓	Profili di scansione e rapporti predefiniti
<b>Requisito 6: Sviluppo e manutenzione della protezione di sistemi e applicazioni</b>					
6.1 Garanzia che tutti i componenti di sistema e software abbiano installate le più recenti patch di protezione fornite dai produttori					
6.1	✓	✓	●	✓	Profili di scansione e rapporti predefiniti
6.2 Istituzione di un processo di identificazione delle vulnerabilità di sicurezza di recente scoperta					
6.2	✓	✓	●	✓	Pianificazione dei controlli di rete
6.4 Rispetto di procedure di controllo per tutte le modifiche di configurazione di sistema e di software					
6.4.3 Verifica della funzionalità operativa					
6.4.3	✓	✓	●	✓	Ripristino distribuzione delle patch
6.5 Sviluppo di tutte le applicazioni web sulla base di linee guida di codifica protetta					
6.5	✓	✓	●		Controlli di vulnerabilità OVAL
6.6 Garanzia che tutte le applicazioni interfacciate con internet siano protette da attacchi noti, ricorrendo all'installazione di un firewall a livello applicativo					
6.6	✓	✓	●	✓	Profili di scansione e rapporti predefiniti
<b>Requisito 8: Assegnazione di un ID esclusivo a chiunque abbia accesso a un computer</b>					
8.2 Attribuzione di ID esclusivi e di password					
8.2	✓	✓	●		Profili di scansione e rapporti predefiniti
8.5 Garanzia di una procedura di autenticazione utente e gestione password adeguate					
8.5.3 Password impostate su un valore esclusivo per l'utente e modifica dopo il 1° uso					
8.5.3	●	●	●		Profili di scansione e rapporti predefiniti
8.5.5 Rimozione di account utenti inattivi almeno ogni 90 giorni					
8.5.5	●	●	●		Profili di scansione e rapporti predefiniti

Requisiti PCI DSS	Controllo di verifica	Monitoraggio e creazione di rapporti	Avvisi	Applicazione	Note
<b>8.5.6</b> Abilitazione di account usati dai produttori per l'assistenza remota soltanto per il periodo di tempo necessario	●	●	●		Profili di scansione e rapporti predefiniti
<b>8.5.9</b> Modifica delle password utenti almeno ogni 90 giorni	✓	✓	●		Profili di scansione e rapporti predefiniti
<b>8.5.10</b> Richiesta di una lunghezza minima della password pari ad almeno sette caratteri	✓	✓	●		Profili di scansione e rapporti predefiniti
<b>Requisito 10: Individuazione e controllo di tutto l'accesso alle risorse di rete e ai dati dei titolari di carte di credito/debito</b>					
<b>10.4</b> Sincronizzazione di tutti i cruciali clock e ore di sistema	✓	✓	●		Profili di scansione e rapporti predefiniti
<b>Requisito 11: Regolari prove dei sistemi e processi di protezione</b>					
<b>11.1</b> Prova annuale dei: controlli di protezione, limitazioni, connessioni di rete e restrizioni per garantire la facoltà di identificare adeguatamente e poi fermare eventuali tentativi di accesso non autorizzati	✓	✓	●	✓	Pianificazione dei controlli di rete
<b>11.2</b> Esecuzione di scansioni di vulnerabilità della rete interne ed esterne almeno con cadenza trimestrale	✓	✓	●	✓	Pianificazione dei controlli di rete
<b>11.4</b> Utilizzo di sistemi di scoperta d'intrusione nella rete e basati su host, e di sistemi di prevenzione dell'intrusione per controllare tutto il traffico di rete e avvertire il personale su eventuali compromissioni	✓	✓	●		Profili di scansione e rapporti predefiniti
<b>11.5</b> Distribuzione del software di monitoraggio dell'integrità dei file per avvertire il personale in caso di modifica non autorizzata del sistema critico o dei content file	✓	✓	●	✓	Profili di scansione e rapporti predefiniti

#### Legenda

✓ Requisito totalmente supportato

● Requisito supportato parzialmente tramite la personalizzazione dei rapporti o del prodotto. Possono applicarsi particolari condizioni.

**NOTA:** Condizioni che, a puro titolo esemplificativo, si applicano a:

- impostazioni di protezione di Windows, quali criteri di password e di controllo
- impostazioni account utenti
- software e dispositivi di terzi, quali firewall, opportunamente installati e configurati

