



# GFI PCI DSS e GFI Network Security Products

Requisiti PCI DSS	ESM 7	LANSS 8
<b>Requisito 1: Installazione e manutenzione di una configurazione firewall per proteggere i dati dei titolari di carte di credito/debito (bancomat)</b>		
<b>1.3</b> Creazione di una configurazione firewall per limitare le connessioni ai dati dei titolari di carte di credito/debito		
<b>1.3.1</b> Limitazione del traffico internet interno a indirizzi IP che rientrano nella DMZ	●	
<b>1.3.6</b> Protezione e sincronizzazione dei file di configurazione del router	●	
<b>1.3.7</b> Negazione di tutto il resto del traffico interno ed esterno non autorizzato esplicitamente	●	
<b>1.3.9</b> 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		✓
<b>Requisito 2: Non utilizzo delle password predefinite fornite dal produttore</b>		
<b>2.1</b> Modifica dei valori predefiniti forniti dal produttore ogni volta che si installa un sistema sulla rete		●
<b>2.2</b> Sviluppo di standard di configurazione per tutti i componenti di sistema		
<b>2.2.2</b> Disabilitazione di tutti i servizi e protocolli non necessari e non protetti	●	●
<b>2.2.3</b> Configurazione di parametri di protezione del sistema per impedire abusi		●
<b>2.2.4</b> Rimozione di tutte le funzionalità non necessarie, quali script, driver e server web		●
<b>Requisito 3: Protezione dei dati dei titolari di carte di credito/debito archiviati</b>		
<b>3.5</b> Protezione delle chiavi usate per cifrare i dati dei titolari di carte di credito contro divulgazione e abuso		
<b>3.5.1</b> Limitazione dell'accesso alle chiavi al minor numero indispensabile di depositari	●	
<b>3.6</b> Documentazione e implementazione completa di tutti i processi e le procedure di gestione delle chiavi adoperate per la cifratura dei dati dei titolari di carte di credito/debito		
<b>3.6.3</b> Protezione dell'archivio delle chiavi	●	
<b>Requisito 5: Utilizzo e aggiornamento regolari di software o programmi antivirus</b>		
<b>5.1</b> Distribuzione di software antivirus su tutti i sistemi comunemente attaccati da virus		✓
<b>5.2</b> Garanzia che tutti i meccanismi siano attivamente in esecuzione		✓
<b>Requisito 6: Sviluppo e manutenzione della protezione di sistemi e applicazioni</b>		
<b>6.1</b> Garanzia che tutti i componenti di sistema e software abbiano installate le più recenti patch dei produttori		✓
<b>6.2</b> Istituzione di un processo di identificazione delle vulnerabilità di sicurezza di recente scoperta		✓
<b>6.4</b> Rispetto di procedure di controllo delle modifiche per tutte le modifiche di configurazione di sistema e di software		
<b>6.4.3</b> Verifica della funzionalità operativa		✓
<b>6.5</b> Sviluppo di tutte le applicazioni web sulla base di linee guida di codifica protetta		●
<b>6.6</b> Garanzia che tutte le applicazioni interfacciate con internet siano protette da attacchi noti, ricorrendo all'installazione di un firewall a livello applicativo		✓
<b>Requisito 7: Accesso limitato ai dati dei titolari di carte di credito/debito da parte di aziende che "hanno necessità di sapere"</b>		
<b>7.1</b> Limitazione dell'accesso alle risorse del computer e alle informazioni sui titolari della carta di credito/debito esclusivamente a quei soggetti il cui compito richiede un tale accesso	●	
<b>7.2</b> Istituzione di un meccanismo, per i sistemi con più utenti, che limiti l'accesso sulla base della necessità di conoscenza dell'utente, e che sia impostato sull'opzione "Nega a tutti" salvo consentito esplicitamente	●	
<b>Requisito 8: Assegnazione di un ID esclusivo a chiunque abbia accesso a un computer</b>		
<b>8.2</b> Attribuzione di ID esclusivi e di password		●
<b>8.5</b> Garanzia di un'autenticazione utente e gestione password adeguate per gli utenti non consumatori e gli amministratori		
<b>8.5.1</b> Controllo dell'aggiunta, eliminazione o modifica di ID, credenziali e altri oggetti identificativi dell'utente	●	
<b>8.5.2</b> Verifica dell'identità dell'utente prima dell'esecuzione di ripristini della password	●	
<b>8.5.3</b> Password iniziali impostate su un valore esclusivo per ogni utente e modifica immediata dopo il primo utilizzo	●	●
<b>8.5.4</b> Revoca immediata dell'accesso a utenti cessati	●	
<b>8.5.5</b> Rimozione di account utenti inattivi almeno ogni 90 giorni	●	●
<b>8.5.6</b> Abilitazione di account usati dai produttori per l'assistenza remota soltanto per il periodo di tempo necessario	●	●

Requisiti PCI DSS	ESM 7	LANSS 8
<b>8.5.9</b> Modifica delle password utenti almeno ogni 90 giorni		●
<b>8.5.10</b> Richiesta di una lunghezza minima della password pari ad almeno sette caratteri		●
<b>8.5.13</b> Limitazione dei tentativi di accesso ripetuto mediante blocco dell'ID utente dopo non oltre sei tentativi	●	
<b>8.5.16</b> Autenticazione di tutti gli accessi a qualsiasi database contenente dati di titolari di carte di credito/debito	●	
<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>10.1</b> Registrazione di tutti i singoli accessi utente ai componenti di sistema, specialmente degli utenti amministrativi	●	
<b>10.2</b> Implementazione di audit trail automatizzati su tutti i componenti di sistema per ricostruire questi eventi:		
<b>10.2.1</b> Tutti i singoli accessi ai dati dei titolari di carte di credito/debito	●	
<b>10.2.2</b> Tutte le azioni eseguite da qualsiasi soggetto munito di privilegi di root o amministrativi	✓	
<b>10.2.3</b> L'accesso a tutti gli audit trail	✓	
<b>10.2.4</b> Tentativi di accesso logico non validi	✓	
<b>10.2.5</b> Utilizzo di meccanismi di identificazione e autenticazione	✓	
<b>10.2.6</b> Inizializzazione dei log di controllo	✓	
<b>10.2.7</b> Creazione ed eliminazione di oggetti a livello di sistema	✓	
<b>10.3</b> Registrazione dei dettagli degli audit trail di tutti gli eventi correlati ai componenti di sistema	✓	
<b>10.4</b> Sincronizzazione di tutti i cruciali clock e ore di sistema	●	●
<b>10.5</b> Protezione degli audit trail affinché non sia possibile alterarli		
<b>10.5.1</b> Visualizzazione degli audit trail limitata ai soggetti con esigenze relative alla loro mansione	●	
<b>10.5.2</b> Protezione dei file degli audit trail contro modifiche non autorizzate	●	
<b>10.5.5</b> Utilizzo di software di monitoraggio dell'integrità dei file e di individuazione di modifiche sui log, per garantire che i dati dei log esistenti non possano essere modificati (tranne che dai nuovi dati) senza generare avvisi	✓	
<b>10.6</b> Analisi dei log di tutti i componenti di sistema almeno quotidianamente	✓	
<b>Requisito 11: Regolari prove dei sistemi e processi di protezione</b>		
<b>11.1</b> Prova annuale dei controlli di protezione, delle limitazioni, delle connessioni di rete e delle restrizioni per garantire la facoltà di identificare in modo adeguato e quindi fermare eventuali tentativi di accesso non autorizzati	●	✓
<b>11.2</b> Esecuzione di scansioni di vulnerabilità della rete interne ed esterne almeno con cadenza trimestrale		✓
<b>11.4</b> Utilizzo di sistemi di scoperta d'intrusione nella rete, di sistemi di scoperta d'intrusione basati su host e di sistemi di prevenzione dell'intrusione per monitorare tutto il traffico di rete e avvertire il personale in merito a eventuali compromissioni	●	●
<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	✓	✓

#### 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