



# PCI DSS e GFI EventsManager 7

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					
1.3.1 Limitazione del traffico internet interno a indirizzi IP che rientrano nella DMZ		●	●		Creazione di nuove regole
1.3.6 Protezione e sincronizzazione dei file di configurazione del router		✓	✓		Personalizzazione di regole e rapporti predefiniti**
1.3.7 Negazione di tutto il resto del traffico interno ed esterno non autorizzato esplicitamente		●	●		Creazione di nuove regole
<b>Requisito 2: Non utilizzo delle password predefinite fornite dal produttore</b>					
2.2 Sviluppo di standard di configurazione per tutti i componenti di sistema					
2.2.2 Disabilitazione di tutti i servizi e protocolli non necessari e non protetti		●	●		Requisito non supportato per default*
<b>Requisito 3: Protezione dei dati dei titolari di carte di credito/debito archiviati</b>					
3.5 Protezione delle chiavi di cifratura usate per cifrare i dati dei titolari di carte contro divulgazione e abuso:					
3.5.1 Limitazione dell'accesso alle chiavi al minor numero indispensabile di depositari		✓	✓		Personalizzazione di regole e rapporti predefiniti**
3.6 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					
3.6.3 Protezione dell'archivio delle chiavi		✓	✓		Personalizzazione di regole e rapporti predefiniti**
<b>Requisito 7: Accesso limitato ai dati dei titolari di carte di credito/debito da parte di aziende che "hanno necessità di sapere"</b>					
7.1 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					
7.2 Istituzione, per i sistemi con più utenti, di un meccanismo che limiti l'accesso in base all'esigenza di conoscenza dell'utente, impostato sull'opzione "Nega a tutti", salvo quanto consentito esplicitamente		✓	✓		Personalizzazione di regole e rapporti predefiniti**
<b>Requisito 8: Assegnazione di un ID esclusivo a chiunque abbia accesso a un computer</b>					
8.5 Garanzia di un'autenticazione utente e gestione password adeguate per gli utenti non consumatori					
8.5.1 Controllo dell'aggiunta, eliminazione o modifica di ID, credenziali e altri oggetti identificativi dell'utente		✓	✓		Regole e rapporti predefiniti
8.5.2 Verifica dell'identità dell'utente prima dell'esecuzione di ripristini della password		✓	✓		Regole e rapporti predefiniti
8.5.3 Password impostate su un valore esclusivo per l'utente e modifica dopo il 1° uso		✓			Rapporti predefiniti
8.5.4 Revoca immediata dell'accesso a utenti cessati		✓	✓		Regole e rapporti predefiniti
8.5.5 Rimozione di account utenti inattivi almeno ogni 90 giorni		✓			Rapporti predefiniti
8.5.6 Abilitazione di account utilizzati dai produttori ai fini dell'assistenza remota soltanto durante il periodo di tempo necessario		✓	✓		Regole e rapporti predefiniti

Requisiti PCI DSS	Controllo di verifica	Monitoraggio e creazione di rapporti	Avvisi	Applicazione	Note
<b>8.5.13</b> Limitazione dei tentativi di accesso ripetuto, bloccando l'ID utente dopo non più di 6 tentativi		✓			Rapporti predefiniti
<b>8.5.16</b> Autenticazione di tutti gli accessi ai database contenenti dati di titolari di carte di credito		✓	✓		Regole 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>10.1</b> Registrazione di tutti i singoli accessi utente ai componenti di sistema, soprattutto utenti amm.vi	✓	✓			Personalizzazione di regole e rapporti predefiniti**
<b>10.2</b> Implementazione di audit trail automatizzati su tutti i componenti di sistema per ricostruire tali eventi:					
<b>10.2.1</b> Tutti i singoli accessi ai dati dei titolari di carte di credito/debito	✓	✓		✓	Personalizzazione di regole e rapporti predefiniti**
<b>10.2.2</b> Tutte le azioni eseguite da qualsiasi soggetto munito di privilegi di root o amministrativi	✓	✓		✓	Regole predefinite
<b>10.2.3</b> Accesso a tutti gli audit trail	✓	✓		✓	Regole e rapporti predefiniti
<b>10.2.4</b> Tentativi di accesso logico non validi	✓	✓		✓	Regole e rapporti predefiniti
<b>10.2.5</b> Utilizzo di meccanismi di identificazione e autenticazione	✓	✓		✓	Regole e rapporti predefiniti
<b>10.2.6</b> Inizializzazione dei log di controllo	✓	✓		✓	Regole e rapporti predefiniti
<b>10.2.7</b> Creazione ed eliminazione di oggetti a livello di sistema	✓	✓		✓	Regole e rapporti predefiniti
<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		✓	✓		Regole predefinite
<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		✓	✓		Regole e rapporti predefiniti
<b>10.5.2</b> Protezione dei file degli audit trail contro modifiche non autorizzate		✓	✓		Regole e rapporti predefiniti
<b>10.5.5</b> Utilizzo di software di controllo integrità dei file e rilevamento modifiche sui log, per garantire che i dati dei log esistenti non siano modificati (tranne che dai nuovi dati) senza generare avvisi		✓	✓	✓	Regole e rapporti predefiniti
<b>10.6</b> Analisi dei log di tutti i componenti di sistema almeno quotidianamente		✓		✓	Planificazione 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		●	●		
<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		●	●	●	Creazione di nuove regole
<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			✓	✓	Regole e rapporti predefiniti

\* Necessità di creare una nuova regola di elaborazione degli eventi che non riesca ad applicare direttamente questo requisito ma assistenza agli amministratori attraverso il monitoraggio, la creazione di rapporti e gli avvisi.

\*\* Necessità di modificare le impostazioni di configurazione di regole e rapporti predefiniti, mediante parametri specifici uniformati all'ambiente della propria rete.

#### 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