



Payment Card Industry (PCI) Data Security Standard (DSS) e Payment Application Data Security Standard (PA-DSS)

Glossario, abbreviazioni e acronimi

Versione 1.2

Ottobre 2008

Termine	Definizione
AAA	Acronimo di Authentication, Authorization, Accounting. Protocollo per l'autenticazione di un utente in base alla sua identità verificabile, per l'autorizzazione di un utente in base ai suoi diritti utente e per la registrazione del consumo di risorse di rete da parte dell'utente.
Accesso remoto	Accesso alle reti di computer da una postazione remota, in genere all'esterno della rete. Un esempio di tecnologia per l'accesso remoto è <i>VPN</i> .
Account predefiniti	Account di accesso predefinito in un sistema, applicazione o dispositivo che permette l'accesso iniziale alla messa in esercizio del sistema.
Acquirente	Definito anche "banca acquirente" o "istituzione finanziaria acquirente". L'entità che inizia e mantiene le relazioni con gli esercenti per l'accettazione delle carte di pagamento.
Addetto alla sicurezza	Primo responsabile degli affari relativi alla sicurezza di un'organizzazione.
Adware	Tipo di software dannoso che, una volta installato, impone a un computer di visualizzare o scaricare automaticamente annunci pubblicitari.
AES	Abbreviazione di Advanced Encryption Standard. Cifratura a blocchi utilizzata nella crittografia a chiave simmetrica adottata da NIST nel novembre 2001 come U.S. FIPS PUB 197 (o FIPS 197). Vedere <i>Crittografia avanzata</i> .
Algoritmo di cifratura	Una sequenza di istruzioni matematiche utilizzate per trasformare testo o dati non cifrati in testo o dati cifrati, e viceversa.
Ambiente dei dati di titolari di carta	Area della rete di computer che contiene i dati dei titolari di carte o dati sensibili di autenticazione, con i sistemi e i seguenti che supportano direttamente l'elaborazione, la memorizzazione o la trasmissione dei dati dei titolari di carte. Una segmentazione di rete adeguata, che isola i sistemi che memorizzano, elaborano o trasmettono i dati dei titolari di carta da quelli che non eseguono tali operazioni, può ridurre l'ambito dell'ambiente dei dati dei titolari di carta e di conseguenza l'ambito della valutazione PCI DSS. Un ambiente dei dati dei titolari di carte è composto dai componenti di sistema. Vedere <i>Componenti di sistema</i> .
Amministratore di database	Definito anche DBA. Individuo responsabile della gestione e dell'amministrazione dei database.
Analisi/valutazione del rischio	Processo che identifica le risorse di sistema preziose e le minacce, quantifica l'esposizione alle perdite (vale a dire la perdita potenziale) sulla base delle frequenze stimate e del costo di occorrenza, e facoltativamente consiglia come allocare le risorse come contromisura per ridurre al minimo l'esposizione totale.
ANSI	Acronimo di American National Standards Institute. Organizzazioni private, senza scopo di lucro, che amministrano e coordinano il sistema di valutazione della conformità e della standardizzazione volontarie degli Stati Uniti.
Antivirus	Programma o software in grado di rilevare, rimuovere e proteggere da diverse forme di software dannoso (dette anche "malware"), tra cui virus, worm, cavalli di Troia, spyware, adware e rootkit.
Applicazione	Comprende tutti i programmi software, o gruppi di programmi, acquistati e personalizzati, di tipo sia interno che esterno (per esempio sul Web).

Termine	Definizione
Area sensibile	Qualunque centro dati, sala server o area che ospita sistemi di memorizzazione, elaborazione o trasmissione dei dati di titolari di carta. Ciò esclude le aree in cui vi sono i terminali dei punti vendita, ad esempio la cassa nei negozi di vendita al dettaglio.
ASV	Acronimo di Approved Scanning Vendor. Società approvata da PCI SSC che conduce servizi di scansione delle vulnerabilità esterni.
Autenticazione	Processo di verifica dell'identità di un individuo, dispositivo o processo.
Autenticazione a due fattori	Metodo di autenticazione di un utente in cui vengono verificati due o più fattori. Tali fattori comprendono qualcosa in possesso dell'utente (ad esempio un token hardware o software), qualcosa che l'utente conosce (una password, passphrase o PIN) o qualcosa che l'utente usa o svolge (ad esempio le impronte digitali o altre forme di biometrica).
Autorizzazione	Concessione dell'accesso o di altri diritti a un utente, programma o processo. Per una rete, l'autorizzazione definisce quello che un individuo o un programma può fare dopo una corretta autenticazione. Per gli scopi di una transazione con carta di pagamento, è l'istanza per cui un esercente riceve il permesso per l'uso di una carta di pagamento in una particolare transazione.
Backup	Copia duplicata dei dati creata a fini di archiviazione o per la protezione contro danni o perdite.
Bluetooth	Protocollo wireless che utilizza una tecnologia di comunicazione a corto raggio per facilitare la trasmissione dei dati a breve distanza tra due dispositivi.
Carte di pagamento	Per gli scopi di PCI DSS, qualsiasi carta di pagamento o dispositivo che porta il logo dei membri fondatori di PCI SSC, vale a dire American Express, Discover Financial Services, JCB International, MasterCard Worldwide o Visa, Inc.
Cavallo di Troia	Definito anche "troiano". Un tipo di software dannoso che, una volta installato, consente a un utente di eseguire una funzione normale mentre il cavallo di Troia esegue funzioni dannosi per il sistema senza che l'utente ne sia a conoscenza.
Chiave	In crittografia, una chiave è un valore che determina l'output di un algoritmo di cifratura durante la trasformazione di testo normale in testo cifrato. La lunghezza della chiave determina in genere la difficoltà di decifratura del testo in un dato messaggio. Vedere <i>Crittografia avanzata</i> .
Cifratura	Processo di conversione delle informazioni in una forma non intellegibile se non per i proprietari di una specifica chiave di crittografia. L'uso della cifratura protegge le informazioni tra il processo di cifratura e quello di decifratura (l'inverso della cifratura) dalla divulgazione non autorizzata.
Cifratura a livello di file	Tecnica o tecnologia (software o hardware) per la cifratura dell'intero contenuto di file specifici. In alternativa, vedere <i>Cifratura del disco</i> o <i>Cifratura del database a livello di colonna</i> .
Cifratura del database a livello di colonna	Tecnica o tecnologia (software o hardware) per la cifratura del contenuto di una colonna specifica in un database piuttosto che del contenuto completo dell'intero database. In alternativa, vedere <i>Cifratura del disco</i> o <i>Cifratura a livello di file</i> .

Termine	Definizione
Cifatura del disco	Tecnica o tecnologia (software o hardware) per cifrare tutti i dati memorizzati su un dispositivo (es. disco rigido, unità flash). In alternativa, per crittografare il contenuto di file o colonne specifici, viene utilizzata la <i>Cifatura a livello di file</i> o la <i>Cifatura del database a livello di colonna</i> .
CIS	Acronimo di Center for Internet Security. Organizzazione senza scopo di lucro con la missione di aiutare le organizzazioni a ridurre il rischio di interruzioni del business e dell'e-commerce derivanti da controlli di sicurezza tecnica inadeguati.
Codice di servizio	Valore di tre o quattro cifre nella striscia magnetica che segue la data di scadenza della carta di pagamento nei dati di traccia. È utilizzato per diversi scopi, quali la definizione degli attributi di servizio, la distinzione tra scambio internazionale e nazionale, o l'identificazione delle limitazioni all'uso.
Codice o valore di verifica della carta	<p>Fa riferimento a: (1) dati della striscia magnetica; (2) caratteristiche di protezione stampate.</p> <p>(1) Gli elementi dei dati sulla striscia magnetica di una carta che utilizzano il processo crittografico sicuro per proteggere l'integrità dei dati sulla striscia e rivelare alterazioni e contraffazioni. Definito CAV, CVC, CVV o CSC in base al marchio della carta di pagamento. Nell'elenco seguente sono forniti i termini per ogni marchio di carta:</p> <ul style="list-style-type: none"> ▪ CAV – Card Authentication Value, valore di autenticazione della carta (carte di pagamento JCB) ▪ CVC – Card Validation Code, codice di validazione della carta (carte di pagamento MasterCard) ▪ CVV – Card Verification Value, valore di verifica della carta (carte di pagamento Visa e Discover) ▪ CSC – Card Security Code, codice di sicurezza della carta (American Express) <p>(2) Per le carte di pagamento Discover, JCB, MasterCard e Visa, il secondo tipo di valore o codice di verifica della carta corrisponde al valore di tre cifre più a destra stampato nell'area della firma sul retro della carta. Per le carte di pagamento American Express, il codice è il numero di quattro cifre stampato in rilievo sopra il numero PAN nella parte anteriore delle carte di pagamento. Il codice è associato in modo univoco ad ogni singolo elemento del materiale plastico e associa il numero PAN al materiale plastico. Di seguito è disponibile una panoramica:</p> <ul style="list-style-type: none"> ▪ CID – Card Identification Number, numero di identificazione della carta (carte di pagamento American Express e Discover) ▪ CAV2 – Card Authentication Value 2, valore di autenticazione della carta 2 (carte di pagamento JCB) ▪ CVC2 – Card Validation Code 2, codice di validazione della carta 2 (carte di pagamento MasterCard) ▪ CVV2 – Card Verification Value 2, valore di verifica della carta 2 (carte di pagamento Visa)
Componenti di rete	Includono, senza limitazioni, firewall, switch, router, punti di accesso wireless, dispositivi di rete e altri dispositivi di sicurezza.
Componenti di sistema	Qualsiasi componente di rete, server o applicazione incluso o connesso all'ambiente dei dati dei titolari di carta.

Termine	Definizione
Compromissione	Definita anche "compromissione dei dati" o "violazione dei dati". Intrusione in un sistema informatico in cui si sospettano furto/divulgazione, modifica o distruzione non autorizzati dei dati dei titolari di carte.
Console	Schermo e tastiera che permettono l'accesso e il controllo del server o del computer mainframe in un ambiente di rete.
Consumatore	Individuo che acquista beni e/o servizi.
Controlli compensativi	<p>È possibile adottare i controlli compensativi quando un'entità non è in grado di soddisfare un requisito nel modo esplicitamente richiesto, a causa di limitazioni aziendali tecniche o documentate legittime, ma ha posto in essere altri controlli sufficienti a mitigare il rischio associato a tale requisito. I controlli compensativi devono:</p> <ol style="list-style-type: none">(1) Rispondere allo scopo e alla severità del requisito PCI DSS originale.(2) Fornire un livello di difesa simile a quello del requisito PCI DSS originale.(3) Superare e integrare altri requisiti PCI DSS (non possono essere semplicemente conformi ad altri requisiti PCI DSS).(4) Essere adeguati al rischio ulteriore provocato dalla mancata adesione al requisito PCI DSS. <p>Vedere Controlli compensativi, Appendici B e C in <i>Requisiti PCI DSS e procedure di valutazione della sicurezza</i> per istruzioni sull'utilizzo dei controlli compensativi.</p>
Controllo dell'accesso	Meccanismi che limitano la disponibilità di informazioni o risorse di elaborazione delle informazioni solo alle persone o alle applicazioni autorizzate.
Controllo duale	Processo di utilizzo di due o più entità separate (solitamente persone) che operano insieme per proteggere funzioni o informazioni sensibili. Entrambe le entità sono egualmente responsabili della protezione fisica dei materiali coinvolti nelle transazioni vulnerabili. Nessuna persona singola può accedere o utilizzare i materiali (ad esempio la chiave di crittografia). Per la generazione manuale delle chiavi, il trasporto, il caricamento, la memorizzazione e il recupero, il controllo duale richiede di dividere la conoscenza della chiave tra le entità. Vedere anche <i>Split knowledge</i> .
Criterio di protezione	Insieme di leggi, regole e pratiche che stabiliscono il modo in cui un'organizzazione gestisce, protegge e distribuisce informazioni sensibili.
Criterio o politica	Regole a livello dell'organizzazione che stabiliscono l'uso accettabile delle risorse informatiche, le pratiche di sicurezza e lo sviluppo delle procedure operative.
Crittografia	Disciplina della matematica e dell'informatica relativa alla sicurezza delle informazioni, in particolare alla cifratura e all'autenticazione. Nella sicurezza di reti e applicazioni, è uno strumento per il controllo dell'accesso, la riservatezza delle informazioni e l'integrità.

Termine	Definizione
Crittografia avanzata	<p>Crittografia basata su algoritmi testati e accettati, insieme a pratiche di gestione delle chiavi e lunghezze elevate delle chiavi. La crittografia è un metodo per proteggere i dati e include sia la cifratura (reversibile) sia l'hashing (irreversibile, o "one way"). SHA-1 è un esempio di algoritmo di hashing testato e accettato. Altri esempi di algoritmi e standard testati e accettati per la cifratura sono AES (128 bit e superiore), TDES (almeno chiavi di lunghezza doppia), RSA (1024 bit e superiore), ECC (160 bit e superiore) ed ElGamal (1024 bit e superiore).</p> <p>Vedere NIST Special Publication 800-57 (http://csrc.nist.gov/publications/) per ulteriori informazioni.</p>
Database	<p>Formato strutturato per organizzare e mantenere informazioni facili da recuperare. Semplici esempi di database sono tabelle e fogli di calcolo.</p>
Dati della striscia magnetica	<p>Definiti anche "dati di traccia". Dati codificati nella striscia magnetica o nel chip utilizzati per l'autorizzazione durante una transazione di pagamento. Possono corrispondere all'immagine della striscia magnetica su un chip o ai dati sulla traccia 1 e/o sulla traccia 2 della striscia magnetica. Le entità non devono conservare i dati completi della striscia magnetica dopo aver ottenuto l'autorizzazione alla transazione.</p>
Dati delle transazioni	<p>Dati relativi alle transazioni con carta di pagamento elettronica.</p>
Dati di titolari di carta	<p>Come minimo, i dati dei titolari di carte contengono l'intero numero PAN. I dati dei titolari di carte possono comprendere, oltre al numero PAN completo:</p> <ul style="list-style-type: none"> ▪ Nome del titolare di carta ▪ Data di scadenza ▪ Codice di servizio <p>Vedere <i>Dati sensibili di autenticazione</i> per ulteriori elementi dati che possono essere trasmessi o elaborati come parte di una transazione di pagamento.</p>
Dati sensibili di autenticazione	<p>Informazioni relative alla sicurezza (codici/valori di validazione della carta, dati completi della striscia magnetica, PIN e blocchi PIN) utilizzate per autenticare i titolari di carte, disponibili in chiaro o in una forma non protetta.</p>
DMZ	<p>Abbreviazione di "demilitarized zone", zona demilitarizzata. Una sottorete fisica o logica oppure un host che fornisce un ulteriore livello di protezione alla rete privata interna di un'organizzazione. La zona DMZ aggiunge un altro livello di protezione della rete tra Internet e la rete interna di un'organizzazione, in modo che le parti esterne abbiano accesso diretto solamente ai dispositivi nella zona DMZ anziché a tutta la rete interna.</p>
DNS	<p>Acronimo di Domain Name System o Domain Name Server. Sistema che memorizza le informazioni associate ai nomi di dominio in un database distribuito sulle reti, ad esempio Internet.</p>
DSS	<p>Acronimo di Data Security Standard; definito anche PCI DSS.</p>
Dynamic Packet Filtering	<p>Vedere <i>Ispezione stateful</i>.</p>
ECC	<p>Acronimo di Elliptic Curve Cryptography. Metodo per la crittografia a chiave pubblica basato su curve ellittiche su campi finiti. Vedere <i>Crittografia avanzata</i>.</p>
Emittente	<p>Definito anche "banca emittente" o "istituzione finanziaria emittente". Ente che emette direttamente le carte di pagamento a consumatori e non consumatori.</p>

Termine	Definizione
Esercente	Per gli scopi di PCI DSS, un esercente è qualsiasi entità che accetta carte di pagamento che portano il logo di uno dei cinque membri di PCI SSC (American Express, Discover, JCB, MasterCard o Visa) come pagamento per beni e/o servizi. Si noti che un esercente che accetta carte di pagamento per il pagamento di beni e/o servizi può anche essere un provider di servizi, se i servizi venduti comportano la memorizzazione, l'elaborazione o la trasmissione dei dati dei titolari di carte per conto di altri esercenti o fornitori di servizi. Ad esempio, un ISP è un esercente che accetta le carte di pagamento per la fatturazione mensile, ma funge anche da provider di servizi se ospita gli esercenti come clienti.
FIPS	Acronimo di Federal Information Processing Standards. Standard riconosciuti pubblicamente dal governo federale degli Stati Uniti, anche per l'uso da parte di agenzie non governative e collaboratori.
Firewall	Tecnologia hardware e/o software che protegge le risorse di rete dall'accesso non autorizzato. Un firewall consente o vieta il traffico informatico tra le reti con livelli di sicurezza differenti in base a un set di regole e altri criteri.
FTP	Acronimo di File Transfer Protocol. Protocollo di rete utilizzato per trasferire i dati da un computer all'altro tramite una rete pubblica come Internet. FTP è ampiamente considerato un protocollo non sicuro, perché le password e il contenuto dei file sono inviati senza protezione e in chiaro. FTP può essere implementato in modo sicuro tramite SSH o altre tecnologie.
GPRS	Acronimo di General Packet Radio Service. Servizio dati mobile disponibile agli utenti dei telefoni cellulari GSM. Famoso per l'uso efficiente di una larghezza di banda limitata. Particolarmente adatto per l'invio e la ricezione di piccoli pacchetti di dati, quali i messaggi e-mail e l'esplorazione del Web.
GSM	Acronimo di Global System for Mobile Communications. Famoso standard per reti e telefoni cellulari. L'ampia disponibilità di GSM ha reso particolarmente diffuso il roaming internazionale tra gli operatori di telefonia mobile, consentendo agli abbonati di utilizzare i loro telefoni in molte parti del mondo.
Hashing	Processo che rende illeggibili i dati dei titolari di carte mediante conversione dei dati in un digest di messaggio di lunghezza fissa tramite la <i>Crittografia avanzata</i> .
Host	Hardware del computer principale su cui risiede il software del computer.
HTTP	Acronimo di HyperText Transfer Protocol. Protocollo Internet aperto per il trasferimento delle informazioni sul World Wide Web.
HTTPS	Acronimo di HyperText Transfer Protocol over Secure Socket Layer. HTTP sicuro che fornisce l'autenticazione e la comunicazione cifrata sul World Wide Web, progettato per la comunicazione di informazioni sensibili quali i dati di accesso basati sul Web.
ID	Identificatore per un particolare utente o applicazione.
IDS	Acronimo di Intrusion Detection System. Software o hardware utilizzato per identificare e avvertire in caso di tentativi di intrusione nella rete o nel sistema. Composto da sensori che generano eventi di protezione, una console per monitorare gli eventi e gli avvisi e per controllare i sensori, un modulo di gestione centrale che registra in un database gli eventi generati dai sensori. Utilizza un sistema di regole per generare avvisi in risposta agli eventi di protezione rilevati.

Termine	Definizione
IETF	Acronimo di Internet Engineering Task Force. Una grande comunità internazionale aperta di designer di reti, operatori, fornitori e ricercatori interessati all'evoluzione dell'architettura Internet e al corretto funzionamento di Internet. IETF non presenta membri formali ed è aperta a tutti gli individui interessati.
Indirizzo IP	Definito anche "indirizzo Internet Protocol". Codice numerico che identifica in modo univoco un particolare computer su Internet.
Indirizzo MAC	Abbreviazione di "indirizzo Media Access Control". Valore di identificazione univoco assegnato dai produttori agli adattatori di rete e alle schede di interfaccia di rete.
IP	Acronimo di Internet Protocol. Protocollo dello strato di rete contenente informazioni sull'indirizzo e alcune informazioni di controllo che consentono il routing dei pacchetti. IP è il principale protocollo dello strato di rete nella suite di protocolli Internet.
IPS	Acronimo di Intrusion Prevention System. Oltre al sistema IDS, IPS si occupa di bloccare i tentativi di intrusione.
IPSEC	Abbreviazione di Internet Protocol Security. Standard per la protezione delle comunicazioni IP mediante cifratura e/o autenticazione di tutti i pacchetti IP. IPSEC garantisce la sicurezza nello strato di rete.
ISO	Più comunemente nota come International Organization for Standardization. Organizzazione non governativa costituita da una rete di istituzioni nazionali per gli standard di oltre 150 paesi, con un membro per paese e un segretariato centrale a Ginevra (Svizzera) che coordina il sistema.
Ispezione stateful	Detta anche "dynamic packet filtering", è una capacità del firewall che garantisce la protezione avanzata mediante traccia dei pacchetti di comunicazione. Solo ai pacchetti in arrivo con una risposta appropriata ("connessioni stabilite") è consentito l'attraversamento del firewall.
LAN	Acronimo di Local Area Network. Rete di computer che copre un'area limitata, spesso un edificio o un gruppo di edifici.
LDAP	Acronimo di Lightweight Direct Access Protocol. Repository dei dati di autenticazione e autorizzazione utilizzato per le query e per la modifica delle autorizzazioni utenti e per concedere l'accesso alle risorse protette.
Log di audit	Definito anche "audit trail". Record cronologico delle attività di sistema. Fornisce una registrazione sufficiente a consentire la ricostruzione, la revisione e l'analisi della sequenza di ambienti e attività che circondano o conducono a un'operazione, procedura o evento in una transazione, dall'inizio al risultato finale.
LPAR	Abbreviazione di "logical partition", partizione logica. Un sistema di suddivisione, o partizionamento, delle risorse totali di un computer (processori, memoria e spazio di memorizzazione) in unità più piccole, che possono eseguire una copia unica e distinta di sistemi operativi e applicazioni. Il partizionamento logico viene in genere utilizzato per consentire l'uso di sistemi operativi e applicazioni diversi su un singolo dispositivo. Le partizioni possono o meno essere configurate per comunicare tra loro o per condividere alcune risorse sul server, ad esempio le interfacce di rete.

Termine	Definizione
MAC	Acronimo di Message Authentication Code. In crittografia, una piccola informazione utilizzata per autenticare un messaggio. Vedere <i>Crittografia avanzata</i> .
Mainframe	Computer progettati per gestire enormi volumi di input e output di dati e per aumentare la velocità di elaborazione. I mainframe possono eseguire più sistemi operativi, così che sembrano gestiti da più computer. Molti sistemi legacy dispongono di una struttura mainframe.
Mascheratura	Metodo di occultamento di un segmento di dati in fase di visualizzazione. La mascheratura è utilizzata quando non esistono requisiti aziendali di visualizzazione dell'intero numero PAN.
Minaccia	Condizione o attività che può causare la perdita, la modifica, l'esposizione, l'inaccessibilità intenzionale o accidentale di informazioni o risorse di elaborazione delle informazioni, o che comunque porta un danno all'organizzazione.
Monitoraggio	Utilizzo di sistemi o processi che controllano costantemente il computer o le risorse di rete al fine di avvertire il personale in caso di interruzioni, allarmi o altri eventi predefiniti.
Monitoraggio dell'integrità dei file	Tecnica o tecnologia secondo la quale alcuni file o registri vengono monitorati per rilevarne le modifiche. Se vengono modificati file o registri importanti, vengono inviati avvisi al personale appropriato della sicurezza.
MPLS	Acronimo di Multi Protocol Label Switching. Rete o meccanismo di telecomunicazioni studiato per connettere un gruppo di reti a commutazione di pacchetto.
NAT	Acronimo di Network Address Translation. Detto anche network masquerading o IP masquerading. La modifica di un indirizzo IP utilizzato in una rete in un indirizzo IP diverso all'interno di un'altra rete.
NIST	Acronimo di National Institute of Standards and Technology. Agenzia federale non di regolamentazione all'interno della Technology Administration del Ministero del Commercio degli Stati Uniti. La sua missione è promuovere l'innovazione e la competitività industriale degli Stati Uniti promuovendo scienze, standard e tecnologie di misurazione per migliorare la sicurezza economica e la qualità della vita.
NMAP	Software per scansioni di protezione che connette le reti e identifica le porte aperte nelle risorse di rete.
NTP	Acronimo di Network Time Protocol. Protocollo per la sincronizzazione degli orologi dei sistemi informatici sulle reti di dati a latenza variabile a commutazione di pacchetto.
Numero di conto	Vedere <i>Numero PAN</i> .
OWASP	Acronimo di Open Web Application Security Project. Un'organizzazione senza scopo di lucro, fondata nel 2004 e mirata a migliorare la sicurezza del software applicativo. OWASP ha rilasciato la OWASP Top Ten, che elenca le dieci vulnerabilità più importanti delle applicazioni Web. Vedere http://www.owasp.org .

Termine	Definizione
Pad	In crittografia, one-time pad è un algoritmo di cifratura che combina il testo con una chiave casuale, o <i>pad</i> , lunga quanto il testo in chiaro e utilizzata una sola volta. Inoltre, se la chiave è realmente casuale, mai riutilizzata e tenuta segreta, one-time pad è inviolabile.
PAN	Acronimo di Primary Account Number e definito anche "numero di conto". Numero univoco della carta di pagamento (tipicamente per le carte di credito o debito) che identifica l'emittente e il conto del titolare della carta.
PA-QSA	Acronimo di Payment Application Qualified Security Assessor, azienda approvata da PCI SSC per condurre valutazioni sulle applicazioni di pagamento nel rispetto di PA-DSS.
Password predefinita	Password di amministrazione del sistema o degli account di servizio predefinita in un sistema, applicazione o dispositivo; generalmente è associata all'account predefinito. Gli account e le password predefiniti sono pubblicati e conosciuti, pertanto possono essere facilmente indovinati.
Password/passphrase	Una stringa di caratteri per l'autenticazione dell'utente.
PAT	Acronimo di Port Address Translation e definito anche "traduzione della porta per l'indirizzo di rete". Un tipo di <i>NAT</i> che converte anche i numeri di porta.
Patch	Aggiornamento del software esistente per aggiungere funzionalità o correggere un difetto.
PCI	Payment Card Industry.
PDA	Acronimo di Personal Data Assistant o Personal Digital Assistant. Dispositivi palmari con funzionalità di telefono cellulare, client e-mail o browser Web.
PIN	Acronimo di Personal Identification Number. Password numerica segreta nota solo all'utente e a un sistema di autenticazione dell'utente. L'utente ottiene l'accesso solamente se il PIN specificato corrisponde a quello nel sistema. I PIN vengono in genere utilizzate agli sportelli Bancomat per le transazioni di anticipo contante. Un altro tipo di PIN è utilizzato nelle carte con chip EMV, dove il PIN sostituisce la firma del titolare della carta.
POS	Acronimo di Point of Sale. Hardware e/o software utilizzato per elaborare le transazioni delle carte di pagamento nelle sedi degli esercenti.
Procedura	Descrizione narrativa di un criterio. La procedura è la "guida pratica" a un criterio e ne descrive l'implementazione.
Prodotti standard	Prodotti in stock, non personalizzati o progettati per uno specifico cliente o utente, e prontamente disponibili per l'uso.
Protocollo	Metodo di comunicazione concordato utilizzato nelle reti. Specifica che descrive regole e procedure che i prodotti per computer devono seguire per svolgere attività su una rete.
Protocollo/servizio/porta non sicuri	Un protocollo, un servizio o una porta che presenta problemi di protezione a causa della mancanza di controlli sulla riservatezza e/o sull'integrità. Questi problemi di protezione comprendono servizi, protocolli o porte che trasmettono dati e credenziali di autenticazione (es. password/passphrase in chiaro su Internet) o che consentono facilmente lo sfruttamento sia per impostazione predefinita sia in caso di errata configurazione. Un esempio di servizio, protocollo o porta non sicuro è FTP.

Termine	Definizione
Provider di hosting	Offre diversi servizi agli esercenti e ad altri provider di servizi. I servizi sono di tipo semplice o complesso, dallo spazio condiviso su un server a un'intera gamma di "carrelli per gli acquisti", dalle applicazioni di pagamento alle connessioni a gateway ed elaboratori di pagamenti, fino all'hosting dedicato a un solo cliente per server. Un provider di hosting può anche essere un provider di hosting condiviso, che ospita più entità su un singolo server.
Provider di servizi	Entità commerciale che non rappresenta un marchio di pagamento ma è direttamente coinvolto nell'elaborazione, nella memorizzazione o nella trasmissione dei dati dei titolari di carte. Sono comprese anche le società che forniscono servizi che controllano o possono influire sulla sicurezza dei dati dei titolari di carte. Gli esempi comprendono provider di servizi gestiti che mettono a disposizione firewall gestiti, IDS e altri servizi, così come provider di hosting e altre entità. Sono escluse le entità come le società di telecomunicazioni, che forniscono solo i collegamenti di comunicazione senza accesso allo strato dell'applicazione.
Pulizia sicura	Detto anche "eliminazione sicura", un programma di utilità utilizzato per eliminare file specifici da un sistema informatico in modo permanente.
Punto di accesso wireless	Definito anche AP. Dispositivo che consente ai dispositivi di comunicazione wireless di connettersi a una rete wireless. Di solito connesso a una rete cablata, può inoltrare i dati tra i dispositivi wireless e cablati della rete.
PVV	Acronimo di PIN Verification Value. Valore discrezionale codificato nella striscia magnetica della carta di pagamento.
QSA	Acronimo di Qualified Security Assessor, azienda approvata da PCI SSC per condurre valutazioni PCI DSS in loco.
RADIUS	Abbreviazione di Remote Authentication And Dial-In User Service. Sistema di autenticazione e accounting. Verifica se le informazioni, quali nome utente e password, passate al server RADIUS sono corrette, quindi autorizza l'accesso al sistema.
Rapporto sulla conformità	Definito anche ROC. Rapporto contenente i dettagli che documentano lo stato di conformità di un'entità in PCI DSS.
Rapporto sulla validazione	Definito anche ROV. Rapporto contenente i dettagli che documentano la conformità di un'applicazione di pagamento con PCI PA-DSS.
RBAC	Acronimo di Role-Based Access Control. Controllo utilizzato per limitare l'accesso da parte di utenti autorizzati specifici in base alle loro mansioni lavorative.
Re-keying	Processo di modifica delle chiavi di crittografia per limitare la quantità di dati da crittografare con la stessa chiave.
Rete	Due o più computer connessi tra loro per condividere risorse.
Rete attendibile	Rete di un'organizzazione che può essere controllata o gestita dall'organizzazione stessa.
Rete non attendibile	Una rete esterna alle reti che appartengono a un'organizzazione e che l'organizzazione non è in grado di controllare o gestire.
Rete privata	Rete stabilita da un'organizzazione che utilizza uno spazio degli indirizzi IP privato. Le reti private sono comunemente pensate come reti locali. L'accesso alla rete privata da parte delle reti pubbliche deve essere opportunamente protetto mediante l'uso di firewall e router.

Termine	Definizione
Rete pubblica	Rete stabilita e gestita da un provider di telecomunicazioni, per lo scopo specifico di fornire servizi di trasmissione dati al pubblico. I dati sulle reti pubbliche possono essere intercettati, modificati e/o deviati durante il transito. Esempi di reti pubbliche nell'ambito di PCI DSS comprendono, senza limitazioni, Internet e le tecnologie wireless e mobile.
Reti wireless	Reti che connettono i computer senza un collegamento fisico mediante fili.
Risanamento	Processo per l'eliminazione dei dati sensibili da un file, dispositivo o sistema, o per la modifica dei dati inutili in caso di accesso a seguito di un attacco.
Rootkit	Tipo di software dannoso che, una volta installato senza autorizzazione, è in grado di celare la sua presenza e di ottenere il controllo amministrativo di un sistema informatico.
Router	Hardware o software che connette due o più reti. Svolge le funzioni di ordinamento e interpretazione osservando gli indirizzi e passando le informazioni alle destinazioni appropriate. I router software sono a volte definite gateway.
RSA	Algoritmo per la cifratura a chiave pubblica descritto nel 1977 da Ron Rivest, Adi Shamir e Len Adleman del Massachusetts Institute of Technology (MIT); le lettere RSA sono le iniziali dei loro cognomi.
SANS	Acronimo di SysAdmin, Audit, Networking and Security. Un istituto che fornisce formazione per la sicurezza informatica e certificazione professionale. Vedere www.sans.org .
SAQ	Acronimo di Self-Assessment Questionnaire, questionario di autovalutazione. Strumento utilizzato da qualsiasi entità per validare la sua conformità a PCI DSS.
Scansione della protezione di rete	Processo mediante il quale i sistemi di un'entità vengono controllati in remoto alla ricerca di vulnerabilità, per mezzo di strumenti automatici o manuali. Scansioni di protezione che includono l'analisi di sistemi interni ed esterni e la creazione di rapporti sui servizi esposti alla rete. Le scansioni possono identificare le vulnerabilità in sistemi operativi, servizi e dispositivi che possono essere utilizzate da utenti non autorizzati.
Scienza legale	Definita anche "scienza forense per l'informatica". Per quanto riguarda la sicurezza delle informazioni, l'applicazione di strumenti di indagine e tecniche di analisi per raccogliere prove dalle risorse informatiche al fine di determinare la causa delle compromissioni dei dati.
SDLC	Acronimo di System Development Life Cycle. Fasi dello sviluppo di un software o di un sistema informatico che comprendono pianificazione, analisi, progettazione, test e implementazione.
Segmentazione di rete	Mezzi per ridurre l'ambito di una valutazione PCI DSS limitando le dimensioni dell'ambiente dei dati dei titolari di carte. Per ottenere questo risultato, i sistemi che non memorizzano, elaborano o trasmettono i dati dei titolari di carte devono essere isolati dai sistemi che memorizzano, elaborano o trasmettono i dati dei titolari di carte mediante controlli di rete. Vedere la sezione Segmentazione di rete in <i>Requisiti PCI DSS e procedure di valutazione della sicurezza</i> per istruzioni sull'uso della segmentazione di rete.
Separazione dei compiti	Pratica di divisione dei passaggi di una funzione tra individui diversi, in modo da evitare che una singola persona possa sabotare il processo.

Termine	Definizione
Server	Computer che fornisce un servizio ad altri computer, ad esempio l'elaborazione delle comunicazioni, la memorizzazione dei file o l'accesso a un servizio di stampa. I server comprendono, senza limitazioni, Web, database, applicazioni, autenticazione, DNS, posta, proxy e NTP.
Server Web	Computer che contiene un programma che accetta richieste HTTP dai client Web e serve le risposte HTTP (in genere pagine Web).
SHA-1/SHA-2	Acronimo di Secure Hash Algorithm. Un insieme di funzioni di hash crittografico correlate che comprende SHA-1 e SHA-2. Vedere <i>Crittografia avanzata</i> .
Sicurezza delle informazioni	Protezione delle informazioni per garantire la riservatezza, l'integrità e la disponibilità.
Sistema informatico	Insieme discreto di risorse dati strutturate, organizzato per la raccolta, l'elaborazione, la manutenzione, l'uso, la condivisione, la distribuzione o lo smaltimento delle informazioni.
Sistema operativo	Software di un sistema informatico responsabile della gestione e della coordinazione di tutte le attività e della condivisione delle risorse del computer. Alcuni esempi di sistemi operativi sono Microsoft Windows, Mac OS, Linux e Unix.
Smagnetizzazione	Definita anche "smagnetizzazione del disco". Processo o tecnica per smagnetizzare il disco in modo tale che tutti i dati memorizzati sul disco siano permanentemente distrutti.
Smart card	Detta anche "carta con chip" o "carta IC (Integrated Circuit)". Un tipo di carta di pagamento in cui sono incorporati circuiti integrati. I circuiti, detti anche "chip", contengono i dati della carta di pagamento, compresi senza limitazioni i dati equivalenti a quelli della striscia magnetica.
SNMP	Acronimo di Simple Network Management Protocol. Supporta il monitoraggio dei dispositivi di rete per qualsiasi condizione che richiede attenzione a livello amministrativo.
Software dannoso/malware	Software progettato per infiltrarsi in un sistema informativo o danneggiarlo senza che l'utente ne sia a conoscenza o abbia dato il consenso. Il software di questo tipo in genere penetra nella rete durante molte attività aziendali approvate, sfruttando così le vulnerabilità del sistema. Gli esempi comprendono virus, worm, cavalli di Troia, spyware, adware e rootkit.
Split knowledge	Condizione in cui due o più entità dispongono separatamente di componenti chiave che singolarmente non trasmettono alcuna conoscenza sulla chiave crittografica risultante.
Spoofing dell'indirizzo IP	Tecnica di attacco utilizzata da un utente non autorizzato per ottenere accesso ai computer. L'utente non autorizzato invia messaggi ingannevoli a un computer con un indirizzo IP che indica che il messaggio proviene da un host attendibile.
Spyware	Tipo di software dannoso che, una volta installato, intercetta o assume il controllo parziale del computer senza il consenso dell'utente.
SQL	Acronimo di Structured Query Language. Linguaggio informatico utilizzato per creare, modificare e recuperare i dati dai sistemi di gestione dei database relazionali.

Termine	Definizione
SQL injection	Forma di attacco su siti Web guidati da database. Un utente non autorizzato esegue comandi SQL non autorizzati sfruttando il codice non sicuro su un sistema connesso a Internet. Gli attacchi SQL injection sono utilizzati per sottrarre informazioni da un database in cui i dati normalmente non sarebbero disponibili e/o per ottenere l'accesso ai computer host di un'organizzazione tramite il computer che ospita il database.
SSH	Abbreviazione di "secure shell". Suite di protocolli che fornisce la cifratura dei servizi di rete, quali accesso remoto o trasferimento di file remoto.
SSL	Acronimo di Secure Sockets Layer. Standard di settore che cifra il canale tra un browser Web e il server Web per garantire la riservatezza e l'affidabilità dei dati trasmessi su questo canale.
Supporto elettronico rimovibile	Supporto che memorizza dati digitalizzati e che può essere facilmente rimosso e/o trasportato da un sistema informatico a un altro. Esempi di supporti elettronici rimovibili comprendono CD-ROM, DVD-ROM, unità flash USB e unità disco rigido rimovibili.
SysAdmin	Abbreviazione di "system administrator", amministratore di sistema. Individuo con privilegi elevati, responsabile della gestione di un sistema o di una rete di computer.
TACACS	Acronimo di Terminal Access Controller Access Control System. Il protocollo di autenticazione remota utilizzato comunemente nelle reti che comunicano tra un server di accesso remoto e un server di autenticazione per determinare i diritti di accesso dell'utente alla rete.
TCP	Acronimo di Transmission Control Protocol. Protocollo o linguaggio di comunicazione di base di Internet.
TDES	Acronimo di Triple Data Encryption Standard; definito anche 3DES o Triple DES. Cifratura a blocchi formata dalla applicazione per tre volte della cifratura DES. Vedere <i>Crittografia avanzata</i> .
TELNET	Abbreviazione di Telephone Network Protocol. Utilizzato in genere per fornire sessioni di accesso ai dispositivi di una rete dalla riga di comando orientata all'utente. Le credenziali dell'utente vengono trasmesse in chiaro.
Test di penetrazione	I test di penetrazione tentano di sfruttare le vulnerabilità per controllare se è possibile accedere in modo non autorizzato o eseguire altre azioni dannose. I test di penetrazione includono test a livello di rete e applicazione nonché altri controlli e processi relativi a reti e applicazioni e vengono eseguiti sia dall'esterno della rete per verificare l'accesso (test esterno) che dall'interno della rete.
Titolare di carta	Cliente consumatore e non per cui viene emessa una carta di pagamento o qualsiasi individuo autorizzato a utilizzare la carta di pagamento.
TLS	Acronimo di Transport Layer Security. Progettato per garantire la segretezza e l'integrità dei dati tra due applicazioni di comunicazione. TLS è il successore di SSL.
Token	Hardware o software che esegue l'autenticazione dinamica o a due fattori.
Token indicizzato	Un token crittografico che sostituisce il numero PAN in base a un dato indice per un valore imprevedibile.
Troncatura	Metodo per rendere illeggibile l'intero numero PAN rimuovendo in modo permanentemente una parte dei dati PAN.

Termine	Definizione
Uso di filtri in ingresso	Metodo di filtraggio del traffico in ingresso in una rete interna attraverso un router, secondo il quale i pacchetti in ingresso vengono verificati per garantire che provengano realmente dalle reti specificate.
Uso di filtri in uscita	Metodo di filtraggio del traffico in uscita da una rete interna attraverso un router, in modo tale che il traffico non autorizzato non lasci mai la rete interna.
Utenti non consumatori	Individui, ad esclusione dei titolari di carte, che accedono ai componenti di sistema, compresi senza limitazioni dipendenti, amministratori e terze parti.
VLAN	Abbreviazione di Virtual LAN o "virtual local area network", rete locale virtuale. Rete locale logica che si estende oltre una singola rete locale fisica tradizionale.
VPN	Acronimo di Virtual Private Network. Una rete di computer in cui alcune connessioni sono circuiti virtuali all'interno di una rete più grande, ad esempio Internet, invece di collegamenti diretti mediante fili fisici. I punti finali della rete virtuale sono in tunneling nella rete più grande, quando è il caso. Se un'applicazione comune è costituita da comunicazioni attraverso la Internet pubblica, una VPN può o meno disporre di caratteristiche di sicurezza avanzata quali l'autenticazione o la cifratura del contenuto.
Vulnerabilità	Punti deboli in un sistema che consentono a un utente non autorizzato di sfruttare quel sistema e violarne l'integrità.
WAN	Acronimo di Wide Area Network. Rete di computer che copre un'area estesa, spesso l'intero sistema informatico di una società o di una zona.
WEP	Acronimo di Wired Equivalent Privacy. Algoritmo debole utilizzato per cifrare le reti wireless. Sono stati identificati diversi punti deboli da parte degli esperti del settore, che consentono di violare una connessione WEP con software disponibile entro pochi minuti. Vedere <i>WPA</i> .
WLAN	Acronimo di Wireless Local Area Network. Rete locale che collega due o più computer o dispositivi senza l'uso di fili.
WPA/WPA2	Acronimo di WiFi Protected Access. Protocollo di protezione creato per proteggere le reti wireless. WPA è il successore di WEP e si ritiene possa fornire una sicurezza maggiore rispetto a WEP. È disponibile anche WPA2, la generazione successiva di WPA.