La sicurezza del sistema informativo

Questionario di valutazione

Con l'avvento di Internet e delle reti aziendali, l'esigenza della protezione del proprio sistema informativo diventa sempre più importante.

Questo questionario **gratuito** ha lo scopo di sensibilizzare i responsabili aziendali sui possibili rischi in cui può incorrere l'Azienda se non vengono adottati comportamenti e misure di sicurezza adeguate.

Le domande del questionario, basate su un sottoinsieme dello standard internazionale ISO17799 (BS7799), sono di tipo generale e non permettono quindi di analizzare in profondità ogni aspetto, ma danno comunque la possibilità di ottenere una valutazione del livello di sicurezza nella gestione dei dati all'interno dell'azienda.

Il questionario è utilizzabile off line e la valutazione finale, elaborata in base alle risposte inserite, è automatica, immediata e rigorosamente anonima.

Per una valutazione più approfondita e personalizzata vi invitiamo sulle pagine di www.tecnoteca.com

Istruzioni per la compilazione

Rispondere alle domande selezionando, dalla lista delle risposte disponibili, quella che si avvicina di più alla situazione aziendale.
Ogni domanda può avere risposta:

SI NO NON SO

Nel caso abbiate dei dubbi sulla risposta e non abbiate la possibilità di informarvi, scegliete la risposta "non so".
Dopo aver risposto a tutte le domande*, fate click sul pulsante "analisi risposte" per avere una valutazione della sicurezza del proprio sistema informativo.
Il questionario può essere liberamente stampato e/o distribuito ad altre persone.

* Se state usando Acrobat Reader per compilare il questionario, alla chiusura del documento, non verranno salvate le risposte; questa limitazione è legata allla versione *Reader* del programma. Utilizzando Acrobat, le risposte verranno salvate.

Sistema informativo in generale

Esiste un registro con l'inventario dell'Hardware/Software posseduto? • Un inventario aggiornato (contenete nome del singolo materiale, matricola, data di acquisto, data di scadenza garanzia, assegnatario del materiale, etc.) consente di rintracciare sempre tutto il proprio materiale informatico	NON SO
Il vostro sistema informativo è salvaguardato dalle interruzioni della energia elettrica? • Uno o più gruppi di continuità permettono di mantenere l'integrità dei dati anche nel caso di mancanza di corrente	NON SO
I salvataggi dei dati (backup su nastro o altro supporto magnetico rimovibile) vengono eseguiti con frequenza giornaliera o comunque sufficiente a garantire un rapido ripistino della funzionalità del sistema informativo? • La frequenza dei salvataggi dipende dalle procedure aziendali ma non deve essere mai superiore alla settimana	NON SO
I salvataggi eseguiti (nastro o altro supporto magnetico rimovibile), vengono adeguatamente custoditi? • Una cassaforte o un contenitore resistente al fuoco possono salvaguardare i dati aziendali da furti e incendi.	NON SO
L'utente di un PC portatile, *organizer* o *PDA*, si assicura che i dati ivi contenuti vengano salvati con regolarità? • Molto spesso i dati contenuti in un portatile sono di rilevante importanza per l'utente/azienda: senza un adeguato salvataggio periodico c'è il rischio di perdere anche mesi di lavoro.	NON SO
Il sistema informativo è adeguatamente salvaguardato contro le perdite di dati con procedure documentate di salvataggio e ripristino? • L'indisponibilità dei sistemi e/o dei dati può rallentare o fermare il normale processo produttivo	NON SO
Le procedure di salvataggio e ripristino dei dati sono adeguatamente documentate e provate? • Nel caso in cui tali procedure non vengano rispettate, i dati possono venire persi o non essere più disponibili, compromettendo l'efficienza aziendale	NON SO
L'uso di dispositivi di supporto rimuovibili (Floppy, nastri, CD-ROM) è disponibile solo al personale autorizzato? • La perdita o "scomparsa" di alcuni supporti può compromettere la riservatezza dei dati aziendali e/o l'integrità degli stessi. • Documenti apparentemente "innocui" potrebbero essere infettati da virus	NON SO
La rete interna è progettata per garantire prestazioni, affidabilità e un corretto grado di controllo degli accessi ? (privilegi/restrizioni) • Prestazioni ridotte della rete possono rallentare la produttività • Un inadeguato controllo degli accessi può inficiare l'integrità dei dati	NON SO
L'Hardware che deve venire rottamato/dismesso viene controllato per evitare che vengano esposte informazioni dell'azienda? • Informazioni e dati dell'azienda possono essere "recuperate" anche da dischi rigidi che sono stati formattati/cancellati.	NON SO
L'azienda rispetta i termini delle licenze di uso del software? • Non essere in regola con le licenze d'uso del software può comportare problemi legali • Eventuali restrizioni all'uso dei programmi possono causare ulteriori spese • Nel caso in cui la licenza del software sia scaduta, il venditore può rifiutare di fornire assistenza al cliente	NON SO
Gli aggiornamenti (*patch*) al software vengono fatti solo quando effettivamente necessari? • In talune situazioni, un aggiornamento al software può comportare più problemi che soluzioni. • Ogni aggiornamento deve essere accuratamente controllato prima di procedere alla installazione sui sistemi dell'azienda	NON SO
L'origine degli aggiornamenti è verificata? • Se non si conosce l'affidabilità (riviste, CD, ...) della fonte di un aggiornamento è consigliabile rivolgersi direttamente al produttore.	NON SO

L'aggiornamento a versioni più recenti di specifico software è accuratamente valutato? • Certi programmi richiedono particolari versioni di software/hardware non disponibili sui sistemi dell'azienda, con conseguente lievitazione dei costi dovuti alla necessità di aggiornare il sistema operativo e/o l'hardware. • Possono esistere incompatibilità con procedure sviluppate internamente all'azienda o con formati file non più supportati. • Per contro, il cliente potrebbe non ricevere più supporto per versioni di software troppo "vecchie"	NON SO
Il sistema informativo è amministrato con procedure accuratamente documentate che garantiscono la sicurezza dei dati? • Il non adempimento di queste regole può portare a interruzioni dei servizi o a scarsa affidabilità	NON SO
La documentazione relativa alla gestione del sistema informativo viene mantenuta costantemente aggiornata? • La documentazione tecnica mancante o non adeguatamente aggiornata (specialmente per sistemi "vecchi") aumenta le difficoltà di gestione e i tempi di analisi: - si deve dipendere totalmente da alcuni dipendenti chiave - non è possibile verificare le proposte di modifica al sistema - non è possibile aggiornare il personale tecnico • La documentazione non aggiornata può causare problemi alle operazioni di manutenzione	NON SO
Le procedure operative del sistema informativo sono correttamente pianificate, autorizzate e documentate? • In mancanza di documentazione, un eventuale aggiornamento del sistema informativo può non essere completato	NON SO

Gestione risorse umane

Nella vostra azienda esiste una figura dedicata alla gestione del sistema informativo che segue anche le procedure di sicurezza? • Un amministratore di sistema che non sia preparato in maniera adeguata può commettere errori molto costosi alla azienda • La stessa figura, per il tipo di lavoro svolto, deve poter garantire una notevole riservatezza	NON SO
Il personale (specialmente i responsabili) è adeguatamente informato degli eventuali rischi che ci possono essere nel non seguire le procedure di sicurezza informatica previste in azienda? • Un dipendente non informato può inavvertitamente rendere disponibili informazioni riservate	NON SO
L'azienda offre (specialmente ai responsabili) dei corsi di aggiornamento sui nuovi sistemi e sulle nuove tecniche di protezione dei dati? • La sicurezza dell'azienda può essere compromessa da tecniche e/o programmi sconosciuti ai responsabili della sicurezza	NON SO
Quando un nuovo dipendente entra in azienda gli viene creato immediatamente un account personale con specifici diritti di accesso? • Un nuovo dipendente potrebbe accedere ad informazioni riservate utilizzando l'account concessogli temporaneamente da un collega	NON SO
Nel caso in cui un dipendente lasci l'azienda, vengono prese le dovute precauzioni relativamente ai suoi diritti di accesso? • Un dipendente che lasci l'azienda in un quadro di rapporti conflittuali potrebbe intraprendere azioni di ritorsione ai danni del sistema informativo aziendale	NON SO
Una volta che un dipendente ha lasciato l'azienda, vengono tempestivamente "bloccati" tutti i suoi accessi al sistema informativo? • L'ex dipendente potrebbe aver lasciato, come eredità a qualche collega, le chiavi di accesso (password) a servizi riservati	NON SO
I dipendenti sono stati informati del fatto che l'utilizzo delle risorse (computer/internet) è ammesso esclusivamente per utilizzi aziendali? • I computer possono venire utilizzati per scaricare materiale pornografico o comunque non pertinente alle attività dell'azienda (bisogna ricordare che ogni sito mantiene un "registro" delle visite in cui può comparire anche il nome della propria azienda) • I dipendenti possono "perdere" tempo utilizzando *chat* o "navigando" su siti non correlati alle attività aziendali	NON SO

Quando un dipendente si assenta dalla postazione di lavoro ha l'accortezza di non lasciare applicazioni "aperte"? • Negli uffici *open space* è facile esporre informazioni riservate se, assentandosi, si lasciano i programmi aperti. • Bastano pochi minuti per copiare/trasferire dati riservati su di un altro PC o su di un floppy disk	NON SO
Quando un utente si assenta dalla propria postazione di lavoro provvede a disconnettersi dal sistema [fa *logout*] o a bloccare il sistema con una password? • Chiunque può accedere, tramite il PC lasciato incustodito, a tutte le risorse, anche di rete, a cui l'utente e' abilitato grazie all'autenticazione già avvenuta	NON SO
Sono state prese adeguate contromisure per impedire l'installazione di *screen-saver* (programmi salva-schermo) da parte di personale non autorizzato? • *Screen-saver* non "sicuri" possono includere *virus* o altri programmi "maliziosi", rendendo la propria rete interna non sicura.	NON SO
L'utilizzo di apparecchiature di proprietà dell'azienda, al di fuori della stessa, è permesso solo a personale autorizzato? • Dati confidenziali possono venire esposti a terzi • Senza regole e procedure precise, un dispositivo può andare "perso" o "smarrito" senza che si possa individuare il responsabile.	NON SO
Il personale che utilizza PC portatili è informato dei rischi insiti nel loro utilizzo? • Un furto del portatile può esporre dati riservati a terzi • Dati confidenziali possono venire mostrati a persone non autorizzate • Un virus può danneggiare i dati in modo irrecuperabile • Molto spesso (per ragioni di praticità), la sicurezza di un portatile che viene connesso a reti che non siano quella dell'azienda, è ridotta al minimo, facilitando notevolmente il furto di dati	NON SO
Gli impiegati in viaggio di lavoro, sanno di essere responsabili dei dati che trasportano? • I documenti trasportati possono venire rubati o andare persi	NON SO
I PC portatili sono usati solo dal loro proprietario e solo per gli utilizzi a cui sono destinati? • Il portatile può essere utilizzato anche da familiari o amici, esponendo dati e informazioni a persone non autorizzate • Il portatile può venire rubato	NON SO

Sicurezza generale

L'amministratore di sistema è adeguatamente informato e conosce a fondo i problemi relativi alla sicurezza? • Un continuo monitoraggio di tutta la rete aziendale ed un continuo aggiornamento sui nuovi possibili attacchi è fondamentale al fine di evitare gravi danni all'azienda. Prevenire è meglio che curare.	NON SO
Sono stati definiti degli standard che gestiscono l'accesso ai dati? • La mancanza di regole può portare all'accesso indiscriminato ai dati dell'azienda • Regole troppo rigide o inflessibili possono rallentare il processo produttivo	NON SO
Esiste un documento (riservato) che specifica i vari livelli di accesso ai dati aziendali? • La gestione non opportunamente documentata dei privilegi può comportare notevoli ritardi nella scoperta di come un attacco è stato portato a termine, o nella gestione di successive modifiche ai livelli di accesso per far fronte a nuove esigenze. È essenziale sapere in ogni istante chi può fare cosa.	NON SO
Le informazioni riservate sono protette contro gli accessi da parte di personale non autorizzato? • Informazioni riservate, non classificate come tali, possono venire divulgate • La pratica di fare copie multiple di file (perché richieste da più persone) può inficiare l'affidabilità. Questa pratica riflette anche la limitatezza del proprio sistema informativo	NON SO
L'accesso da parte di terzi alle informazioni aziendali è correttamente protetto/gestito? • Informazioni riservate e/o strategiche possono essere accedute da terzi e divulgate all'esterno con grave danno per l'azienda.	NON SO
Le password vengono scelte in base a principi di sicurezza? • Password note a più persone, possono comportare l'accesso al sistema informativo anche da parte di persone non autorizzate • Utenti che devono accedere a più sistemi/servizi possono avere trascritto le password in una agenda, vanificando quindi la sicurezza del sistema	NON SO

Il personale considera le password come materiale altamente confidenziale? • Il non ottemperare a questa regola può rendere disponibili informazioni riservate	NON SO
L'accesso alla rete aziendale dall'esterno, se permesso, è protetto da procedure di autenticazione, crittografazione e da una appropriata gestione dei privilegi? • Procedure inadeguate di sicurezza possono portare ad accessi non autorizzati, con conseguenze anche disastrose	NON SO
Sono implementate procedure di controllo sull'accesso dall'esterno ai dati aziendali? • Il solo utilizzo di un *nomeUtente/Password* molto spesso non è sufficiente: può essere necessario crittografare i dati	NON SO
L'accesso alle risorse del sistema informativo è monitorato per identificare l'utilizzo improprio delle risorse? • Senza un monitoraggio continuo, un accesso non autorizzato può non venire identificato, dando origine ad un "buco" nella sicurezza del sistema. • Senza un archivio degli accessi al sistema, non è possibile documentare una eventuale intromissione, vanificando le eventuali azioni legali contro l'intruso.	NON SO
L'accesso alle informazioni/documenti è permesso solo al personale autorizzato? • Un mancato controllo sugli accessi (attraverso password o altro), può far si che i documenti possano venire copiati, modificati o anche distrutti per errore o maliziosamente • Se l'accesso è troppo restrittivo, gli utenti possono essere tentati a condividere le password per accedere ai dati.	NON SO
I documenti vengono archiviati in modo da rispettare le esigenze legali e/o interne? • La cancellazione di archivi considerati "inutili" può portare a rallentamenti nel flusso di lavoro e/o a situazioni imbarazzanti • E' necessario accertarsi che i documenti siano archiviati per il tempo legale minimo	NON SO
I documenti riservati sono protetti tramite password o sono comunque memorizzati in *directory* protette contro accessi non autorizzati? • Le password di accesso ad un documento possono andare perse o dimenticate, mentre l'accesso a documenti protetti è comunque sempre possibile per l'amministratore di sistema	NON SO
Il personale ha cura di evitare la stampa di documenti riservati su stampanti di rete? • Quando si stampano documenti riservati su di una stampante di rete, ci si deve assicurare che sia presente un responsabile che ritiri subito la stampa.	NON SO

Internet

I dipendenti sono stati edotti dei potenziali rischi insiti nella navigazione su internet e sull'utilizzo della posta elettronica? • L'accesso a siti "inappropriati" e lo scaricamento di file non autorizzati possono essere in contrasto con la politica aziendale e, in alcuni casi, anche illegali. • Molto spesso l'utente non è a conoscenza del fatto che che ogni sito visitato registra tutte le operazioni svolte e che molto spesso memorizza dei *cookies* relativi alle abitudini/preferenze del visitatore	NON SO
Il personale è stato informato dei possibili rischi insiti nell'utilizzo di un *browser* (Internet Explorer, Netscape, …) o un programma di posta elettronica non configurato secondo le esigenze di sicurezza dell'azienda? • Se in uno di questi programmi è attivato l'utilizzo dei *cookies* o l'esecuzione di *Java Applets, Java Script* e *ActiveX*, c'è la possibilità che venga eseguito del codice "malizioso", dando la possibilità a *virus* di infettare la macchina • Un firewall (dispositivo che respinge gli attacchi alla propria rete interna) non può nulla contro attacchi provenienti da un browser mal configurato. • Informazioni riservate possono venire memorizzate e lette utilizzando i *cookies*, senza che l'utente ne sia al corrente	NON SO
Il personale addetto alla configurazione dell'accesso a Internet, ha predisposto le protezioni adeguate perché i rischi siano ridotti al minimo (es. uso di un *firewall* [dispositivo che respinge gli attacchi alla propria rete interna])? • Le connessioni fisse a Internet offrono notevoli opportunità ad *hacker* ed altri malintenzionati di verificare se esistono punti deboli nella rete aziendale. • I rischi possono provenire anche dall'interno: l'accesso non autorizzato ad Internet da parte dei dipendenti porta ad una riduzione delle prestazioni della connessione e ad una minore efficienza.	NON SO

È stata data priorità alla difesa del sistema informativo da eventuali attacchi esterni? • Il proprio sito web può venire "violato", esponendo informazioni riservate o dando la possibilità all'attaccante di modificare i dati contenuti. Ciò può essere imbarazzante per l'immagine aziendale • Senza una precisa politica di difesa dagli attacchi, gli accessi non autorizzati possono passare inosservati o può essere impossibile identificare i punti deboli del proprio sistema	NON SO
Esistono procedure (analizzate, aggiornate e regolarmente provate) che, in caso di attacco della propria rete, permettano un rapido ripristino del funzionamento del proprio sistema? • I crimini informatici possono avere un notevole impatto sul proprio sistema informativo e sulla immagine aziendale. Senza una pianificazione contro tali eventi, la riattivazione delle normali funzioni lavorative può essere molto dispendiosa in termini di tempo e risorse.	NON SO
Ogni macchina che può accedere a internet è protetta da un *antivirus* AGGIORNATO? • Non aggiornare gli antivirus può essere più pericoloso che non averne: si crea una falsa sicurezza che può portare a situazioni catastrofiche	NON SO
Esistono procedure per gestire le eventuali infezioni da *virus*? • Senza tali procedure, una infezione può ripetersi più volte, rendendone difficile la sua completa eliminazione. • Non rispondendo immediatamente alla infezione, il proprio sistema informativo può arrivare in tempi rapidi ad uno stato di blocco totale	NON SO
I documenti riservati, quando spediti, sono garantiti da una firma digitale e sono protetti dalle eventuali modifiche? • La inadempienza di tali procedure di sicurezza comporta il fatto che le informazioni spedite non sono garantite	NON SO
I documenti che vengono spediti in forma elettronica (email, CD-ROM, …) sono controllati relativamente al loro contenuto e alla possibilità di infezioni da parte di virus? • La trasmissione di *virus* può danneggiare l'immagine della azienda • Trasmettere documenti riservati via e-mail senza averli protetti è come spedire una cartolina: chiunque può leggerne il contenuto. • La spedizione di messaggi personali usando gli *account* dell'azienda può portare a spiacevoli conseguenze: un documento contenente considerazioni personali può avere come conseguenza immediata l'attribuzione all'azienda di posizioni ufficiali non condivise con grave compromissione dell'immagine aziendale.	NON SO
I documenti ricevuti via e-mail vengono aperti solo dopo un controllo preventivo del loro contenuto? • Il rischio di infezioni da parte di *virus* e *cavalli di troia* (programmi apparentemente innocui) attraverso la posta elettronica è estremamente elevato.	NON SO
I messaggi di posta elettronica non richiesti (di cui non si conosce il mittente) vengono trattati con la massima circospezione? • Rispondere ad uno di questi messaggi potrebbe rivelare informazioni relative alla propria azienda o dare la conferma ad un potenziale attaccante che l'indirizzo usato è valido ed effettivamente usato.	NON SO
Viene eseguito un controllo adeguato sul materiale scaricato dalla rete (internet)? • Quando vengono scaricati programmi [download], alcuni di essi, specialmente se provenienti da siti non sicuri, possono essere infettati da *virus* o *cavalli di troia* (programmi apparentemente innocui). • Vengono lette con accuratezza le licenze di uso di tali programmi? • Le informazioni presenti su internet possono non essere accurate, non valide o deliberatamente false: ogni decisione basata su di esse deve essere controllata	NON SO
Il personale abilitato all'uso della carta di credito, è informato sui rischi degli acquisti su internet? • Trasferire informazioni relative alla carta di credito su canali di trasmissione non sicuri (non crittografati) può compromettere la sicurezza della transazione • Un eventuale furto dal sito dove è stato fatto un acquisto, può esporre a malintenzionati il numero della carta di credito • Si ha la certezza che il sito su cui viene fatto l'acquisto sia affidabile?	NON SO
Gli indirizzi di dominio (es: www.azienda.it) vengono trattati come bene di valore? • Dimenticare di rinnovare la registrazione del proprio dominio, può renderlo disponibile a terzi che, di conseguenza, possono ricevere informazioni relative alla propria azienda e trasmettere informazioni per conto della propria azienda	NON SO
Se il proprio sito è ospitato da un fornitore di servizi [ISP], ci si è accertati della effettiva esperienza dell'ISP in termini di sicurezza? • In caso di problemi, la perdita dell'immagine è comunque della azienda, non dell'ISP	NON SO

Il vostro sito WEB è gestito solo da personale autorizzato e qualificato, capace di garantirne la sicurezza? • L'accesso alla rete interna (attraverso il sito WEB) può portare alla esposizione di informazioni a persone non autorizzate. • Intrusioni da parte di hacker sul vostro sito possono compromettere l'immagine della azienda.	NON SO
Se si possiede un sito web che offra un servizio di commercio elettronico, è stata data la massima priorità a tutti gli aspetti di sicurezza? • Anche una minima crepa nella sicurezza del sito può portare a conseguenze disastrose per la immagine della azienda	NON SO

Analisi Risposte