

Servizio "Ask the Expert" - Linee guida questionario

Glossario

Amministratore di sistema: Individuo o gruppo di individui responsabile della supervisione dell'operatività di un sistema informatico o di una rete. Questa posizione comporta normalmente privilegi speciali, tra cui l'accesso al livello di protezione, al software e alla configurazione di un sistema.

Mobile Device Management: Consiste nell'amministrazione dei dispositivi mobili come smartphone, tablet, computer, laptop e desktop. L'MDM viene solitamente implementato attraverso un prodotto di terze parti che permette la gestione remota dei dispositivi mobili (es. configurazioni, blocco dispositivo, aggiornamenti obbligatori).

NAC (Network Access Control): Una funzione fornita da alcuni sistemi di firewall che consente l'accesso in base alle credenziali dell'utente e ai risultati dei controlli di sicurezza eseguiti sul dispositivo che richiede l'accesso alla rete (es. verifica aggiornamenti antivirus).

Proxy: Dispositivo o programma che funge da intermediario allo scopo di fornire servizi di comunicazione e di altro tipo tra un client e un server. Il software agisce per conto del client inviando la richiesta alla destinazione desiderata. L'utilizzo del proxy chiude il percorso diretto tra le reti interne ed esterne, rendendo più difficile per un utente malintenzionato ottenere indirizzi interni e altri dettagli della rete interna dell'organizzazione.

Rete informatica interna: Una rete informatica la cui creazione, manutenzione e fornitura di controlli di sicurezza sono sotto il controllo diretto di dipendenti dell'organizzazione o dei suoi fornitori. Una rete interna è tipicamente di proprietà dell'organizzazione e non esposta all'esterno. In alcuni casi l'organizzazione può gestire reti di cui non è proprietaria (outsourcing). Le connessioni interne sono connessioni che avvengono all'interno di una rete informatica interna.

Server: Computer o dispositivo di una rete che gestisce le risorse di rete. Alcuni esempi includono i file server (per archiviare i file), i web server (per pubblicare le pagine web), i print server (per gestire una o più stampanti), i server di rete (per gestire il traffico di rete) e i server di database (per elaborare le query di database).

Soluzioni di DNS protection & filtering: Il DNS è il sistema che converte i nomi di dominio (es. www.example.com) in indirizzi IP delle risorse pubblicate (es. sito web). Questo permette un accesso semplificato alle risorse utilizzando il solo nome di dominio e un web browser. Spesso le organizzazioni si dotano di meccanismi di protezione come il DNS protection & filtering che include sistemi di anti-malware, anti-phishing e di filtraggio dei contenuti sospetti utilizzando specifiche blacklist.

Tipologie di dati:

- **Dati personali:** Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc. Particolarmente importanti sono i dati che permettono l'identificazione diretta - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio: il codice fiscale, l'indirizzo IP, il numero di targa).
- **Dati sensibili:** dati che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale.
- **Dati giudiziari:** dati che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio: i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
- **Altri dati personali:** con l'evoluzione delle nuove tecnologie altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

Trattamento dei dati: Trattamento è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali.

URL: Un riferimento a una risorsa Web che specifica la sua posizione su una rete di computer e un meccanismo per recuperarla. Un tipico URL può avere la forma <http://www.example.com/index.html>, che indica un protocollo (http), un nome di host (www.example.com) e un nome di file (index.html). A volte viene definito anche indirizzo web.

Linee guida questionario

Domanda 2:

#numero di workstation

Elementi da considerare per la corretta interpretazione della domanda:

Include tutti gli asset aziendali come laptop, desktop e tablet.

Domanda 3:

#numero di server

Elementi da considerare per la corretta interpretazione della domanda:

Include web server, Database server, mail server, file server, proxy server.

Domanda 8:

Nell'ambito degli asset oggetto della polizza, ve ne sono alcuni in Cloud?

Elementi da considerare per la corretta interpretazione della domanda:

L'utilizzo di tecnologie cloud offre numerosi vantaggi ma è necessario considerare i rischi associati all'utilizzo di questa tecnologia tra cui, primariamente, quello legato alla sicurezza dei dati. È quindi fondamentale accertare l'affidabilità del fornitore, valutandone le misure di sicurezza adottate, la ripartizione delle responsabilità tra le parti, e le misure adottate per garantire la continuità operativa a fronte di eventuali e imprevisti malfunzionamenti.

Domanda 9:

Nell'ambito degli asset oggetto della polizza, ve ne sono alcuni qualificabili come Mobile Device?

Elementi da considerare per la corretta interpretazione della domanda:

L'utilizzo di Mobile Device quali smartphone e tablet richiede una adeguata consapevolezza dei rischi e delle vulnerabilità ad essi legati. È quindi fondamentale la presenza di metodologie definite di Mobile Device Management che includano la sicurezza dei dispositivi e una formazione dedicata al personale che utilizza tali strumenti.

Domanda 10:

Esiste un processo di IT e Security Governance per il quale sono state chiaramente definite responsabilità per la sicurezza IT/delle informazioni?

Elementi da considerare per la corretta interpretazione della domanda:

La definizione di un processo di IT e Security Governance garantisce che le strategie di sicurezza delle informazioni siano allineate con gli obiettivi aziendali e coerenti con la normativa applicabile attraverso la predisposizione di policy, processi e procedure e la definizione di ruoli e responsabilità.

Domanda 11:

La Società ha designato un responsabile per la protezione dei dati personali?

Elementi da considerare per la corretta interpretazione della domanda:

Secondo quanto stabilito dal regolamento UE 2016/679, la nomina del DPO è adempimento obbligatorio quando il titolare del trattamento: a) è autorità/organismo pubblico (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali); b) effettua trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; c) effettua come attività principali trattamenti su larga scala di dati sensibili, genetici, biometrici, giudiziari. Il DPO ha compiti di informazione, formazione, consulenza e sorveglianza dell'adempimento della disciplina Privacy, ed è l'interlocutore dell'autorità di controllo.

Domanda 12:

Un elenco di tutti gli asset ICT (a titolo illustrativo e non esclusivo, workstation, server, database, applicazioni, network appliance, communication appliance, etc.) è regolarmente mantenuto per riflettere l'ambiente tecnologico tempo per tempo in essere?

Elementi da considerare per la corretta interpretazione della domanda:

Un inventario degli asset ICT è un elenco completo di tutte le risorse hardware e software sulla rete per consentire alle aziende di gestire efficacemente le proprie risorse IT. L'inventario deve essere costantemente aggiornato, tramite apposite procedure, per tenere traccia delle risorse e garantire che queste vengano utilizzate in modo efficace per supportare i processi aziendali.

Inoltre, la presenza di un inventario è fondamentale per monitorare e assicurare il corretto livello di sicurezza dell'intera infrastruttura IT, per la risposta agli incidenti di sicurezza e per attività di disaster recovery.

Domanda 13:

Indica le eventuali tipologie di dati particolari che la tua attività custodisce, gestisce o tratta (anche per conto terzi) relativi a:

Elementi da considerare per la corretta interpretazione della domanda:

In linea con il GDPR, sono considerati particolarmente sensibili: a) i dati che permettono l'identificazione diretta - come i dati anagrafici, le immagini, ecc., e i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad esempio: il codice fiscale, l'indirizzo IP, il numero di targa); b) i dati che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale, i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale; c) i dati relativi a condanne penali e reati, i dati c.d. "giudiziari".

Domanda 14:

Sono previsti corsi e/o test per l'intera popolazione aziendale per aumentare la consapevolezza dei rischi connessi alla privacy ed alla sicurezza delle informazioni?

Elementi da considerare per la corretta interpretazione della domanda:

La formazione aziendale in ambito privacy e sicurezza delle informazioni è necessaria per rendere i dipendenti consapevoli dei trattamenti di dati personali che svolgono quotidianamente, ma anche per limitare i rischi di sicurezza ed eventuali sanzioni.

Domanda 15:

Sono state definite, condivise e spiegate agli utenti le buone norme di utilizzo del Sistema IT e degli strumenti informatici dati in dotazione?

Elementi da considerare per la corretta interpretazione della domanda:

L'adozione di un regolamento interno sull'uso degli strumenti informatici dati in dotazione ai lavoratori è necessaria per stabilire le procedure per una corretta e adeguata gestione del patrimonio informativo aziendale.

L'azienda è tenuta a garantire a tutti i soggetti autorizzati al trattamento di dati o all'utilizzo dei sistemi IT un'adeguata e continuativa formazione in merito ai rischi di sicurezza in materia di trattamento dei dati tramite l'utilizzo degli strumenti informatici.

Domanda 16:

È fisicamente prevista una zona dedicata al contenimento degli apparati e degli archivi strategici / sensibili ad accesso limitato?

Elementi da considerare per la corretta interpretazione della domanda:

Le infrastrutture fisiche dell'azienda devono essere resilienti e adeguatamente protette da una varietà di minacce.

L'accesso alle zone e agli uffici in cui vengono trattati dati sensibili deve essere controllato e limitato. Controlli fisici negli uffici possono includere videosorveglianza, sensori di movimento, sistemi di controllo degli accessi, sistemi di allarme, serrature manuali, aree vietate all'accesso e/o altre misure analoghe che garantiscano lo stesso livello di sicurezza.

Domanda 17:

Esiste una soluzione antivirus / antimalware aggiornata periodicamente?

Elementi da considerare per la corretta interpretazione della domanda:

Una soluzione antivirus/antimalware aggiornata regolarmente svolge un ruolo fondamentale nella sicurezza informatica rilevando, prevenendo e rimuovendo malware e virus dai sistemi e dalle reti informatiche. Attraverso la scansione di file, e-mail, pagine web vengono individuate eventuali attività malevoli. L'implementazione di queste soluzioni permette una protezione dagli attacchi informatici e la riduzione del rischio di violazione dei dati, perdite finanziarie e danni reputazionali.

Domanda 18:

Esiste un sistema di accesso sicuro (es. VPN, MFA) per le connessioni esterne per la connessione al sistema informativo da parte del personale e dei fornitori esterni?

Elementi da considerare per la corretta interpretazione della domanda:

I controlli sulle connessioni esterne devono essere implementati in modo appropriato per evitare che gli utenti non autorizzati accedano ai dati e agli applicativi aziendali.

Di seguito alcuni esempi di meccanismi per la protezione degli accessi:

L'autenticazione a più fattori (MFA) è un metodo di autenticazione che richiede a un utente di fornire almeno due fattori di verifica per poter accedere a un sito web, a un'applicazione o a una risorsa. Il MFA è necessario su tutte le applicazioni che prevedono meccanismi di autenticazione, comprese le soluzioni in cloud e ibride;

Single Sign-On è un metodo di autenticazione che consente agli utenti di accedere usando un set di credenziali per più sistemi software indipendenti;

L'uso di VPN permette l'accesso sicuro alle risorse informatiche anche agli utenti remoti che lavorano da casa o su device mobili.

Domanda 19:

Esiste un sistema di accesso sicuro (es. NAC) per le connessioni interne per la connessione al sistema informativo da parte del personale e dei fornitori esterni?

Elementi da considerare per la corretta interpretazione della domanda:

Il Network Access Control (NAC) è l'insieme di processi e strumenti che limitano l'accesso di utenti e dispositivi non autorizzati a una rete aziendale o privata. Il NAC garantisce che solo gli utenti autenticati e i dispositivi autorizzati e conformi ai criteri di sicurezza possano accedere alla rete.

Domanda 20:

Esiste ed è costantemente aggiornato un sistema anti-spam e anti-phishing per tutte le caselle di posta elettronica?

Elementi da considerare per la corretta interpretazione della domanda:

I sistemi di posta elettronica devono essere protetti tramite controlli tecnici di sicurezza per prevenire attacchi di spam e phishing, modifiche non autorizzate e spoofing. Ai fini della sicurezza e di evitare la compromissione dell'utente, un sistema anti-phishing permette di definire un insieme di controlli sul livello di rischio del messaggio ricevuto e/o inviato.

Domanda 21:

Il sistema di navigazione internet è adeguatamente protetto attraverso sistemi di filtraggio delle URL, proxy e soluzioni di DNS protection & filtering?

Elementi da considerare per la corretta interpretazione della domanda:

L'utilizzo di sistemi di filtraggio delle URL, proxy e soluzioni di DNS protection & filtering consente di proteggere i sistemi dalle minacce come malware e phishing provenienti da Internet. Tramite questi sistemi è possibile bloccare l'accesso degli utenti ai siti web con contenuti potenzialmente dannosi.

Domanda 22:

Esiste un dispositivo di sicurezza perimetrale (e.g. firewall), attivo e funzionante, che protegge la rete interna comprese le eventuali sedi/ filiali esterne?

Elementi da considerare per la corretta interpretazione della domanda:

La presenza di dispositivi per la sicurezza della rete permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi. Un firewall è un sistema che costituisce una barriera tra le reti interne, sicure e controllate, e le reti esterne, e che permette di bloccare o consentire in maniera selettiva pacchetti, segmenti e protocolli.

Domanda 23:

Viene verificato periodicamente che i programmi installati siano stati correttamente acquistati e abbiano attivo il supporto del vendor?

Elementi da considerare per la corretta interpretazione della domanda:

Deve essere implementato un processo di verifica periodica sugli asset acquistati ed installati, al fine di garantirne la compliance con i requisiti di sicurezza delle informazioni e la presenza di un modello di supporto del vendor. Questo garantisce l'assistenza del fornitore nell'identificazione e nella risoluzione dei problemi tramite, ad esempio, funzionalità di supporto, eventuale escalation e aggiornamenti periodici di sicurezza sul software.

Domanda 24:

Vengono definite e mantenute delle configurazioni di sicurezza base da applicare agli apparati di rete, agli endpoint device e ai server?

Elementi da considerare per la corretta interpretazione della domanda:

La definizione e la manutenzione di configurazioni standard di sicurezza dei dispositivi (considerando anche i suggerimenti del vendor di riferimento) permettono alle aziende di proteggere dalle minacce informatiche i dispositivi che i dipendenti utilizzano per scopi lavorativi o i server che si trovano in rete o nel cloud. La corretta configurazione di sicurezza applicata agli endpoint, agli apparati di rete, o ai server, garantisce una protezione preventiva e funzionalità di rilevamento e risposta continui.

Domanda 25:

Una politica di full disk encryption è applicata sugli asset aziendali?

Elementi da considerare per la corretta interpretazione della domanda:

La full disk encryption è un metodo di sicurezza che consente di proteggere i dati sensibili a livello hardware crittografando tutti i dati presenti su un'unità disco. Questo tipo di encryption è fondamentale quando la memorizzazione e il trattamento dei dati avvengono su computer fissi, portatili, dispositivi mobili e supporti di memorizzazione esterni. I dati contenuti al loro interno saranno inaccessibili ad individui non autorizzati poiché protetti da una chiave di cifratura.

Domanda 26:

Le connessioni alla rete aziendale da remoto avvengono per il solo tramite di dispositivi sicuri forniti dall'azienda?

Elementi da considerare per la corretta interpretazione della domanda:

È necessario che tutti gli strumenti utilizzati dal personale, quali PC, notebook, tablet, smartphone, e-mail ed altri strumenti siano messi a disposizione dall'azienda per svolgere la propria attività lavorativa. Tali strumenti informatici devono essere verificati con regolarità e dotati di sistemi di sicurezza adeguati.

Domanda 27:

La soluzione antivirus / anti-malware è configurata per scansionare in automatico un media rimovibile quando inserito o connesso?

Elementi da considerare per la corretta interpretazione della domanda:

Alcune applicazioni dannose sfruttano le vulnerabilità del sistema operativo per replicarsi tramite reti locali e unità rimovibili. La predisposizione di una soluzione antivirus e anti-malware consente di eseguire automaticamente la scansione delle unità rimovibili inserite o connesse al computer alla ricerca di malware.

Domanda 28:

I device sono configurati per non eseguire in automatico il contenuto di media rimovibili quando inseriti o connessi?

Elementi da considerare per la corretta interpretazione della domanda:

Ogni volta che si collega o si inserisce un nuovo dispositivo rimovibile, il computer potrebbe tentare di eseguirne automaticamente il contenuto. È fondamentale che i device siano configurati per non eseguire in automatico il contenuto di media rimovibili, quando connessi, per evitare la diffusione di virus o l'esecuzione di script o programmi indesiderati.

Domanda 29:

È stata predisposta una password policy che preveda l'aggiornamento delle password con frequenza (almeno) annuale e dei criteri di complessità minimi in linea con le best practice di mercato?

Elementi da considerare per la corretta interpretazione della domanda:

È importante stabilire e condividere una rigorosa policy sull'utilizzo delle password. I controlli di complessità delle password devono essere implementati includendo almeno un mix di caratteri alfanumerici, lettere maiuscole e minuscole, caratteri speciali, la definizione di una lunghezza minima, della scadenza e del blocco dopo un certo numero di tentativi falliti.

Domanda 30:

Gli utenti hanno diritti di Amministratore / Super Utente sui loro device?

Elementi da considerare per la corretta interpretazione della domanda:

La possibilità, da parte degli utenti, di accedere ai loro dispositivi con diritti di amministratore permette loro un maggior livello di controllo del dispositivo ottenendo in alcuni casi la possibilità di modificare o aggirare le configurazioni di sicurezza implementate dall'organizzazione permettendo quindi il download e la successiva installazione di software malevoli da siti web potenzialmente dannosi.

Domanda 31:

Gli amministratori dispongono di credenziali univoche e privilegiate per le attività amministrative separate dalle credenziali utente per l'accesso quotidiano, la posta elettronica, ecc.?

Elementi da considerare per la corretta interpretazione della domanda:

Sono previsti una serie di adempimenti relativi alla designazione e alla presenza di amministratori di sistema all'interno di un'organizzazione. Tra questi risulta fondamentale la creazione di account nominali dedicati all'accesso amministrativo al sistema, che siano separati dall'utenza utilizzata quotidianamente. Questo permette di evitare, ad esempio, che l'attacco di un malware durante le attività quotidiane possa intaccare i servizi o i dispositivi accessibili solo tramite apposita utenza amministrativa.

Domanda 32:

Prima di installare o utilizzare un asset, le password di default vengono cambiate ed allineate ad una password policy definita?

Elementi da considerare per la corretta interpretazione della domanda:

Le credenziali di accesso sono inizialmente rilasciate a ciascun utente dal Dipartimento IT che fornisce l'asset al fine di consentire l'accesso solo alle persone autorizzate. La password iniziale deve poter essere cambiata dopo il primo accesso ai sistemi IT, in modo che la nuova password sia comunicata all'utente in modo sicuro.

Inoltre, è necessario implementare il processo di cambio password anche per i nuovi asset acquistati e installati all'interno dell'infrastruttura dell'organizzazione (es. firewall, proxy, switch, router).

Domanda 33:

Gli aggiornamenti software / patch automatici sia per sistemi operativi che per software di terze parti sono applicati regolarmente?

Elementi da considerare per la corretta interpretazione della domanda:

L'aggiornamento regolare di software e dispositivi, oltre a garantire l'accesso a nuove funzionalità o interfacce, consente di mantenere un livello alto di sicurezza. I vendor testano regolarmente i loro prodotti alla ricerca di nuove vulnerabilità che potrebbero essere sfruttate dai criminali informatici e per questo motivo l'installazione tempestiva degli aggiornamenti è una difesa efficace contro gli attacchi informatici.

Domanda 34:

La scansione delle vulnerabilità viene eseguita sugli asset aziendali regolarmente per mezzo di tool automatizzati?

Elementi da considerare per la corretta interpretazione della domanda:

L'attività regolare di Vulnerability Assessment (VA) tramite tool automatizzati permette di determinare la vulnerabilità di un asset mediante test applicato al codice software dell'infrastruttura IT aziendale, di tutti i sistemi informatici, e delle applicazioni web. Il VA è usato come mezzo di prevenzione dalle minacce poiché l'identificazione tempestiva delle vulnerabilità del codice permette di rimediare le vulnerabilità o le criticità riscontrate.

Domanda 35:

È implementato un processo di backup dei dati dei sistemi aziendali su base regolare?

Elementi da considerare per la corretta interpretazione della domanda:

Il backup riguarda il processo mediante il quale le informazioni critiche vengono copiate e archiviate in un luogo sicuro, al fine di proteggerle da eventi imprevisti come guasti hardware, errori umani, attacchi informatici o catastrofi naturali. Per essere efficace, la procedura di backup deve prevedere la copia dei dati in dispositivi di archiviazione diversi da quelli dove sono stati generati o elaborati. Un processo di backup regolare e affidabile proteggerà il patrimonio informativo dell'azienda da perdite di dati inaspettate.

Domanda 36:

I dati di backup sono adeguatamente protetti a livello fisico (nel caso di spostamenti di supporti dati) o logico (tramite crittografia)?

Elementi da considerare per la corretta interpretazione della domanda:

È fondamentale proteggere i backup da accessi non autorizzati crittografando i dati in modo da renderli sicuri sia durante il trasporto che durante l'archiviazione. Le strutture in cui sono archiviate le copie di backup devono essere adeguatamente protette da minacce attraverso l'adozione di misure di sicurezza fisiche e logiche.

Domanda 37:

I test di backup e restore dei dati sono eseguiti con cadenza almeno annuale?

Elementi da considerare per la corretta interpretazione della domanda:

Testare e verificare i backup e la relativa procedura di ripristino con cadenza almeno annuale è fondamentale per verificare la loro integrità e la possibilità di ripristino. Questo assicura che, in caso di necessità, i dati possano essere recuperati correttamente.

Domanda 38:

È stato predisposto e testato regolarmente un piano di disaster recovery?

Elementi da considerare per la corretta interpretazione della domanda:

Realizzare un piano di disaster recovery, come parte del piano di continuità operativa, consente alle aziende di formalizzare le misure tecniche e organizzative necessarie per ripristinare il funzionamento delle apparecchiature hardware e dei software e limitare la perdita di dati nel caso si verifichi un evento disastroso o gravi emergenze in grado di renderli inutilizzabili. L'azienda deve provvedere all'esecuzione di test periodici e operativi in modo che sia garantito l'aggiornamento e il controllo dei piani. Per una corretta protezione i test dovrebbero essere eseguiti almeno annualmente oppure in caso di modifica del piano.

Domanda 39:

È stato predisposto e testato un piano di business continuity?

Elementi da considerare per la corretta interpretazione della domanda:

È fondamentale la predisposizione ed il test di un Business Continuity Plan con il quale vengono definite ed elencate le azioni da intraprendere prima, durante e dopo un incidente, per assicurare la continuità dell'attività produttiva e massimizzare l'efficacia della reazione all'incidente stesso, stabilendo a priori tutti gli adempimenti necessari, i ruoli e le responsabilità.

Domanda 40:

Affidamento, anche parziale, della gestione del Sistema IT aziendale a fornitori esterni?

Elementi da considerare per la corretta interpretazione della domanda:

Per una corretta gestione della sicurezza dei sistemi IT è necessario identificare, se presenti, i fornitori a cui è stata affidata la gestione parziale o totale dei sistemi IT.

Una corretta gestione dei fornitori richiede inoltre un approccio strategico nella valutazione di adeguatezza delle misure di sicurezza, necessario per garantire la protezione del perimetro aziendale.

Domanda 41:

I contratti con i fornitori introducono dei requisiti minimi di sicurezza il cui rispetto è verificato regolarmente?

Elementi da considerare per la corretta interpretazione della domanda:

È importante che vengano stabilite le modalità di verifica periodica del fornitore in merito al rispetto delle misure di sicurezza definite contrattualmente. Il processo di verifica dovrà essere continuo avendo cura di definire una frequenza di verifica proporzionale alla criticità del fornitore.

Domanda 42:

Il Contraente dichiara di essersi dotato di una procedura scritta per il trattamento, la protezione e la riservatezza dei dati personali conformemente a quanto stabilito dal Codice Privacy italiano e dal regolamento europeo 679/16 (GDPR)?

Elementi da considerare per la corretta interpretazione della domanda:

In osservanza al principio di accountability, il titolare del trattamento deve essere in grado di testimoniare, documentare e governare tutto il processo della Data Protection in azienda. Rientrano nell'ambito della predisposizione degli adempimenti in materia di Data Protection l'adozione del registro delle attività di trattamento; le designazioni dei responsabili del trattamento; la messa in atto di misure di sicurezza tecnico-organizzative adeguate al rischio; la redazione di un corretto modello di consenso informato e l'esecuzione di una valutazione di impatto sulla protezione dei dati.

Domanda 43:

Qualora la voce "STRUMENTI DI PAGAMENTO" sia stata selezionata, la società rispetta gli standards per la sicurezza dei dati dell'industria dei pagamenti con carta (Payment Card Industry Data Security Standards)?

Elementi da considerare per la corretta interpretazione della domanda:

Il Payment Card Industry (PCI) Data Security Standards (DSS) è uno standard di sicurezza delle informazioni globale progettato per prevenire le frodi attraverso un maggiore controllo dei dati delle carte di credito. L'adozione dello standard PCI DSS è obbligatoria per tutte le organizzazioni che archiviano, elaborano o trasmettono dati di pagamento e dei titolari di carte di credito.

Domanda 44:

Esiste un processo documentato / o ci si è dotati di un servizio di incident management?

Elementi da considerare per la corretta interpretazione della domanda:

Lo scopo del processo è quello di definire le attività di risposta ad un incidente relativo alla sicurezza informatica e di fornire una panoramica delle procedure e delle pratiche principali che l'azienda utilizzerà per gestire e rispondere agli incidenti, nonché delle parti interessate che saranno coinvolte nel processo.

Domanda 45:

Esiste un processo documentato / o ci si è dotati di un servizio che monitora la rete ed i sistemi informatici per identificare eventuali violazioni della sicurezza dei dati (es. Security Operation Center, SOC o Network Operation Center, NOC)?

Elementi da considerare per la corretta interpretazione della domanda:

Un Security Operation Center (SOC) o un Network Operation Center (NOC) migliorano le capacità di rilevamento, risposta e prevenzione delle minacce di un'organizzazione unificando e coordinando tutte le tecnologie e le operazioni di sicurezza informatica. Solitamente la tecnologia di base per il monitoraggio, il rilevamento e la risposta è il SIEM (Security Information and Event Management), che monitora gli avvisi da software e hardware sulla rete in tempo reale. Questi avvisi vengono poi analizzati per identificare potenziali minacce.

Domanda 46:

[Se SI alla 45] Tra le soluzioni di sicurezza adottate, l'azienda include una soluzione di tipo Endpoint Detection & Response (EDR)?

Elementi da considerare per la corretta interpretazione della domanda:

La presenza di una soluzione di tipo Endpoint Detection and Response (EDR) contribuisce a mitigare i rischi di attacchi informatici tramite meccanismi di monitoraggio degli endpoint e individuazione delle minacce in tempo reale, questo permette una rapida gestione delle anomalie identificate.

Domanda 47:

Le funzionalità di logging / tracciatura delle attività sono state opportunamente configurate su tutti i device ed apparati di rete?

Elementi da considerare per la corretta interpretazione della domanda:

La configurazione di funzionalità di registrazione dei log è essenziale per ricostruire l'iter di operazioni che hanno riguardato un determinato sistema informativo consentendo il tracciamento delle eventuali anomalie o minacce. I log devono registrare l'attività degli utenti, le eccezioni, le patch e gli incidenti sui sistemi e sulle reti IT. Devono essere definiti inoltre i criteri di conservazione, le autorizzazioni di accesso e le misure di protezione dei log.

Domanda 48:

Esiste un sistema di conservazione sicura e monitoraggio dei log per la ricostruzione di incidenti di sicurezza?

Elementi da considerare per la corretta interpretazione della domanda:

La registrazione e la conservazione dei log si realizza mediante l'impiego di specifici software di log management che, inseriti all'interno dell'architettura di rete aziendale, consentono la gestione centralizzata dei log mediante un apposito server all'interno del quale vengono veicolati i log provenienti dalle diverse componenti, hardware e software, appartenenti alla medesima infrastruttura IT. I log registrati e conservati mediante i software di log management devono essere sottoposti a procedure di backup allo scopo di garantire la ridondanza delle informazioni relative alle operazioni eseguite sui sistemi.

Domanda 49:

Sono previsti controlli periodici (audit, incluse le verifiche tecniche come i penetration test) per assicurare che le procedure di sicurezza della Società siano rispettate?

Elementi da considerare per la corretta interpretazione della domanda:

L'esecuzione di controlli periodici come audit o penetration test, permettono una valutazione completa del sistema informativo di un'organizzazione. Questa valutazione verifica la conformità delle misure di sicurezza implementate rispetto ad un elenco di best practice del settore oltre a verificare la presenza di vulnerabilità sui sistemi e sugli applicativi in utilizzo.

Domanda 50:

Sono state conseguite certificazioni relativamente al Sistema di Gestione della Sicurezza delle Informazioni aziendali?

Elementi da considerare per la corretta interpretazione della domanda:

La presenza di certificazioni (es. ISO / IEC 27001) riconosciute a livello internazionale, aiuta le organizzazioni ad implementare un solido sistema per la gestione della sicurezza delle informazioni grazie alla definizione di tecnologie, policy e processi dedicati alla protezione delle informazioni aziendali.

Domanda 51:

Negli ultimi 36 mesi si sono verificati incidenti in ambito di sicurezza informatica o privacy?

Elementi da considerare per la corretta interpretazione della domanda:

Indicare se negli ultimi 36 mesi si sono verificati eventi che hanno comportato un impatto sulla sicurezza delle informazioni o sui dati personali trattati dall'organizzazione.

Domanda 52:

[Se SI alla 51] Fornisci i dettagli degli incidenti avvenuti negli ultimi 36 mesi

Elementi da considerare per la corretta interpretazione della domanda:

I dettagli relativi ad incidenti di sicurezza devono riguardare data e ora di rilevamento dell'evento; data e ora cui si riferiscono i danni rilevati; sistemi coinvolti dall'incidente; servizi coinvolti dall'incidente e relativa criticità; livello di classificazione assegnato; rapporto di constatazione incidente, comprensivo delle cause e degli impatti.

In caso di data breach i dettagli devono includere anche le cause della violazione, il luogo, la tipologia dei dati personali violati, gli effetti e le conseguenze della violazione.