Documento	CHECK LIST PRIVACY 4.0 + ISO27001 + CSF/NIST
Adempimenti	VERIFICA VR-DPIA E AUDIT PERIODICO SISTEMA
Documenti relati	INDEX679, SOP3_3, DT679, PolPP, RDTA, DVR/IP
Basi giuridiche	Modulo lista di controlli Sistema TQM integrato

Procedura operativa di risposta agli incidenti informatici

La Sicurezza Informatica aziendale è condotta a diversi livelli di implementazione

AUDIT ICT (*SISTEMA TQM integrazione ISO-27001/ISO-20000)*

1. HARDWARE: check list di controllo e/o configurazioni

- *Controlli sugli Apparati*
- *Badge di identificazione*
- *Privilegi per l'accesso fisico*
- *Protezione fisica dei dispositivi*
- *Data Centers*
- *Controlli ambientali*
- *Cavi e armadi di cablaggio*
- *Utilizzo e distruzione di dispositivi elettronici*
- *Stampe*

2. SOFTWARE: check list di controllo e/o configurazioni

- *Applicazione e sistemi operativi*
- *Assegnazione Privilegi*
- *Utilizzo Applicazioni*
- *Circolazione dati e modifiche*
- *Sistemi di autenticazione*
- *Policy di Autenticazione*
- *Passwords*
- *Autenticazione Avanzata*
- *Biometria*

3. NETWORK: check list di controllo e/o configurazioni

- *Connettivitá costante*
- *Connessione di un apparato alla rete*
- *Dispositivi non autorizzati*
- *Gestione della rete*
- *Monitoraggio di rete*
- *Connettivitá Cloud e Piattaforme di condivisione*
- *Connettivitá e mobilitá*
- *Laptop e smartphone*
- *VPN e Modem*
- *Cifratura*
- *Sicurezza preventiva, firewall etc*

4. AUTOMAZIONE: check list di controllo e/o configurazioni
   - *Strategie di backup*
   - *Dispositivi periferici*
   - *Sensori remoti e sistemi di controllo*

5. FATTORI UMANI: check list di controllo e/o configurazioni
   - *Gestione degli incidenti (dipendenti / incaricati e soggetti autorizzati)*
   - *Amministrazione della sicurezza*
   - *Azioni amministrative*
   - *Audit e review esterne*
   - *Senior Management*
   - *Azioni individuali dei dipendenti*
   - *Attività di reporting da parte dei soggetti autorizzati*
   - *Monitoraggio delle attività dei dipendenti*
   - *Formazione dei dipendenti in materia di cyber security*
   - *Responsabilità personale in tema di sicurezza*

Sez.1.AUDIT HARDWARE

Controllo degli apparati

- *1.1 In azienda esiste un inventario accurato delle apparecchiature elettroniche presenti in ciascuna stanza delle sue varie sedi?*
- *1.2 L'inventario include un dettaglio di tutti i dispositivi autorizzati per l'utilizzo all'interno dell'azienda (es. hard disk, pen drive, ecc.)?*
- *1.3 Avvengono periodicamente dei controlli ispettivi a sorpresa per verificare che gli apparati elettronici siano effettivamente presenti nei luoghi riportati nell'apposito inventario?*
- *1.4 Se vi sono discrepanze tra l'inventario dei dispositivi elettronici e quelli effettivamente individuati avviene rapidamente una investigazione del motivo?*
- *1.5 Ogni volta che un dipendente responsabile di un certo apparato ne autorizza lo spostamento, esiste una procedura rapida ed efficiente per aggiornare tale inventario?*
- *1.6 L'inventario dei dispositivi elettronici per ciascuna sede viene aggiornato ogni volta che un nuovo dispositivo viene aggiunto o rimosso?*
- *1.7 C'è in azienda una politica esplicita che definisce quali tipologie di apparati possano essere trasportate fuori dai confini aziendali, nonché le autorizzazioni necessarie a tale tipo di movimentazione?*
- *1.8 Se un dispositivo di memorizzazione contenente dati sensibili deve essere portato fuori dall'azienda ci sono procedure di cifratura sui dati?*
- *1.9 C'è una policy che vieta ai dipendenti di pubblicare foto/video di attività che si svolgono all'interno di aree che includono informazioni sensibili?*
- *1.10 I dipendenti possono portare dispositivi elettronici personali all'interno dell'azienda o vi è un esplicito divieto?*
- *1.11 Se un dipendente viene identificato mentre porta al di fuori dell'azienda dispositivi di memorizzazione non autorizzati, ci sono policy che autorizzano l'azienda all'analisi del dispositivo stesso?*
- *1.12 Se un dispositivo viene smarrito ci sono procedure che permettono di identificarne rapidamente il contenuto e se tale contenuto è cifrato o meno?*
- *1.13 Sono disponibili dispositivi sostitutivi per le funzionalità più rilevanti (server, desktop, laptop) in caso di smarrimento o danneggiamento fisico?*
- *1.14 Tali dispositivi sono già configurati e pronti per essere resi opera*

Badge di identificazione

- *1.15 I dipendenti devono indossare un badge identificativo con foto durante le attività lavorative?*
- *1.16 Ai visitatori esterni viene fornito un badge identificativo temporaneo, eventualmente con foto?*

Privilegi per l'accesso fisico

- *1.17 Vi sono delle chiare disposizioni formali portate a conoscenza di tutto il personale per ciò che riguarda le autorizzazioni necessarie per l'accesso al CED, e queste disposizioni vengono fatte rigorosamente rispettare?*
- *1.18 Sono presenti controlli per identificare chi entra ed esce dagli ambienti in cui operano i sistemi informativi?*
- *1.19 Sono presenti sistemi di logging degli accessi (data di entrata e data di uscita) da determinati ambienti?*
- *1.20 I permessi relativi agli accessi a determinate aree fisiche dell'azienda devono essere rinnovati alla loro scadenza o sono automaticamente validi fino alla loro disattivazione?*

- *1.21 E' identificato chi sono i soggetti che possono apportare modifiche alla lista dei soggetti autorizzati ad accedere a una specifica area?*
- *1.22 Al momento dell'aggiunta di un nuovo soggetto nella lista delle persone autorizzate, è prevista una verifica con il soggetto che lo ha autorizzato?*
- *1.23 Avviene un controllo a intervalli predefinito delle liste di accesso per verificare i soggetti che possono essere rimossi?*
- *1.24 I privilegi di accesso fisico e i relativi badge vengono immediatamente modificati nel momento in cui un dipendente cambia il suo ruolo di lavoro in azienda?*
- *1.25 I privilegi di accesso fisico e i relativi badge vengono immediatamente disattivati nel momento in cui un dipendete viene licenziato, lascia l'azienda o va in pensione?*
- *1.26 I privilegi di accesso fisico e i relativi badge concessi a fornitori esterni vengono immediatamente disattivati nel momento in cui termina il rapporto di collaborazione?*
- *1.27 Avviene una attività di audit dei log di accesso dei dipendenti alle aree contenenti dati sensibili, per verificare che tali accessi siano compatibili con il ruolo del dipendente stesso?*
- *1.28 Se vi è una discrepanza che emerge in fase di audit sono previste delle modalità di investigazione?*
- *1.29 Se vengono utilizzate delle videocamere, specialmente quelle di tipo wireless (senza fili), a scopo di monitoraggio, esse risultano protette contro tentativi di interferenza, visioni non autorizzate, e alterazione delle immagini registrate?*

Protezione fisica dei dispositivi

- *1.30 Sono previste delle barriere fisiche per impedire l'utilizzo di porte sui dispositivi (es. USB e lettori CD)?*
- *1.31 Gli armadi contenenti i dispositivi di rete e cavi di rete sono sempre chiusi a chiave?*
- *1.32 Le porte non utilizzate sugli switch di rete, in particolare le SPAN ports, sono disattivate per prevenire accessi non autorizzati?*
- *1.33 L'accesso con privelgi di root a router o switch è disattivato di default per impedire l'accesso non autorizzato?*
- *1.34 L'accesso fisico alle console di gestione di dispositivi di sicurezza della rete (es. firewall, IPS, IDS) è ristretto unicamente agli utenti autorizzati?*
- *1.35 Sono presenti fax e sono gli stessi protetti dall'accesso da parte di soggetti non autorizzati?*
- *1.36 I dispositivi elettronici sono etichettati con un codice a barra o altro identificativo?*
- *1.37 Se un apparato elettronico deve comunque lasciare i confini dell'azienda, esiste una procedura efficiente che permetta di seguirne gli spostamenti?*
- *1.38 Se un apparato informatico è molto sensibile dal punto di vista della sicurezza, esso risulta corredato di chip a tecnologia RFID (identificazione a radiofrequenza), così da permetterne la localizzazione in tempo pressoché reale?*
- *1.39 Quando le persone escono dalla sede dell'azienda vengono sottoposte a qualche forma di scansione per verificare la presenza di dispositivi elettronici?*
- *1.40 Esiste un sistema informatico per verificare che ciascun dispositivo connesso alla rete e al quale è assegnato un determinato indirizzo IP si trovi proprio in quel posto?*
- *1.41 Se una porta di accesso è attivata, in quanto in uso, ci sono procedure per monitorarne l'accesso non autorizzato?*
- *1.42 Se i dipendenti notano un utilizzo non autorizzato di dispositivi elettronici all'interno dell'azienda esiste un canale di facile utilizzo e privato per fare un reporting? Vi sono eventuali incentivi per chi lo fa?*

Data Centers

- *1.43 L'accesso al centro di elaborazione dati (CED) aziendale viene controllato in modo continuo, con porte di ingresso tenute sempre chiuse?*

- *1.44 L'accesso al CED è controllato da tecnologie tipo badge a scansione, smartcard, tessere di prossimità, biometria o serrature a combinazione individuale?*
- *1.45 E' necessario inserire altre forme di credenziali di accesso (es. password, PIN, ecc.) per accedere al CED?*
- *1.46 Tali sistemi sono sottoposti ad audit o review costanti?*
- *1.47 Esiste un controllo sui fornitori che hanno accesso al CED?*
- *1.48 Esiste un inventario e uno schema dettagliato dei dispositivi presenti nei data center?*
- *1.49 L'accesso al CED è inibito a soggetti terzi che non ne hanno necessità (es. impresa di pulizia) oppure tali accessi sono monitorati/effettuati alla presenza di soggetti preposti al controllo?*
- *1.50 Lo stesso inventario viene aggiornato ogni volta che un dispositivo o il modo in cui lo stesso è collegato viene cambiato?*
- *1.51 Viene impiegata la videosorveglianza per controllare gli spazi di ingresso al CED o ad altre aree che ospitano apparecchiature di elaborazione dati?*
- *1.52 Se il CED è videosorvegliato, il monitoraggio avviene da un sito remoto?*
- *1.53 Se il CED è videosorvegliato, il video stesso viene registrato su un supporto permanente e resistente alla contraffazione?*
- *1.54 In caso di videosorveglianza dei centri elaborazione dati, le registrazioni video restano a disposizione per un tempo sufficiente per acconsentire indagini su una violazione di sicurezza a distanza di diversi mesi?*
- *1.55 Chi si occupa delle informazioni fornite all'esterno (es. sito web) è istruito per non pubblicare specifiche relative ai data centers?*
- *1.56 I centri critici di elaborazione dati e di telecomunicazione sono sufficientemente lontani da altri complessi permanenti che si possano rivelare fonti pericolose di incendio, di esplosioni o di perdita di liquidi tossici?*
- *1.57 I centri critici di elaborazione dati e di telecomunicazione sono posti a distanza sufficiente da posteggi pubblici, strade ed altre aree dove sarebbe facile deporre sostanze esplosive?*
- *1.58 Le apparecchiature informatiche e di telecomunicazione più critiche sono a distanza di sicurezza da finestre non blindate, che potrebbero costituire bersaglio di bombe, armi da fuoco o armi a microonde?*
- *1.59 I componenti degli apparati elettronici o di altra natura che devono essere trasferiti all'interno del centro elaborazione dati, vengono ispezionati con la necessaria attenzione per controllare la presenza di eventuali manomissioni?*
- *1.60 In caso di incendio all'interno del CED sono previste idonee misure di gestione dell'incidente?*
- *1.61 I dispoisitivi elettronici presenti all'interno del CED sono protetti con lucchetti o altre misure di sicurezza fisica?*
- *1.62 Il CED è dotato di allarme che monitori la presenza di personale non autorizzato all'interno?*
- *1.63 Sui sistemi più sensibili sono presenti allarmi o altri sistemi anti-intrusione?*
- *1.64 Se i dipendenti notano un accesso non autorizzato nel CED dell'azienda esiste un canale di facile utilizzo e privato per fare un reporting? Vi sono eventuali incentivi per chi lo fa?*
- *1.65 Esiste un piano per spostare le attività più critiche del CED dell'azienda a altri computer/sistemi aziendali nel caso in cui il CED primario dovesse essere evacuato o spento?*
- *1.66 Il sito secondario individuato è sufficientemente lontano da quello primario affinchè non sia afflitto dallo stesso problema?*

Controlli ambientali

- *1.67 Esistono sistemi di controllo ambientale - riscaldamento e raffreddamento - in grado di mantenere costante la temperatura operativa delle apparecchiature elettroniche?*
- *1.68 Tali apparecchiature sono protette dalla presenza d'acqua e da eccessiva umidità?*
- *1.69 Se i controlli ambientali possono essere azionati da postazioni remote, tali controlli sono adeguatamente protetti da accessi non autorizzati?*

- *1.70 Esistono controlli ambientali che proteggono i sistemi da altri fattori che non siano temperatura ed umidità, ad esempio fumo, polvere, gas chimici?*
- *1.71 Nei locali del CED e negli armadi da cablaggio, vi sono sensori di controllo ambientale, in particolare di rilevazione della temperatura, di fumo e d'acqua?*
- *1.72 Le aree che ospitano apparati elettronici sono dotate di un sistema antincendio adeguato alla tipologia degli apparati presenti?*
- *1.73 Tali sistemi sono configurati per generare un allarme nel caso in cui l'ambiente non fosse più sicuro per i soggetti che sono all'interno?*
- *1.74 Esiste un documento prontamente consultabile che elenchi la posizione e i tipi di controlli ambientali in essere, quali rilevatori di incendio, termostati, rilevatori di acqua, ecc.?*
- *1.75 Esiste un documento prontamente consultabile che elenchi le condizioni ambientali richieste affinchè i dipositivi elettronici possano operare correttamente?*
- *1.76 I fornitori che gestiscono la sicurezza ambientali dell'azienda sono ammoniti dal non pubblicizzare il fatto che l'azienda sia propria cliente?*

Cavi e armadi di cablaggio

- *1.77 Esiste un piano dettagliato dell'intero cablaggio dati aziendale?*
- *1.78 Esiste un piano dettagliato dell'intero cablaggio elettronico aziendale?*
- *1.79 La documentazione relativa ai cablaggi è protetta da accessi non autilizzati?*
- *1.80 Esiste una etichettatura puntuale di tutti i cablaggi, anche all'interno degli armadi, per facilitare un riconfigurazione?*
- *1.81 Tale etichettatura è studiata in modo tale che non sia immediatamente compensibile ad un occhio esterno?*
- *1.82 Esiste un piano per il fabbisogno energatico sia nei momenti di attività normale sia nei momenti di picco?*
- *1.83 Esistono sistemi di allarme che identifichino che un determinato cavo è stato tagliato?*
- *1.84 Sono presenti sistemi anti-intrusione di qualche tipo negli armadi di cablaggio?*
- *1.85 Esiste un piano di sorgente di corrente di backuè per tutti i sistemi critici?*
- *1.86 Sono presenti gruppi di continuità nelle vicinanze di sistemi di videosorveglianza?*
- *1.87 Se sono installati degli UPS, risultano protetti da accessi remoti non autorizzati?*
- *1.88 I generatori di riserva vengono protetti tramite dispositivi di sicurezza fisica quali serrature, allarmi, o recinti con filo spinato?*
- *1.89 I dispositivi di alimentazione di riserva sono collocati in luoghi non esposti a fenomeni di inondazione?*
- *1.90 E' predisposto un meccanismo di protezione contro i picchi anomali di tensione provocati da fulmini o da mezzi artificiali?*
- *1.91 Sono effettuati regolarmente dei test relativi alla tenuta del sistema di energia secondaria?*

Utilizzo e distruzione di dispositivi elettronici

- *1.92 Esistono procedure per il wiping o la distruzione sicura di qualsiasi dispositivo elettronico di memorizzazione?*
- *1.93 Esistono procedure sufficientemente rigorose per effettuare la distruzione o la cancellazione irreversibile dei supporti di memoria, quali dischi fissi, nastri, dischi flash o zip, al termine della loro vita utile in azienda?*
- *1.94 Esistono procedure sufficientemente rigorose per la cancellazione irreversibile dei supporti di memoria che vengono consegnati ad altri in caso di sostituzione in garanzia, di vendita al pubblico, o di donazioni ad enti di volontariato?*
- *1.95 Viene seguita un rigorosa catena di custodia per la distruzione dei dispositivi di memorizzazione?*
- *1.96 Ci sono procedure relativamente all'utilizzo di dispositivi esterni di memorizzazione?*
- *1.97 I dispositivi da distruggere sono conservati in un ambiente idoneo e cotnrollato prima della distruzione?*
- *1.98 I CD contenenti dati sensibili aziendali vengono fisicamente distrutti?*
- *1.99 Viene verificata l'effettiva cancellazione sicura dei dati, ad esempio tramite un soggetto terzo?*
- *1.100 Quando un dipendente lascia l'azienda, i dispositivi che utilizzava sono riutilizzati?*
- *1.101 In caso affermativo, si procede ad effettuarne una copia forense?*
- *1.102 In caso negativo, si procede a conservare il dispositivo (o il relativo contenitore di dati) per*
- *eventuali successive attività investigative?*
- *1.103 Se un documento contiene informazioni altamente sensibili viene mantenuto un record di ogni volta che viene stampato o copiato?*
- *1.104 Ci sono procedure per restringere l'accesso a stampe contenenti dati particolarmente sensibili?*
- *1.105 Esistono contenitori sicuri dove inserire i documenti cartacei che devono essere distrutti in modo sicuro?*
- *1.106 I dipendendi sono formati per una distruzione dei documenti cartacei contenenti dati sensibili?*

sez.2. AUDIT SOFTWARE

Applicazione e sistemi operativi

- *2.1 In azienda esiste un inventario accurato dei software di sitema e applicativi installati?*
- *2.2 Esiste una policy inerente quali software i dipendendi possano/non possano usare?*
- *2.3 Esiste un inventario di quali applicazioni richiedano accessi amministrativi e quali utenti posseggano tali privilegi?*
- *2.4 Esiste una procedura per la documentazione e il tracking delle applicazioni*
- *2.5 Esiste una lista comprensiva di tutti gli script/applicazioni che utilizzano credenziali embedded?*
- *2.6 Esiste il patch management tracking, cioè log delle patch richieste, delle patch pronte, date di ricezione e date di applicazione?*
- *2.7 Viene effettuato un approfondito test di vulnerabilità sulle applicazioni prima che esse vengano messe in produzione?*
- *2.8 Le impostazioni di sicurezza di default (impostate dal vendor) di un software, vengono modificate?*
- *2.9 Le password per gli account di servizio (es backup server, etc) sono complesse per numero di caratteri e loro tipologia?*
- *2.10 La sequenza di boot dei computer aziendali è impostata per fare il boot solo dal disco del sistema operativo (no CD, no USB)?*
- *2.11 "Gli account ""Amministratore"" sono stati rinominati?"*
- *2.12 Gli account di servizio sono stati rinominati?*
- *2.13 I sistemi aziendali vengono regolarmente controllati alla ricerca di malware e hacking tool?*
- *2.14 Gli innalzamenti di privilegio vengono loggati e controllati?*
- *2.15 Le richeste di privilegi amministrativi (es: Domain Administrator) sono loggati e immediatamente controllati?*
- *2.16 Dopo patch/upgrade le configurazioni e le impostazioni del software vengono verificate (automaticamente)?*
- *2.17 Esiste una procedura per verificare che patch e update sono state installate nei tempi e modi corretti?*
- *2.18 L'azienda effettua vulnerability testing dopo il deploy di applicazioni/sistemi?*
- *2.19 "L'azienda mantiene la cosiddetta ""golden image"" di riferimento per ogni OS a suite di applicativi?"*
- *2.20 Viene effettuato un approfondito test da esperti sulle golden image?*
- *2.21 Le golden image sono mantenute in un repository sicuro, accessibile solo da determinati indirizzi e utenti?*
- *2.22 Vengono calcolati e mantenuti hash (anche multipli) delle golden image?*
- *2.23 Esistono procedure dettagliate per l'aggiornamento (path/upgrade) delle golden image?*
- *2.24 Le procedure di path/upgrade prevedono una fase di test prima di essere applicate in produzione?*
- *2.25 I tempi di applicazione delle patch/upgrade sono scelti in modo da ridurre eventuali malfunzionamenti?*

Assegnazione Privilegi

- *2.26 L'accesso alle applicazioni critiche è permesso solo a quegli utenti che lo necessitano?*
- *2.27 Viene chiesto agli utenti una lista delle applicazioni cui loro richiedono accesso?*
- *2.28 La lista delle richieste d'uso delle applicazioni è controllata ed il controllo loggato?*
- *2.29 In caso di prolungata assenza d'uso di una applicazione, all'utente viene rimosso l'accesso?*
- *2.30 Nel caso l'utente cambi mansione, la lista delle sue applicazioni viene rivista?*
- *2.31 Esiste una procedura di controllo (es: annuale) dei privilegi assegnati agli utenti?*
- *2.32 I privilegi di root/domain admin sono ristretti ai soli utenti che li necessitano?*

- *2.33 I privilegi locali di amministrazione sono disabilitati sui sistemi degli utenti?*

Utilizzo Applicazioni

- *2.34 In caso di nuove vulnerabilità software/hardware, le persone in carico di decidere le misure prima del rilascio delle patch vengono informate?*
- *2.35 I messaggi di errore sono stati impostati per non rivelare informazioni sul design e configurazione interna dell'applicazione?*
- *2.36 In produzione, è stato verificato che le feature di debug (o anche semilavorati) siano state eliminate?*

Patch e Update (*domande condivise con altre sezioni*)

Circolazione dati e modifiche

- *2.37 "La disseminazione delle informazioni in azienda segue il principio del ""need to know""?"*
- *2.38 L'azienda ha formalmente assegnato una classificazione ai proprio documenti?*
- *2.39 La classificazione delle informazioni, e ciò che ne deriva, è stata comunicata in modo chiaro ai dipendenti?*
- *2.40 La classificazione delle informazioni viene (es: annualmente) rivista?*
- *2.41 L'accesso ai dati sensibili ristretto ai solo utenti che ne hanno necessità?*
- *2.42 Le informazioni classificate al massimo livello sono mantenute in uno storage cifrato quando non in uso?*
- *2.43 Agli utenti che accedono a dati sensibili vengono richieste ulteriore forme di autenticazione (es: password, 2FA)?*
- *2.44 Esistono informazioni finte mescolate con le vere in modo che un attaccante non sappia distinguerle?*
- *2.45 Il database o contenitore di informazioni classificate è configurato in modo che tali informazioni non possano essere sovrascritte, ma corrette con revisioni loggate e archiviate?*
- *2.46 I file di log che devono essere preservati, sono opportunamente trattati (diverse copie a prova di contraffazione)?*
- *2.47 Nella circolazione di documenti aziendali al di fuori dell'azienda viene usato un formato di file resistente alle modifiche?*
- *2.48 Nella circolazione di documenti aziendali al di fuori dell'azienda esse vengono firmate digitalmente?*
- *2.49 Vengono utilizzate firme digitali nello scambio di email interne?*
- *2.50 E' in uso un meccanismo per il controllo e log di tutti i cambiamenti ai database critici?*
- *2.51 Gli upload verso l'esterno di dati sensibili sono monitorati?*
- *2.52 Gli upload verso l'esterno di dati cifrati sono monitorati?*
- *2.53 L'azienda controlla accesso ai dati (almeno quelli sensibili) inusuali?*
- *2.54 L'azienda controlla modifiche ai dati (almeno quelli sensibili) inusuali?*
- *2.55 L'azienda previene fortuiti upload/download di dati sensibili da parte degli utenti fra i sistemi?*
- *2.56 L'azienda previene la stampa di email/allegati/etc da parte degli utenti non autorizzati?*
- *2.57 Ai dipendenti viene impedito di salvare dati sensibili su dispositivi come DVD, USB, salvo specifiche autorizzazioni?*
- *2.58 Esiste un limite alla quantità di dati che può essere acceduta/scaricata da un sistema ad un altro?*
- *2.59 Se gli utenti possono memorizzare localmente informazioni sensibili, tale azione è monitorata?*
- *2.60 L'azienda applica watermark ai documenti particolarmente sensibili?*
- *2.61 L'azienda applica beacon ai documenti particolarmente sensibili?*

Sistemi di autenticazione

- *2.62 Esiste policy per l'immediata deattivazione delle password (e altri sistemi di autenticazione) quando un dipendente fuoriesce dall'azienda?*
- *2.63 Le username login degli utenti sono differenti dal loro nome e indirizzo email?*
- *2.64 Esiste una policy per il cambio password ogni x giorni?*
- *2.65 Alla richiesta di cambio password, gli utenti possono inserire password giá utilizzate in precedenza?*
- *2.66 I computer/software applicativi vanno in lock dopo un determinato periodo di inattivitá da parte dell'utente?*
- *2.67 Esiste una policy che richieda il logging di tutti i tentativi di accesso (positivi e negativi) per le applicazioni/sistemi critici?*
- *2.68 I log di accesso a sistemi critici sono mantenuti su dischi non riscrivibili o comunque resistenti a manipolazioni?*
- *2.69 Esiste un sistema di allarme automatico in caso di multipli accessi falliti, anche se questi ultimi sono sparsi nel tempo e fra gli utenti?*
- *2.70 Accessi autorizzati ma temporalmente inusuali vengono analizzati?*
- *2.71 Esiste un sistema di allarme in caso di sottrazione di un file contenente password di accesso a sistemi?*
- *2.72 Se un amministratore cambia delle password, tali cambiamenti sono loggati e analizzati in tempo utile?*
- *2.73 Esiste un sistema di allarme in caso di uso di 2FA (es: smart card) che é stato revocato?*
- *2.74 Esiste un sistema di allarme in caso di uso di un account disabilitato?*
- *2.75 Esiste una procedura per il cambio rapido e sicuro di password all'interno dell'organizzazione (in caso di compromissione)?*
- *2.76 In caso un utente necessiti di recuperare o cambiare una password, vengono utilizzate domande segrete di cui egli é il solo a conoscerne la risposta?*
- *2.77 In caso un utente necessiti di recuperare o cambiare una password, viene inviato un link all'email aziendale dell'utente?*
- *2.78 Esiste una procedura rapida e sicura per la deattivazione di token di sicurezza (in caso di compromissione/smarrimento)?*
- *2.79 L'azienda ha la possibilitá, se necessario, di accedere in modo controllato ad applicazione e dati protetti dalla password e/o token di un utente?*

Policy di Autenticazione

- *2.80 I sistemi aziendali sono tutti protetti con sistemi di autenticazione di base, come username e password?*
- *2.81 I tentativi di login sono limitati ad un massimo di x/minuto (piuttosto che in numero senza limite temporale)?*
- *2.82 Il tempo minimo fra due possibili tentativi di login viene gradualmente aumentato in caso di fallimenti?*
- *2.83 Se un account o sistema viene acceduto dopo molteplici tentativi falliti, esso viene immediatamente monitorato per possibile uso improprio?*
- *2.84 Esiste una procedura sicura ed automatica per eliminare gli accessi di un dipendente una volta fuoriuscito dall'azienda?*

Passwords

- *2.85 Le password devono rispettare criteri minimi di lunghezza e complessitá?*
- *2.86 Vengono eseguiti dei check durante la creazione delle password per verificare se essere rispettino i criteri minimi impostati?*
- *2.87 Viene impedito l'uso di password note e/o appartenenti alle comuni liste online?*
- *2.88 Esistono policy che richiedano procedure sicure per la generazione e la trasmissione di password?*
- *2.89 Le password sono sempre e comunque memorizzate in forma cifrata?*

Autenticazione Avanzata

- *2.90 Le informazioni e i sistemi critici richiedono 2FA?*
- *2.91 Le informazioni e i sistemi critici richiedono autenticazione doppia (due utenze)?*

Biometria

- *2.92 Vengono utilizzati sistemi biometrici per l'autenticazione?*

sez.3. AUDIT NETWORKS

Connettivitá costante

- *3.1 Reti per attivitá che richiedono livelli di sicurezza differenti sono separate fra di loro?*
- *3.2 L'azienda mantiene una lista di tutti i dispositivi in uso, compresi i loro indirizzi MAC?*
- *3.3 L'azienda mantiene una lista di tutti i protocolli e porte usate dagli applicativi installati sui propri sistemi?*
- *3.4 L'azienda mantiene una lista di tutti i nomi di sistema e loro indirizzi IP?*
- *3.5 Esiste una dettagliata topologia della rete aziendale?*
- *3.6 Il dettaglio della topologia di rete contiene i protocolli ed i percorsi dei servizi?*
- *3.7 I documenti sulla topologia di rete vengono puntualmente verificati e aggiornati?*
- *3.8 I documenti sulla topologia di rete sono accuratamente protetti da accessi non autorizzati?*
- *3.9 I dispositivi di rete (router, switch, etc.) dispongono di ACL per il loro accesso?*
- *3.10 I cambiamenti di configurazione dei dispositivi di rete richiedono almeno una seconda revisione prima di essere applicati?*
- *3.11 I cambiamenti di configurazione dei dispositivi di rete vengono opportunamente loggati?*
- *3.12 Se viene rilevata un'attivitá sospetta da parte di un MAC, tale attivitá viene monitorata e investigata?*
- *3.13 I sistemi critici hanno connessioni ridondanti per HA?*
- *3.14 Reti critiche hanno ridondanza a livello di switch?*

Connessione di un apparato alla rete

- *3.15 Prima di connettere/inserire un apparato nella rete, esso deve superare dei test di sicurezza?*
- *3.16 Le impostazioni di default di un apparato vengono modificate prima di connetterlo in rete (es: username e password)?*
- *3.17 Vengono eseguiti vulnerability scan e pentesting sui dispositivi critici prima di connetterli alla rete e successivamente?*
- *3.18 E' fatto divieto ai dipendenti di inserire propri dispostivi in rete (flash drive, ipod, kindle, smartphone, camera, etc)?*

Dispositivi non autorizzati

- *3.19 La rete é costantemente monitorata per rilevare dispositivi non nella lista di quelli autorizzati?*
- *3.20 L'azienda monitora lo spoofing degli indirizzi MAC (confrontando ad esempio OS, porte, posizionamento, etc.)?*
- *3.21 La rete wifi é monitorata per rilevare l'accesso di dispositivi non autorizzati?*
- *3.22 I modem dial up sono monitorati per rilevare accessi non autorizzati dall'esterno?*

Gestione della rete

- *3.23 L'accesso alla rete, come per i sistemi, richiede autenticazione?*
- *3.24 Sono in uso precise e rigorose regole per l'accesso alla rete aziendale via wireless?*
- *3.25 L'accesso wifi é limitato ai soli dispositivi autorizzati?*
- *3.26 L'uso di dispositivi di rete interni é rigorsamente specificato/impedito?*

- *3.27 La connettivitá con i partner avviene tramite vpn?*
- *3.28 Esiste un processo per approvare l'accesso alle VPN?*
- *3.29 La rete é segmentata e le comunicazioni inter-segmento rigorosamente configurate?*
- *3.30 Esiste una policy che limiti l'uso di protocolli insicuri (ftp, telenet, snmp)?*
- *3.31 Le richieste SNMP sono limitate ai soli sistemi autorizzati?*
- *3.32 Esistono policy che impediscano o limitino l'uso di tool per la gestione remota di sistemi (logmein, teamviewer, etc.)?*
- *3.33 Esiste un meccanismo automatico che avverta gli amministratori quando un dispositivo critico é spento o ha eseguito un reboot?*
- *3.34 Esiste una meccanismo di controllo che rilevi cambi di configurazione sui sistemi di rete?*
- *3.35 Esiste una meccanismo di controllo che rilevi cambi di configurazione sui sistemi server?*
- *3.36 In caso di cambio di configurazione, ne viene verificato l'impatto sulla sicurezza?*
- *3.37 Le modifiche alle configurazione di server e sistemi di rete sono loggate?*

Monitoraggio di rete

- *3.38 Il traffico di rete é monitorato per stabilire i normali pattern d'uso?*
- *3.39 Il traffico di rete fra segmenti con differente livelli di sicurezza é monitorato?*
- *3.40 Pattern di traffico inusuali vengono prontamente rilevati e analizzati?*
- *3.41 I server DND sono monitorati per evitare modifiche che re-indirizzino il traffico?*
- *3.42 Il traffico di rete é regolarmente monitorato alla ricerca di possibili covert channel?*

Connettivitá Cloud e Piattaforme di condivisione

- *3.43 Sono chiare all'azienda le necessitá di sicurezza specifiche per l'uso di cloud computing?*
- *3.44 L'azienda é a conoscenza che mantenere dati nel cloud senza cifratura puó essere particolarmente rischioso?*
- *3.45 Esiste una policy aziendale su quali documenti, sulla base dei dati sensibili, possano essere gestiti tramite Google Docs, Dropbox, etc.?*
- *3.46 L'accesso degli amministratori dei sistemi in cloud richiede 2FA?*
- *3.47 Le macchine virtuali che eseguono servizi critici sono separate da quelle che eseguono servizi meno critici?*
- *3.48 Le comunicazioni con i server cloud sono tutte cifrate?*
- *3.49 I database / file server nel cloud sono monitorati per rilevare trasferimenti di grandi moli di dati?*
- *3.50 I log di accesso ai sistemi cloud sono trasferiti su altri server, anche garantendone la non modificabilitá da parte degli amministratori?*
- *3.51 Le chiavi di cifratura e/o i certificati per la cifratura dei dati cloud sono memorizzate e gestite in modo sicuro?*
- *3.52 L'azienda ha preparato un set di procedure per essere pronta a trasferire velocemente le operazioni nel cloud fuori dal cloud?*
- *3.53 Esiste una policy che impedisca agli utenti la memorizzazione nelle piattaforme di condivisione cloud (Dropbox etc) di dati sensibili?*
- *3.54 Esiste una policy che limiti il tempo in cui un determinato tipo di informazione possa essere memorizzato nel cloud?*
- *3.55 Esiste una procedura per verificare che documenti aziendali non esistano o siano stati rimossi dal cloud?*

Connettivitá e mobilitá

- *3.56 I dispositivi mobili (laptop, smartphone) degli utenti sono standardizzati in modo da rispettare i requisiti minimi di sicurezza aziendale?*
- *3.57 Le utenze dei dispositivi mobili sono impedite dal possedere diritti di amministrazione?*
- *3.58 In caso di BYOD, l'azienda impedisce la memorizzazione su tali dispositivi di dati aziendali sensibili?*
- *3.59 Nei dispositivi mobili viene utilizzata FDE?*
- *3.60 Microfoni e telecamere dei dispositivi mobili sono disabilitati in aree o riunioni sensibili?*
- *3.61 Viene impedito il boot da dispositivi esterni (CD, USB) sui laptop?*
- *3.62 Le email aziendali contenenti dati sensibili sono cifrate?*
- *3.63 Se i dispositivi rimovibili sono in uso nell'azienda, il loro uso viene monitorato?*
- *3.64 Le attivitá dei dispositivi mobili di terzi (fornitori) temporaneamente connessi all'azienda sono monitorate?*
- *3.65 Le comunicazioni VoIP sono cifrate?*
- *3.66 Le comunicazioni VoIP sono monitorate per rilevare trasmissione dati?*
- *3.67 Le connessioni remote sono monitorate con particolare attenzione?*
- *3.68 L'azienda mette a disposizione un servizio che permetta agli utenti di segnalare possibili malware/malfunzionamenti sospetti?*

Laptop, Notebook, tablet, smartphone e BYOD

- *3.69 Tutti i dispositivi aziendali sono protetti da antivirus?*
- *3.70 Gli agenti antivirus sono gestiti centralmente?*
- *3.71 Gli smartphone aziendali sono gestiti centralmente?*
- *3.72 I dispositivi utente hanno installato un software di protezione che blocchi l'accesso a IP o hostname noti come malevoli?*
- *3.73 I dispositivi infrarosso, bluetooth e wireless sono disabilitati sui laptop, salvo diverse necessitá?*
- *3.74 Viene effettuato un controllo sulle login da laptop di utenti remoti, che siano consistenti con la posizione geografica dell'utente?*
- *3.75 Viene effettuato un controllo sulle login da smartphone di utenti remoti, che siano consistenti con la posizione geografica dell'utente?*
- *3.76 Le comunicazione VoIP sono cifrate, specie per le chiamate sensibili?*
- *3.77 I sistemi aziendali e di terze parti vengono analizzati per ricecare malware o vulnerabilitá (missing patch) prima di concedere l'accesso alla rete interna?*

VPN e Modem

- *3.78 L'accesso VPN richiede 2FA?*
- *3.79 L'accesso a VPN per sistemi critici, richiede 2FA, token e/o sistemi di autenticazione biometrica?*
- *3.80 Una volta autenticati alla VPN, i sistemi vengono sottoposti a check di sicurezza prima di acconsentire l'accesso alla rete interna?*
- *3.81 In caso di Web VPN, le informazioni di sessione vengono eliminate dal computer remoto?*
- *3.82 L'azienda utilizza modem per la gestione remota di sistemi?*
- *3.83 I modem sono provvisti di feature di sicurezza per verificare se un utente é autorizzato?*
- *Web e E-Commerce*
- *3.84 I portali web sono implementati da specialisti anche per la parte sicurezza?*
- *3.85 I banner dei server che ospitano le pagine web pubbliche sono stati rimossi?*
- *3.86 Le pagine/script di test sono stati rimossi dai siti in produzione?*
- *3.87 L'azienda ha acquistato tutti i domini che potrebbero essere interpretati come propri?*
- *3.88 Le informazioni sensibili dei clienti (es: carte di pagamento) sono gestite da sistemi differenti da quelli web che gestiscono le transazioni?*
- *3.89 Eventuali social media account (Twitter) utilizzando 2FA?*

- *3.90 L'azienda ricerca costantemente siti fasulli che pretendono di essere un sito dell'azienda?*
- *3.91 L'azienda fornisce pubblicamente un contatto (email, telefono) che puó essere usato per segnalare problemi di sicurezza?*
- *3.92 Esiste una procedura per un'azione rapida di rimozione di notizie fasulle dai social media?*
- *3.93 Esiste una procedura per un'azione rapida di rimozione di siti fasulli?*
- *3.94 In caso di problemi di sicurezza web, esistono procedure per la gestione e la messa in sicurezza?*
- *3.95 Le transazioni economiche sono gestite da terzi?*
- *3.96 Le transazioni economiche sono gestite in modo sicuro?*

Cifratura

- *3.97 Esiste una policy che definisca quali comunicazioni debbano essere cifrate e come?*
- *3.98 L'azienda mantiene una lista dei certificati utilizzati nei propri sistemi e applicazioni?*
- *3.99 Le VPN utilizzano certificati digitali?*

Sicurezza preventiva e controllo difesa perimetrale (IDS/IPS, Proxy e firewalls)

- *3.100 Viene utilizzato IPv6?*
- *3.101 Viene disabilitato, se non in uso, il protocollo IPv6?*
- *3.102 Se disabilitato, esistono meccanismi di rilevamento di traffico IPv6?*
- *3.103 Il firewall é utilizzato solo sul perimetro o anche internamente per separare reti a diverso livello di sicurezza?*
- *3.104 L'azienda utilizza anche Host Firewall?*
- *3.105 Esiste un processo scritto e approvato per il cambio delle regole del firewall?*
- *3.106 L'accessp all'interfaccia di management di un dispositivo di sicurezza é limitata a soli determinati indirizzi IP?*
- *3.107 Ogni modifica alla regole di un dispositivo di sicurezza é loggato?*
- *3.108 I log dei firewall vengono periodicamente analizzati?*
- *3.109 L'azienda utilizza IPS/IDS?*
- *3.110 L'azienda analizza malware e/o esempi di attacchi reali ad altri aziende?*
- *3.111 L'azienda utilizza un sistema di content filtering?*

sez.4. AUDIT AUTOMAZIONE

Sensori remoti e sistemi di controllo

- *4.1 In azienda è disponibile uno schema completo che identifichi accuratamente tutti i percorsi di comunicazione tramite i quali sono connessi i sistemi di controllo?*
- *4.2 Tutti i documenti che riportano le corrispondenze tra percorsi logici di accesso e sistemi di controllo sono rigorosamente protetti contro accessi non autorizzati?*
- *4.3 Tutti i sistemi di controllo che non hanno l'esigenza di una connessione Internet sono effettivamente isolati da Internet?*
- *4.4 I sistemi di controllo vengono isolati dalla rete aziendale quando non vi sia giustificato motivo di connetterli?*
- *4.5 Se un determinato sistema di controllo non può essere isolato dalla rete aziendale, è perlomeno protetto da firewall e sistemi IDS altamente selettivi?*
- *4.6 Si pone attenzione affinché ad eventuali estranei non sia concessa la presa in visione di diagrammi e schemi contenenti chiari riferimenti ai processi fisici ed ai sistemi che li gestiscono?*
- *4.7 I sensori remoti sono stati progettati o aggiornati in modo da rendere difficile per un malintenzionato alterarne le misurazioni tramite un'operazione di manomissione fisica?*
- *4.8 Vi sono insiemi di sensori secondari che controllano i processi critici tramite una tecnica alternativa di misurazione, così che una lettura falsa effettuata dal set primario di sensori possa essere rapidamente messa in evidenza?*
- *4.9 Esistono piani e procedure operative per gestire i casi in cui i collegamenti wireless considerati critici vengano messi fuori uso?*
- *4.10 I nuovi dispositivi terminali remoti o altri dispositivi di controllo che vengono installati sulla rete aziendale sono corredati della funzione di cambio della password o di altri meccanismi di autenticazione riprogrammabili?*
- *4.11 Tutti i componenti della rete sono sincronizzati sulla medesima ora, fuso orario e data?*
- *4.12 Gli aggiornamenti ai sistemi operativi dei dispositivi terminali remoti sono trasmessi in modalità sicura da fonte autorizzata?*
- *4.13 Le interrogazioni sullo stato dei dispositivi terminali remoti sono trasmesse in modalità sicura da fonte autorizzata?*

Dispositivi periferici

- *4.14 Prima di acquistare un prodotto se ne valutano le caratteristiche in termini di sicurezza?*
- *4.15 Il supporto di sistemi di cifratura è un parametro che viene tenuto in considerazione quando si acquistano dispositivi periferici?*
- *4.16 Sono presenti procedure per l'update sicuro dei firmware dei dispositivi hardware installati in azienda?*
- *4.17 E' presente una lista di tutti i dispositivi periferici come stampanti, scanner che sono condivisi tra diversi utenti e che contempli la lista dei computer/utenti che vi hanno accesso?*
- *4.18 E' presente una lista di tutti i computer che hanno accesso ad Internet?*
- *4.19 Le password di default dei dispositivi wireless e bluetooth sono modificate prima che questi vengano messi in funzione?*
- *4.20 La connettività bluetooth e wirelesse dei dispositivi perifireci quali stampanti e scanner viene disabilitata se non utilizzata?*
- *4.21 Quando un dispositivo deve essere collegato solo occasionalmente alla rete Internet, sono presenti procedure per il controllo dell'effettiva disconnessione fisica dalla rete?*

- *4.22 Le comunicazioni che intercorrono tra dispositivi periferici e i computer sono generalmente cifrate?*
- *4.23 Tutti i dispositivi periferici sono dotati di password distinte?*
- *4.24 Se un dispositivo periferico come una stampante o uno scanner può contenere una grossa quantità di dati, vi è un blocco per impedire che lo stesso possa comunicare tali grosse quantità verso l'esterno?*
- *4.25 Se un dispositivo locale connesso ad Internet trasmette o riceve dati ad un orario inatteso, per frequenza e/o volume, viene attivata una qualche forma di warning?*
- *4.26 Se vi è indicazione di una elevata quantità di traffico generato da un dispositivo si procede rapidamente con una attività ispettiva?*
- *4.27 Il traffico generato da dispositivi periferici viene ispezionato per verificarne l'effettiva cifratura?*
- *4.28 Se un dispositivo contiene impostazioni personalizzate, le stesse vengono regolarmente verificate per controllare che non siano state cambiate?*
- *4.29 Se un dispositivo contiene impostazioni personalizzate, esiste una copia di backup di tali impostazioni?*
- *4.30 L'eventuale copia di backup è cifrata?*

Strategie di backup

- *4.31 Esiste un piano completo di ciò che deve essere sottoposto a backup?*
- *4.32 I dati vengono salvati con una cadenza che ne riflette il valore economico e la frequenza di aggiornamento?*
- *4.33 Sono oggetto di backup (cioè di creazione di copie di sicurezza) i sistemi operativi, i programmi, e le informazioni di configurazione, oltre naturalmente ai dati dell'azienda?*
- *4.34 Esiste un piano specifico per il backup regolare dei laptop e dei dispositivi mobile degli utenti?*
- *4.35 Le configurazioni di switch e router sono regolarmente oggetto di backup?*
- *4.36 Se è necessario trasferire i dispositivi di backup al di fuori dell'azienda vengono mantenuti segreti il luogo di destinazione e il percorso?*
- *4.37 Esiste una copia di backup dei dati che viene trasferita con regolarità in un luogo isolato dalla rete aziendale?*
- *4.38 I dati vengono salvati con una cadenza che ne riflette il valore economico e la frequenza di aggiornamento?*
- *4.39 I dati salvati sono memorizzati per un periodo sufficientemente lungo da poter garantire la disponibilità di una copia integra di dati, nel caso che questi siano stati fatti oggetto di alterazioni di difficile rilevazione per un periodo di tempo anche prolungato?*
- *4.40 La procedura di backup include la verifica della presenza di codice malevolo (virus/trojan) prima/dopo il backup?*
- *4.41 Sono presenti procedure rigorose per restringere l'accesso ai dispositivi di backup?*
- *4.42 Se la copia di backup viene trasferita elettronicamente ad un sistema remoto, le informazioni vengono trasmesse in forma crittografata o per il tramite di una rete dedicata sicura?*
- *4.43 Se i dati di backup sono trasportati fisicamente in una posizione secondari sono trattati con misure di sicurezza?*
- *4.44 Se le informazioni da copiare sono sensibili o di natura proprietaria, vengono criptate durante il processo di backup, così che sui supporti di memorizzazione siano registrate in forma crittografata?*
- *4.45 Le chiavi crittografiche usate per il backup sono memorizzate in un luogo sicuro, e distribuite in modo che una chiave compromessa non possa mettere a repentaglio la totalità dei dati salvati?*
- *4.46 Le chiavi crittografiche usate per il backup, insieme alla documentazione riportante la data e il sistema dove sono state utilizzate, vengono memorizzate in formato sicuro, in una località diversa dal luogo che ospita i supporti di backup? **
- *4.47 Se una perdita di informazioni salvate può mettere a repentaglio l'attività aziendale, è previsto che altre copie di backup vengano mantenute presso più di una località remota?*

- *4.48 I supporti di backup sono protetti da tentativi di furto durante la permanenza nel luogo in cui sono custoditi, sia esso locale o remoto?*
- *4.49 Quando i supporti di memoria di backup non servono più alla funzione di copia di salvataggio, sono previste procedure per la distruzione o il riuso dei supporti, che siano custoditi localmente o in località remota?*
- *4.50 Sono pianificati ed effettuati con regolarità test per garantire che i backup siano leggibili e non corrotti?*
- *4.51 Sono effettuati test a campione per verificare che i dati non siano stati alterati?*
- *4.52 Se le copie di backup sono trasportate fisicamente in località remota, vengono poste in contenitori di sicurezza anti-manomissione, trasportate in mezzi sicuri, e monitorate durante il transito? **
- *4.53 Tali dispositivi di protezione contengono sistemi GPS?*
- *4.54 I file di log delle attività rilevanti ai fini della sicurezza vengono salvati regolarmente e memorizzati in un formato che ne minimizzi le possibilità di manomissione?*
- *4.55 I file di log degli accessi delle applicazioni vengono periodicamente salvati ed inviati in luogo sicuro?*
- *4.56 I file di log degli accessi delle applicazioni sono disponibili per periodi sufficientemente lunghi da permettere di rintracciare le cause di una graduale corruzione di informazioni?*
- *4.57 Vengono eseguiti backup multipli, in maniera che se anche una copia venisse persa o manomessa, il sistema possa comunque essere ripristinato da un'altra copia?*
- *4.58 Esistono procedure per gestire dati di backup che non sono più integri, in particolare durante una situazione di crisi?*
- *4.59 Esistono procedure per gestire la perdita o il furto di nastri di backup non criptati che contengono informazioni proprietarie o sensibili?*

sez.5. AUDIT FATTORI UMANI

Gestione degli incidenti (*dipendenti / incaricati e soggetti autorizzati*)
Amministrazione della sicurezza
Azioni amministrative
Audit e review esterne
Senior Management
Azioni individuali dei dipendenti
Attività di reporting da parte dei soggetti autorizzati
Monitoraggio delle attività dei dipendenti
Formazione dei dipendenti in materia di *cyber security*
Responsabilità personale in tema di sicurezza

- *5.1 La salvaguardia della sicurezza dell'azienda Þ resa parte integrante in modo formale di ciascuna mansione delle persone che vi lavorano?*
- *5.2 Ai dipendenti viene fatto obbligo di sottoscrivere accordi sulla riservatezza e sulla proprietÓ intellettuale?*
- *5.3 Ogni componente del parco hardware informatico di cui l'azienda Þ proprietaria o licenziataria risulta essere di esplicita responsabilitÓ di un determinato dipendente?*
- *5.4 Esistono etichettature permanenti o altri marchi di identificazione che rendono facile per gli altri impiegati determinare chi ôpossiedaö un dato componente informatico?*
- *5.5 Al dipendente cui si assegna la responsabilitÓ di un dato apparato informatico viene richiesto anche di salvaguardarne la sicurezza in generale?*
- *5.6 I dipendenti sono abituati a tenere i computer portatili e altri apparati informatici trasportabili sotto osservazione diretta o riposti in locali sicuri quando vengono fatti uscire dai confini dell'azienda?*
- *5.7 Le politiche aziendali regolamentano l'uso corretto della posta elettronica, dell'accesso a internet e della messaggistica istantanea da parte dei dipendenti?*
- *5.8 Le policy aziendali definiscono quali dati possono essere postati su social media dai dipendenti e quali informazioni, invece, debbano rimanere riservate?*
- *5.9 I dipendenti sono ritenuti personalmente responsabili di eventuali azioni compiute sul sistema informativo aziendale che violano le politiche di sicurezza aziendali?*
- *5.10 Ai dipendenti viene impedita la condivisione del proprio computer con altri dipendenti?*
- *5.11 Ai dipendenti viene fatto divieto di scambiarsi le password tra colleghi?*

Formazione dei dipendenti in materia di cyber security

- *5.12 A tutti i dipendenti viene fatta periodicamente formazione sulle politiche di sicurezza adottate in azienda, e sui motivi per cui tali politiche debbano essere ritenute importanti?*
- *5.13 Ai dipendenti vengono indicate quali siano le categorie di informazioni gestite dall'azienda che vanno considerate sensibili?*
- *5.14 Ai dipendenti si insegna a diffidare di qualsiasi tipo di software arrivi per posta, anche se appare confezionato e spedito da fornitori di fiducia?*
- *5.15 Ai dipendenti si insegna a non cadere vittime di manipolazioni sociali tramite telefono o Internet, che potrebbero convincerli a rivelare informazioni strettamente private oppure indurli a digitare / chiamare determinate sequenze di numeri o caratteri?*
- *5.16 Ai dipendenti si raccomanda periodicamente di non scaricare tipi di file che possano contenere del codice eseguibile, di non aprire e-mail sospette, e di non installare software personale sui sistemi dell'azienda?*

- *5.17 Ai dipendenti vengono illustrati i rischi di sicurezza che possano correre se sono soliti memorizzare informazioni private, quali i codici di identificazione personali, sui propri telefoni cellulari?*
- *5.18 Durante il training vengono realizzate anche esercitazioni pratiche?*
- *5.19 I dipendenti sono sottoposti a test periodici per verificare la loro conoscenza sulle procedure di sicurezza, nonchÚ la conoscenza sulle minacce di ultima generazione?*

Monitoraggio delle attività dei dipendenti

- *5.20 Esiste un sistema per la raccolta di informazioni relative ai luoghi fisici e alle risorse informatiche alle quali ciascun dipendente ha accesso?*
- *5.21 Sono poste in essere attivitÓ di verifica dei log di accesso (fisci e elttronici) per identificare comportamenti abituali di accesso che non sono motivati dal ruolo del dipendente?*
- *5.22 Sono effettuate ricerche su web per verificare che i dipendenti non abbiano pubblicato informazioni che potrebbero causare problemi alla sicurezza informatica dell'azienda?*
- *5.23 Esiste un sistema per il monitoraggio puntuale delle risorse e dei dati ai quali un dipendente ha avuto accesso, in particolare quando ha comunicato di voler lasciare l'azienda?*
- *5.24 L'azienda fa una attivitÓ di analisi dei dati acceduti da un dipendente almeno nei 90 giorni antecedenti alla data in cui ha dato notizia di voler lasciare l'azienda stessa?*

Attività di reporting da parte dei soggetti autorizzati

- *5.25 I dipendenti sono consapevoli che ogni volta che installano un nuovo software applicativo in un computer aziendale, sono tenuti a fare reporting al personale di cyber-security dell'azienda?*
- *5.26 Esiste un modo semplice per i dipendenti per segnalare vulberabilitÓ di sicurezza, tentativi di cyber-attacco, telefonate sospette, ecc. e i dipendenti sono premiati per fare ci_?*
- *5.27 Le principali strategie di attacco sono descritte in modo abbastanza esaustivo ai dipendenti, in modo tale che ci sia una buona probabilitÓ di un riconoscimento fin da subito di tali segnali?*
- *5.28 Se un dipendente riceve un link a una risora Internet da un altro dipendente o da chiunque altro, sono formati perchÚ verifchino sempre la URL per verificare che punti a un dominio corretto/atteso?*

Azioni individuali dei dipendenti

- *5.29 Esiste un divieto contrattuale per i dipendenti di postare su Internet informazioni relative ai sistemi critici aziendali ai quali hanno accesso?*
- *5.30 Esiste un divieto contrattuale per i dipendenti di postare su Internet informazioni che possano permettere di individuare qualli misure di sicurezza sono state implementate dall'azienda?*
- *5.31 I dipendenti sono adeguatamente formati rispetto ai rischi di sicurezza che derivano dalla memorizzazione di informazioni personali (es. PIN, password) all'interno dei propri smart phone?*
- *5.32 I dipendenti sono istruiti a non fornire all'esterno informazioni rilevanti per la sicurezza, anche informazioni che sembrano apparentemente innocue?*
- *5.33 E' fatto divieto ai dipendenti di cedere i propri dispositivi di identificazione personale per permettere l'accesso alla struttura ad altri impiegati?*
- *5.34 I dipendenti sono formati sull'evitare l'utlizzo di password costruitre su dati biografici e fatti personali che potrebbero essere pubblicamente accessibili?*
- *5.35 I dipendenti sono formati su come costruire password che non appartengono a dizionari o basate su frasi?*

- *5.36 I dipendenti sono formati sui rischi di conservare le password in posti non sicuri, come ad esempio post-it nell'area di lavoro?*
- *5.37 I dipendenti sono formati sui rischi che potrebbero derivare dal collegamento di dispositivi personali (es. smartphone, tablet, digital camera) in computer aziendali, anche solo per caricare la batteria?*
- *5.38 Il personale addetto alla sicurezza Þ stato istruito sul fatto che impedire il collegamento non autorizzato di dispositivi elettronici, incluse pen drive, ai computer aziendali Þ tanto importante quanto prevenire che il furto o il danneggiamento del dispositivo?*
- *5.39 I dipendenti sono formati sul rischio che deriva dall'apertura di un alllegato presente in una e-mail generica, non apparentemente sensata o con comportamenti strani?*
- *5.40 I dipendenti sono formati sul fatto di non installare software per scopi personali sui computer aziendali?*
- *5.41 I dipendenti sono formati sul fatto di diffidare dai software che arrivano via mail (es. aggiornamenti) anche se la sorgente sembra essere trusted?*
- *5.42 I dipendenti sono formati sul fatto che non dovrebbero collegare nessun dispositivo di cui non conosce la provenienza solo per guardare cosa c'Þ dentro?*
- *5.43 I dipendenti sono formati sul fatto di non scaricare da Internet tipi di file che potrebbero contenere codice eseguibile?*
- *5.44 I dipendenti sono formati sul fatto che anche software di massa potrebbero comunque contenere malware?*
- *5.45 I dipendenti sono formati sul non cadere vittime di manipolazioni sociali attraverso telefono o via Internet che li potrebbe portare a rivelare informazioni legate alla sicurezza?*
- *5.46 I dipendenti sono formati sul non fornire telefonicamente sequenze di numero o di caratteri (es. password) quando qulcuno glielo chiede?*
- *5.47 Ci sono restrizioni formalli per gli utenti rispetto all'acceso a sistemi critici quando si trovano in posizioni strane?*
- *5.48 I ruoli dei dipendenti sono distinti in modo tale che un singolo dipendente non possa portare a termine una operazione crtica senza la consapevolezza degli altri impiegati?*
- *5.49 L'esecuzione di operazioni estremamente critiche richiede la partecipazione simultanea di duo o pi¨ impiegati?*
- *5.50 I dipendenti nell'area IT sono resi consapevoli di quanto sia pericoloso installare collegamenti di rete (es. Wi-Fi) che siano non documentati e non autorizzati del personale della sicurezza anche quando questa richiesta proviene da un capo?*
- *5.51 L'azienda ammonisce tutti i dipendenti che lasciano l'azienda che devono rispettarne la proprietÓ intellettuale?*
- *5.52 L'azienda ha procedure per la raccolta di evidenze forensi per ogni tentativo da parte di un dipendente di utilizzare un sistema aziendali per rubare dei dati o causare un danno?*

Senior Management

- *5.53 I manager senior dell'azienda sono regolarmente informati sullo stato di cyber security dell'azienda e sulle possibili conseguenze delle minacce emergenti?*
- *5.54 I manager senior dell'azienda sono resi edotti che un buon piano di cyber security parte dal comprendere come sono utilizzati i sistemi informatici aziendali ai fini della produzione del business?*
- *5.55 I manager senior dell'azienda sono resi edotti del fatto che la migliore strada per la gestione della maggior parte dei problemi di sicurezza non Þ quella di aggiungere pi¨ misure di cyber-security, ma di fare piccoli cambiamenti nel modo in cui le attivitÓ sono svolte?*
- *5.56 I manager senior dell'azienda sono resi edotti del fatto che la gestione di problemi di cyebr-security Þ generalmente pi¨ semplice e molto meno costosa quando questi possibili problemi sono presi in considerazione quando nuove operazioni di business sono attivate?*

- *5.57 L'azienda ha un Chief Information Security Officer?*
- *5.58 Il CISO Þ tenuto a fare un reporting al CFO e al CEO senza la presenza di altri dipendenti?*
- *5.59 L'azienda utilizza le notizie relative a nuovi attacchi alla cybersecurity che sono stato portati a termine contro altre organizzazioni per aggiornare i propri piani e programmi di cyber-security?*
- *5.60 L'azienda ha un canale attraverso il quale il personale dedicato alla cyber-security pu_ fornire consigli e avvisi riguardo alle implicazioni per la cyber-security nelle strategia, policy, procedure e rapporti verso l'esterno dell'azienda?*
- *5.61 Il personale di cyber-security è correttamente premiato se fa emergere considerazioni ai manager o ad altro personale esterno al team di ciberscurity, fino a che ha fatto in modo corretto?*

Audit e review esterne

- *5.62 Le policy di sicurezza di una azienda e la loro implementazione sono valutate annualmente da un auditor esperto esterno?*
- *5.63 Le policy di sicurezza dell'azienda e la loro implementazione sono attentamente verificate rispetto alle leggi vigenti e agli standar dell'industria?*
- *5.64 La review annuale delle policy di sicurezza delll'azienda e l'implementazione delle stesse Þ abbastanza approfondita per scoprire nuove vulnerabilitÓ?*
- *5.65 Gli audit effettuati sono esaminati in modo analitico per identificare le aree dove Þ necessario attivare delle contro misure?*
- *5.66 I diversi audit effettuati negli anni sono comparati, in modo tale da permettere al management di valutare se la sicurezza sta crescendo anzichÚ diminuendo?*

Azioni amministrative

- *5.67 Il personale addetto alle pubbliche relazioni e commerciale Þ reso edotto sul fatto che le loro attivitÓ potrebbero avere impatto sull'organizzazione aziendale della cybersecurity?*
- *5.68 L'azienda evita attivitÓ pubblicitarie e materiale pubblicitario che potrebbero portare l'attenzione dei punti e dei sistemi critici aziendali?*
- *5.69 L'azienda evita attivitÓ di marketing che possano semprare provocazioni per la comunitÓ del underground hacker, rendendo l'azienda un possibile target?*
- *5.70 Se l'azienda Þ un target potenzialmente di alto profilo, gli annunci di lavoro per l'assunzione di personale nel ramo della cyber-security sono fatte in modo tale da evitare l'identitÓ dell'azienda?*
- *5.71 Sono effettuati approfonditi backgroun checks sui dipendenti che hanno un livello di accesso elevato alle informazioni, anche se i loro salari e il titolo di lavoro potrebbero non far intendere tale accesso?*
- *5.72 Se un dipendente viene promosso a un livello pi¨ alto in termini di responsabilitÓ e di accesso alle informazioni, viene effettuato un nuovo background check su di lui?*
- *5.73 Viene effettuato un background check del personale addetto al mentenimento degli edifici dell'azienda (es. guardiani, pulizie, ecc.) che hanno un accesso fisico elevato alle componenti dei sistemi?*
- *5.74 Se avviene un cambio consdierevole nel comportamento personale o ecomonico di un dipendente, esiste una procedure per effettuare un background check non intrusivo e capire le ragioni?*
- *5.75 Se un dipendente sta attraversando un periodo di grandi difficolta personali, esiste una policy per ridurre temporaneamente le sue responsabilitÓ rispetto ai sistemi critici aziendali?*
- *5.76 Gli impiegati addetti al monitoraggio dei sistemi critici sono ruotati al fine di rendere il proprio lavoro meno noioso?*
- *5.77 L'azienda provvede a premiare pubblicamente in meeting interni i dipendenti che operano nei sistemi informativi per aver fatto un lavoro particolarmente di pregio o rilevante per l'azienda stessa?*

- *5.78 L'azienda fornisce un canale attraverso il quale gli impiegati possono nominare in modo anonimo gli altri dipendenti per una riconoscimento speciale, basato sul fatto di aver creato qualcosa di particolarmente innovativo rispetto ai sistemi informativi?*
- *5.79 L'azienda fornisce un canale per i dipendenti per manifestare le proprie lamentele senza che questo comporti punizioni e permettendo ai dipendenti di verificare che le lamentele siano state correttamente considerate?*
- *5.80 L'azienda gestisce il ridimensionamento di certi settori in una maniera che minimizzi i sentimenti ostili da parte degli ex dipendenti?*
- *5.81 Se un dipendente che ha un ruolo che gli permette accesso ai dati interessanti per la concorrenza lascia l'azienda, viene effettuatao un check per verificare segnali di utilizzo di tali informazioni nel nuovo lavoro?*
- *5.82 L'azienda fornisce ai dipendenti una procedure che gli permette di segnalare tentativi da parte di soggetti esterni di estorcere la loro collaborazione nel superare i sistemi di sicurezza dell'azienda?*
- *5.83 L'azienda monitora le attivitÓ di ex dipendenti nelle nuove aziend dove questi si trovano, soprattutto relativamente a quelli che avevano accesso a sistemi e procedure critiche?*

Amministrazione della sicurezza

- *5.84 Esiste un sistema affidabile per tenere traccia di tutti i log e le altre sorgenti di informazioni di cui ha bisogno il team di security e per verificare che siano stati trattati con uno schedule appropriato?*
- *5.85 Esiste un sistema affidabile e costantemente aggiornato per il tracking di tutte le vulnerabilitÓ evidenziate dai dipendenti, scoperte dal audit, riportate dai vendors o diffuse dai giornali?*
- *5.86 Il sistema di tracking delle vulnerabilitÓ permette al personale addetto alla sicurezza di determinare rapidamente quali vulnerabilitÓ devono ancora essere gestite, quali siano attualmente in gestione e quali siano state giÓ sistemate?*
- *5.87 Alle vulnerabilitÓ viene assegnato un livello di prioritÓ elevato in modo tale che le vulnerabilitÓ pi¨ critiche siano gestite pi¨ rapidamente?*
- *5.88 Il livello di prioritÓ assegnato tiene in considerazione la natura delle operazioni di business e produzione che utilizzano il sistema informatico in cui la vulnerabilitÓ si verifica?*
- *5.89 Il sistema di tracking delle vulnerabilitÓ Þ coordinato con il sistema di tracking delle patch e degli aggiornamenti di sicurezza, in modo tale che non si perda produttivitÓ nella gestione dello stesso problema pi¨ di una volta?*
- *5.90 Esiste un security manager che verifichi con continuitÓ che tutte le vulnerabilitÓ siano state prese in considerazione per tempo e nel corretto ordine di prioritÓ?*
- *5.91 Il CISO fa una review mensile dei programmi e delle procedure per la cyber security per verificare che siano allineati con le attese?*
- *5.92 Il team di security ha un tempo sufficiente per mettere in pratica misure di sicurezza e rinnovare quelle vecchie, anzichÚ dover spendere tutto il proprio tempo a mettere patch alle vulnerabilitÓ e rispondere agli attacchi?*

Gestione degli incidenti (*dipendenti / incaricati e soggetti autorizzati*)

- *5.93 L'azienda ha piani dettagliati per la gestione degli incidenti di sicurezza, sia quando stanno accadendo sia immediatamente dopo?*
- *5.94 I piani dettagliati per la gestione degli incidenti di sicurezza, specificamo chiaramente i punti in cui i senior manager devono essere avvisati?*
- *5.95 I dipendenti sanno chi avvertire, sia dentro che fuori dell'azienda, nell'eventualitÓ di un possibile attacco?*
- *5.96 Sono effettuate con regolaritÓ esercitazioni in cui sono coinvolti i dipendenti responsabili della gestione degli incidenti, attraverso simulazioni realistiche?*

- *5.97 Le persone chiave hanno avuto l'opportunitÓ di mettere in pratica la propria capacitÓ di gestione delle emergenze in situazioni reali?*
- *5.98 Gli incidenti reali o simulati sono seguiti da una discussione per identificare la lesson learned?*
- *5.99 L'azienda utilizza costantemente le news relative agli attacchi subiti da altre aziende per aggiornare e rinforzare i piani di risposta agli attacchi che potrebbero arrivare?*
- *5.100 I piani dettagliati per la gestione degi incidenti sono conservati come strattamente confidenziali?*
- *5.101 I risultati delle simulazioni di attacco sono trattati come elemento altamente confidenziale?*
- *5.102 I dipendenti sanno come interrompere o spegnere rapidamente i canali di comunicazione che sono apparentemente utilizzati da un attacco informatico?*
- *5.103 Se un particolare account Þ stato utilizzato durante un attacco, gli amministratori dei sistemi sono in grado di forzare rapidamente un logout e disabilitare l'account nelle rete aziendale?*
- *5.104 Se c'Þ ragione di credere che un attacco informatico possa essere imminente, c'Þ un piano per disabilitare temporaneamente i sistemi vulnerabili e interrompere i canali di comunicazione, al fine di limitare l'effetto dell'attacco?*
- *5.105 Se si Þ verificato un attacco grave, esistono procedure che possono essere rapidamente impementate per isolare o mettere in quarantena i sistemi che possono essere stati contaminati, senza necessitÓ di spegnerli?*
- *5.106 Sono presenti delle procedure che possono essere rapidamente adottate per isolare o mettere in quarantena i sistemi infetti se vi Þ una ragione per non fidarsi della procedura informatiica?*
- *5.107 I cavi che devono essere disconnessi in caso di un cyber attacco sono chiaramente etichettati?*
- *5.108 I dipendenti sanno quali cavi debbanno essere staccati nel caso di un attacco e quali eventi debbano triggerare questa risposta?*
- *5.109 Se un attacco sta causando la cancellazioni o la cifrature dei dati su un computer locale i dipendenti sono stati autorizzati a spegnere immediatamente il computer?*