ANALISI DEI REQUISITI PRESENTI NEI CAPITOLATI DI GARA IN TEMA DI CYBER SECURITY

Versione 1.0

10 maggio 2023

SOMMARIO

AUTORI

Analisi realizzata da:

coordinatore prof. **Roberto Setola**
(UCBM)

Hanno collaborato

- Luigi Ballarano (Terna)
- Francesco Ceraso (ENI)
- Massimo Cottafavi (SNAM)
- Luca Faramondi (UCBM)
- Antonella Fascioli (Unindustria)
- Fabiola Furlai (Poste Italiane)
- Aniello Gentile (ENEL)
- Maria Teresa Gonnella (UCBM)
- Alessandro Lamesa (Elettronica spa)
- Matteo Lucchetti (Cyber 4.0)
- Rocco Mammoliti (Poste Italiane)
- Mario Mangano (AdR)
- Pierluigi Martusciello (BNL Paribas)
- Bianca Mazzà (UCBM)
- Marta Menci (UCBM)
- Mario Merone (UCBM)
- Francesco Morelli (Ferrovie dello Stato Italiane)
- Gabriele Oliva (UCBM)
- Marco Papi (UCBM)
- Stefania Sica (Cy4Gate)
- Massimo Tedeschi (Leonardo)
- Antonio Truglio (Unindustria)
- Luca Vollero (UCBM)

Società coinvolte

Alla ricerca hanno contributo diverse realtà nazionali, fra le quali quelle elencate qui di seguito oltre ad altre che hanno preferito non esplicitare la loro collaborazione. A tutti coloro va la nostra gratitudine per le informazioni e il supporto offertoci

- A2A
- ADR
- BNL Paribas
- Cy4Gate
- Elettronica Spa
- ENI
- Leonardo
- Poste Italiane
- SNAM
- Terna
- Tim

Attività realizzata dal Gruppo di Lavoro "Cyber Resilienza delle Infrastrutture Critiche" coordinato dal Prof. Roberto Setola nell'ambito del "Gruppo Tecnico Cyber Security di Unindustria" presieduto dall'Ing. Lorenzo Benigni

PREMESSA

Questo documento nasce all'interno del gruppo di lavoro su "Cyber Resilienza delle Infrastrutture Critiche" di Unindustria con la collaborazione dell'Associazione dei security manager AIPSA e del Centro di Competenze Cyber 4.0.

L'obiettivo alla base del lavoro era quello di aiutare le PMI, sia sul territorio regionale che nazionale, ad assumere una migliore postura di cyber security nella convinzione che ciò sia fondamentale tanto per tutelare il tessuto produttivo nazionale (costituito per la stragrande maggioranza di piccole e piccolissime realtà) quanto per garantire il corretto funzionamento delle infrastrutture vitali per il Paese che vedono quali loro fornitori una miriade di piccole imprese.

Purtroppo, la minaccia cyber è sempre più attuale ed è tale che un'inadeguata gestione della stessa può esporre, soprattutto realtà medio piccole, a contraccolpi devastanti che possono anche portare al fallimento della singola realtà industriale.

Le grandi realtà imprenditoriali hanno compreso questa problematica e da tempo hanno attuato specifici programmi con l'obiettivo di mettere in atto un processo virtuoso per costantemente innalzare la cultura aziendale e le soluzioni tecnologiche in modo che siano adeguate a fronteggiare lo scenario cyber.

Lo stesso non sempre può dirsi per le PMI caratterizzate in larga parte da mancanze di competenze culturali specifiche che portano in primo luogo a dare una visione minimalista della problematica con conseguente sottostima della gravità e tendenza ad allocare le scarse risorse economiche su aspetti percepiti come più profittevoli.

Per fornire una visione alternativa, con questo lavoro ci si è posto l'obiettivo di evidenziare come le "spese" in cyber security, purché ben orientate, rappresentano in primo luogo degli **"investimenti abilitanti"** per il consolidamento e la tenuta del business di ogni azienda.

Infatti, come evidente dalla lettura di questo documento, i requisiti di una adeguata postura cyber sono sempre più considerati essenziali dalle grandi realtà industriali per accreditare un'azienda quale proprio fornitore. Tendenza questa che andrà ad aumentare nei prossimi anni alla luce della crescente presa di coscienza a tutti i livelli della rilevanza del tema cyber e quindi della volontà da parte dei grandi gruppi industriali di preservare la propria reputazione imponendo ai propri fornitori un'adeguata postura cyber.

Come meglio illustrato nel paragrafo successivo l'indagine ha coinvolto 32 aziende, alcune delle quali hanno ritenuto opportuno palesarsi come partecipanti all'analisi e la cui lista è riportata nel frontespizio di questo documento. Altre hanno preferito mantenere l'anonimato.

A tutti coloro che hanno voluto contribuire all'indagine va il nostro incondizionato plauso e ringraziamento così come ci corre l'obbligo di ringraziare i colleghi di Unindustria che hanno proficuamente collaborato creando i link ed i canali di contatto con le diverse realtà laziali e non solo.

MODALITÀ DI INDAGINE

Il gruppo di Lavoro ha analizzato i requisisti presenti nei capitolati e nei documenti per le procedure di accreditamento dei fornitori di 32 aziende di rilevanza nazionale che si sono rese disponibili a fornire in modo anonimizzato le richieste che in tema di cyber security usualmente inseriscono nei propri documenti commerciali. Si è deciso di escludere dall'analisi le forniture di servizi e prodotti di cyber security, poiché si è ritenuto che la loro inclusione avrebbe inutilmente elevato l'asticella delle richieste. Ci si è pertanto concentrati su tutti quei contratti che hanno

per oggetto la fornitura di beni e servizi, inclusi quelli di natura IT, per la cui erogazione è necessario che il fornitore entri in contatto diretto, in qualunque forma, con i sistemi informatici del committente.

L'indagine ha anche attinto ad alcuni capitolati di gara presenti su internet in quanto facente parte di procedure di gara ad evidenza pubblica.

Ulteriore oggetto di indagine sono stati i questionari di valutazione. Nello specifico sono stati analizzati 20 questionari di valutazione utilizzati dalle aziende per avere un quadro sintetico e confrontabile della postura cyber dei propri fornitori, questionari che per altro possono anche essere di ausilio al fornitore per un'attività di auto-valutazione.

REQUISITI TECNICO-INFORMATICI PER FORNITORI DI SERVIZI SPECIFICI

Confrontando i documenti delle aziende che hanno partecipato alla survey del progetto si possono evidenziare quelle che sono le condizioni minime e imprescindibili di cyber security che vengono richieste alle PMI che intendano operare quali fornitori di beni o servizi, siano essi servizi di ICT (Information and Communication Technologies) o altro tipo, a patto che per le attività connesse con il servizio vi sia la necessità da parte del fornitore di interfacciarsi in una qualunque forma con i sistemi informatici del committente[1].

L'analisi ha evidenziato che i requisiti fondamentali richiesti alle PMI possono essere divisi in quelli legati alla politica per la sicurezza delle informazioni e quelli connessi alle condizioni propedeutiche ai processi di sviluppo e programmazione, due elementi distinti che possono essere a loro volta divisi in processi di controllo e processi di gestione dei rischi.

Si noti che, come meglio illustrato nel seguito, sebbene ad oggi esistano numerose certificazioni nel campo della cyber security, **non tutte le aziende richiedono espressamente alle PMI di essere in possesso di detti certificati**, ma richiedono che vengano rispettati degli standard minimi che tutelino le informazioni condivise e consentano continuità nell'erogazione del servizio.

Dall'analisi condotta risulta che il 62% delle compagnie richiede il possesso della certificazione ISO 27001, ma soltanto per il 30% delle stesse il possesso è un vincolo indispensabile per la stipula del contratto, mentre la restante parte preferisce che i fornitori siano in grado di soddisfare una serie di requisiti tecnici minimi senza condizionare la collaborazione all'effettivo possesso della certificazione. La stessa discrepanza tra richiesta e vincolo contraddistingue anche il rispetto delle linee guida presenti nella norma ISO 31000 e il possesso della certificazione ISO 28000 (per i dettagli sulle certificazioni richieste e sul loro contenuto vedere l'appendice di questo documento).

Con riferimento al campione di aziende analizzato, le richieste che maggiormente vengono fatte alle PMI che vogliano collaborare in qualità di fornitori di servizi risultano essere le seguenti (fra parentesi la percentuale rispetto al campione della specifica richiesta):

- sviluppo e conservazione in archivio di Audit periodici (100%), con richiesta di poter effettuare controlli anche da parte del committente stesso (47%) o da esperti esterni (38%);
- protocolli di controllo, gestione e memorizzazione degli accessi e dei log (94%);
- manutenzione correttiva e preventiva degli asset con dismissione degli strumenti ritenuti obsoleti (91%);

1 Come evidenziato in premessa dal novero sono stati esclusi i servizi di cyber security.

- formazione del personale, tanto per la diffusione della conoscenza dei protocolli interni quanto per la prevenzione di incidenti cyber, per i quali si richiede una formazione attiva, in cui i dipendenti vengono messi alla prova, ad esempio, tramite la diffusione di e-mail di phishing appositamente generate. La formazione è bene che sia periodica e che preveda tematiche specifiche in base al livello di responsabilità del dipendente a cui è rivolta (84%);
- sviluppo di processi specifici per la gestione degli incidenti che permettano una continuità nella fornitura del servizio (84%);
- esistenza di responsabili che rispondano di eventuali errori, incidenti o malfunzionamenti (84%);
- presenza di firewall e antivirus installati a protezione della rete e degli asset (75%);
- compilazione di questionari per la valutazione da parte del committente delle prassi applicate per la gestione della sicurezza aziendale dell'ipotetico fornitore (72%);
- presenza di business continuity e/o disaster recovery plan (72%);
- tempestiva segnalazione in caso di sospette o comprovate violazioni, tanto per la compromissione di dati sensibili quanto per l'alterazione delle funzionalità del sistema (72%);
- applicazione di protocolli per la gestione delle chiavi, siano esse chiavi di decriptazione o password di accesso ad aree e servizi specifici (69%);
- rispetto di protocolli per il trasferimento di dati sensibili previamente valutato e approvato da parte del committente (59%);
- fornitura al committente di un inventario aggiornato degli asset che verranno utilizzati durante il contratto, richiedendo anche, in alcuni casi, un elenco dei dipendenti che avranno accesso alle informazioni durante tutta la durata del rapporto tra committente e fornitore con visione dei curricula degli stessi (56%);
- segregazione e/o segmentazione delle reti, in modo da poter isolare e limitare i danni in caso di attacco malevolo e compromissione di parte del sistema (50%).

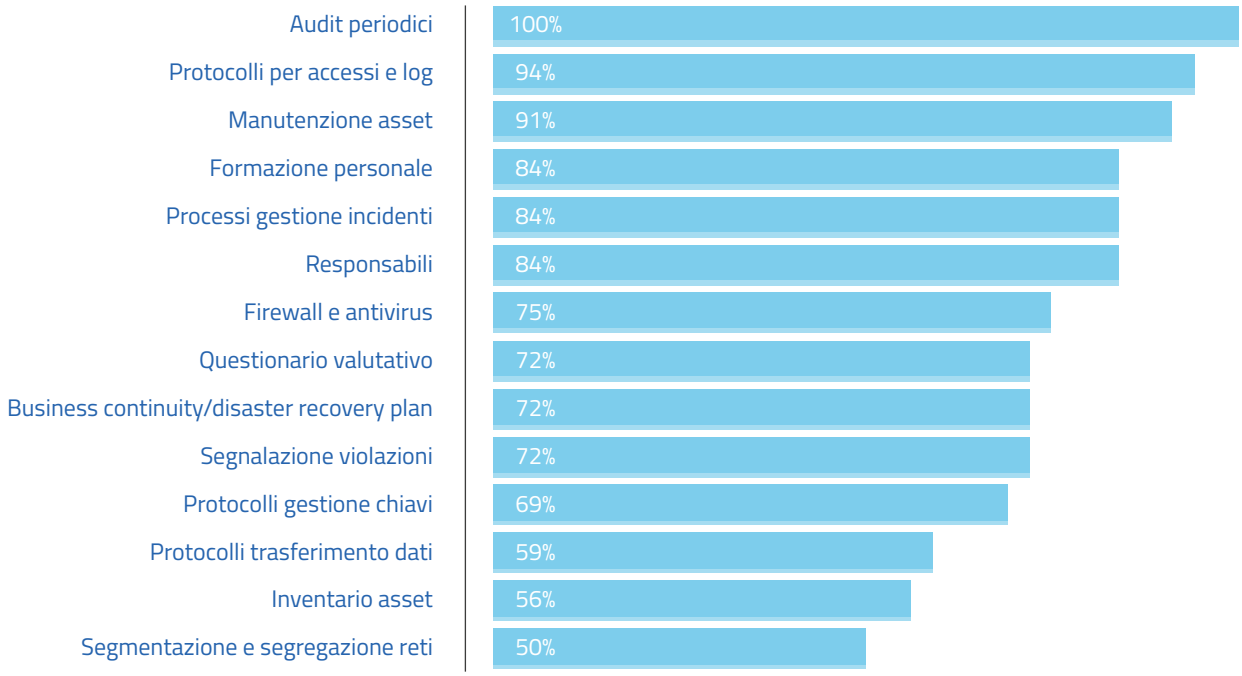

Figura 1 - Principali richieste per gli ipotetici fornitori

Nella figura 1 è riportata la percentuale di adozione della specifica misura nei capitolati/contratti di fornitura analizzati. In particolare, si nota come **la totalità dei soggetti richiede audit periodici**. Analogamente, la stragrande maggioranza delle aziende analizzate richiede ai propri fornitori la presenza di protocolli per la gestione di accessi e log (94%) e la manutenzione degli asset (91%). Parimenti importanti sono considerati gli aspetti connessi con la formazione del personale, la presenza di responsabili e di procedure per la gestione degli incidenti (tematiche presenti nell'84% del campione).

La richiesta di elementi più direttamente connessi con la tecnologia appare meno pressante essendo presente solo in un sottoinsieme, seppur elevato, di casi. Questo aspetto origina in parte da alcune peculiarità legate alle diverse tecnologie impiegate, ma sottolinea anche come le grandi aziende **valorizzino maggiormente gli aspetti procedurali e di formazione del personale** piuttosto che l'esistenza di elementi tecnici che appaiono sulla scorta dell'analisi effettuata, non completamente adeguati a garantire livelli di cyber security rilevanti.

In questo contesto si segnala che oltre il 70% del campione richiede ai propri fornitori di compilare degli specifici questionari in materia di cyber security il cui contenuto è analizzato nel paragrafo a loro dedicato. Va specificato che i questionari hanno generalmente un doppio scopo, aiutano infatti non solo le grandi aziende a mappare correttamente la postura cyber del fornitore, ma consentono al (potenziale) fornitore di effettuare un'attività di autovalutazione che ha il merito di aiutare le singole aziende ad individuare le aree di miglioramento, sia in termini generali che con riferimento alle specifiche sensibilità in tema di cyber security dell'intera realtà aziendale.

Nei paragrafi a seguire verrà fornita una disamina dei requisiti minimi richiesti suddivisi in macro aree e micro sezioni.

1 POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Quando si parla di "politica per la sicurezza delle informazioni" si fa riferimento a tutti gli aspetti che interessano la gestione della sicurezza delle informazioni che vengono acquisite, visualizzate, modificate e conservate dall'azienda. Per mantenere la riservatezza di tali dati è necessario consolidare una serie di procedure che consentano di avere il continuo controllo tanto degli accessi a ogni livello del sistema quanto della gestione delle vulnerabilità note e nascenti.

A livello di standard internazionali la gestione dei dati è normata dalla ISO 27001:2022 che identifica i requisiti per mantenere e migliorare continuamente il sistema gestionale delle singole organizzazioni. Analizzando la norma è possibile individuare procedimenti e pratiche attuabili per l'edificazione di un'efficace organizzazione aziendale, che spaziano dalla sicurezza fisica degli ambienti e delle apparecchiature utilizzate, alla gestione degli accessi ai dati e delle chiavi di crittografia. Non mancano indicazioni sulla gestione degli incidenti a diversi livelli, tanto relativamente ad un ipotetico attacco hacker quanto eventualmente causati dall'utilizzo improprio degli strumenti da parte di fornitori o appaltatori.

La diffusione di tali certificazioni, sebbene recenti analisi di mercato dimostrino che sia in forte crescita, non è ancora tale da indurre le aziende a considerarne il possesso come condizione ineludibile per la partecipazione ai bandi di gara. Di fatto, **il 62% delle società inserisce nei propri capitolati la richiesta di possesso della certificazione ISO 27001** ma, di queste, soltanto il 30% la ritiene necessaria per la stipula di eventuali contratti. **Il restante 70% delle società ritiene che il possesso della certificazione possa essere disatteso se vengono rispettati requisiti specifici richiesti in modo indipendente dalla normativa**.

La mancata obbligatorietà di tale certificazione non va intesa come una mancata attenzione alle politiche di gestione della sicurezza dei dati. Di fatto, si evince che le aziende che non richiedono il possesso della certificazione hanno sostituito tale richiesta con

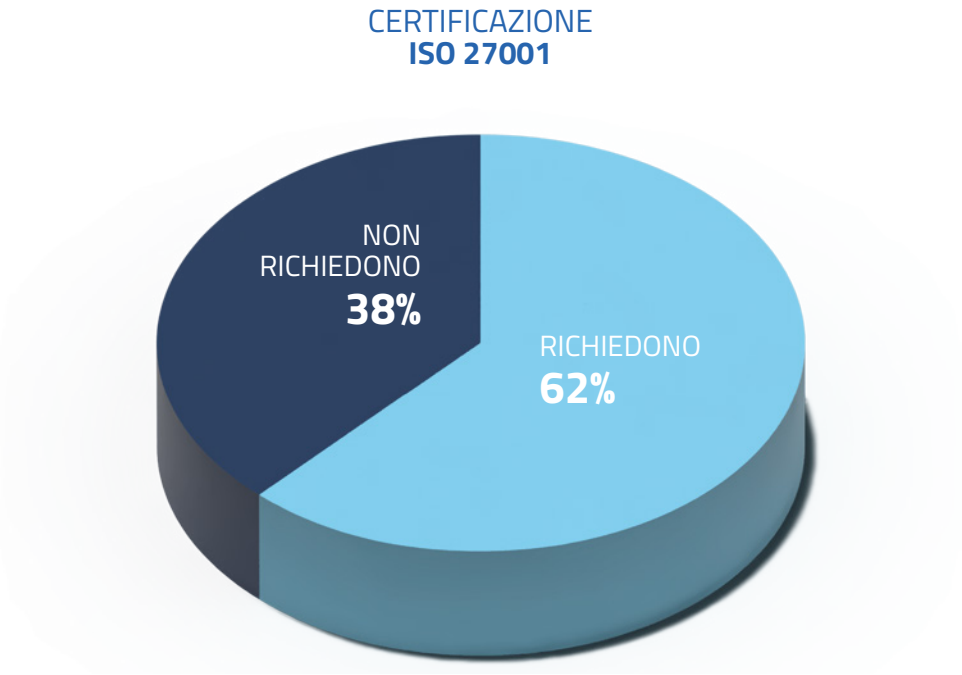

Figura 2 - Percentuale di capitolati contenenti richieste relative alla norma ISO 27001

una serie di disposizioni similmente strutturate che vanno a creare la base necessaria per una corretta e sicura gestione dei dati. **Appare infatti che le aziende che hanno sviluppato una più capillare politica di cyber security sono fra quelle che non richiedono in modo esplicito la certificazione ISO 27001 ai propri fornitori**. Questo è in parte legato ad una profonda conoscenza che esse hanno della norma e dei rischi legati alla cyber security che consente loro di richiedere alle proprie controparti l'adozione di specifiche misure di valutazione e gestione del rischio che, sulla base dalla loro esperienza, vengono reputate idonee a garantire adeguati livelli di sicurezza evitando di appesantire il processo con gli iter burocratici propri della certificazione. In altri termini, risulta che **più un'azienda ha maturato un significativo livello di cultura in tema** di cyber security più spingerà i suoi fornitori a far conoscere una postura proattiva a tale tema, vedendo nel mero possesso della certificazione un approccio eccessivamente orientato ad una visione a compliance non sempre adatte a gestire la dinamicità dello scenario cyber. Occorre però evidenziare che la non richiesta della certificazione si traduce nella **necessità per l'azienda di effettuare specifiche attività di audit** presso i propri (potenziali) fornitori per l'istaurazione di un forte legame di "trust", aspetti che sono in parte alleggeriti in presenza di una certificazione essendo l'attività di verifica demandata all'ente certificante.

Si potrebbe quindi concludere che, sebbene non tutti richiedano la certificazione ISO, tutte le grandi aziende prevedono intensi controlli sulla gestione delle informazioni che andranno eventualmente a condividere con le PMI fornitrici di un determinato servizio.

1.1 MANUTENZIONE E GESTIONE DEGLI ASSET

Alcuni requisiti vengono trattati con unanime attenzione dalle diverse aziende, tra questi vi è la necessità, da parte dei fornitori, di rispettare una serie di protocolli di gestione e manutenzione degli asset.

L'elemento a cui è dedicata maggiore attenzione è quello dei **protocolli di manutenzione e gestione che vengono visionati e valutati dal 91% delle aziende coinvolte**.

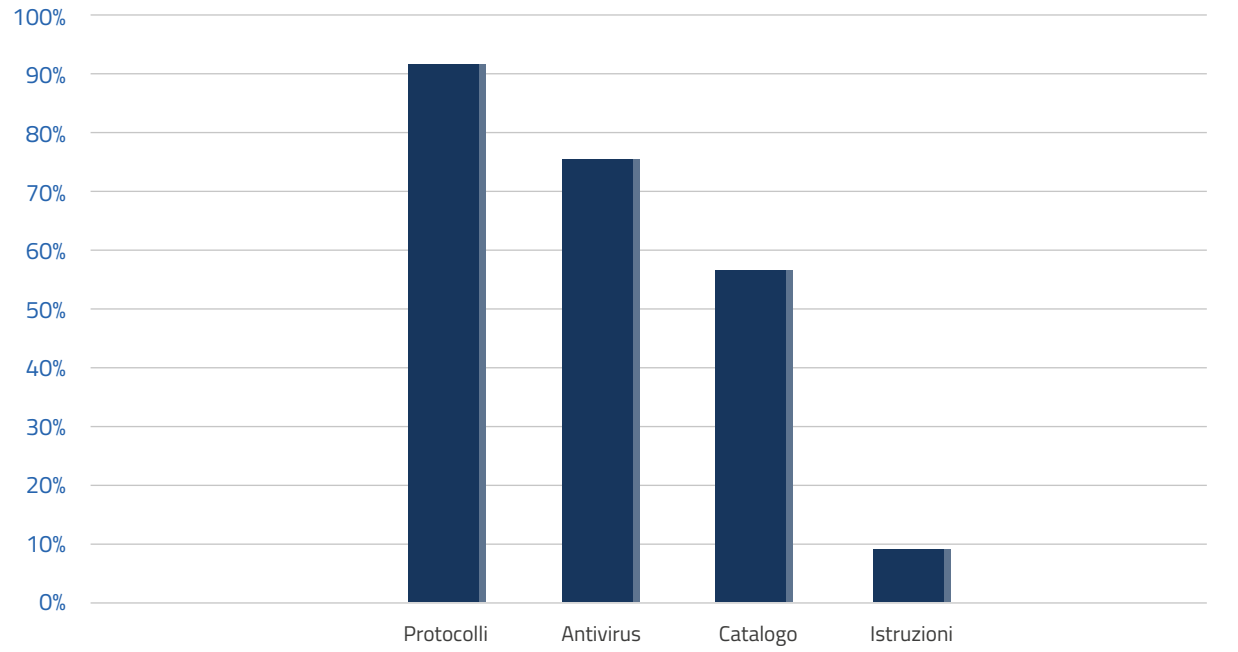

Figura 3 - Richieste relative alla manutenzione e alla gestione degli Asset

Nello specifico, secondo quanto si legge nella norma ISO 27001, rientrano nelle pratiche manutentive tutte le azioni volte a preservare gli strumenti da:

- minacce e pericoli ambientali;
- accessi non autorizzati;
- manomissioni durante eventuali trasporti;
- danneggiamenti che ne alterino l'integrità;
- compromissione della fornitura per mancata alimentazione elettrica degli asset;
- riassegnazione degli strumenti al personale;
- corretta dismissione e smaltimento di asset obsoleti.

Si noti che insieme a tali protocolli di gestione nel 56% del campione è associata la richiesta di condivisione di un **catalogo periodicamente aggiornato degli apparati fisici, delle piattaforme e delle applicazioni software presenti in struttura**, comprendendo un catalogo di sistemi informativi esterni all'organizzazione. La richiesta è dettata dalla necessità di conoscere chi avrà accesso alle informazioni trattate e attraverso quali strumenti, per poter poi condurre una valutazione dell'Audit aziendale, argomento che verrà descritto nei capitoli successivi.

Altro aspetto su cui le richieste aziendali collimano è l'attenzione data alla presenza di **antivirus aggiornati** sui dispositivi in uso presso il (probabile) fornitore. Di fatto, il 75% delle aziende si accerta che i propri collaboratori attuino protocolli di gestione degli asset che prevedano il costante aggiornamento degli antivirus.

Va specificato che, in caso di subappalto delle forniture, è richiesto dal 66% dei committenti il controllo periodico di tutti i dispositivi hardware e software forniti da terzi con conservazione e condivisione degli assesment.

Vi è attenzione anche alla manutenzione fisica degli Asset, dove per manutenzione fisica si intende tanto la capacità di assicurare l'integrità e il corretto funzionamento degli strumenti anche in caso di eventi naturali che possano causare allagamenti o interruzioni elettriche, quanto la gestione della riassegnazione degli hardware e/o la loro dismissione. Nello specifico, per prevenire il danneggiamento dei Data Center il 20% delle aziende intervistate richiede che questi siano posti in ambienti separati e adeguatamente protetti, mentre per la riassegnazione e la dismissione degli Asset il 25% delle compagnie richiede che sia attuato un Data Wiping che assicuri la totale e irreversibile cancellazione dei dati e la conseguente impossibilità di compromissione aziendale in caso di utilizzo di software di Data Recovery da parte di eventuali soggetti terzi.

Tenendo conto del fatto che la normativa ISO 27001 dedica molta attenzione a tutto l'aspetto gestionale della strumentazione e che tutti gli argomenti finora trattati sono presenti nella normativa stessa sotto diverse diciture, la mancata richiesta specifica, più o meno dettagliata, non deve essere necessariamente interpretata come una minore attenzione da parte di un'azienda, ma può essere dettata dal fatto che il possesso della certificazione viene ritenuto adeguato per il rispetto di gran parte delle richieste sopracitate.

Le discrepanze fra i requisiti dedicati alla manutenzione degli asset riguardano alcune procedure che vengono analizzate più o meno dettagliatamente dalle diverse aziende. Nello specifico, vediamo come solamente il 9% delle strutture coinvolte richiede espressamente che le istruzioni di determinate apparecchiature siano facilmente reperibili e consultabili da qualsiasi operatore lo ritenga necessario. Questa richiesta assume particolare rilevanza se si pensa a tutti quegli strumenti condivisi da diversi operatori e quindi maggiormente esposti a vulnerabilità tanto gestionali (trattamento, disposizione e trasmissione di dati) quanto funzionali (maggiore esposizione a malware, riavvio o aggiornamenti non controllati e malfunzionamenti causati da errori tecnici commessi da operatori inesperti), ma non deve sorprendere la poca attenzione a questo fattore se si considera che l'accesso a tali dispositivi è solitamente vincolato a diversi livelli di autorizzazione e autenticazione e subordinato a formazione specifica.

Relativamente alla gestione degli asset vi sono anche specifiche richieste di "training" dei dipendenti, ma poiché questo ricopre diverse sfaccettature della politica per la sicurezza delle informazioni e dei processi di sviluppo, vi si dedicherà una sezione più ampliamente dettagliata nelle pagine successive.

1.2 CONTROLLO DEGLI ACCESSI

Sostanzialmente tutte le aziende coinvolte nel progetto presentano nei propri capitolati requisiti specifici sul **controllo degli accessi, tanto fisici quanto informatici**.

Per controllo degli accessi fisici si intende un protocollo di sicurezza che assicuri l'accesso controllato ai locali, con maggiore sorveglianza per le aree che ospitano database e/o server per le quali è richiesto che vi siano videocamere di sorveglianza per poter visionare le registrazioni in caso di attività anomale che facciano sospettare l'accesso non autorizzato ai locali.

Più complesso e articolato è il protocollo di gestione e registrazione dei log, in quanto prevede una serie di controlli da ripetere periodicamente per poter avere contezza dell'effettiva protezione dei dati sensibili e dei dipen-

denti che possono visualizzarli e modificarli. Tale maggiore complessità emerge anche dalla constatazione che solo il 59% del campione richiede in modo esplicito una specifica attenzione alla gestione dei log.

Primo e imprescindibile elemento su cui fondare la gestione dei log è la diversificazione dei permessi di accesso alle informazioni. Attraverso una diversa etichettatura e catalogazione dei dati è possibile identificare i dati maggiormente sensibili e renderli accessibili soltanto a determinati operatori e dipendenti. L'assegnazione dei diversi diritti dovrebbe essere conforme ai principi di "minimum privilege", "need to know" e "segregation of duties". Inoltre, prevedere protocolli diversi per la consultazione, l'elaborazione, la modifica o la conservazione dei dati consente di avere un controllo completo sulla gestione degli stessi.

Una volta stabilito quali dipendenti possono accedere o meno a determinate banche dati, va periodicamente controllato che alle modifiche contrattuali corrispondano immediati aggiornamenti dei permessi a livello informatico. Ad esempio, successivamente ad una rescissione contrattuale si deve provvedere all'eliminazione di eventuali e-mail aziendali e ci si deve assicurare che l'utenza dell'ex dipendente non possa più accedere a nessuna informazione. Le stesse verifiche vanno fatte in seguito a variazioni di livello dei dipendenti o dell'etichettatura dei dati. **L'attenzione e l'osservazione di tali permessi deve essere garantita da protocolli di gestione che vengono espressamente richiesti dal 94% delle aziende**.

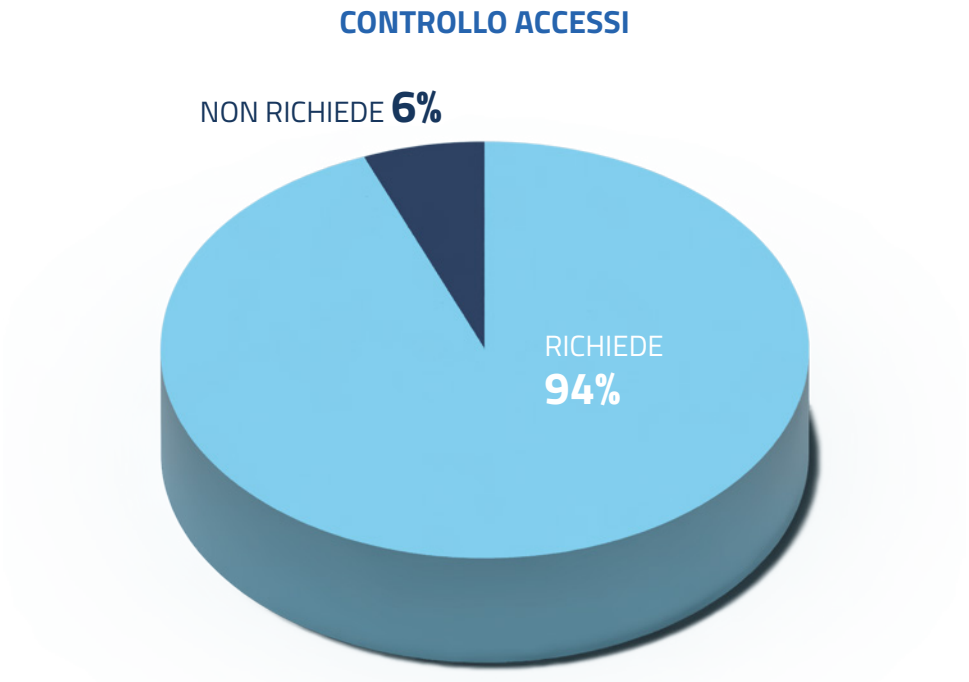

Figura 4 - Percentuale richiesta protocolli di gestione accessi

Al fine di poter analizzare la corretta gestione dei dati è inoltre richiesto un archivio dei log (59% delle aziende) in cui siano registrati non soltanto gli accessi, ma anche le principali attività svolte da uno specifico codice identificativo e le coordinate orarie in cui queste sono state svolte. Tutte le azioni di lettura, scrittura, modifica o cancellazione dei dati devono essere tracciate e conservate, con particolare attenzione ai log a dati bancari (piattaforme, software o app che consentono l'accesso ai conti o l'invio di pagamenti) per i quali deve essere garantita la completezza e l'autenticità delle informazioni. L'archivio deve consentire d'individuare la possibile causa di eventuali disservizi attraverso l'analisi delle attività che si sono registrate al momento del disservizio stesso, motivo per cui queste sono le informazioni minime che vengono rilevate:

- Eventuali tentativi di accesso falliti;
- Accessi effettuati;
- Modifica o tentata modifica delle credenziali di accesso;
- Attività di consultazione e/o apertura di documenti, programmi e software specifici;
- Attività di modifica ai file;
- Accesso a funzioni privilegiate;
- Errori di sistema e informazioni sullo stesso.

Ogni attività registrata deve essere associata allo User ID che l'ha eseguita e devono esserci informazioni sulla data e sull'ora in cui è avvenuta.

Per quanto riguarda la gestione di tale archivio, solo una piccola percentuale delle aziende (3%) richiede che i dati in esso contenuti siano catalogati ed etichettati secondo il formato illustrato nella normativa ISO 8601. Si noti che quanto previsto nella ISO 8601 non differisce in modo significativo rispetto a quanto esposto precedentemente, ma fornisce indicazioni sull'ordine in cui i dati devono essere conservati e sotto quali nomenclature specifiche.

Mentre alcune aziende (59%) ritengono che sia sufficiente la buona gestione e archiviazione dei log e delle attività svolte da ogni utente, altre richiedono specifici requisiti di sicurezza in caso di collegamenti al sistema da remoto. Per tali utenze viene infatti richiesto dal 41% delle aziende che si acceda solamente tramite l'utilizzo della VPN fornita dal committente.

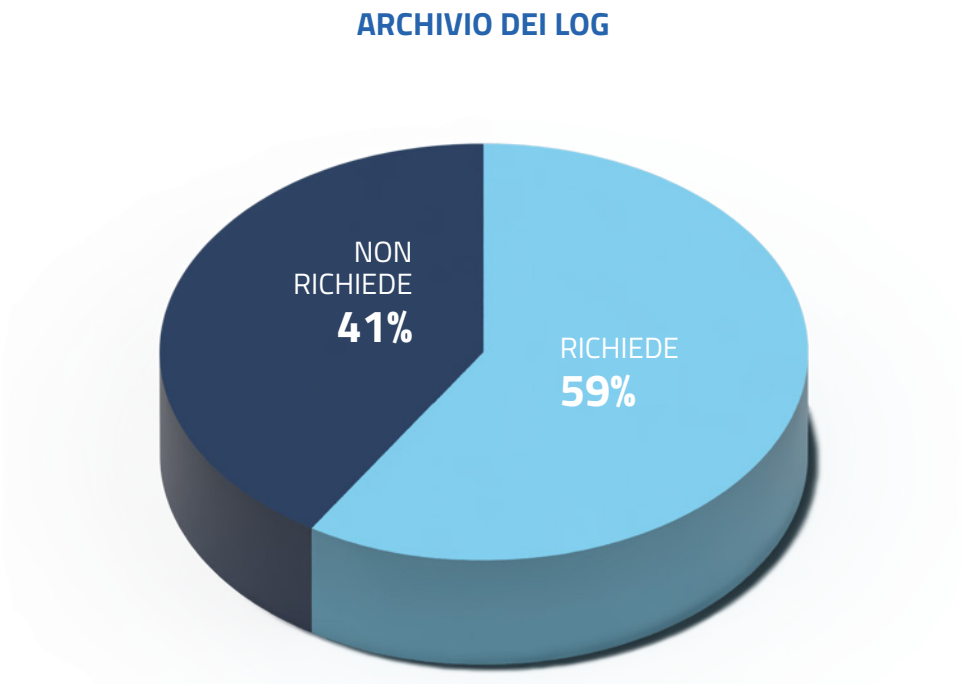

Figura 5 - Percentuale richiesta archivio log

Per consentire alle PMI di alleggerire il proprio lavoro di controllo, che andrebbe svolto periodicamente (ogni sei o dodici mesi), in alcuni casi è possibile configurarsi all'interno delle piattaforme di Identity Governance del committente e demandare lo svolgimento dei controlli alla piattaforma stessa.

1.3 CRITTOGRAFIA E GESTIONE CHIAVI

Assicurare un uso corretto ed efficace delle chiavi di accesso ai sistemi informativi e della crittografia è ritenuto un elemento necessario per proteggere la riservatezza, l'autenticità e l'integrità dei dati all'interno dell'intero sistema e il 69% delle grandi aziende richiede di conoscere i protocolli di gestione delle chiavi utilizzati dalle imprese con le quali collaborano.

Nella già citata norma ISO 27001 si legge che è necessario sviluppare protocolli per l'uso dei controlli crittografici e per la gestione delle loro chiavi per tutta la loro durata, senza dare maggiori indicazioni e, conseguentemente, lasciando libertà decisionale alle società sui processi da eseguire e sul tipo di crittografia da applicare.

Come accennato nel paragrafo precedente, esiste tutto un processo di etichettatura dei dati che serve a sviluppare una classificazione tale da permettere di applicare protezioni distinte per i diversi livelli di dati identificati. L'etichettatura è un processo utile per diversificare il tipo di crittografia da applicare, ma questa stratificazione non rientra nelle specifiche richieste dalla norma ISO 27001 e solamente il 50% delle aziende la richiede espressamente in modo da poter proteggere con una crittografia più complessa quei dati ritenuti maggiormente sensibili.

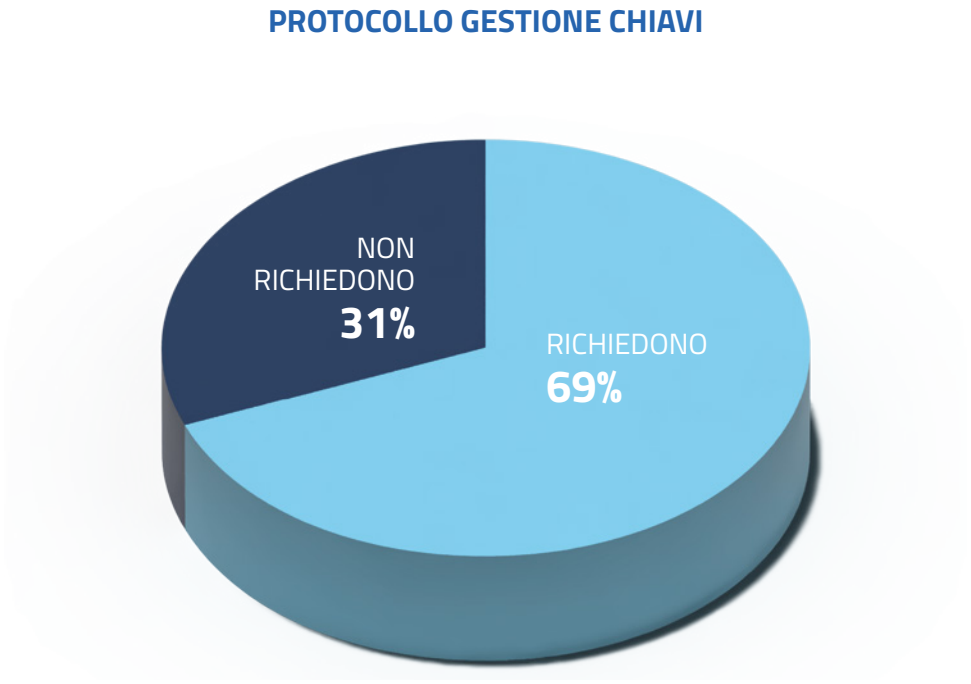

Figura 6 - Percentuale richiesta protocolli gestione chiavi

Sebbene si sia già parlato di diversi tipi di protocolli, il quadro si complica quando si parla di protocolli di gestione delle chiavi, perché con il termine "chiavi" s'identificano tanto le effettive chiavi di decriptazione quanto le password di accesso ai diversi ambienti fisici e virtuali del sistema e i protocolli devono tener conto di entrambi gli elementi e di tutte le vulnerabilità che li contraddistinguono. A tal proposito le aziende propongono una serie di requisiti minimi da rispettare, tra i quali:

- Impossibilità di modificare le chiavi da dispositivi non previamente autorizzati (69%);
- Utilizzo di password complesse e obbligo di modifica delle stesse periodicamente (69%);
- Trasmissione di dati sensibili solo se opportunamente criptati (66%);
- Divieto di memorizzare e impossibilità di visualizzare in chiaro i dati del committente (41%);
- L'accesso alle chiavi di decriptazione deve essere permesso ai soli utenti amministratori e in caso di estrema necessità (31%);
- Mantenimento in archivio della crittografia sostituita (25%);
- Uso di protocolli TLS (19%).

Il protocollo TLS (Transport Layer Security) viene utilizzato per proteggere le comunicazioni e lo scambio di informazioni tra due nodi della rete (client e server) da possibili manomissioni o intrusioni. La protezione è affidata all'utilizzo di certificati crittografici asimmetrici e allo scambio di chiavi di sessione simmetriche che consentono il riconoscimento di eventuali intromissioni non autorizzate. Questo protocollo specifico è richiesto solamente dal 19% delle aziende.

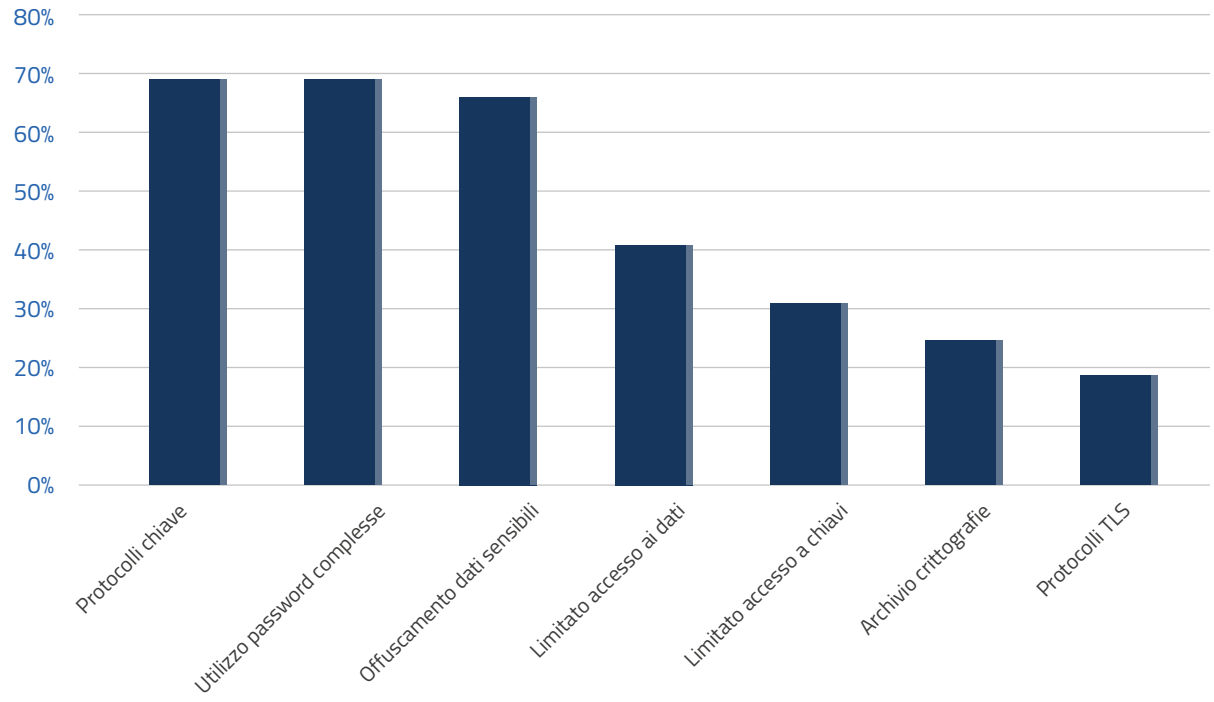

Figura 7 - Richieste per gestione crittografia e chiavi

1.4 TRASFERIMENTO INFORMAZIONI SENSIBILI (E-MAIL E SUPPORTI DI MEMORIZZAZIONE)

Il trasferimento delle informazioni può avvenire attraverso diversi canali (e-mail, supporti rimovibili, database condivisi o ambienti cloud) e tra diversi soggetti (all'interno della stessa organizzazione o tra fornitore e committente).

Ricoprendo un così ampio campo d'azione, quello del trasferimento dati è stato riconosciuto dalla normativa ISO 27001 come potenziale vulnerabilità e per questo trattato approfonditamente con l'obiettivo di fornire indicazioni che, se correttamente applicate, limitino i rischi connessi all'utilizzo dei diversi strumenti di trasferimento.

Dall'analisi condotta emerge che quelle società che richiedono il possesso della certificazione ISO 27001 (62%) non inseriscono all'interno dei loro capitolati specifici requisiti sulla gestione dei processi di trasferimento delle informazioni. Al contrario, il restante 38% esplicita quali procedure ritiene vincolanti ai fini della stipula dei contratti di collaborazione.

Nello specifico, rispetto al numero totale delle aziende interrogate:

- il 22% delle aziende ritiene fondamentale l'utilizzo dell'e-mail aziendale per le comunicazioni sensibili, di cui una più bassa percentuale richiede l'utilizzo specifico della PEC;
- il 50 % richiede il rispetto di protocolli dettagliati che regolino l'uso dei supporti rimovibili,
- il 53% delle aziende verifica la gestione della tempestiva segnalazione in caso di sospetta compromissione dei dati;
- il 75% delle aziende pongono maggiore attenzione all'aspetto della vulnerabilità connessa all'errore umano, motivo per cui ritiene necessario il training di tutti gli operatori per prevenire casi di phishing, man-in-the-middle o utilizzo improprio di dispositivi removibili che espongano il sistema a virus e malware.

Le procedure di utilizzo dei supporti rimovibili devono essere sviluppate in base allo schema di classificazione adottato dall'organizzazione e devono garantire che le informazioni non siano visualizzate, utilizzate o manomesse da soggetti non autorizzati, né durante l'utilizzo dei dispositivi, né durante il loro trasferimento e nemmeno dopo la loro dismissione.

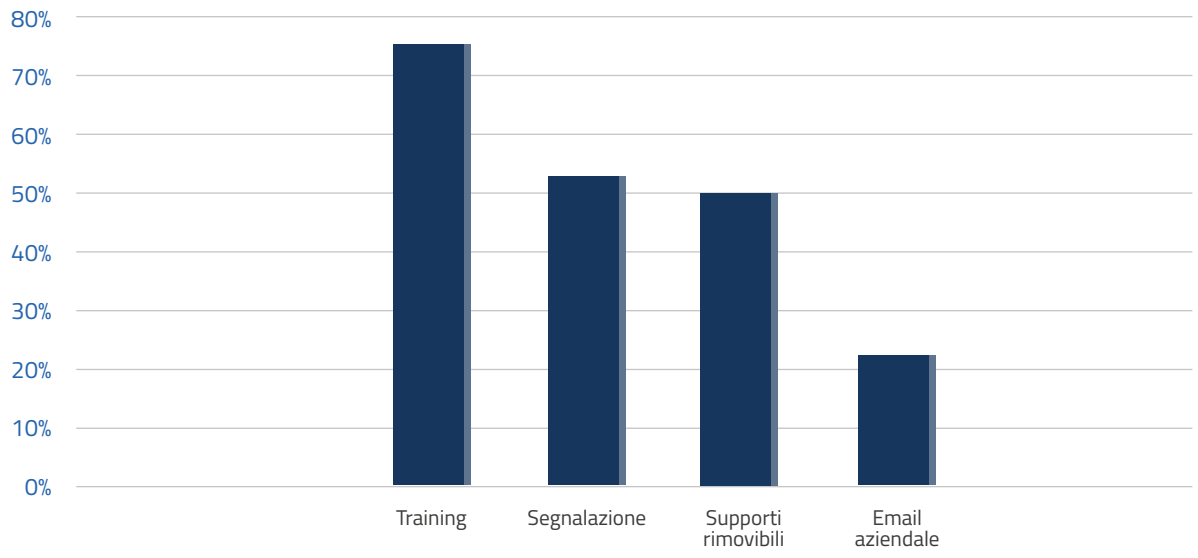

Figura 8 - Elementi richiesti per il controllo del trasferimento delle informazioni

L'aspetto relativo al training del personale quanto quello della gestione delle segnalazioni verranno più ampiamente trattati nei paragrafi ad essi dedicati

1.5 AUDIT, VULNERABILITY ASSESSMENT E PENETRATION TEST

Gli Audit, i Vulnerability Assessment e i Penetration Test sono processi lievemente diversi tra loro che vengono sviluppati con l'obiettivo di verificare la conformità dei sistemi informativi, riconoscere, monitorare ed eventualmente correggere le vulnerabilità del sistema.

L'audit permette di analizzare le attività svolte dal sistema per verificarne la conformità alle procedure stabilite, considerando norme, regolamenti e pratiche interne. Un tipico audit di sicurezza prevede la valutazione di una serie di elementi tra cui: i dispositivi posseduti, gli accessi e i log, le e-mail, le configurazioni hardware, la rete, la configurazione fisica del sistema e dell'ambiente. Obiettivo dell'audit è quello d'identificare potenziali vulnerabilità presenti per ciascun elemento, in modo tale da poterle monitorare o poter lavorare alla loro correzione.

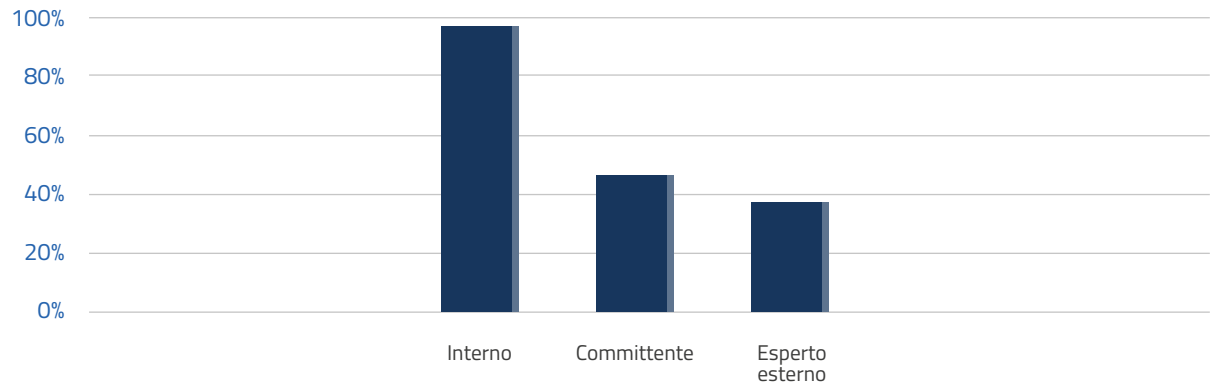

Figura 9 - Autori degli audit

Il Vulnerability Assessment e il Penetration Test sono procedure simili che hanno l'obiettivo d'identificare le vulnerabilità presenti nel sistema. La differenza tra le due procedure risiede nel fatto che il Vulnerability Assessment è un processo automatico di scansione e verifica che fornisce segnali di allerta lì dove incontra un potenziale pericolo, mentre il Penetration Test è sviluppato da un esperto IT che tenta di accedere ai dati di sistema simulando un attacco hacker ai danni dell'azienda.

Tutte le aziende richiedono che vi sia un controllo del sistema aziendale, ma vi sono discrepanze tra le richieste specifiche per la conduzione del controllo. I requisiti aziendali si differenziano infatti in: autore del controllo, frequenza dei controlli, modalità di archiviazione e comunicazione degli stessi.

Generalmente, l'analisi delle vulnerabilità viene svolto direttamente dal fornitore dei servizi (97% dei casi), ma il committente può richiedere un controllo previa assegnazione della fornitura condotto direttamente da lui (47% dei casi) o da esperti esterni ad entrambe le aziende coinvolte (38% dei casi). Inoltre, il committente può svolgere analisi sulla sicurezza interna in qualsiasi momento del contratto e, in caso di rilevamento di vulnerabilità

ritenute particolarmente gravose, può richiederne la correzione entro un tempo stabilito, pena la decadenza del contratto stesso.

Un archivio dei controlli svolti è necessario per poter monitorare le vulnerabilità note, tanto per comprenderne l'evoluzione e considerarne la correzione, quanto per valutare le azioni intraprese per la gestione delle stesse. Inoltre, attraverso l'archivio è possibile risalire ad attacchi o minacce subite e valutare quali azioni permettano di evitare perdite di dati o danni a strumenti e/o dipendenti causando il minor disservizio possibile. Di fatto, il 53% delle aziende richiede che vi sia una corretta gestione degli archivi e il **75% richiede una pronta segnalazione di eventuali violazioni rilevate**, con comunicazione anche delle azioni di rientro previste.

Il controllo di tutti i dispositivi hardware e software, inclusi quelli forniti da terzi (come specificato dal 66% dei documenti presi in esame), va svolto periodicamente, a cadenza semestrale o annuale per quanto riguarda l'aspetto generale e ogni qualvolta sia necessario un aggiornamento.

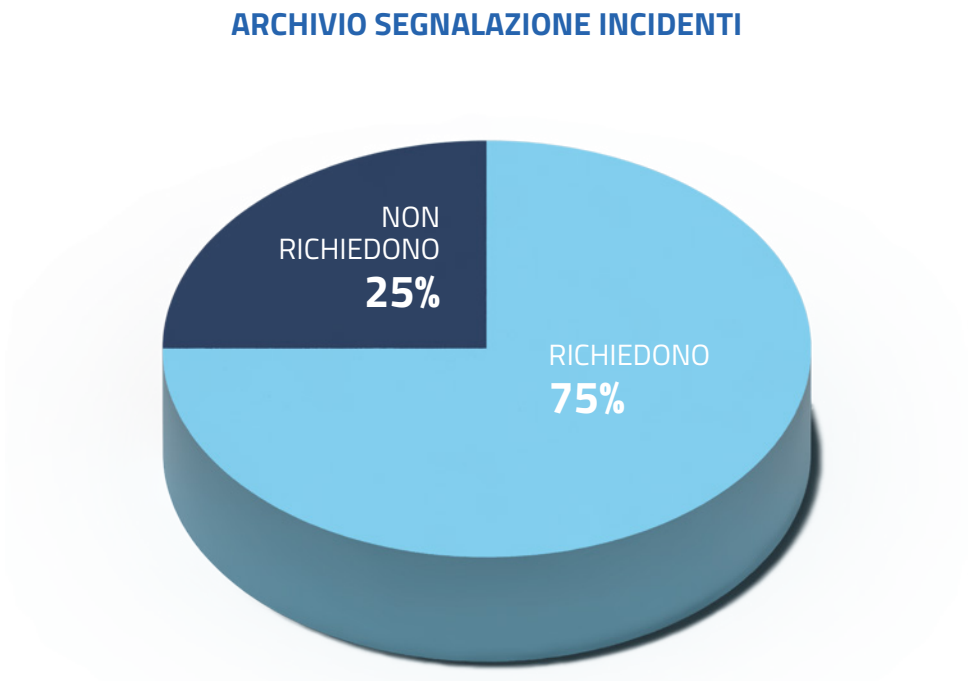

Figura 10 - Percentuale di richiesta di un archivio delle segnalazioni

1.6 CONTROLLO RETI INTERCONNESSE

In un mercato sempre più interconnesso è necessario tutelarsi anche da quei pericoli legati alle vulnerabilità che possono caratterizzare la rete e per questo non tutte le aziende ritengono sufficiente la difesa assicurata da strumenti quali firewall e antivirus. Per incrementare la sicurezza delle reti interconnesse, il 41% delle aziende richiede che il fornitore sia in possesso di una rete intranet aziendale e di un accesso alla stessa solo tramite VPN per i collegamenti da remoto o per tutte quelle connessioni da o verso reti esterne non direttamente gestite o controllate dal committente stesso.

Inoltre è richiesto che le reti interconnesse presentino una struttura segmentata che renda più complesso l'attacco da parte di agenti malevoli e che permetta una più facile gestione degli incidenti garantendo la minor compromissione possibile del sistema (50% dei casi esaminati).

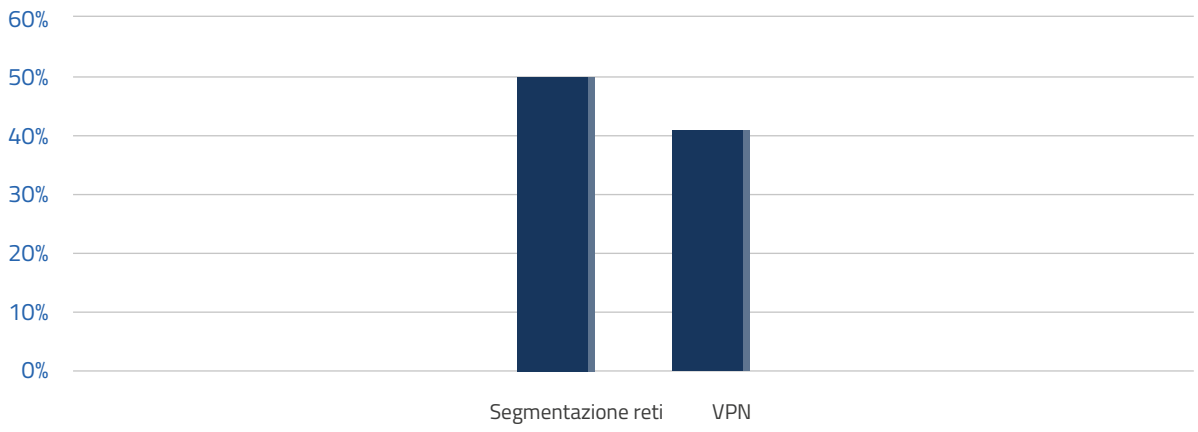

Figura 11 - Richieste relative per la gestione delle reti interconnesse

1.7 PROCEDURE DI GESTIONE DEI RISCHI E DI RISPOSTA AGLI INCIDENTI

Finora abbiamo analizzato tutte quelle che sono le richieste legate al rilevamento e alla valutazione delle vulnerabilità del sistema e degli strumenti aziendali, senza considerare le azioni di correzione delle stesse o di risposta agli incidenti.

Queste ultime sono ampliamente regolate dalle seguenti norme:

- ISO 27001, in cui è possibile trovare indicazioni sulla corretta gestione degli incidenti relativi alla sicurezza delle informazioni e sugli aspetti relativi alla gestione della continuità operativa a seguito di incidenti;
- ISO 28000, che definisce i requisiti per l'implementazione di un sistema di gestione della sicurezza lungo tutta la catena di fornitura (Supply Chain Security);
- ISO 31000, dedicata a tutto il processo di valutazione e gestione del rischio e risposta agli incidenti.

Sottraendo al computo totale i dati inerenti i bandi pubblici che, molto spesso, non presentano il possesso delle certificazioni quale elemento imprescindibile, la percentuale delle aziende che citano le norme sopra indicate sono: oltre il già noto 62% di richiesta della certificazione ISO 27001, che escludendo i bandi pubblici sale al 67%, soltanto il 13% delle aziende richiede richiede il rispetto delle linee guida della norma ISO 31000, e il 7% richiede la certificazione ISO 28000. È bene sottolineare ancora una volta che la mancata richiesta di possesso delle cer-

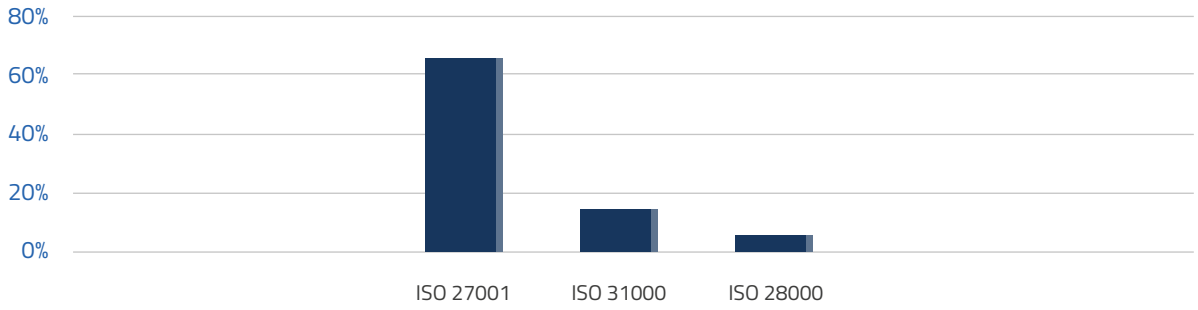

Figura 12 - Percentuale di richiesta delle certificazioni ISO

tificazioni è probabilmente dettata dalla volontà di evitare appesantimenti processuali dovuti agli iter burocratici propri della certificazione, preferendo invece richiedere una serie di requisiti tecnici minimi che assicurino una corretta gestione degli incidenti e dei rischi anche in assenza della certificazione stessa.

Di fatto, il 72% delle aziende fornisce dei questionari valutativi alle PMI (ai quali è dedicato un paragrafo a parte) e l'84% esegue una valutazione dei protocolli previsti dai fornitori in risposta a eventuali incidenti. Questi protocolli devono contenere una serie di azioni preventive e correttive, tra le quali rientrano:

- nomina di responsabili per la gestione dei dati e degli incidenti (84%);
- aggiornamento costante dei sistemi di protezione quali firewall (75%);
- segnalazioni di allerta inviate tempestive e automaticamente da applicativi che riconoscano funzionamenti anomali o accessi sospetti (72%);
- sviluppo di Disaster recovery plan (72%);
- capacità di rapido ripristino dei sistemi di business compromessi nel rispetto dei livelli definiti dal RTO (Recovery Time Objective – massimo lasso di tempo tollerato da un computer, un sistema, un network o un'applicazione in stato di errore dopo un incidente) e dal RPO (Recovery Point Objective – massima quantità di dati che il sistema può perdere a seguito di un incidente, elemento che dipende dalla distanza temporale tra l'ultimo backup utile e l'incidente stesso) (34%);
- separazione chiara dei compiti e delle diverse mansioni con personale specializzato (16%).

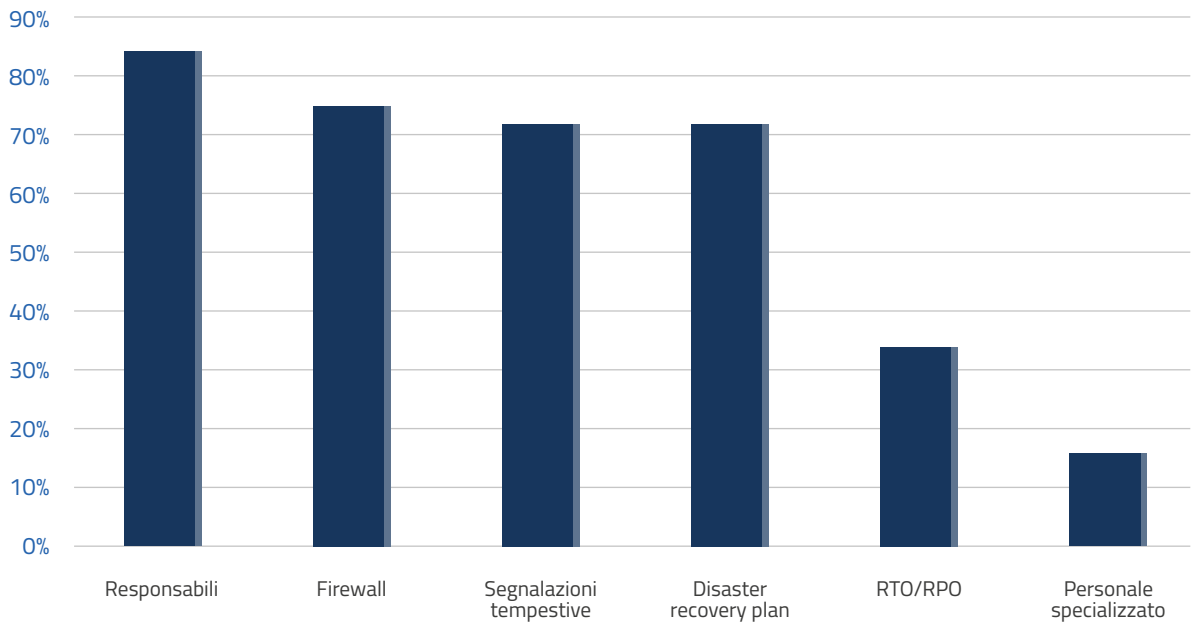

Figura 13 - Strumenti e protocolli per la gestione degli incidenti

La presenza di firewall richiesta dal 75% delle aziende assicura che, in caso di rilevamento di compromissioni, siano inviati segnali di allerta agli amministratori del sistema in modo che questi possano provvedere al controllo e alla correzione degli stessi, ma non sono gli unici segnali di allerta da tenere in considerazione, infatti le aziende specificano che è necessario che esistano strumenti in grado di inviare segnalazioni di violazioni da tutti i dispo-

sitivi di sicurezza, siano essi cyber (anti-virus e firewall) o fisici (porte o armadietti blindati e ambienti protetti).

In caso di fornitura di software o applicazioni, queste devono essere progettati in modo tale da poter eseguire protocolli di gestione del rischio adeguatamente strutturati in caso di necessità. Il 14% delle aziende richiede espressamente che gli sviluppatori delle applicazioni prevedano che, in caso di sospetta alterazione dei dati, queste cancellino le chiavi di crittografia e terminino l'esecuzione immediatamente.

1.8 FORMAZIONE DEL PERSONALE

La formazione riguarda numerosi aspetti, a partire dal corretto utilizzo degli strumenti in uso fino alla conoscenza approfondita e meditata delle politiche di trattamento delle informazioni adottate dall'azienda. Le vulnerabilità legate all'errore umano sono numerose e difficilmente gestibili, per questo **lo sviluppo di corsi di formazione è ritenuto un elemento basilare da parte di un alto numero di aziende (84%)**. Questo tipo di formazione del personale ha l'obiettivo di tutelare l'azienda da perdite o sottrazioni illecite di dati sensibili perpetrati attraverso il phishing o l'utilizzo di strumenti di memorizzazione esterna al cui interno sono nascosti malware. In genere il training deve avvenire attraverso corsi di formazione e il personale è tenuto a firmare un documento che attesti l'avvenuta partecipazione a tali corsi prima di poter accedere al materiale e agli strumenti condivisi da parte del committente. Usualmente il percorso di formazione ricopre tutti i processi finora descritti: gestione degli incidenti; modalità di trasferimento dati; corretto utilizzo degli asset; etc.. Di norma, la formazione è da considerarsi obbligatoria anche per eventuali subcontraenti.

Altro tipo di training è quello legato alla fornitura di software o di nuovi applicativi, per i quali il committente inserisce all'interno dei documenti contrattuali anche le spese legate alla trasmissione della conoscenza degli strumenti forniti a favore dei propri dipendenti. Si tratta dunque di una formazione realizzata dal fornitore per il committente il cui scopo è quello di assicurare il corretto utilizzo degli strumenti da parte dei dipendenti di quest'ultimo anche al fine di poter effettuare interventi correttivi di primo livello senza dover richiedere assistenza al produttore. Questo secondo tipo di formazione compare soltanto nel 6% dei capitolati (in particolare in parte di quelli che hanno come oggetto la fornitura di servizi di sviluppo software).

Altro elemento specifico che rientra nel concetto di "formazione" è la richiesta di personale specializzato e certificato presente soltanto nel 16% dei capitolati.

2 QUESTIONARI

L'analisi ha riguardato anche i questionari di valutazione utilizzati da 20 realtà industriali. Alcuni di tali questionari sono proposti in modo cartaceo o comunque stand-alone, mentre la maggior parte consentono la compilazione attraverso un apposito sito web.

Rispetto alla disamina degli elementi presenti nei capitolati, una comparazione dei questionari appare maggiormente complessa alla luce della forte eterogeneità che li contraddistingue in termini di: obiettivi del questionario, organizzazione del questionario e tipologia di risposta (risposta in forma chiusa multipla o singola, ovvero risposta aperta).

Tale eterogeneità è plasticamente evidente andando già solo a considerare la numerosità delle domande presenti in ciascun questionario. Infatti, sebbene la media delle domande per singolo questionario sia pari a 66 vi è una significativa varianza fra un questionario e l'altro, si passa infatti da un minimo di 14 domande (2 questionari hanno meno di 20 domande) ad un massimo di 227 domande (5 questionari hanno oltre 100 domande e di questi 2 oltre le 200 domande).

Quasi tutti i questionari sono articolati in sezioni con titoli che possono essere utilizzati per effettuare una sommaria aggregazione dei diversi elementi al fine di effettuare una comparazione ed evidenziare quali argomenti sono reputatati di maggior interesse. Occorre, però, precisare che la suddivisione in sezioni è in qualche misura arbitraria ed esistono sovrapposizioni fra il contenuto di sezioni etichettate in modo diverso nei singoli questionari. Si noti che nei questionari analizzati non si osserva alcuna correlazione fra il numero delle sezioni e il numero totale di domande presenti nel questionario.

Alcuni dei questionari analizzati sono strutturati secondo il framework NIST, pertanto, le domande sono raggruppate in termini di elementi legati alle attività di: Identify; Protect; Detect e Respond. In altri casi le domande sono raggruppate in termini di attività svolta per prevenire problematiche rispettivamente di Riservatezza, Integrità e Disponibilità (paradigma CIA). Alcuni questionari hanno un taglio rivolto alla disamina di solo alcuni specifici aspetti, come ad esempio le modalità di attuazione delle attività di Business Continuity, mentre altri, infine, risultano "flat" senza cioè una suddivisione in sezioni (questo accade in presenza di questionari con poche domande, in genere meno di 20).

Tralasciando queste tipologie di questionari e concentrandoci su quelli per i quali le sezioni hanno una titolazione esplicativa possiamo osservare che la quasi totalità dei questionari analizzati (86%) ha una sezione dedicata a domande relative alle modalità di gestione degli aspetti connessi con la sicurezza dei sistemi, delle reti e delle informazioni.

Egualmente importante appare il tema della sicurezza fisica la cui specifica sezione è presente nel 79% dei questionari; stessa percentuale che ritroviamo anche con riferimento alle sezioni dedicate al tema della gestione delle identità e del controllo degli accessi. Si noti che, sebbene le due tematiche siano in genere considerate contigue, se osserviamo la Figura 15 notiamo che non sempre le due sezioni sono presenti nei medesimi questionari.

Nel 71% dei questionari ritroviamo una sezione dedicata a domande relative alla modalità di gestione degli aspetti di Business Continuity e nel 64% per ciò che attiene la gestione degli incidenti.

Le modalità con le quali sono sviluppate le attività di awareness e formazione del personale sono analizzate in specifiche sezioni nel 50% dei questionari.

La Figura 14 riporta per le più frequenti voci la percentuale di capitolati dove appare la specifica sezione.

Interessante notare che nel 36% dei questionari vi è una specifica sezione dedicata alle modalità con la quale l'azienda fornitrice si relaziona con i suoi fornitori (sub-fornitori) in tema di garanzie di cyber security.

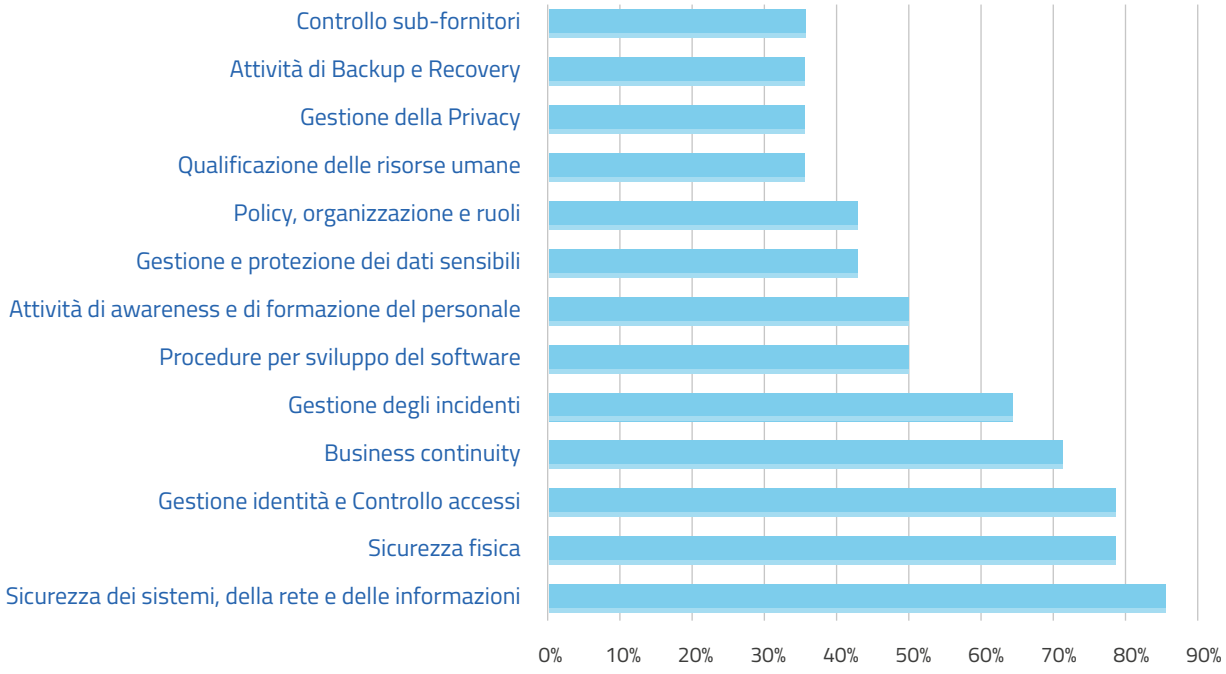

Figura 14 - Principali sezioni presenti nei questionari

Volendo maggiormente dettagliare, è possibile analizzare anche il numero di domande associato a ciascuna sezione/tematica. Sebbene il numero di domande non rappresenti di per sé un indicatore esaustivo della rilevanza attribuita ad uno specifico argomento la cardinalità delle domande presenti è indice quanto meno dell'interesse rispetto a molteplici aspetti connessi con l'argomento.

Sicurezza dei sistemi, della rete e delle informazioni	X	X	X	X		X		X	X	X	X	X	X	X
Sicurezza fisica		X	X	X	X	X	X	X		X	X		X	X
Gestione identità e Controllo accessi		X	X	X		X		X	X	X	X	X	X	X
business continuity		X		X	X	X	X	X	X		X	X		X
Gestione degli incidenti		X		X		X	X	X	X			X	X	X
Procedure per sviluppo del software		X			X	X				X	X		X	X
Attività di awareness e di formazione del personale			X	X	X	X	X	X			X			
Gestione e protezione dei dati sensibili	X			X		X			X	X		X		
Policy, organizzazione e ruoli		X		X	X		X			X				X
Qualificazione delle risorse umane		X			X			X			X			X
Gestione della Privacy		X	X		X		X						X	
Attività di backup e Recovery			X		X	X				X			X	
Controllo sub-fornitori					X		X		X			X		X
Analisi dei Rischi		X				X		X			X			
Asset inventory e management			X			X	X							X
Audit, protocolli e certificazioni			X	X			X					X		
Classificazione, gestione e protezione dei dati				X		X						X	X	
Vulnerability assestment & management					X				X		X	X		
Sicurezza dei dispositivi mobili e IoT		X		X						X				
Gestione del processo di patching						X				X	X			
Utilizzo strumenti di crittografia							X			X				X
Protezione contenuti multimediali	X							X						
Sicurezza del Cloud		X	X											
Gestione smart working e accesso da remoto			X			X								

Figura 15 - Tipologia di sezione per singolo questionario

La maggioranza dei questionari (74% del totale) presenta domande in forma chiusa su due valori (si/no) ovvero su scale a 3 o 5 valori in alcuni casi utilizzando etichette parlanti (ad esempio "non-applicato", … "totalmente applicato"). Si noti che in alcuni casi alle domande in forma chiusa è aggiunta la possibilità di specificare meglio la risposta utilizzando appositi campi. Nel 26% dei questionari sono preferite risposte aperte.

In media un terzo delle domande del questionario (30%) sono dedicate agli aspetti connessi con sicurezza dei sistemi, delle reti e delle informazioni, sebbene esistano alcuni questionari in cui il numero di domande relative a tale argomento è estremamente elevato arrivando in un caso a rappresentare il 62% delle domande presenti (5 questionari hanno più del 40% delle domande che vertono su tale argomento).

Sebbene nel 76% dei questionari vi sia una sezione specificatamente rivolta alla sicurezza fisica, complessivamente il numero di domande su questo tema è limitato al 4% del totale (sebbene in alcuni questionari si superi anche il 10%). Tale apparente contraddizione può trovare una sua giustificazione nella maggiore conoscenza della tematica per cui il committente individua pochi elementi atti a ben qualificare la postura del fornitore.

Per quel che riguarda le domande connesse con gli aspetti di Gestione identità e Controllo accessi esse rappresentano in media il 13% del totale (ma esistono situazioni in cui si arriva anche a superare il 30%), ma quello che appare maggiormente significativo è che in nessun questionario il numero di domande su questo argomento è inferiore al 10% del totale, a riprova della rilevanza riversata su questo tema.

TIPO DI DOMANDE

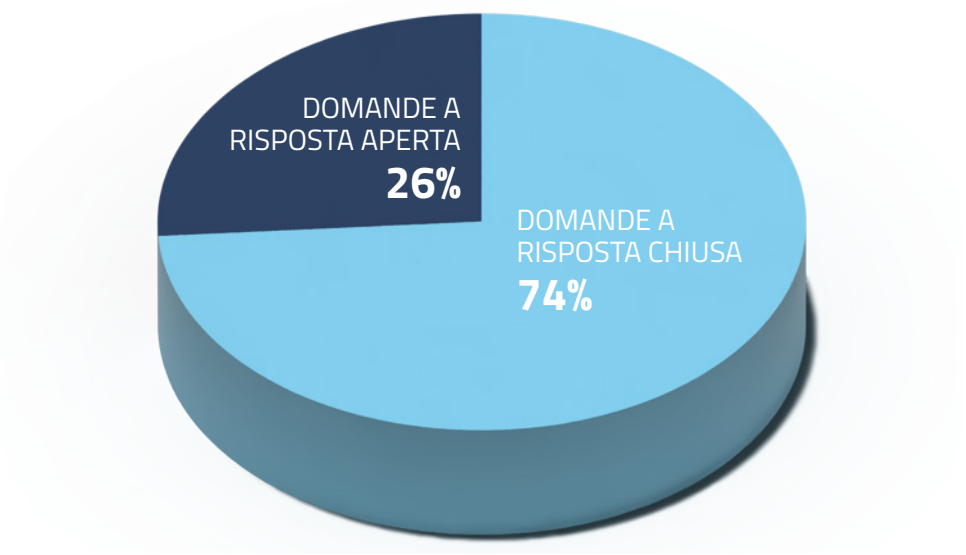

Figura 16 - Ripartizione questionari per tipologia di domanda

Una media del 9% delle domande nei questionari è dedicata agli aspetti legati alla gestione degli incidenti; sebbene esista una forte variabilità passando da situazioni in cui il tema non è presente fra le domande del questionario (2 casi) a situazioni in cui più del 20% delle domande sono dedicate al tema.

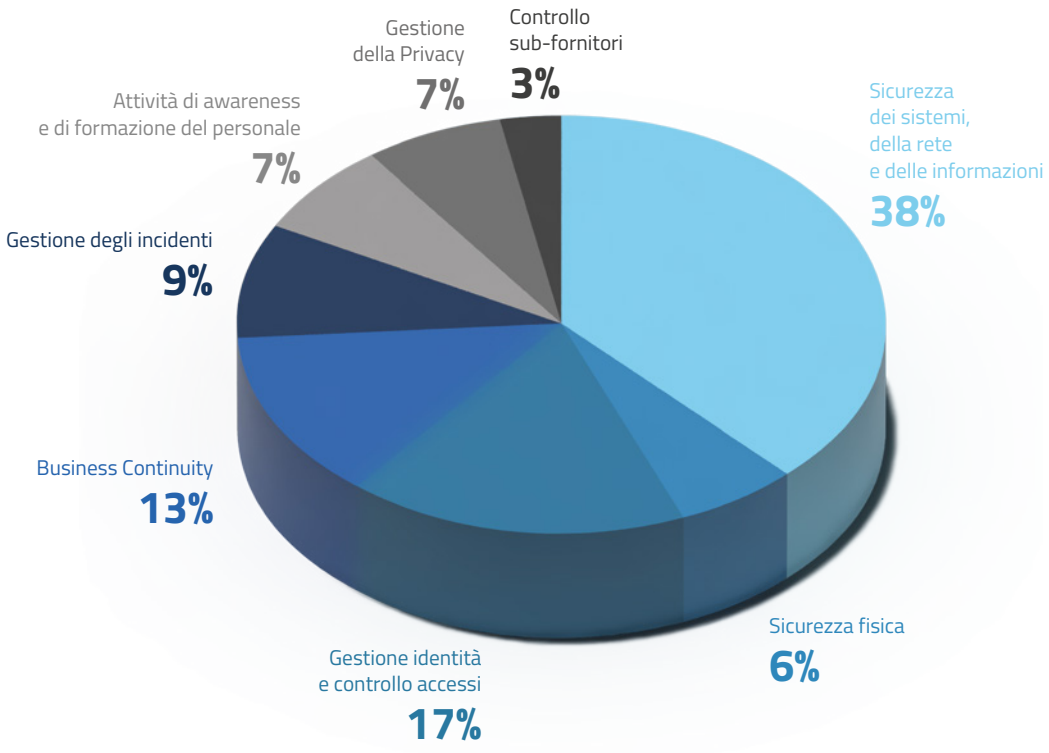

Figura 17 - Ripartizione percentuale domande su principali topic

Un percentuale media leggermente maggiore (11%) riguarda il tema della Business Continuity con una varianza ancor maggiore del caso della gestione degli incidenti alla luce del fatto che 6 questionari non hanno alcuna specifica domanda su questa tematica e 3 questionari presentano più del 15% delle proprie domande relative a tale tema (con un picco del 46% di un soggetto che ha ben 13 domande relative alla continuità operativa).

Decisamente modesta la percentuale di domande legate al tema privacy (circa il 3%). È probabile che tale aspetto sia assorbito all'interno di quelli che sono obblighi normativi e quindi non vi è uno specifico interesse ad acquisire maggiori informazioni tramite l'utilizzo di questionari.

Una ultima osservazione riguarda il fatto che i questionari vanno letti insieme con quelle che sono le ulteriori richieste presenti nei capitolati, per cui l'assenza di specifiche domande su determinati argomenti all'interno del questionario non è necessariamente da ricondurre ad un poco interesse per il topic, ma potrebbe anche essere l'effetto della trattazione dello stesso all'interno di altre sezione del capitolato dove al tema può anche essere assegnato una maggiore rilevanza attribuendovi una valutazione maggiormente pregnante per gli esiti della procedura di gara.

3 PROCESSI DI SVILUPPO

Ai fornitori di prodotti software o di applicazioni vengono presentate alcune richieste specificatamente legate ai processi di sviluppo, quali la gestione dei codici sorgente, l'interoperabilità tra il sistema sviluppato e l'ambiente all'interno del quale sarà installato o specifici tempi di risposta agli incidenti in caso di applicativi che coinvolgano dati personali e/o finanziari.

Le richieste che vengono presentate ai fornitori sono tra loro molto diverse in quanto diversi sono i servizi oggetto dei vari capitolati, gli strumenti attraverso cui essi vengono offerti e le esigenze degli utenti che ne usufruiscono. Nonostante il naturale divario tra i requisiti finali imposti dai diversi casi analizzati, vi sono elementi che si ripresentano con maggiore frequenza rispetto ad altri:

- garanzie di sicurezza per tutto il ciclo di vita del prodotto (61%);
- protocolli specifici per la gestione e condivisione del codice sorgente (39%);
- il controllo periodico dei requisiti di sicurezza del prodotto, da parte del fornitore, del committente o da terzi (33%);
- programmazione e sviluppo che siano in grado di prevedere futuri aggiornamenti per contrastare l'obsolescenza precoce del prodotto (33%);
- comunicabilità tra sistemi con un'adeguata riconciliazione degli strumenti aggiornati o sostituiti (22%);

Normativamente, lo sviluppo dei servizi informatici e la valutazione della loro qualità sono elementi regolati dalla serie di norme ISO 25000 che consentono di esaminare e monitorare eventuali difettosità durante tutte le fasi del ciclo di vita dei prodotti, avendo come conseguenza il miglioramento della qualità tecnica dello stesso tanto quanto la sua comoda usufruibilità da parte dell'utente a cui è destinato. Tuttavia, per i processi di sviluppo la percentuale di enti che fanno esplicita richiesta del possesso delle certificazioni ISO è decisamente bassa, ammontando solamente al 11% del totale.

Nei paragrafi a seguire, un'analisi dei requisiti più richiesti.

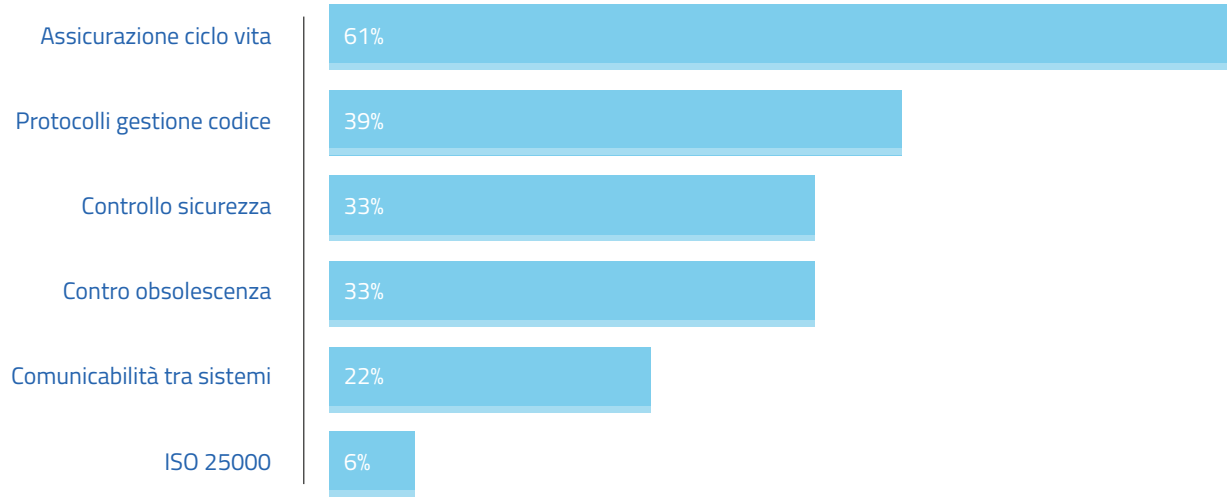

Figura 18 - Ripartizione percentuale domande su principali topic

3.1 GARANZIA DI SICUREZZA PER L'INTERO CICLO DI VITA

Si è da tempo superata l'idea di poter valutare e validare la sicurezza di un software nella fase di rilascio dello stesso e si sono andati sviluppando e consolidando diversi protocolli di Secure Software Development Life Cycle (SSDLC). Questi protocolli prevedono che la sicurezza sia un elemento implementato e testato nello sviluppo del software in ogni sua fase: progettazione, pianificazione dell'architettura, sviluppo, rilascio, utilizzo e aggiornamento. Questa nuova procedura consente di migliorare la sicurezza del software in quanto permette di identificarne eventuali vulnerabilità e difetti per correggerli prima di passare alla fase di sviluppo successiva.

L'interesse in materia di sicurezza del software si è notevolmente accresciuto nell'ultimo triennio al punto che l'Agenzia per l'Itala Digitale nel maggio del 2020, ha pubblicato diverse linee guida per gli sviluppatori di software per la Pubblica Amministrazione.

Anche il settore privato pone particolare attenzione all'argomento, attenzione che si concretizza nel fatto che **il 78% delle aziende analizzate esige che il software fornito sia stato sviluppato nel rispetto di procedure di controllo che ne garantiscano la conformità a standard di sicurezza minimi**.

Nello specifico, i test richiesti sono:

- valutazione del rischio durante la progettazione e la pianificazione dell'architettura del software, col fine di poter identificare possibili vulnerabilità strutturali e funzionali (66%);
- analisi del codice, prevedendo un'analisi statica per valutarne la sicurezza durante la fase di sviluppo dello stesso e un'analisi dinamica, per implementare la sicurezza là dove necessario (38%);
- Penetration Test prima della distribuzione, che garantiscano un uso protetto all'utente, e condivisione delle vulnerabilità riscontrate (22%).

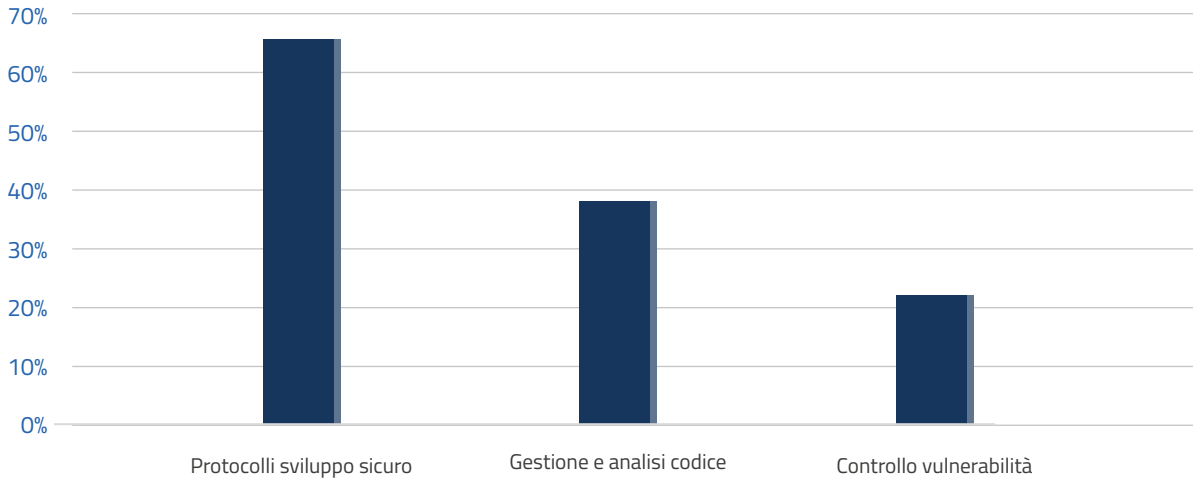

Figura 19 - Ripartizione percentuale domande su principali topic

3.2 OBSOLESCENZA

Se precedentemente si è parlato di protocolli contro l'obsolescenza in riferimento alla gestione degli asset, per i quali era prevista la dismissione e sostituzione di tutti gli strumenti ritenuti desueti e inadatti all'uso, parlare di obsolescenza in relazione ai processi di sviluppo del software significa prevedere un codice che sia compatibilmente aggiornabile con i prevedibili sviluppi tecnologici.

Perché ciò sia possibile è necessario che il codice sia dinamicamente modificabile, che preveda la possibilità di essere aggiornato e, soprattutto, che il prodotto finito sia monitorabile tanto per valutarne l'efficacia quanto per identificare e correggere eventuali vulnerabilità. A richiedere che vi siano protocolli di sviluppo che prevengano l'obsolescenza del prodotto sono il 38% delle compagini coinvolte nella survey.

3.3 INTEROPERABILITÀ TRA SISTEMI

L'interoperabilità tra sistema riguarda in modo specifico due diverse capacità degli strumenti realizzati: la coesistenza e l'interoperabilità.

La capacità di coesistenza è la possibilità di utilizzare il prodotto finale insieme ad altri software indipendenti con i quali potrebbe condividere risorse, ma senza necessità di comunicazione e condivisione dati, mentre la capacità d'interoperabilità è la possibilità di scambiare informazioni con altri sistemi o componenti specifici.

Queste caratteristiche vengono specificatamente richieste dal 22% delle aziende.

4 CONCLUSIONI

Lo studio di quelli che sono i requisiti in materia di cyber security presenti nei capitolati di gara delle più importanti aziende nazionale evidenzia la crescente rilevanza che le stazioni appaltanti pongono su questa tematica. Ciò è legato alla costatazione che eventuali falle di cyber security all'interno del perimetro di un fornitore non solo possono impattare sull'operatività della committenza, ma anche essere sfruttate quale trampolino da cui sferrare un attacco cyber alla rete informatica dell'azienda con significative conseguenze oltre che sul piano operativo, su quello reputazionale e di immagine. Aspetti che si vanno a sommare a tutte le implicazioni legate agli obblighi di legge in presenza di incidenti e di data breach in termini di notifiche e di sanzioni che la committenza tende a prevenire anche con il fattivo coinvolgimento dei propri partner.

Il tema per altro ha trovato una sua collocazione anche nel nuovo Codice Appalti (D.Lgs n. 36 del 31 marzo 2023) che al comma 4 dell'art. 108 recita " Nelle attività di approvvigionamento di beni e servizi informatici, le stazioni appaltanti, incluse le centrali di committenza, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità prezzo per l'aggiudicazione, tengono sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico e peculiare rilievo nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici".

Un aspetto che emerge dall'analisi è la costatazione che l'interesse dei committenti è maggiormente orientato agli aspetti procedurali del fornitore più che sugli aspetti tecnologici. Quello che appare premiante nei capitolati è la capacità da parte del fornitore di gestire in modo adeguato tutti gli aspetti di cyber security grazie **all'adozione di un adeguato modello organizzativo che preveda chiare responsabilità e procedure**.

A questa tematica si affianca poi il tema della **formazione del personale** visto come prerequisito necessario affinché le procedure delineate risultino poi effettivamente implementate. Ciò alla luce della costatazione che la quasi totalità delle compromissioni cyber sono legate a comportamenti inappropriati da parte degli operatori.

In questa ottica il **possesso delle certificazioni** in ambito cyber appare utile ma non necessario, è ritenuto dalla committenza un elemento di valore in quanto evidenzia un'attenzione e l'adozione di un approccio proattivo al tema della cyber security, ma di per sé il possesso di una certificazione non è considerato, nella maggioranza dei casi, né esaustivo né vincolante.

APPENDICE

ISO 27001

Il testo di questa normativa è stato redatto dal Comitato Tecnico ISO/IEC "Information Technology", dall'Organizzazione Internazionale di Normazione (ISO) e dalla Commissione Elettrotecnica Internazionale (IEC), da qui il nome completo di Norma EN ISO/IEC 27001:2022.

Questa norma ha l'obiettivo di guidare le organizzazioni di diverso livello nello sviluppo e nell'attuazione di un sistema di gestione delle informazioni che tenga conto dei processi e della dimensione aziendale e che sia commisurato alle necessità e agli obiettivi dell'azienda stessa andando a definire i requisiti per un programma efficace di Information Security (Information Security Management System – Requirements).

Tale sistema consente di preservare la riservatezza, l'integrità e la disponibilità delle informazioni attraverso processi di prevenzione e gestione del rischio.

La norma è studiata secondo il modello PDCA (Plan-Do-Check-Act), che prevede la pianificazione, l'attuazione, il monitoraggio e l'aggiornamento di ogni protocollo per garantire l'esecuzione di azioni che siano efficaci. Il modello PDCA prevede quattro diverse fasi:

- La fase di pianificazione prevede che si stabiliscano in modo chiaro gli obiettivi e le policy aziendali in modo da realizzare una serie di protocolli, processi e procedure di sicurezza che siano in linea con la natura e il contesto dell'organizzazione stessa.
- La seconda fase è quella attuativa, durante la quale si diffondono i protocolli pianificati a tutti i dipendenti e si mettono in atto in modo uniforme.
- Durante la fase successiva si procede al monitoraggio delle azioni intraprese in modo da revisionare e aggiornare quelle procedure che possono essere migliorate per ottenere risultati più efficaci.
- Infine, una volta stabilita una prassi operativa che soddisfi le aspettative dirigenziali, si consolidano i protocolli di sicurezza adottati mantenendoli costantemente aggiornati e monitorati per una costante rivalutazione del campo di applicazione del sistema di gestione della sicurezza e della politica e degli obiettivi di sicurezza.

Le organizzazioni che intendano ottenere questa certificazione s'impegnano a pianificare azioni atte a riconoscere e gestire rischi specifici integrando e attuando particolari processi all'interno del proprio sistema di gestione e valutando l'effettiva efficacia dei processi applicati.

La normativa si divide in obiettivi specifici per le diverse categorie e all'interno di ogni sezione è possibile individuare informazioni e indicazioni dettagliate. Le categorie sono 17 e ricoprono tutti gli aspetti della gestione della sicurezza, tanto fisica e strutturale quanto informatica e organizzativa dei protocolli. Nel dettaglio, le categorie trattano:

- L'organizzazione interna aziendale, per stabilire un quadro di riferimento gestionale in cui siano chiaramente divisi i ruoli e le responsabilità e in cui vengano regolati i contatti con le autorità e i gruppi specialistici;
- La gestione dei dispositivi portatili e del telelavoro:
- La sicurezza legata alle risorse umane per tutta la durata del contratto, con riferimenti alla formazione del personale, alla gestione dei processi disciplinari e alle procedure da applicare in caso di cessazione del contratto;
- La gestione degli asset, per i quali vengono specificate le procedure di creazione e aggiornamento dell'inventario, di gestione degli spostamenti e della restituzione degli strumenti;
- La classificazione delle informazioni, con procedure di etichettatura e trattamento degli asset;

- Il trattamento dei supporti removibili, in modo da prevenire divulgazione, modifica o perdita di dati archiviati su supporti esterni;
- Il controllo degli accessi, siano essi fisici alla struttura che accessi alla rete. Questo punto dedica particolare attenzione a tutte le procedure di registrazione, provisioning e rimozione o adattamento dei diritti di accesso alle informazioni;
- Il sistema di gestione delle password e del controllo crittografico;
- La sicurezza fisica degli ambienti;
- La manutenzione delle apparecchiature, con disposizioni sulla manutenzione e sulla loro disposizione in ambienti che ne garantiscano la salvaguardia in caso di eventi naturali o disservizi sulle reti energetiche;
- Le procedure operative e di responsabilità. In questa sezione si danno indicazioni sulle pratiche da adottare in caso di cambiamento operativo. È richiesto di tenere traccia di ogni cambiamento (aggiornamenti o modifiche procedurali), ma anche di fare proiezioni sui futuri requisiti di capacità tecniche del sistema. In questa sezione è inserito anche tutto l'aspetto legato alla protezione da malware e al controllo dei software di produzione, la gestione dei Backup, la raccolta e il monitoraggio dei log e la gestione degli Audit;
- La gestione della sicurezza delle comunicazioni, relative alla sicurezza delle reti e al trasferimento delle informazioni;
- L'acquisizione, lo sviluppo e la manutenzione dei sistemi;
- Le relazioni con i fornitori;
- La gestione degli incidenti relativi alla sicurezza delle informazioni;
- Gli aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa.

L'intera organizzazione si fonda sulla realizzazione di strutture di leadership che siano in grado di pianificare, attuare e valutare l'iter gestionale in ogni suo aspetto e che siano pronte ad attuare modifiche che consentano un continuo aggiornamento e miglioramento dei protocolli di sicurezza.

La famiglia della serie ISO 27000 comprende diverse norme che vanno ad analizzare aspetti specifici, ad esempio la ISO 27005, "Information technology — Security techniques — Information security risk management" particolarizza quanto previsto dalla ISO 31000 in tema di Risk Management al settore Information Security (si veda paragrafo successivo).

Il tema del Information Security Incident Management è coperto dalla ISO 27035.

Aspetti più tecnici sono coperti dalla ISO27032 per ciò che attiene alle tematiche relative all'Information Security, dalla ISO 27033 che si occupa della Network Security e dalla ISO 27034 focalizzata sul tema della Application Security (ISO 27034).

ISO 31000

La normativa UNI ISO 31000:2018 fornisce le linee guida per una corretta gestione dei rischi che le diverse organizzazioni potrebbero trovarsi ad affrontare. Le procedure in essa presenti non sono specificatamente settoriali, al contrario, sono applicabili in tutti i contesti aziendali che intendano sviluppare delle prassi di gestione del rischio che siano efficienti, efficaci e sistematiche.

Con "rischio" s' identifica l'effetto diverso da quanto atteso causato da un'azione, effetto che, se non adeguatamente compreso e gestito, può creare nuove minacce a cascata. La norma contiene una serie di principi base che dovrebbero permettere all'organizzazione che li adotta di gestire gli effetti dell'incertezza.

Coinvolgendo la leadership di tutta l'organizzazione, la struttura di riferimento per la gestione dei rischi si fonda

su una serie di elementi tra cui:

- la progettazione di una prassi condivisa, che tenga conto del contesto interno ed esterno dell'organizzazione e che identifichi autorità e risorse di riferimento;
- l'integrazione e la collaborazione di ogni parte della struttura dell'organizzazione;
- l'attuazione, attraverso la comunicazione e lo sviluppo dei piani stabiliti;
- la valutazione periodica dell'efficacia delle prassi adottate e dei rischi a cui l'organizzazione è soggetta;
- l'aggiornamento e il miglioramento delle pratiche obsolete o inadatte;

La valutazione del rischio dovrebbe essere effettuata sistemicamente e vedere coinvolte in modo collaborativo tutte le parti interessate. Non vanno sottostimati i fattori di rischio legati alla natura degli strumenti utilizzati e alla loro possibile degradazione nel tempo, così come i cambiamenti nel contesto esterno a quello aziendale e i rischi emergenti non ancora esaustivamente noti.

Il monitoraggio e il riesame continuo permettono di identificare, analizzare e ponderare i rischi e di optare per il trattamento della minaccia più efficace tanto dal punto di vista preventivo che da quello correttivo. Di fatto, parte dell'analisi del rischio consiste nel valutare la complessità e la connettività della vulnerabilità riscontrata, valutazione necessaria per cercare di ponderarne le possibili conseguenze e sviluppare una risposta alla stessa, che può concretizzarsi in una rosa di possibilità che spazia dal monitoraggio alla correzione tempestiva della vulnerabilità.

ISO 28000

La norma ISO 28000 è integrabile alla ISO 27001 in quanto anch'essa relativa agli standard minimi per una corretta gestione della sicurezza, ma è più dettagliatamente dedicata alla sicurezza lungo l'intera catena di fornitura.

Come la ISO 27001, anche questa norma è pensata secondo il modello PDCA (Plan-Do-Check-Act), che prevede la pianificazione, l'attuazione, il monitoraggio e l'aggiornamento di ogni protocollo affinché sia sempre assicurato l'approccio più moderno ed efficace possibile.

Tale norma è nata in risposta alla necessità del settore logistica e trasporti di avere uno standard di riferimento per la security di tutto il processo di fornitura: packaging, immagazzinaggio e trasferimento delle merci. In aggiunta agli aspetti pratici della fornitura, la norma dedica attenzione anche agli aspetti finanziari e di gestione delle informazioni legati alla stessa.

La norma viene spesso adottata come strumento per l'identificazione e la valutazione dei rischi e delle minacce legate alla supply chain da tutte quelle organizzazioni che, sebbene non legate al settore trasporti, si trovano a dover controllare una serie di forniture per cui sono potenzialmente esposte ai rischi connessi ai traffici di merci e alle leggi in continua evoluzione a questo connesse.

L'adozione della certificazione ISO 28000 mira a fornire una serie di vantaggi specifici per ciò che attiene la riduzione dei tempi di consegna e la semplificazione dei controlli effettuati dalle autorità doganali, ma anche la riduzione di perdite dovute a frodi, contraffazioni e furti durante il flusso logistico e un conseguente risparmio economico dovuto alla riduzione degli incidenti.

ISO 25000

La serie di norme dipendenti dalla ISO/IEC 25000 è anche denominata SQuaRE "Systems and Software Quality Requirements and Evaluation", è stata sviluppata dall'ISO/IEC JTC1 SC7 Working Group WG6 "Software product and system quality".

Questa serie di norme assicura che vengano rispettati degli standard di qualità nello sviluppo di sistemi IT, favorendo una facile gestione dei sistemi e garantendo la comunicabilità tra i diversi software e applicativi. Di fatto, queste norme sono state redatte con l'obiettivo di contribuire alla sicurezza, alla funzionalità e alla manutentibilità dei prodotti software di nuova generazione e per farlo suggeriscono circa 180 misure di monitoraggio che riguardano aspetti quali:

- requisiti di qualità;
- modelli di qualità su software, dati e servizi IT;
- valutazione della qualità realizzate da valutatori indipendenti, acquirenti e sviluppatori.

Proponendo modelli di qualità a priori, che superano la sola gestione e correzione delle difettosità del prodotto finito, la norma assicura una maggiore accuratezza nello sviluppo del software e il soddisfacimento degli obblighi normativi quali quelli legati al GDPR.

ISO 25010

La norma ISO 25010, parte della serie di norme 25000, è espressamente dedicata allo sviluppo di software applicativi di cui analizza e determina le caratteristiche qualitative in base alle quali viene valutato il prodotto finale.

Il modello di qualità proposto dalla norma si basa su otto caratteristiche principali:

- idoneità funzionale;
- usabilità, ossia la possibilità da parte dell'utente di comprendere e utilizzare consapevolmente il software. Il tutto si realizza valutando l'accessibilità, l'interfaccia grafica e la capacità di segnalazione degli errori che caratterizzano il software stesso;
- affidabilità. Si valuta analizzando la capacità del sistema di soddisfare le necessità di affidabilità in condizioni normali, ma anche la capacità del sistema di garantire alcune operazioni anche in caso di errori hardware o software e la capacità di recuperare dati eventualemente compromessi dagli stessi errori;
- sicurezza, rappresentata dalla capacità di proteggere informazioni e dati in modo che persone o sistemi non autorizzati non possano leggerli o modificarli;
- compatibilità con altri sistemi. In questo campo si valutano sia la capacità di coesistenza con altri software indipendenti con cui condividere eventuali strumenti, sia la capacità d'interoperabilità e quindi la capacità d'intercambiare e processare informazioni con altri software;
- portabilità, o meglio, capacità del prodotto di essere trasferito e utilizzato in un altro contesto hardware, software o operazionale;
- performance, come ad esempio tipo di connessione e banda;
- manutenibilità. In questo campo, oltre al concetto di riusabilità, si valuta la possibilità di poter aggiornare e modificare in modo effettivo ed efficace il software per rispondere a necessità evolutive, correttive o perfettive.

Un software che rispetti le caratteristiche descritte dalla norma ISO 25010 è in grado di soddisfare completamente le necessità dell'utente finale e della compagnia che lo utilizza in quanto, oltre ad avere un'interfaccia intuitiva, può essere riutilizzato in diversi ambienti e contesti offrendo sempre un servizio di buona qualità.

NIST

In parallelo agli standard internazionali il National Institute of Standard and Technology (NIST) ha sviluppato un framework per la gestione degli aspetti di cyber security che si compone di 5 dimensioni:

- **Identify (Identificare):** Questa fase coinvolge l'identificazione dei sistemi, delle risorse e dei dati critici per l'organizzazione, nonché l'individuazione delle minacce, dei rischi e delle vulnerabilità ad essi associati.
- **Protect (Proteggere):** In questa fase, vengono implementate misure di protezione per mitigare i rischi identificati. Ciò può includere l'implementazione di controlli di sicurezza tecnici, politiche, procedure e formazione del personale per proteggere i sistemi e i dati sensibili.
- **Detect (Rilevare):** L'obiettivo di questa fase è rilevare tempestivamente le attività sospette o anomale che potrebbero indicare una violazione della sicurezza. Ciò implica l'implementazione di sistemi di monitoraggio, rilevamento delle intrusioni e analisi dei log per individuare eventuali violazioni o anomalie.
- **Respond (Rispondere):** In caso di violazione o incidente di sicurezza, questa fase si concentra sulla risposta tempestiva ed efficace per mitigare gli effetti negativi. Questo può includere l'attuazione di piani di risposta agli incidenti, la collaborazione con le autorità competenti e l'implementazione di misure correttive per ripristinare la sicurezza.
- **Recover (Recuperare):** Dopo un incidente di sicurezza, questa fase si concentra sulla ripresa delle attività normali e sul ripristino dei sistemi e dei dati compromessi. Ciò può includere il ripristino dei backup, l'analisi delle cause dell'incidente e l'implementazione di misure per prevenire future violazioni.

In Italia il NIST Framework è stato interamente adottato e sviluppato dall'Università La Sapienza (CIS – Cyber Intelligence and Information Security) in collaborazione con il Cyber Security National Lab del CINI creando il "Framework Nazionale per la Cyber Security e la Data Protection".

Il framework NIST è completato da una serie di pubblicazioni tecniche raccolte sotto la famiglia SP 800 che forniscono raccomandazioni, best practice e standard per la sicurezza informatica, la gestione dei rischi e la protezione delle informazioni. La serie NIST SP 800 copre una vasta gamma di argomenti legati alla sicurezza informatica, tra cui la gestione dei rischi, i controlli di sicurezza, la crittografia, la protezione delle infrastrutture critiche, la gestione delle identità digitali e molto altro. Queste pubblicazioni sono ampiamente utilizzate sia nel settore pubblico che privato, soprattutto negli Stati Uniti, e sono spesso adottate come base per la conformità normativa e l'implementazione delle misure di sicurezza. Fra le altre possiamo citare:

- NIST SP 800-30: "Risk Management Guide for Information Technology Systems" - Fornisce una metodologia dettagliata per la gestione del rischio nel contesto dei sistemi informatici, guidando le organizzazioni nella valutazione, mitigazione e gestione dei rischi di sicurezza informatica.
- NIST SP 800-53: "Security and Privacy Controls for Information Systems and Organizations" - Fornisce un set completo di controlli di sicurezza e privacy che possono essere implementati per proteggere i sistemi informativi e le organizzazioni dalle minacce interne ed esterne.
- NIST SP 800-61: "Computer Security Incident Handling Guide" - Offre linee guida per gestire gli incidenti di sicurezza informatica, compresi gli aspetti di prevenzione, rilevamento, risposta e recupero.
- NIST SP 800-63: "Digital Identity Guidelines" - Stabilisce le linee guida per l'implementazione di sistemi di identità digitale sicuri, inclusi requisiti per l'autenticazione, la gestione delle password e l'uso di tecnologie di autenticazione multifattore.

Nonostante la rilevanza delle NIST a livello internazionale esse appaiono solo nel 13% dei capitolati analizzati.

www.un-industria.it