Complex Systems & Security Laboratory
www.coseritylab.it

Analisi dei requisiti presenti nei capitolati di gara in tema di cybersecurity

Prof. Roberto Setola
r.setola@unicampus.ir

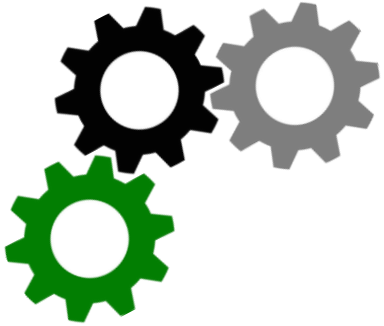
Università Campus Bio-Medico di Roma
Via Alvaro del Portillo, 21
00128 Roma
Italy

Obiettivi

Scopo:

- Aiutare le PMI ad assumere una migliore postura in Cyber Security.

Tutelare il tessuto produttivo nazionale



Garantire il corretto funzionamento delle infrastrutture di cui sono fornitrici

Tramite l'analisi di cosa è presente nei capitolati di gare evidenziare che le «spese» in campo cyber rappresentano **investimenti abilitanti**

In totale 32 aziende hanno collaborato al progetto fornendo la documentazione necessaria per condurre l'analisi

Partecipanti al gruppo di lavoro:

Luigi Ballarano (Terna)
Massimo Cottafavi (Snam)
Antonella Fascioli (Unindustria)
Fabiola Furlai (Poste Italiane)
Aniello Gentile (ENEL)
Alessandro Lamesa (Elettronica Spa)
Matteo Lucchetti (Cyber 4,0)
Rocco Mammoliti (Poste Italiane)
Mario Mangano (AdR)
Pierluigi Martusciello (BNL Paribas)
Francesco Morelli (Ferrovie dello stato)
Stefania Sica (Cy4Gate)
Massimo Tedeschi (Leonardo)
Antonio Truglio (Unindustria)

SOMMARIO

REQUISITI TECNICO-INFORMATICI

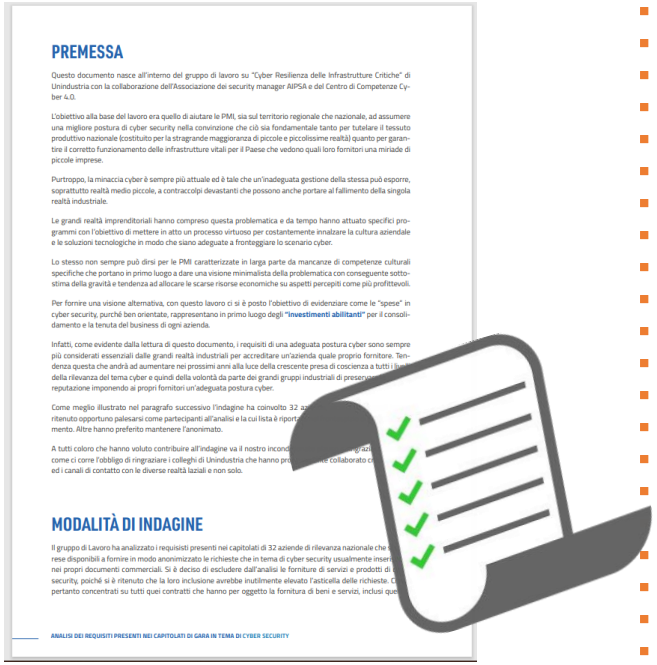
- POLITICA PER LA SICUREZZA DELLE INFORMAZIONI
- QUESTIONARI
- PROCESSI DI SVILUPPO

Modalità d'indagine

32 Analisi dei capitolati tecnici aziendali (Pubblici e privati)

20 Studio dei questionari valutativi proposti dalle aziende

Documento riassuntivo



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, purchè 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 preserv... reputazione imponendo ai propri fornitori un'adeguata postura cyber.

Come meglio illustrato nel paragrafo successivo l'indagine ha coinvolto 32 az... ritenuto opportuno palesarsi come partecipanti all'analisi e la cui lista è riport... mento. Altre hanno preferito mantenere l'anonimato.

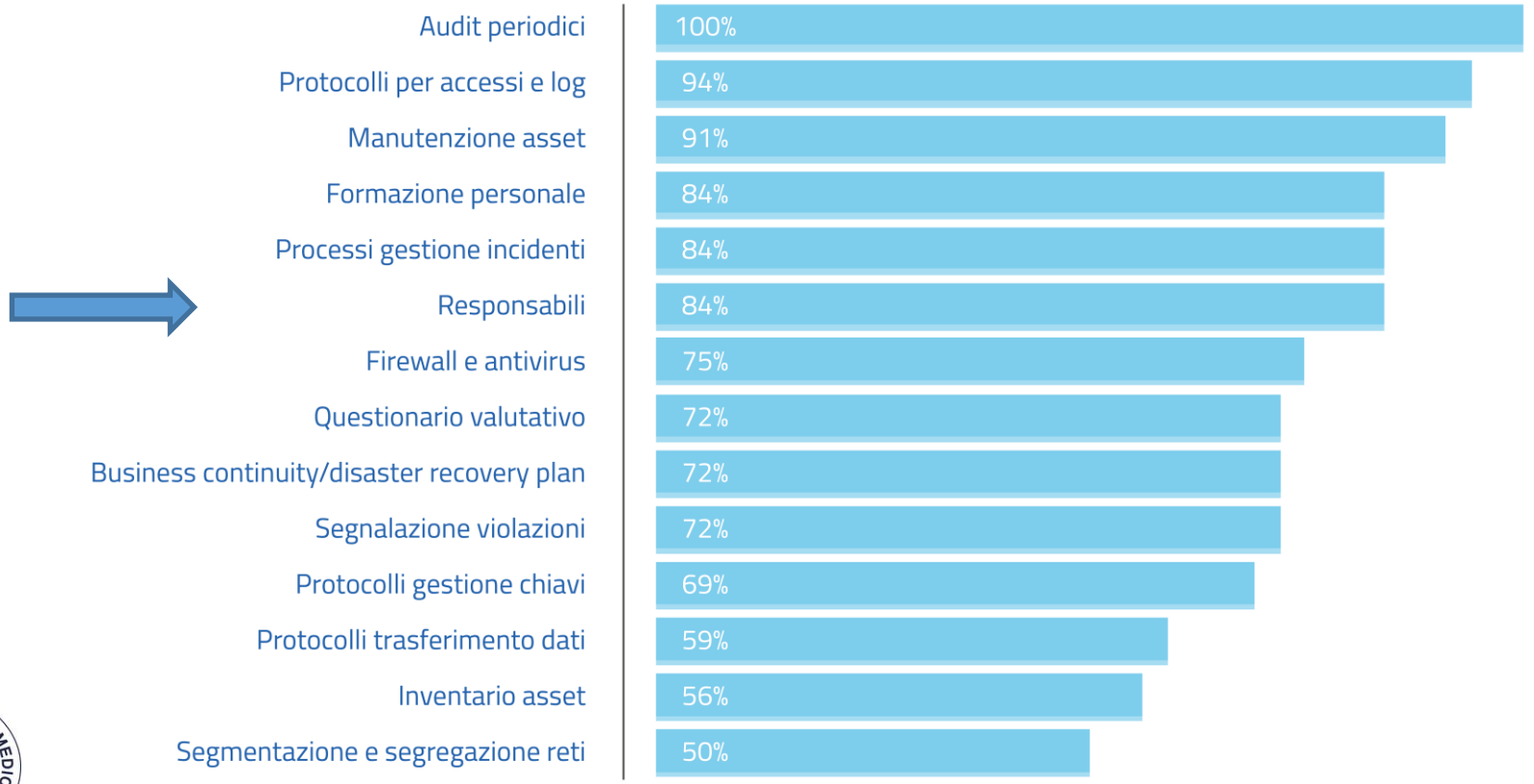
A tutti coloro che hanno voluto contribuire all'indagine va il nostro incond... come ci corre l'obbligo di ringraziare i colleghi di Unindustria che hanno pr... ed i canali di contatto con le diverse realtà laziali e non solo.

MODALITÀ DI INDAGINE

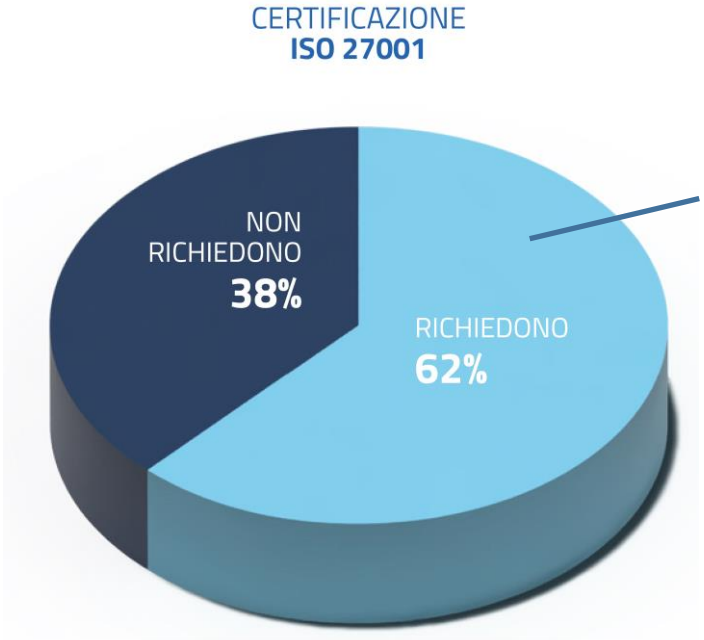
Il gruppo di Lavoro ha analizzato i requisiti presenti nei capitolati di 32 aziende di rilevanza nazionale che ... rese disponibili a fornire in modo anonimizzato le richieste che in tema di cyber security usualmente inser... nei propri documenti commerciali. Si è deciso di escludere dall'analisi le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

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

Quali requisiti sono presenti nei capitolati?



ISO 27001



ma soltanto il **30%** la ritiene necessaria per la stipula di eventuali contratti.

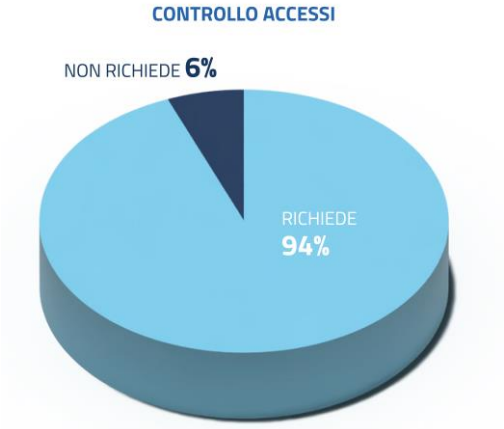
Il 70% delle società ritiene che il possesso della certificazione possa essere disatteso se vengono rispettati requisiti specifici richiesti in modo indipendente dalla normativa.

Alcune considerazione sulle certificazioni

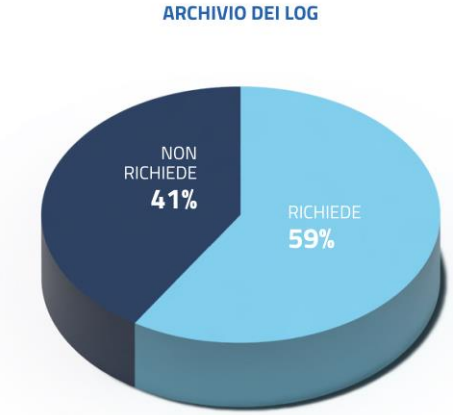
- La mancata obbligatorietà di tale certificazione non va intesa come una mancata attenzione alle politiche di gestione della sicurezza dei dati.
- **Le aziende che hanno sviluppato una più capillare politica di cyber security sono fra quelle che non richiedono in modo esplicito la certificazione ISO 27001 ai propri fornitori**
- 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
- 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

Controllo accessi

Una ben strutturata politica di controllo degli accessi (fisici o informatici) è richiesta dal 94% delle aziende interrogate, ma solamente il 59% richiede che vi sia un archivio dei log

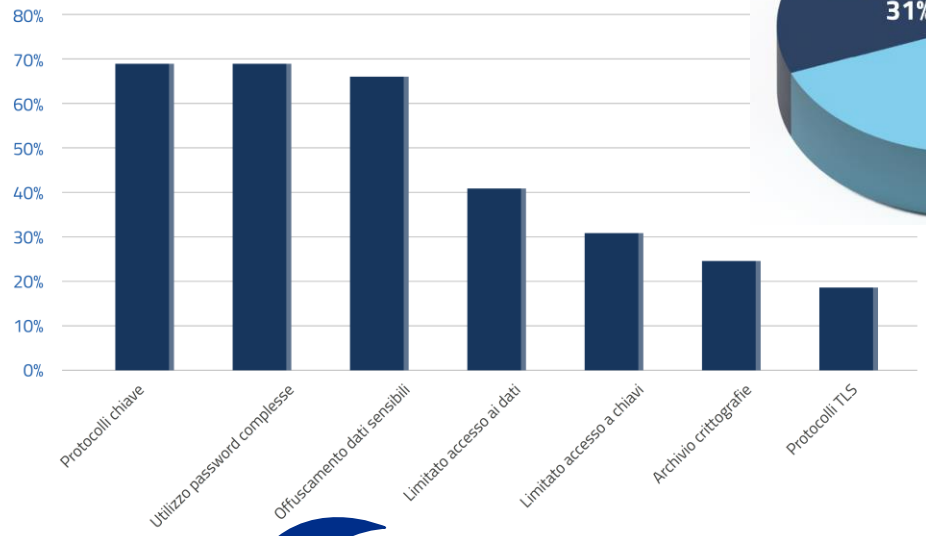


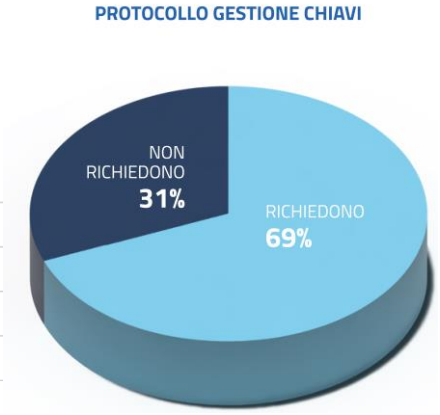
Strumento necessario in caso di manomissione dei dati o malfunzionamento per risalire alle azioni che li hanno causati



Crittografia e gestione chiavi

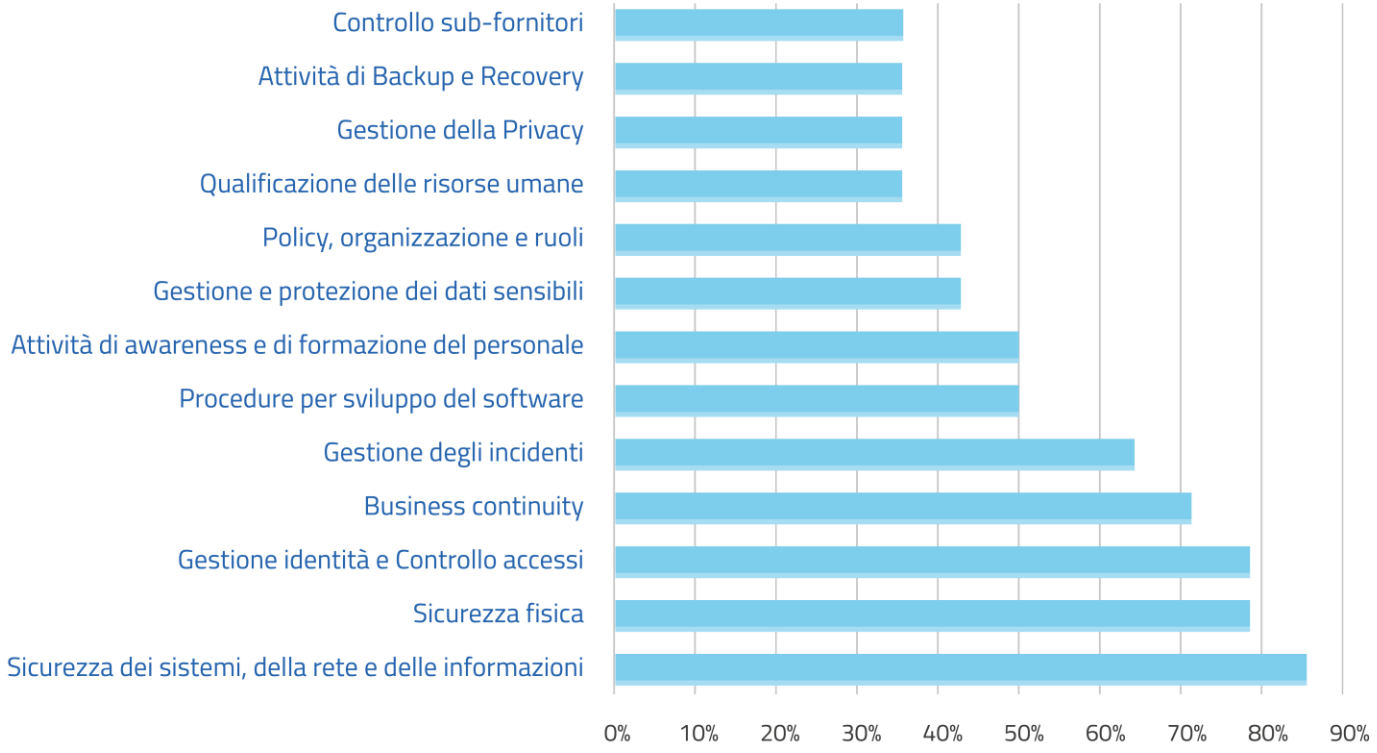
Con il termine “chiavi” s’identificano tanto le effettive chiavi di decriptazione quanto le password di accesso ai diversi ambienti fisici e virtuali del sistema



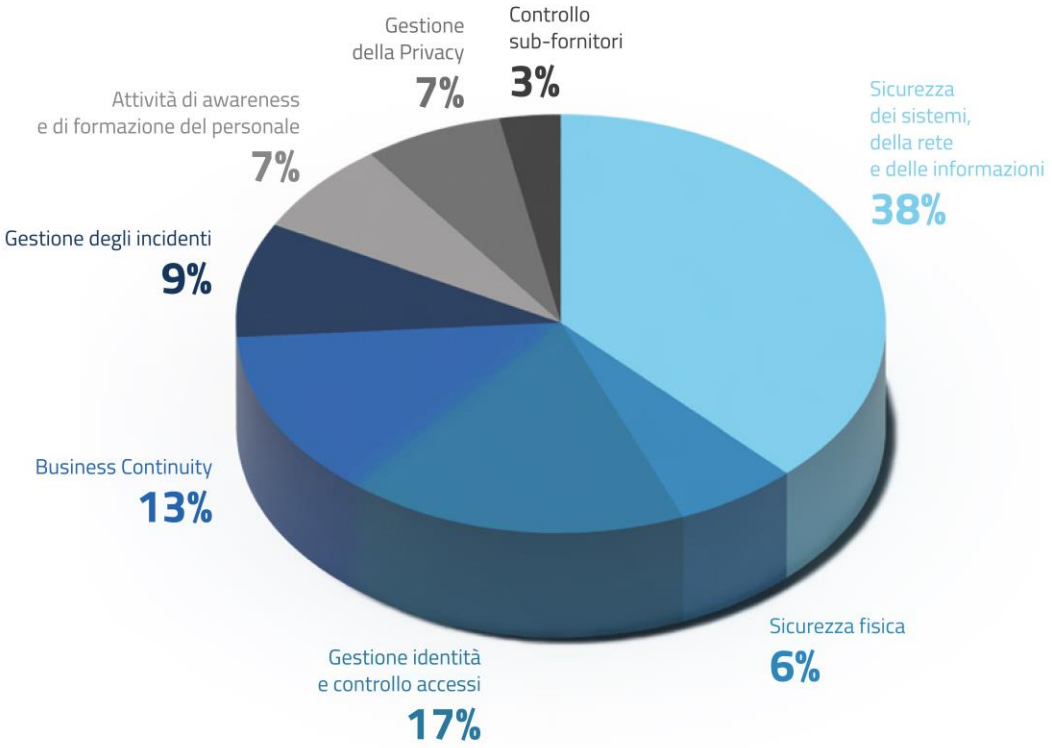


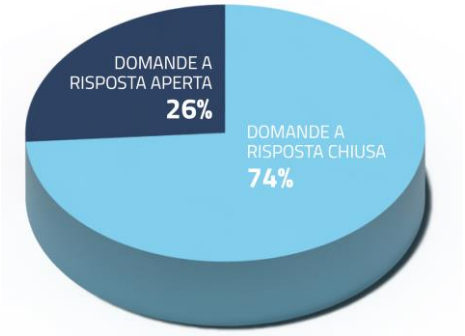
Solamente il 50% delle aziende richiede espressamente che i dati siano etichettati e abbiano crittografie diverse in base al livello di sensibilità del dato

Questionari di autovalutazione (sezioni)

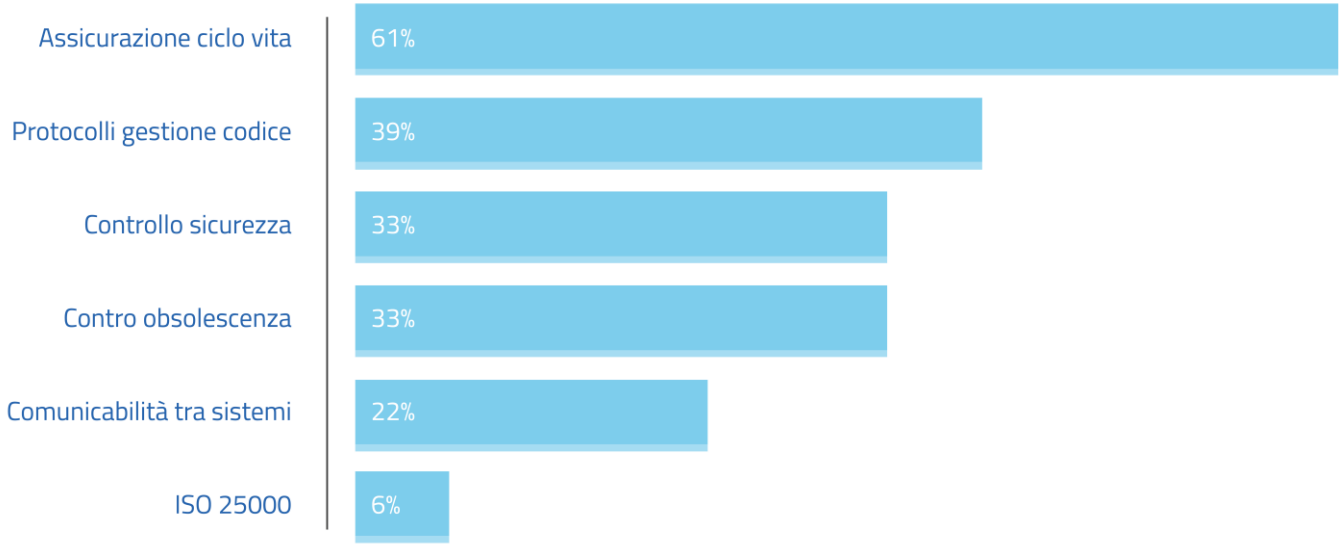


Questionari autovalutazione (domande)





Processi di sviluppo



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.

Conclusioni

- 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.
- Il **possesso delle certificazioni** appare utile ma non necessario, è ritenuto 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 deicasi, né esaustivo né vincolante.


Thank
you