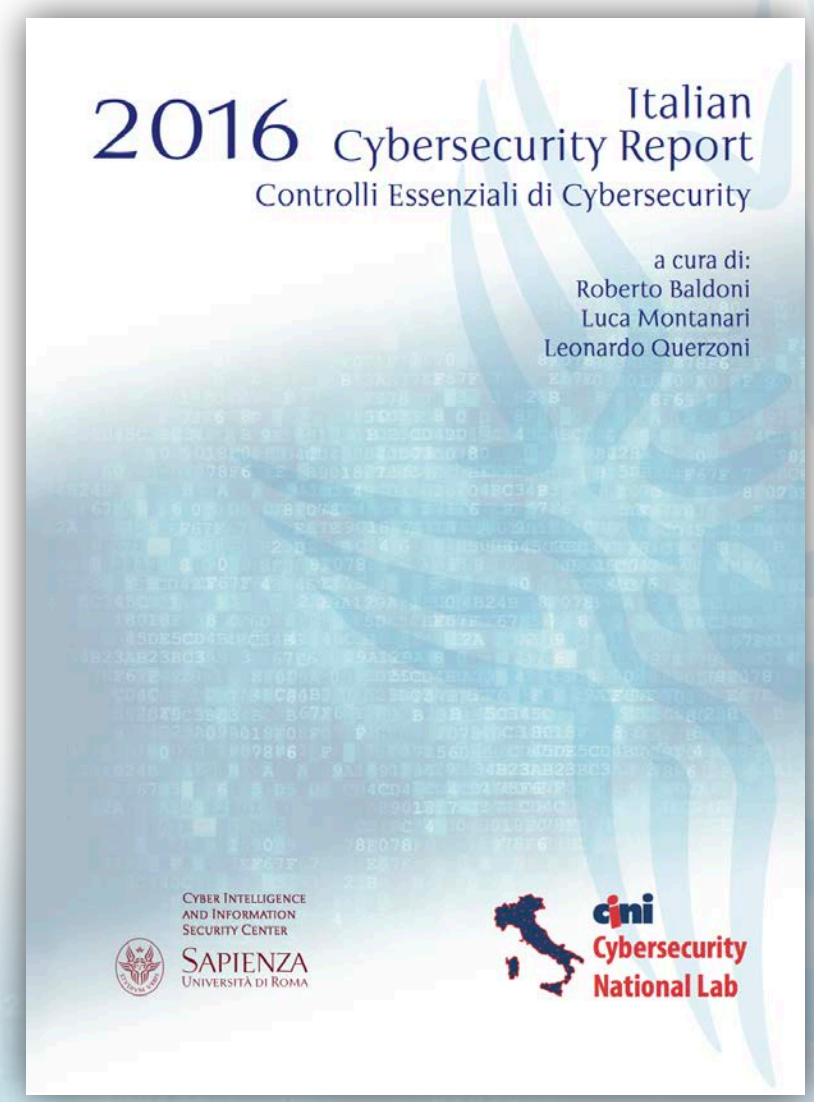


CONTROLLI ESSENZIALI DI CYBERSECURITY

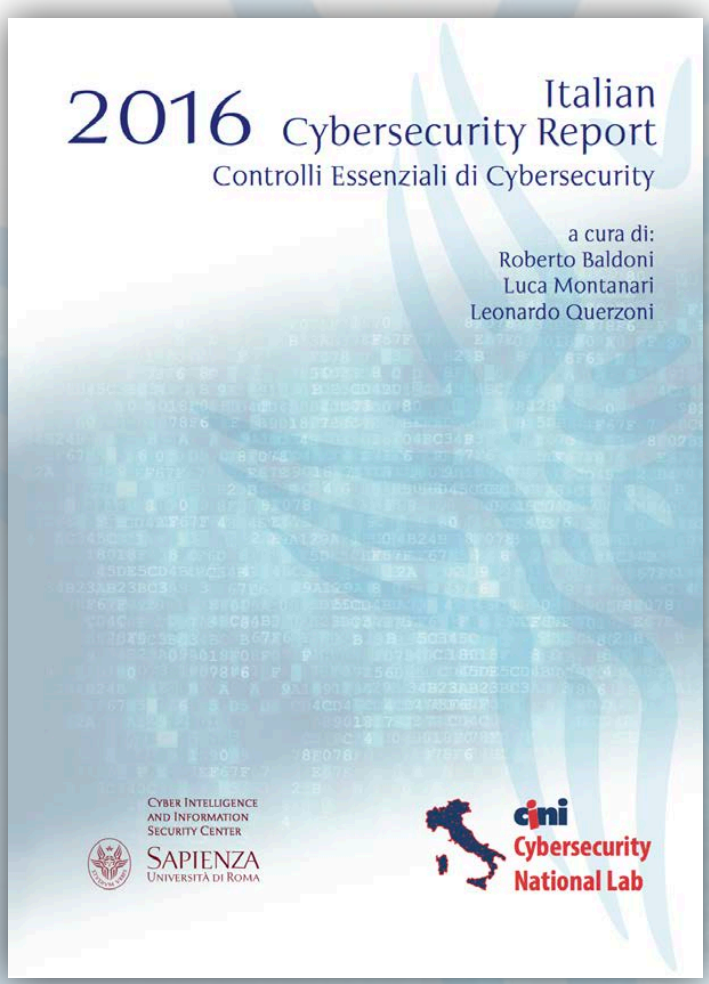
CIS Sapienza
Cyber Intelligence and information Security

cini
Cybersecurity National Lab

Definizione di Controllo Essenziale

“una pratica relativa alla cybersecurity che, qualora ignorata oppure implementata in modo non appropriato, causa un aumento considerevole del rischio informatico”

Controlli Essenziali sono parte dello stesso processo del Framework Nazionale



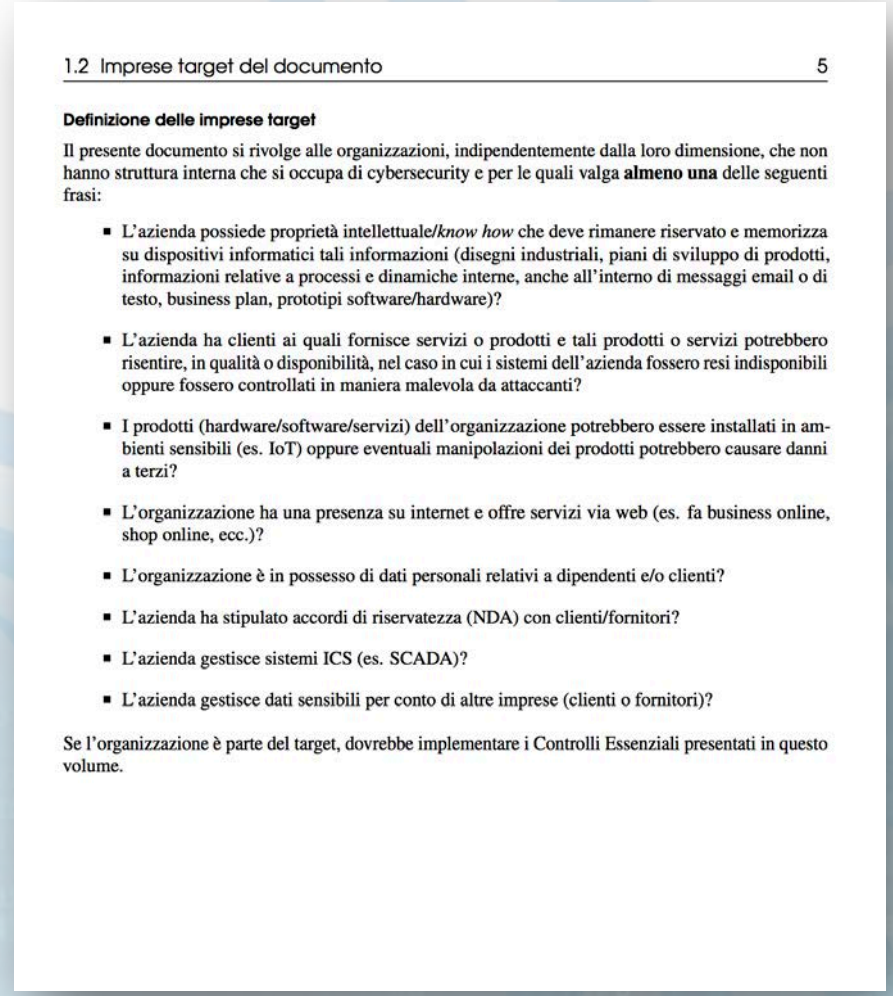
Strumento che permette di "iniziare" a parlare la lingua del Framework Nazionale dedicato a uno specifico target d'imprese

CIS Sapienza
Cyber Intelligence and Information Security

cini
Cybersecurity National Lab

Imprese target

Le imprese che non hanno sufficienti risorse per adottare il Framework Nazionale



1.2 Imprese target del documento 5

Definizione delle imprese target

Il presente documento si rivolge alle organizzazioni, indipendentemente dalla loro dimensione, che non hanno struttura interna che si occupa di cybersecurity e per le quali valga **almeno una** delle seguenti frasi:

- L'azienda possiede proprietà intellettuale/*know how* che deve rimanere riservato e memorizza su dispositivi informatici tali informazioni (disegni industriali, piani di sviluppo di prodotti, informazioni relative a processi e dinamiche interne, anche all'interno di messaggi email o di testo, business plan, prototipi software/hardware)?
- L'azienda ha clienti ai quali fornisce servizi o prodotti e tali prodotti o servizi potrebbero risentire, in qualità o disponibilità, nel caso in cui i sistemi dell'azienda fossero resi indisponibili oppure fossero controllati in maniera malevola da attaccanti?
- I prodotti (hardware/software/servizi) dell'organizzazione potrebbero essere installati in ambienti sensibili (es. IoT) oppure eventuali manipolazioni dei prodotti potrebbero causare danni a terzi?
- L'organizzazione ha una presenza su internet e offre servizi via web (es. fa business online, shop online, ecc.)?
- L'organizzazione è in possesso di dati personali relativi a dipendenti e/o clienti?
- L'azienda ha stipulato accordi di riservatezza (NDA) con clienti/fornitori?
- L'azienda gestisce sistemi ICS (es. SCADA)?
- L'azienda gestisce dati sensibili per conto di altre imprese (clienti o fornitori)?

Se l'organizzazione è parte del target, dovrebbe implementare i Controlli Essenziali presentati in questo volume.

Razionale:

- Indipendenza dalla dimensione
- Possibilità di danni verso terzi in servizi/prodotti
- Esposizione su internet
- Dati sensibili, personali, know how nei dispositivi

Imprese target

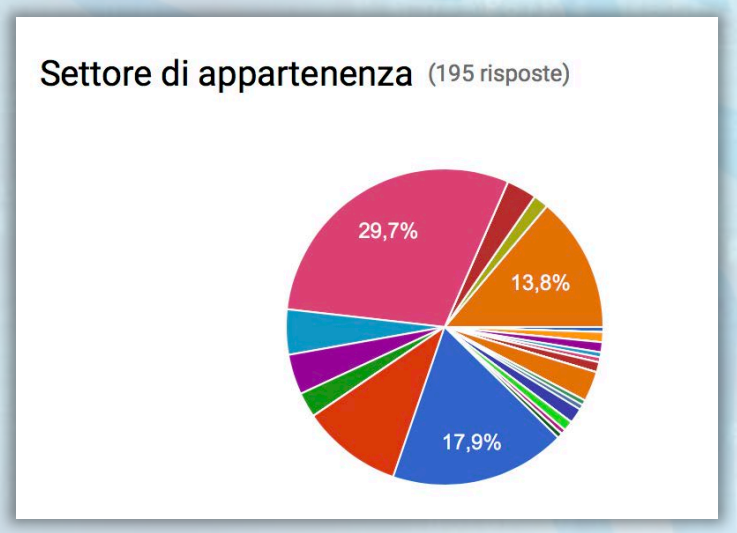
Se l'organizzazione è parte del target dovrebbe implementare tutti i Controlli Essenziali di Cybersecurity

Definizione di Controllo Essenziale

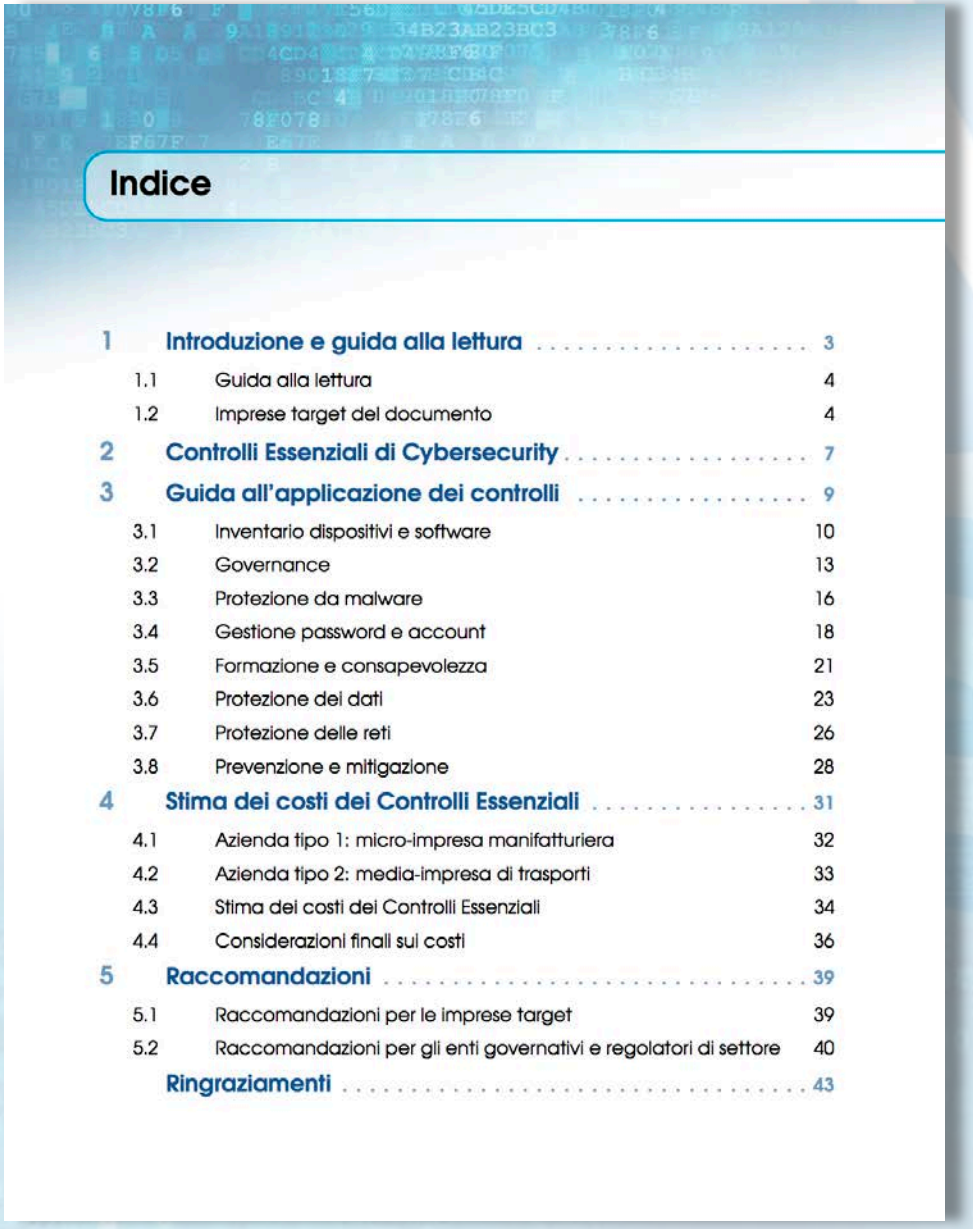
Pratica di cybersecurity che, se ignorata, causa un aumento inaccettabile del rischio

Processo di definizione di controlli

- Definizione del set iniziale dei controlli definito dagli autori accademia, industria pubblica amministrazione)
- Consultazione pubblica (circa 200 commenti tra esperti e imprese)



Il Cybersecurity Report 2016



Indice

1 Introduzione e guida alla lettura 3
1.1 Guida alla lettura 4
1.2 Imprese target del documento 4
2 Controlli Essenziali di Cybersecurity 7
3 Guida all'applicazione dei controlli 9
3.1 Inventario dispositivi e software 10
3.2 Governance 13
3.3 Protezione da malware 16
3.4 Gestione password e account 18
3.5 Formazione e consapevolezza 21
3.6 Protezione dei dati 23
3.7 Protezione delle reti 26
3.8 Prevenzione e mitigazione 28
4 Stima dei costi dei Controlli Essenziali 31
4.1 Azienda tipo 1: micro-impresa manifatturiera 32
4.2 Azienda tipo 2: media-impresa di trasporti 33
4.3 Stima dei costi dei Controlli Essenziali 34
4.4 Considerazioni finali sui costi 36
5 Raccomandazioni 39
5.1 Raccomandazioni per le imprese target 39
5.2 Raccomandazioni per gli enti governativi e regolatori di settore 40
Ringraziamenti 43

CIS Sapienza
Cyber Intelligence and Information Security

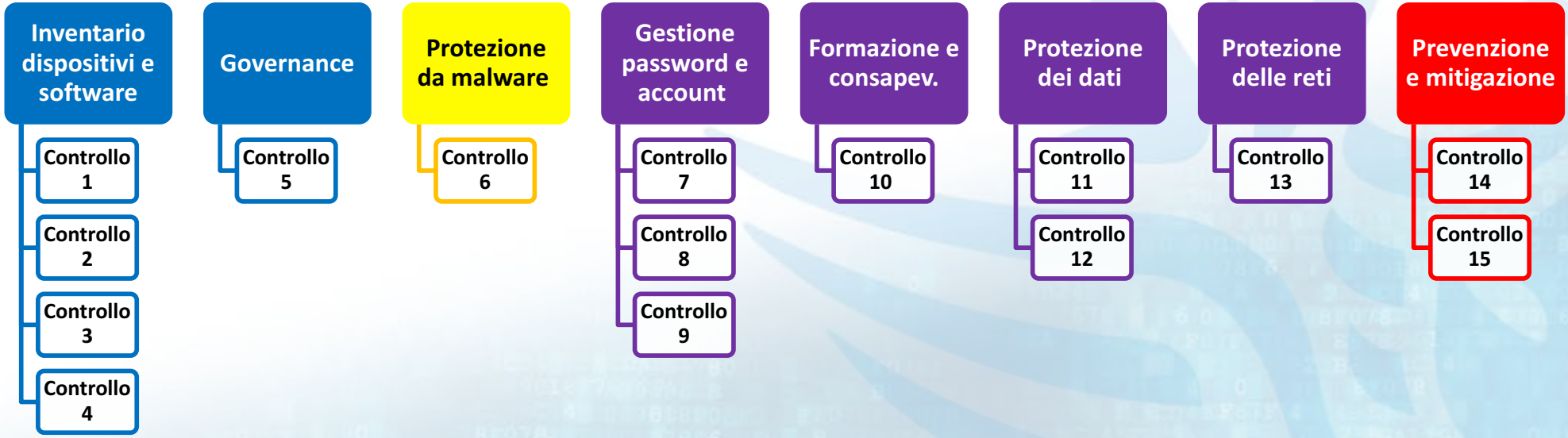
cini Cybersecurity National Lab

I 15 Controlli Essenziali di Cybersecurity

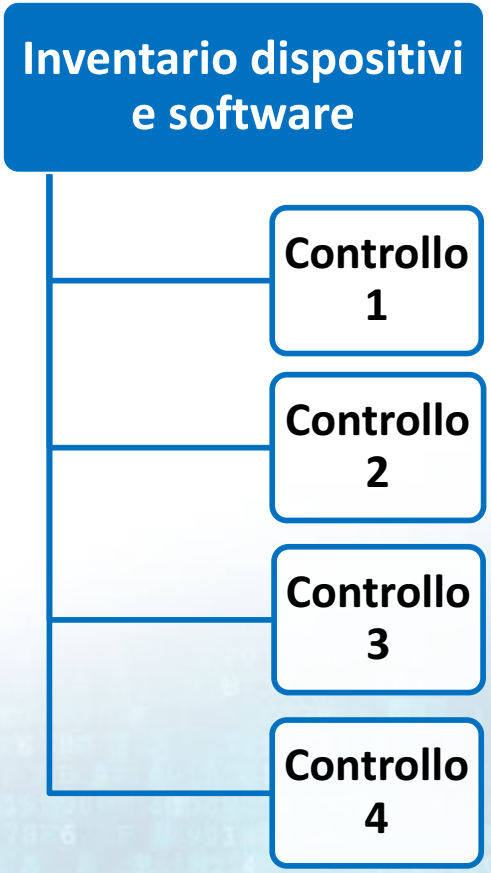
Tabella 2.1: I Controlli Essenziali di Cybersecurity

1	Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.
2	I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc...) offerti da terze parti a cui si è registrati sono quelli strettamente necessari.
3	Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.
4	È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.
5	Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda.
6	Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.
7	Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).
8	Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati.
9	Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.
10	Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, ...). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza.
11	La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.
12	Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono conservati in modo sicuro e verificati periodicamente.
13	Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione).
14	In caso di incidente (es. venga rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.
15	Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.

I 15 Controlli Essenziali di Cybersecurity



I 15 Controlli Essenziali di Cybersecurity



Creare inventari di **sistemi, dispositivi, software, servizi**

Minimizzare l'esposizione sui social/servizi da terzi

Creare inventari di **informazioni, dati e sistemi critici**

Nominare un **referente per la cybersecurity**

I 15 Controlli Essenziali di Cybersecurity

Governance

Controllo 5

Identificare e **rispettare le leggi** e i regolamenti relativi alla cybersecurity

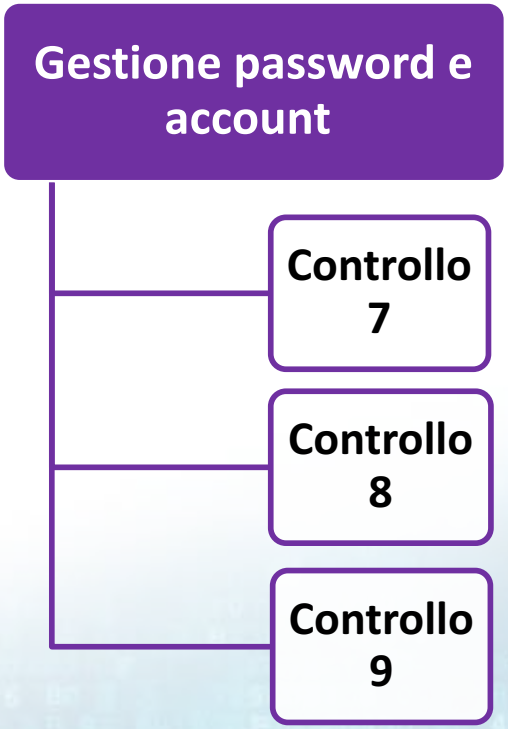
I 15 Controlli Essenziali di Cybersecurity

Protezione da Malware

Controllo 6

Utilizzare e mantenere aggiornato **software antimalware** su tutti i dispositivi che lo consentono

I 15 Controlli Essenziali di Cybersecurity



Utilizzare **password lunghe e diverse per ogni account, dismissione vecchi account, autenticazione forte**

Effettuare l'accesso ai sistemi usando **utenze personali**, non condivise con altri

Applicare il **principio del privilegio minimo** di accesso alle risorse

I 15 Controlli Essenziali di Cybersecurity

Formazione e consapevolezza

Controllo 10

Eseguire adeguata **formazione** per tutto il personale, coordinata dai vertici aziendali

I 15 Controlli Essenziali di Cybersecurity

Protezione dei dati

- **Controllo 11** — Effettuare la **configurazione iniziale** dei dispositivi tramite di esperti
- **Controllo 12** — Definire procedure di **backup** dei dati critici

Protezione delle reti

- **Controllo 13** — Utilizzare dispositivi di **protezione delle reti**

I 15 Controlli Essenziali di Cybersecurity

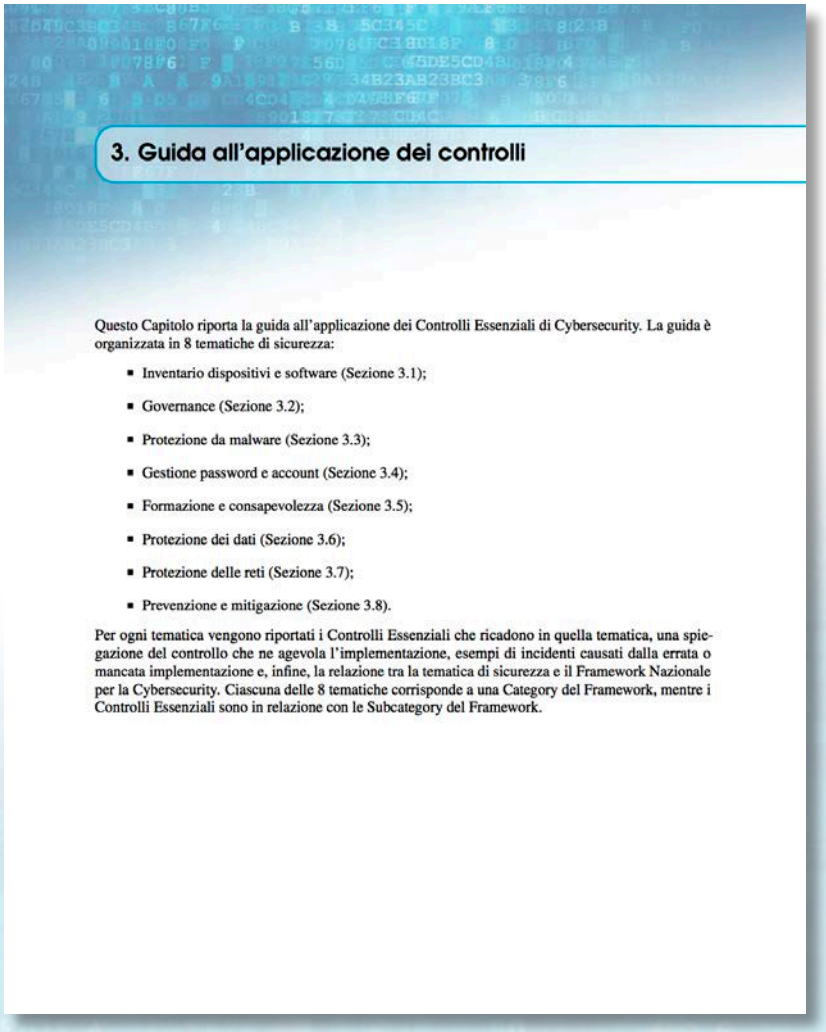
Prevenzione e mitigazione

- **Controllo 14**
- **Controllo 15**

In caso di incedente **informare i responsabili**. Il ripristino viene curato da **personale esperto**

Eseguire gli **aggiornamenti software/firmware** e dismettere hardware e software **non più supportato**

Guida all'applicazione



3. Guida all'applicazione dei controlli

Questo Capitolo riporta la guida all'applicazione dei Controlli Essenziali di Cybersecurity. La guida è organizzata in 8 tematiche di sicurezza:

- Inventario dispositivi e software (Sezione 3.1);
- Governance (Sezione 3.2);
- Protezione da malware (Sezione 3.3);
- Gestione password e account (Sezione 3.4);
- Formazione e consapevolezza (Sezione 3.5);
- Protezione dei dati (Sezione 3.6);
- Protezione delle reti (Sezione 3.7);
- Prevenzione e mitigazione (Sezione 3.8).

Per ogni tematica vengono riportati i Controlli Essenziali che ricadono in quella tematica, una spiegazione del controllo che ne agevola l'implementazione, esempi di incidenti causati dalla errata o mancata implementazione e, infine, la relazione tra la tematica di sicurezza e il Framework Nazionale per la Cybersecurity. Ciascuna delle 8 tematiche corrisponde a una Category del Framework, mentre i Controlli Essenziali sono in relazione con le Subcategory del Framework.

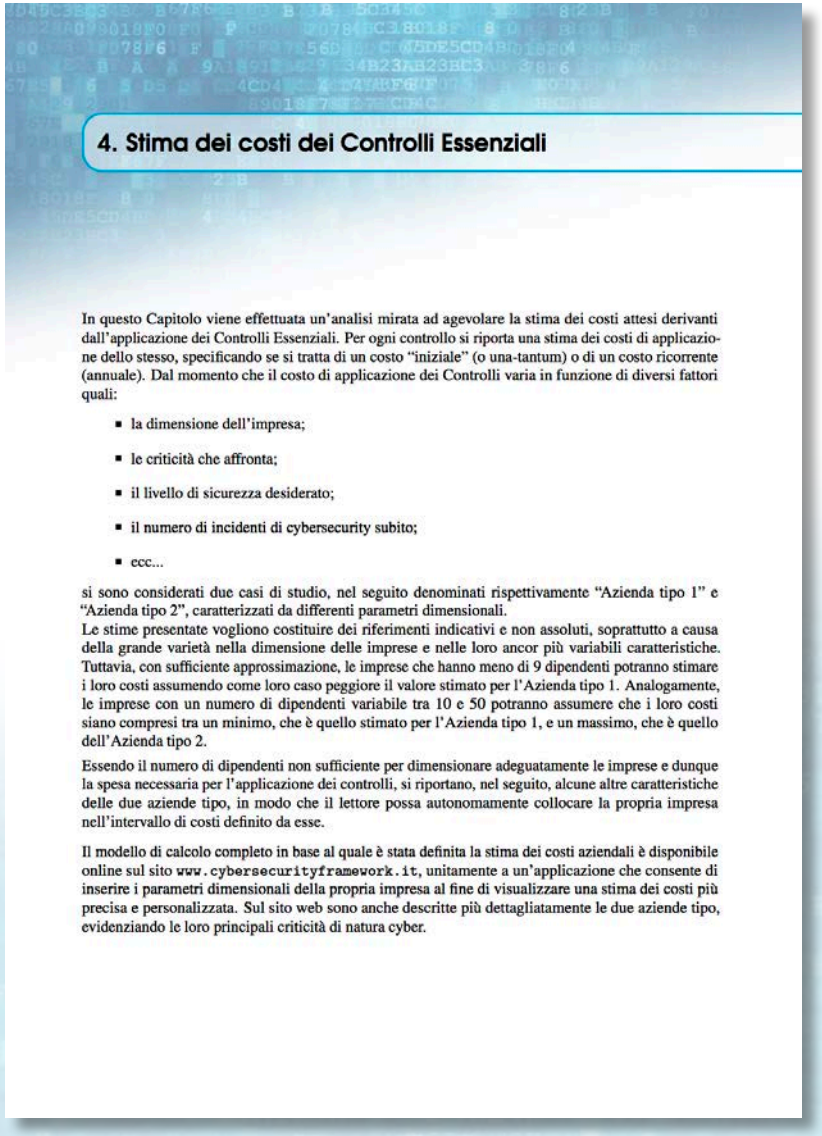
Organizzata per **tematiche di sicurezza, per ognuna:**

- **Descrizione dei Controlli Essenziali**
- **Esempi di incidenti** dovuti alla carente/errata applicazione
- Relazione tra **Controlli Essenziali e Framework Nazionale**

Relazione con il Framework Nazionale

FUNCTION	CATEGORY	SUBCATEGORY	CONTROLLO
PROTECT (PR)	Access Control (PR.AC): L'accesso agli asset ed alle relative risorse è limitato al personale, ai processi, ai dispositivi, alle attività ed alle transazioni effettivamente autorizzate	PR.AC-1:Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate	**7 – Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).**
		PR.AC-3: L'accesso remoto alle risorse è amministrato	**8 – Il personale autorizzato all'accesso, sia esso remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati**
		PR.AC-4: Gli accessi alle risorse sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	**9 – Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.**

Stima dei costi



4. Stima dei costi dei Controlli Essenziali

In questo Capitolo viene effettuata un'analisi mirata ad agevolare la stima dei costi attesi derivanti dall'applicazione dei Controlli Essenziali. Per ogni controllo si riporta una stima dei costi di applicazione dello stesso, specificando se si tratta di un costo "iniziale" (o una-tantum) o di un costo ricorrente (annuale). Dal momento che il costo di applicazione dei Controlli varia in funzione di diversi fattori quali:

- la dimensione dell'impresa;
- le criticità che affronta;
- il livello di sicurezza desiderato;
- il numero di incidenti di cybersecurity subito;
- ecc...

si sono considerati due casi di studio, nel seguito denominati rispettivamente "Azienda tipo 1" e "Azienda tipo 2", caratterizzati da differenti parametri dimensionali.
Le stime presentate vogliono costituire dei riferimenti indicativi e non assoluti, soprattutto a causa della grande varietà nella dimensione delle imprese e nelle loro ancor più variabili caratteristiche. Tuttavia, con sufficiente approssimazione, le imprese che hanno meno di 9 dipendenti potranno stimare i loro costi assumendo come loro caso peggiore il valore stimato per l'Azienda tipo 1. Analogamente, le imprese con un numero di dipendenti variabile tra 10 e 50 potranno assumere che i loro costi siano compresi tra un minimo, che è quello stimato per l'Azienda tipo 1, e un massimo, che è quello dell'Azienda tipo 2.

Essendo il numero di dipendenti non sufficiente per dimensionare adeguatamente le imprese e dunque la spesa necessaria per l'applicazione dei controlli, si riportano, nel seguito, alcune altre caratteristiche delle due aziende tipo, in modo che il lettore possa autonomamente collocare la propria impresa nell'intervallo di costi definito da esse.

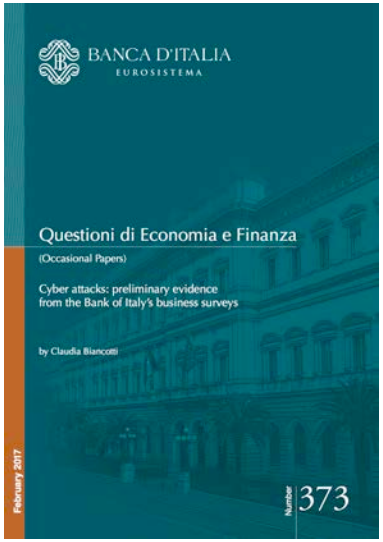
Il modello di calcolo completo in base al quale è stata definita la stima dei costi aziendali è disponibile online sul sito `www.cybersecurityframework.it`, unitamente a un'applicazione che consente di inserire i parametri dimensionali della propria impresa al fine di visualizzare una stima dei costi più precisa e personalizzata. Sul sito web sono anche descritte più dettagliatamente le due aziende tipo, evidenziando le loro principali criticità di natura cyber.

Cerchiamo di **fornire una stima dei costi** di applicazione dei controlli:

- Basata su un modello (sarà disponibile a breve sul sito)
- Prendendo come riferimento **2 aziende tipo italiane:**
  - Micro da 9 dipendenti
  - Piccola da 50 dipendenti

La cybersecurity è ancora un costo certo a fronte di danno incerto?

Stima dei costi

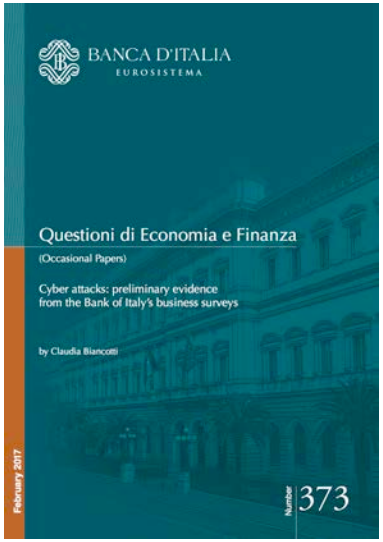


Tra settembre 2015 e settembre 2016 il **45.2%** delle imprese **italiane** ha subito almeno un attacco che ha provocato danni

CIS Sapienza
Cyber Intelligence and Information Security

cini
Cybersecurity National Lab

Stima dei costi



Tra settembre 2015 e settembre 2016 il **45.2%** delle imprese **italiane** ha subito almeno un attacco che ha provocato danni

Danno medio per le **PMI** nel mondo **35.000€** per anno

CIS Sapienza
Cyber Intelligence and Information Security

cini Cybersecurity National Lab

Stima dei costi

CONTROLLO	STIMA DI COSTO PER AZIENDA TIPO 1	STIMA DI COSTO PER AZIENDA TIPO 2	COSTO MEDIO AZIENDA TIPO 1	COSTO MEDIO AZIENDA TIPO 2
1 – Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale. 2 – I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc...) offerti da terze parti a cui si è registrati sono quelli strettamente necessari. 3 – Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.	700 €	1.500 €	Basso	Basso
4 - È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.	300 €	300 €	Basso	Basso
5 – Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di Cybersecurity che risultino applicabili per l'azienda.	1.000 €	5.000 €	Medio	Alto
6 – Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato.	650 €	1.000 €	Basso	Basso
7 – Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori).	500 €	600 €	Basso	Basso
8 – Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati	0 €	0 €	Basso	Basso
9 – Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.	0 €	0 €	Basso	Basso
10 – Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, ...). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire le nozioni basilari di sicurezza	2.500 €	7.500 €	ALTO	ALTO

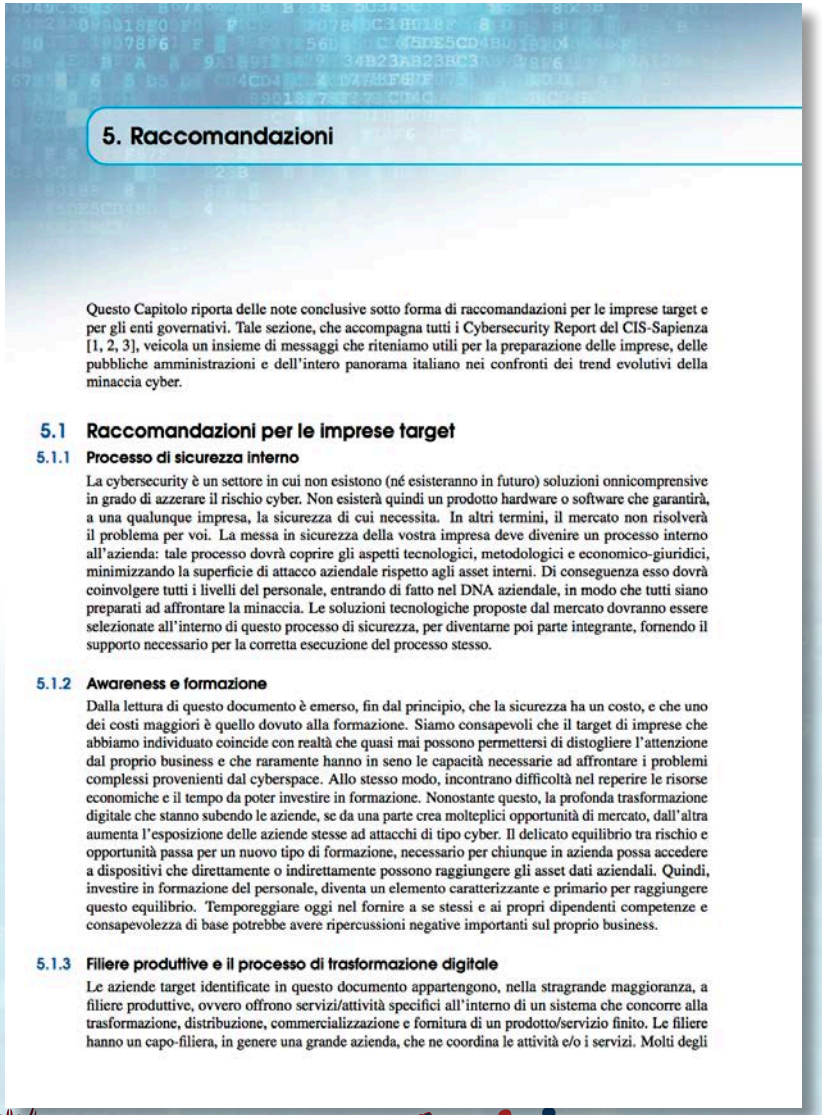
CONTROLLO	STIMA DI COSTO PER AZIENDA TIPO 1	STIMA DI COSTO PER AZIENDA TIPO 2	COSTO MEDIO AZIENDA TIPO 1	COSTO MEDIO AZIENDA TIPO 2
11 – La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.	250 €	250 €	Basso	Basso
12 – Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono verificati periodicamente e sono conservati in modo sicuro	600 €	2.100 €	Basso	Basso
13 – Le reti ed i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione)	2.150 €	4.100 €	Alto	Medio
14 – In caso di incidente (es. sia rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.	1.850 €	2.100 €	Medio	Basso
15 – Tutti i software in uso (inclusi firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.	0 €	0 €	Basso	Basso
Stima costi annui:	7.800 €	19.800 €		
Stima costi iniziali:	2.700 €	4.650 €		

In 5 anni
costo cybersecurity dal 41%
al 76% inferiore al danno
medio

CIS Sapienza
Cyber Intelligence and Information Security

cini
Cybersecurity National Lab

Raccomandazioni



5. Raccomandazioni

Questo Capitolo riporta delle note conclusive sotto forma di raccomandazioni per le imprese target e per gli enti governativi. Tale sezione, che accompagna tutti i Cybersecurity Report del CIS-Sapienza [1, 2, 3], veicola un insieme di messaggi che riteniamo utili per la preparazione delle imprese, delle pubbliche amministrazioni e dell'intero panorama italiano nei confronti dei trend evolutivi della minaccia cyber.

5.1 Raccomandazioni per le imprese target

5.1.1 Processo di sicurezza interno

La cybersecurity è un settore in cui non esistono (né esisteranno in futuro) soluzioni onnicomprensive in grado di azzerare il rischio cyber. Non esisterà quindi un prodotto hardware o software che garantirà, a una qualunque impresa, la sicurezza di cui necessita. In altri termini, il mercato non risolverà il problema per voi. La messa in sicurezza della vostra impresa deve divenire un processo interno all'azienda: tale processo dovrà coprire gli aspetti tecnologici, metodologici e economico-giuridici, minimizzando la superficie di attacco aziendale rispetto agli asset interni. Di conseguenza esso dovrà coinvolgere tutti i livelli del personale, entrando di fatto nel DNA aziendale, in modo che tutti siano preparati ad affrontare la minaccia. Le soluzioni tecnologiche proposte dal mercato dovranno essere selezionate all'interno di questo processo di sicurezza, per diventarne poi parte integrante, fornendo il supporto necessario per la corretta esecuzione del processo stesso.

5.1.2 Awareness e formazione

Dalla lettura di questo documento è emerso, fin dal principio, che la sicurezza ha un costo, e che uno dei costi maggiori è quello dovuto alla formazione. Siamo consapevoli che il target di imprese che abbiamo individuato coincide con realtà che quasi mai possono permettersi di distogliere l'attenzione dal proprio business e che raramente hanno in seno le capacità necessarie ad affrontare i problemi complessi provenienti dal cyberspace. Allo stesso modo, incontrano difficoltà nel reperire le risorse economiche e il tempo da poter investire in formazione. Nonostante questo, la profonda trasformazione digitale che stanno subendo le aziende, se da una parte crea molteplici opportunità di mercato, dall'altra aumenta l'esposizione delle aziende stesse ad attacchi di tipo cyber. Il delicato equilibrio tra rischio e opportunità passa per un nuovo tipo di formazione, necessario per chiunque in azienda possa accedere a dispositivi che direttamente o indirettamente possono raggiungere gli asset dati aziendali. Quindi, investire in formazione del personale, diventa un elemento caratterizzante e primario per raggiungere questo equilibrio. Temporeggiare oggi nel fornire a se stessi e ai propri dipendenti competenze e consapevolezza di base potrebbe avere ripercussioni negative importanti sul proprio business.

5.1.3 Filiere produttive e il processo di trasformazione digitale

Le aziende target identificate in questo documento appartengono, nella stragrande maggioranza, a filiere produttive, ovvero offrono servizi/attività specifici all'interno di un sistema che concorre alla trasformazione, distribuzione, commercializzazione e fornitura di un prodotto/servizio finito. Le filiere hanno un capo-filiera, in genere una grande azienda, che ne coordina le attività e/o i servizi. Molti degli

- Come ogni anno concludiamo il report con alcune **raccomandazioni**
- 5 per le imprese target
- 3 per gli enti governativi

CIS Sapienza
Cyber Intelligence and Information Security

cini Cybersecurity National Lab

Raccomandazioni per imprese target

- Processo di sicurezza interno
- **Awareness e formazione**
- Filiere produttive e il processo di trasformazione digitale
- Controllo, monitoraggio e valutazione delle vulnerabilità
- **Il rischio cyber all'attenzione dei vertici aziendali**

Raccomandazioni per enti governativi e regolatori di settore

- Evoluzione verso il Framework Nazionale per la Cybersecurity
- Aspetti economici della cybersecurity: sgravi fiscali e incentivi per i virtuosi
- **Una certificazione leggera e dinamica per fornitori di servizi**

Conclusioni

- I controlli sono un mezzo per avvicinare le imprese target al **Framework Nazionale**

Conclusioni

- I controlli sono un mezzo per avvicinare le imprese target al **Framework Nazionale**

- Il processo può essere supportato dalle **associazioni di categoria**

Conclusioni

- I controlli sono un mezzo per avvicinare le imprese target al **Framework Nazionale**
- Il processo può essere supportato dalle **associazioni di categoria**
- L'obiettivo per le imprese target è **non far più parte del target**

GRAZIE

- Stefano Armenia
- Roberto Baldoni
- Claudia Biancotti
- Camillo Carlini
- Fabrizio d'Amore
- Luisa Franchina
- Michele Kidane Mariam
- Luca Montanari
- Leonardo Querzoni
- Lorenzo Russo
- Federico Ruzzi
- Marco Spada
- Emanuele Spagnoli
- Annalisa Vitale

CIS Sapienza
Cyber Intelligence and information Security

cini
Cybersecurity National Lab

GRAZIE

www.cybersecurityframework.it/csr2016

staff@cybersecurityframework.it

@CIS_Sapienza

@lucamontanari

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

cini
Cybersecurity National Lab