FRAMEWORK NAZIONALE PER LA CYBERSECURITY

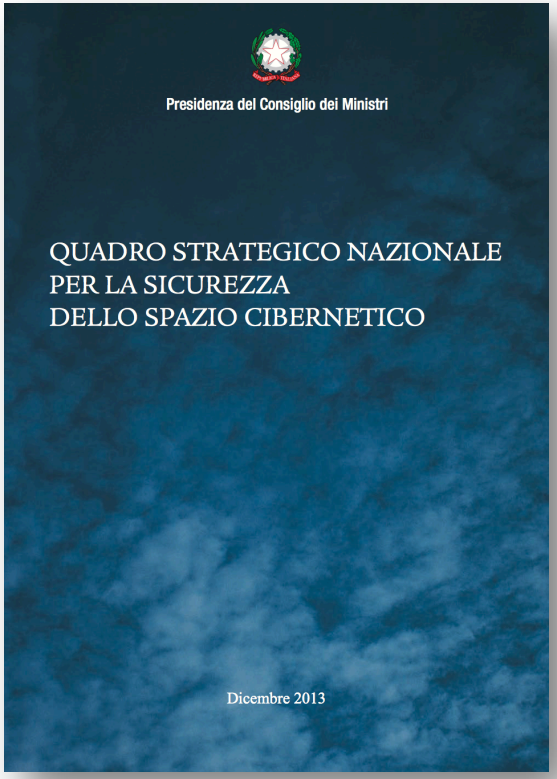
Luca Montanari

@itasec17
#ITASEC

cini
Cybersecurity National Lab

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

Nascita del Framework



Dalla Strategia Nazionale al Framework Nazionale

Nascita del Framework

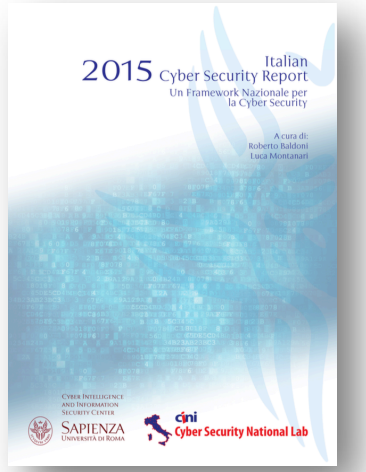
INDIRIZZO OPERATIVO 7

COMPLIANCE A *STANDARD* E PROTOCOLLI DI SICUREZZA

La compliance *a* standard *e protocolli di sicurezza, elaborati sia a livello nazionale che internazionale, consente di garantire un comune ed elevato livello qualitativo nell'assicurare la protezione cibernetica e la sicurezza informatica dei sistemi e delle reti.*

7.2	***Documenti di riferimento***	**a.** Elaborare e pubblicare documenti di riferimento quali manuali, elenchi di procedure *standard* e raccomandazioni (*best practices* di settore), tassonomia e lessico uniforme da utilizzare per lo scambio di informazioni

Nascita del Framework



2014 → 2015

Strategia Nazionale 27/12/2013	Definizione degli obiettivi	Definizione del tavolo di lavoro	Allargamento del tavolo a imprese e PA (PPP)	4 Febbraio 2016

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini Cybersecurity National Lab

Obiettivi iniziali

- **Portare la consapevolezza del rischio cyber ai massimi livelli aziendali**
  - non più una cosa per soli tecnici
  - portare le organizzazioni a considerare il rischio cyber come rischio economico parte del risk management

- **Considerare il panorama economico italiano**
  - 69% del PIL prodotto da Piccole-Medie Imprese
  - Pochissime grandi imprese nazionali, 0,1%

Obiettivi iniziali

- **Creare qualcosa che sia riconosciuto a livello internazionale**
  - migliorare la capacità di information sharing
  - innalzare il livello di duty of care nazionale

- **Non reinventare la ruota**
  - non ha senso creare un nuovo framework da zero
  - siamo partiti dal **NIST Framework for Improving Critical Infrastructure Cybersecurity**

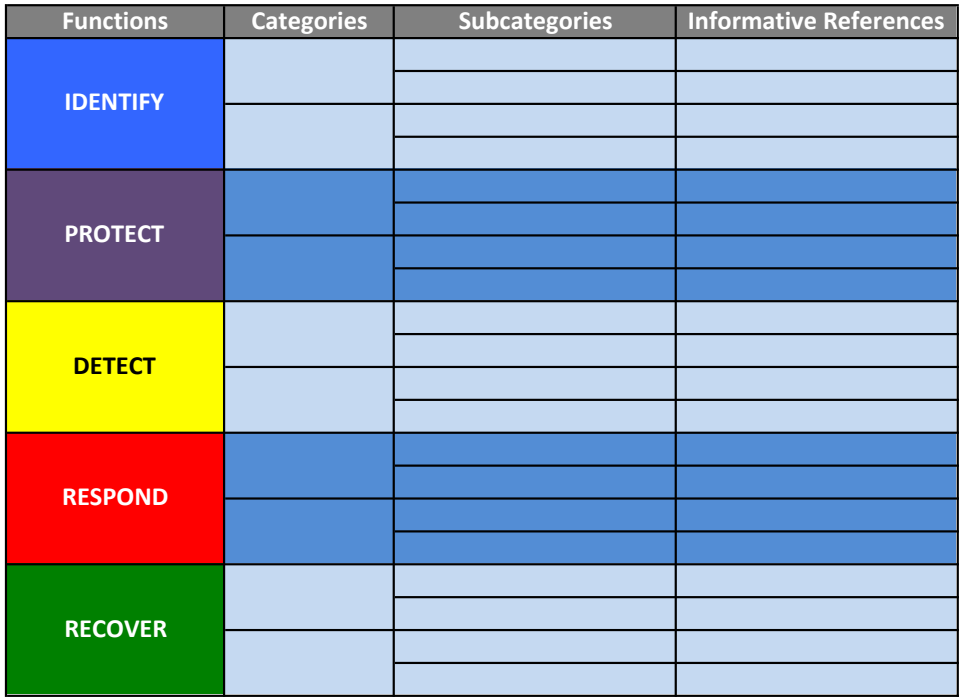
Il Framework Nazionale è uno strumento di autovalutazione del rischio cyber

Il Framework Nazionale è uno strumento di autovalutazione del rischio cyber

- Non è uno standard (non è certificabile)
- Permette di definire il proprio **profilo attuale** e il **profilo target**
- Aiuta nella definizione della **roadmap** per passare dal profilo attuale al profilo target

NIST Framework for Improving Critical Infrastructure Cybersecurity

- **Framework core**
- **Profiles**



Framework Nazionale per la

Function	Category	Subcategory	Priorità	Informative References
IDENTIFY (ID)		ID.AM-1: Sono censiti i sistemi e gli apparati fisici	ALTA	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4

Function	Subcategory	Rif.Guida	Livello 1	Livello 2	Livello 3
IDENTIFY (ID)	ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	Tabella 6.1: Identificazione degli Asset (IA)	Il censimento, la classificazione e l'aggiornamento degli asset (intesi come informazioni, applicazioni, sistemi ed apparati presenti) avviene in modalità per lo più manuale secondo un processo definito e controllato	Il censimento, la classificazione e l'aggiornamento degli asset avviene attraverso un sistema parzialmente automatico, che consenta di automatizzare almeno la fase di "discovery" dei sistemi connessi in rete, rilevando le principali caratteristiche degli stessi (caratteristiche hardware, software installati, configurazioni adottate, ecc.) e registrando l'inventario ottenuto in un repository centralizzato	Il censimento, la classificazione e l'aggiornamento degli asset avviene attraverso un sistema completamente automatico, che consenta di gestire l'intero ciclo di vita di un asset (identificazione, assegnazione, cambiamenti di stato, dismissioni)
	ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	Tabella 6.1: Identificazione degli Asset (IA)	Vedi ID.AM-1	Vedi ID.AM-1	Vedi ID.AM-1
	ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	Tabella 6.2: Assegnazione Responsabilità (AR)	La Proprietà e/o il Vertice Aziendale nomina il referente per la Cyber Security, definendo formalmente le attività in carico. Formalizza inoltre il disciplinare tecnico per l'utilizzo consono delle informazioni e degli strumenti informatici da parte di tutte le parti interessate (e.g. dipendenti, consulenti, terze parti)	Deve essere predisposto un documento di Politica Aziendale per la Cyber Security che definisca e formalizzi chiaramente i ruoli, le responsabilità e le attività richieste a ciascuna parte coinvolta a vario titolo nella gestione della Cyber Security (dipendenti, consulenti, terze parti), comunicando chiaramente l'impegno della Proprietà o dei Vertici Aziendali rispetto a tali necessità	N/A
	ID.GV-3: I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti	Tabella 6.3: Conformità a leggi e regolamenti (CLR)	La conformità a leggi e regolamenti è raggiunta e verificata, anche ricorrendo a specialisti e fornitori esterni, ove ritenuto necessario, in grado di agevolare l'individuazione e la gestione degli aspetti normativi e di conformità, soprattutto quando direttamente o indirettamente connessi con gli aspetti di Cyber Security	N/A	N/A

Framework Nazionale per la Cybersecurity

- Framework core
- Profiles

Abbiamo Aggiunto:

- Livelli Priorità*
- Livelli di Maturità*
- Linee Guida*
- Riferimenti normativi (privacy, CAD, altro*)
- Metodologia di contestualizzazione

*validi per nell'ambito della contestualizzazione

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini Cybersecurity National Lab

Contestualizzazioni

Il Framework può essere ”customizzato” tramite:

- la **selezione** delle Subcategory
- **definizione** di livelli di **priorità** per ogni subcategory
- **definizione** livelli di **maturità** per ogni subcategory

Scope della Contestualizzazione

La singola contestualizzazione può essere valida per **organizzazioni**:

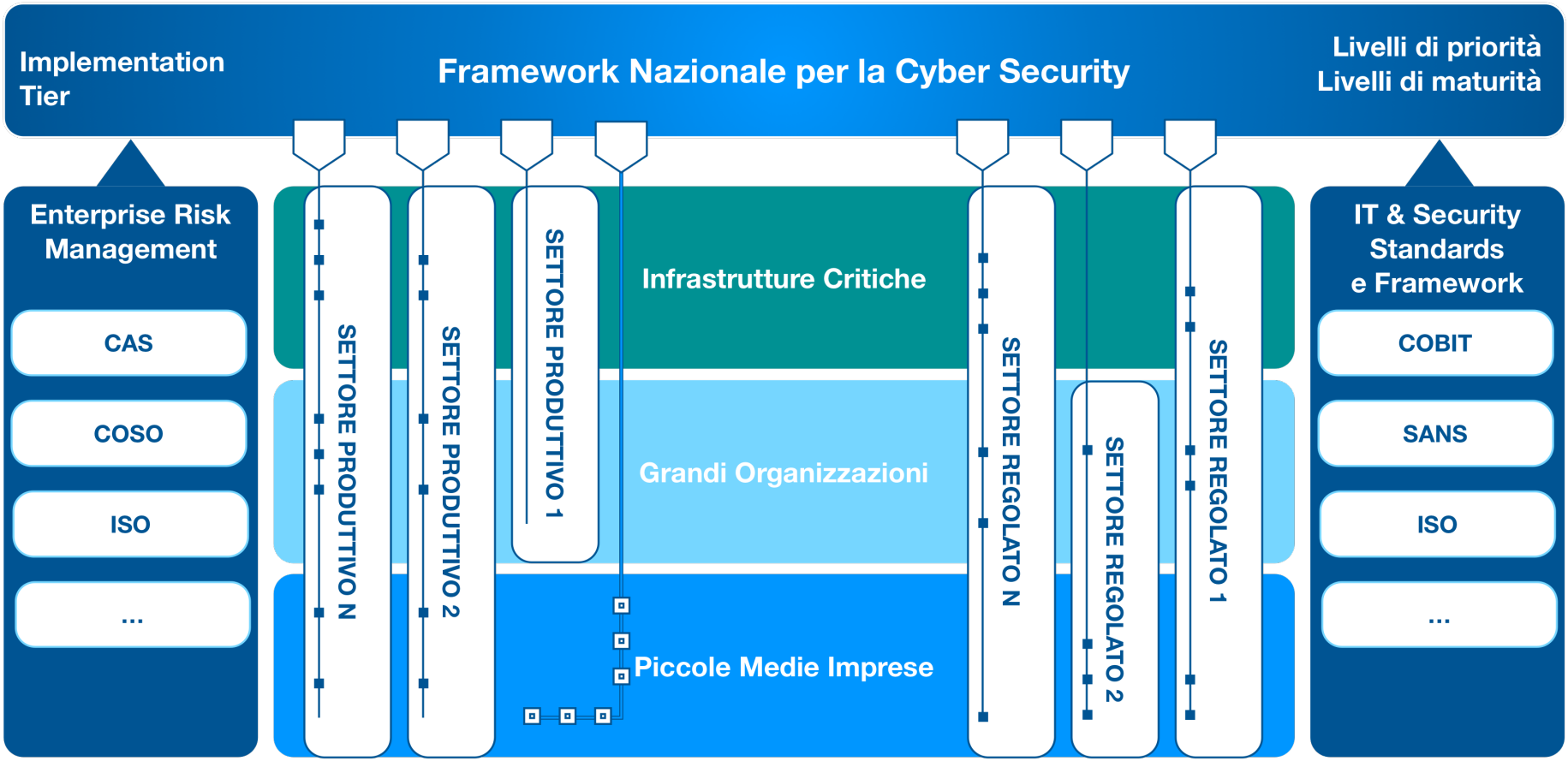
- di un dato **settore economico**/produttivo
- di una certa **dimensione**
- appartenenti a un **settore regolato**
  - per pubbliche amministrazioni centrali/locali
  - banche
  - ...
- Per business unit di IC o GI

Chi ~~può~~ dovrebbe creare contestualizzazioni del Framework

- **Associazioni di Settore** (confindustria, federsanità,…)
- Un **regolatore di settore**
- La **singola azienda**

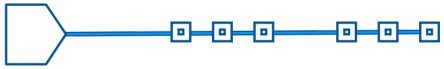
(che potrebbe modificare una contestualizzazione fatta da altri)

- Un **qualsiasi attore** che definisce una contestualizzazione del Framework e la rende disponibile



Contestualizzazione per un settore produttivo/regolato

Contestualizzazione del framework



Vantaggi per le grandi imprese

- Strumento per la **top management awareness**
- Un aiuto a definire **piani di spesa** per la gestione del rischio cyber
- Gestione della **catena di approvvigionamento**
- Strumento per rafforzare/rivedere la gestione del **rischio cyber**
- Strumento di **comunicazione** con le altre imprese

- **Raccomandazioni** e suggerimenti sulla gestione del rischio cyber (presentazione successiva)

Vantaggi per le PMI

- Qualcosa da cui partire*!
- Una contestualizzazione del Framework dedicata a loro
- Guida all'implementazione delle subcategory a priorità alta

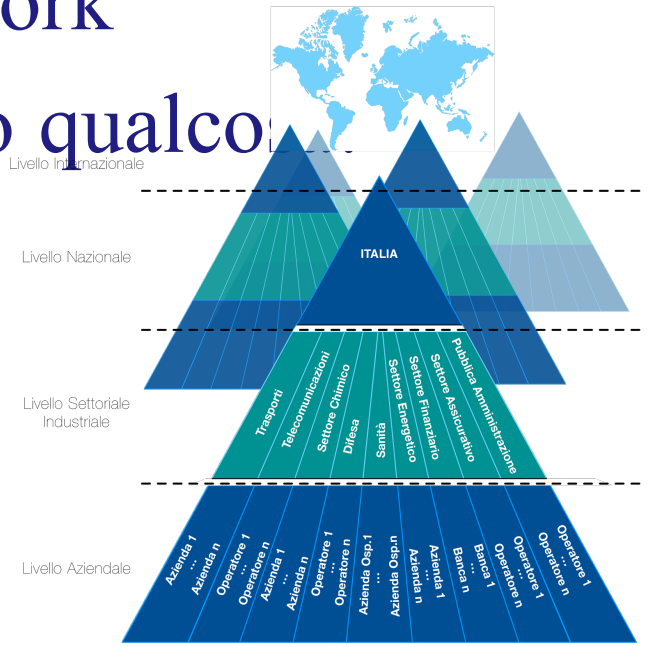
Function	Category	Subcategory	Priorità	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi di business e con la strategia di rischio dell'organizzazione	ID.AM-1: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	ALTA	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	ALTA	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati.	BASSA	· CCS CSC 1 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: I sistemi informativi esterni all'organizzazione sono catalogati	NON SELEZIONATA	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Le risorse (es: hardware, dispositivi, dati e software) sono prioritizzati in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione	MEDIA	· COBIT 5 APO03.03, APO03.04, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 · **Obbligatorio per le PP.AA. ai sensi dell'art. 50-bis, comma 3, lett. a) del CAD**
		ID.AM-6: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	ALTA	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
	Business Environment (ID.BE): La mission dell'organizzazione, gli obiettivi, le attività e gli attori coinvolti sono compresi e valutate in termini di priorità. Tali informazioni influenzano i ruoli, le responsabilità di cybersecurity e le decisioni in materia di gestione del rischio.	ID.BE-1:Il ruolo dell'organizzazione all'interno della filiera produttiva è identificato e reso noto	NON SELEZIONATA	· COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 · NIST SP 800-53 Rev. 4 CP-2, SA-12
		ID.BE-2: Il ruolo dell'organizzazione come infrastruttura critica e nel settore industriale di riferimento è identificato e reso noto	NON SELEZIONATA	· COBIT 5 APO02.06, APO03.01 · NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Sono definite e rese note delle priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione.	MEDIA	· COBIT 5 APO02.01, APO02.06, APO03.01 · ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 · NIST SP 800-53 Rev. 4 PM-11, SA-14
		ID.BE-4: Sono identificate e rese note interdipendenze e funzioni fondamentali per la fornitura di servizi critici	MEDIA	· ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 · NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Sono identificati e resi noti i requisiti di resilienza a supporto della fornitura di servizi critici	MEDIA	· COBIT 5 DSS04.02 · ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

* non abbastanza…

Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini Cybersecurity National Lab

Vantaggi per la Nazione

- Fornire un **linguaggio comune** a diversi soggetti in modo da poter emanare regole in maniera coerente e.g.,Garante Privacy, AGID, PCM, ecc.
- **Internazionalità** del framework
- Poter dire che stiamo facendo qualcosa



Framework Nazionale

- **Più generale del** NIST CI-Framework
  - le contestualizzazioni permettono di creare Framework ”custom”
- Viene mantenuta la **compliance** con il NIST CI-Framework
  - riconosciuto internazionalmente
- **Profili di sicurezza** più accurati
  - sono definiti sui livelli di maturità
- **Riconosciuto a livello nazionale**
  - potrebbe rafforzare la **supply chain** dell’intero panorama nazionale
  - Fornisce un linguaggio comune per le **interazioni tra pubblico e privato**

Il team (oltre 30 persone)
Public-Private-Partnership

- CIS-Sapienza
- Laboratorio Nazionale

- PCM (Intelligence)
- CERT Nazionale
- CERT-PA
- Garante della Privacy
- Agid

- Panel di aziende

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini Cybersecurity National Lab

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Garante per la protezione dei dati personali

Ministero dello Sviluppo Economico

Computer Emergency Response Team Pubblica Amministrazione
CERT - PA

CERT nazionale Italia

AON

Deloitte.

Enel

eni

hermesbay

KPMG

INTELLIUM

Microsoft

pwc

Il team (oltre 30 persone)
Public-Private-Partnership

Consultazione pubblica:
più di 300 emendamenti!

quasi un anno dalla pre

- 4 febbraio 2016 il framework viene presentato
- viene citato dalla ”Relazione sulla politica dell’informazione della sicurezza” del DIS
- Il NIST **partecipa alla presentazione**, pubblica sul proprio sito **il link al nostro Framework** e ci invita a presentarlo a **Washington** (domani introdurrà la versione 1.1)

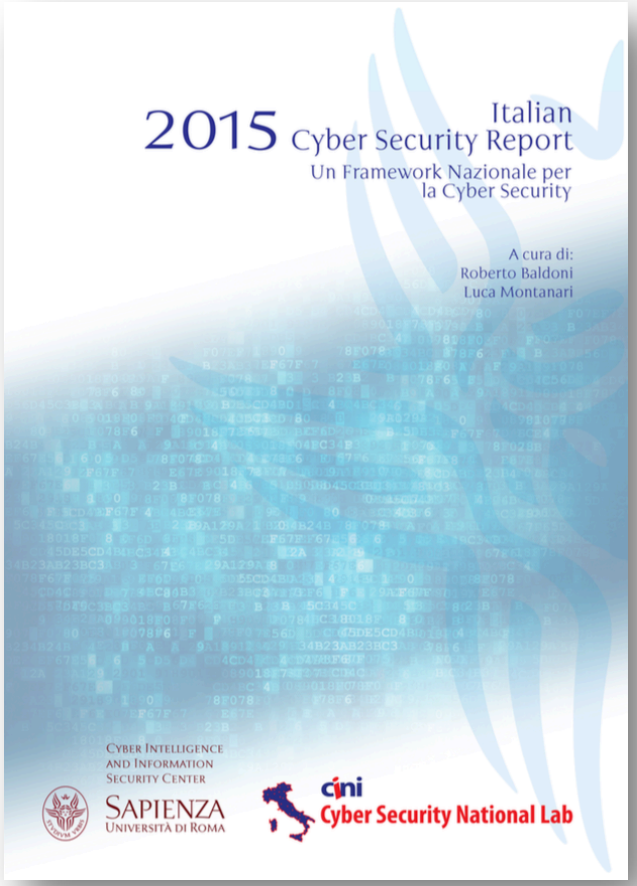
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

quasi un anno dalla pre

- **Agid** pubblica le **misure minime di sicurezza** con il mapping con le Subcategory del Framework
- **Potomac** Institute cita e descrive il framework affiancandolo alla strategia nazionale
- Diversi attori interessati a collaborazioni per **sviluppare contestualizzazioni**

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Cybersecurity Report ~~2015~~ 2016

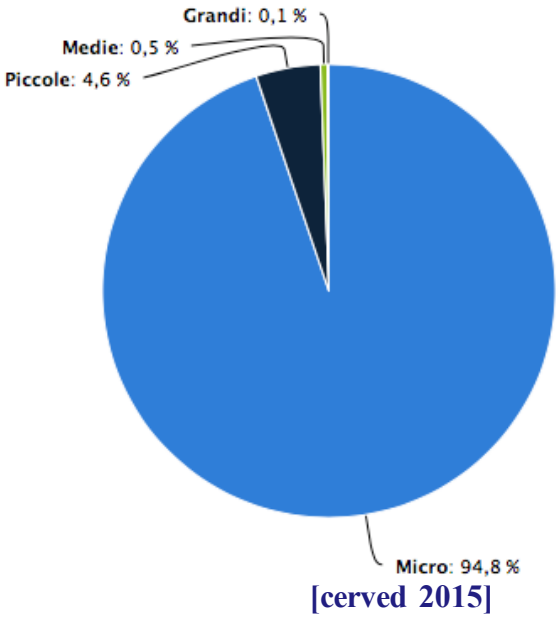


[cerved 2015]

Cybersecurity Report 2016

- Il Framework è semplice ma in molti casi non abbastanza
- In Italia **il 99,9% delle organizzazioni sono Micro/Piccole/Medie**
  - non hanno tempo né capacità per occuparsi di cybersecurity
- La critica più frequente da non addett stata

"per me è troppo complesso"



[cerved 2015]

Cybersecurity Report 2016

Presenterà **15 controlli essenziali di cybersecurity** corredati da una guida all'implementazione

- **I controlli sono rivolti alle organizzazioni che non hanno competenze di cybersecurity,** per le quali il Framework è troppo complesso
- Sono **derivati dalle subcategory del Framework**
- Sono le pratiche base, il minimo per stare al mondo di oggi

Cybersecurity Report 2016

FUNCTION	CATEGORY	SUBCATEGORY	CONTROLLO
DETECTION (DE)	Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati periodicamente per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	DE.CM-4: Il codice malevolo viene rilevato	7 – Tutti i dispositivi che lo consentono sono protetti da software antivirus regolarmente aggiornato.

Cybersecurity Report 2016

Da oggi i controlli sono in consultazione pubblica fino al 3/2, diteci cosa ne pensate:

http://bit.ly/2j7FqiT

2 questionari,

uno per esperti, uno

per le imprese

Il link è anche sul sito

www.cybersecurityframework.it/csr2016

Cyber Intelligence and Information Security Center
Sapienza Università di Roma
cini Cybersecurity National Lab

Cybersecurity Report 2016

Save the date:

2 Marzo 2017

Aula magna Sapienza Roma

Stay tuned:

@CIS_Sapienza

www.cybersecurityframework.it

staff@cybersecurityframework.it

Cyber Intelligence and Information Security Center
Sapienza Università di Roma

cini Cybersecurity National Lab

Tool web Framework Nazionale

Disponibile da oggi:

http://tool.cybersecurityframework.it

Sviluppato da: NAXE

Permette di creare:

- contestualizzazioni
- profili da un contestualizzazione
- modificare contestualizzazioni esistenti
- Visualizzare profili e contestualizzazioni

Disponibile da oggi:

Consultazione pubblica CSR2016:

http://cybersecurityframework.it/csr2016

Tool del Framework:

http://tool.cybersecurityframework.it