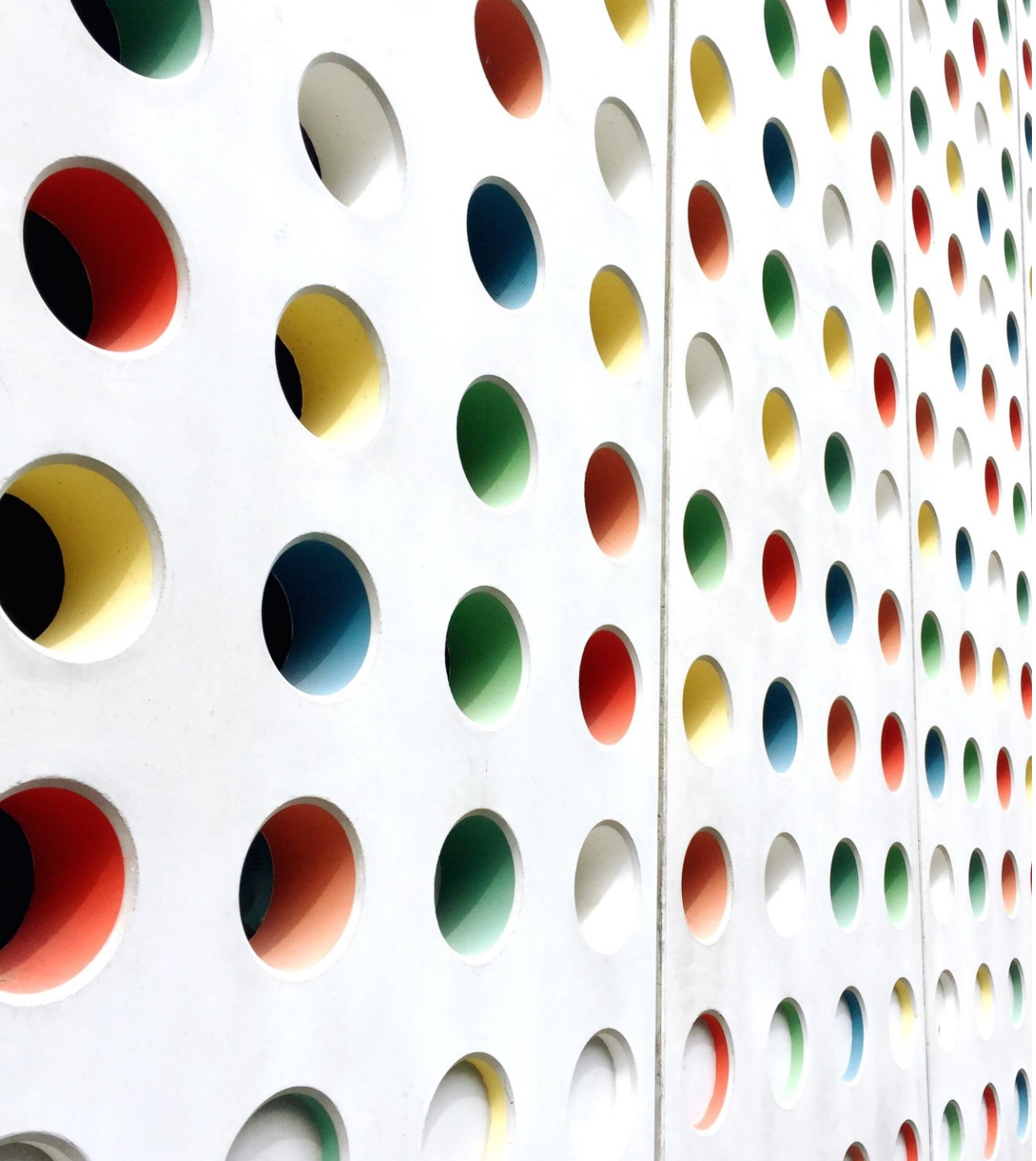


Presidenza del Consiglio dei Ministri
Scuola Nazionale dell'Amministrazione

La cybersecurity e la protezione dei dati

VINCENZO CALABRÒ
Ministero dell'Interno

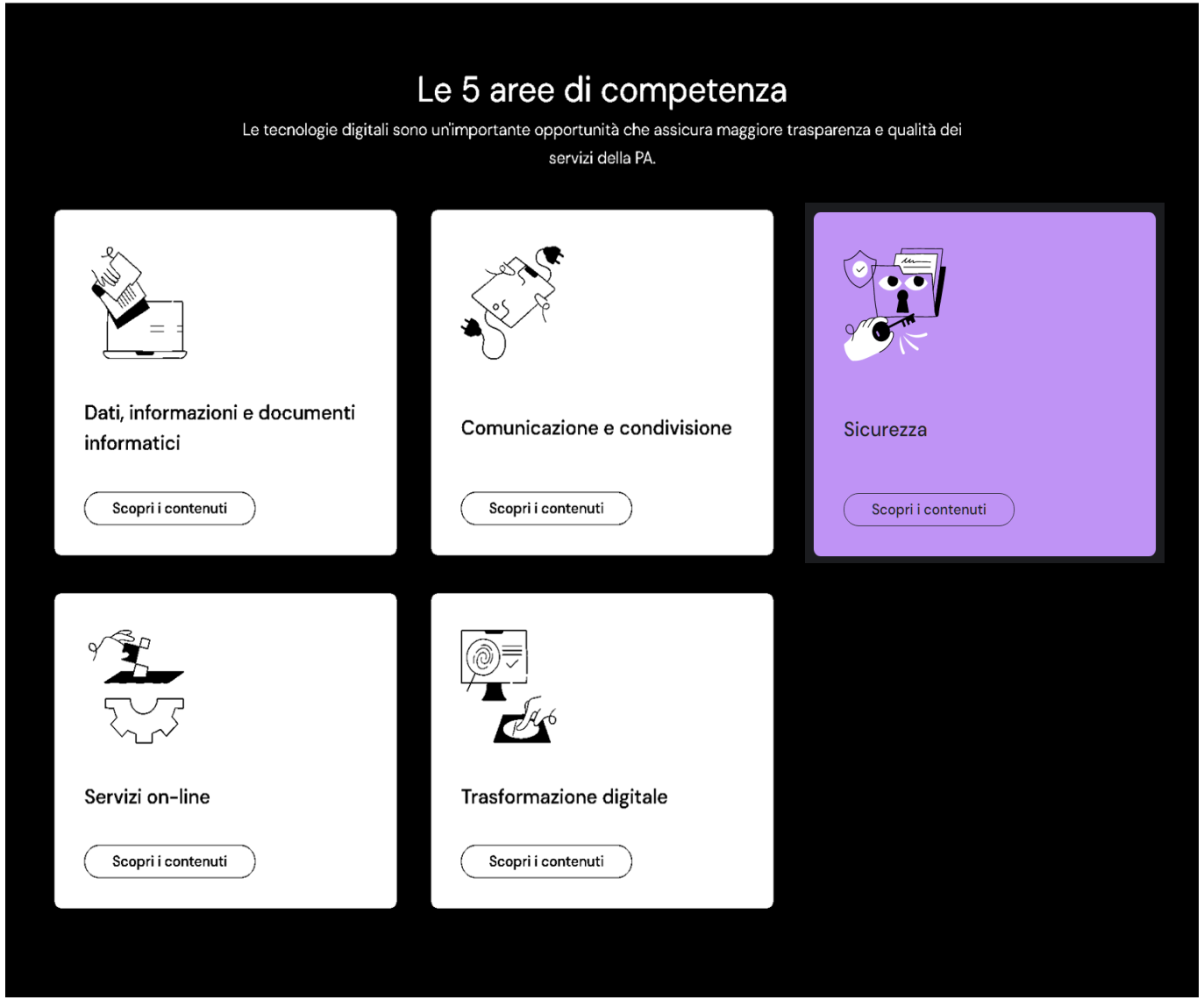
9 maggio 2023

Competenze digitali per la PA

Le tecnologie digitali sono un'importante opportunità che assicura maggiore trasparenza e qualità dei servizi della PA.

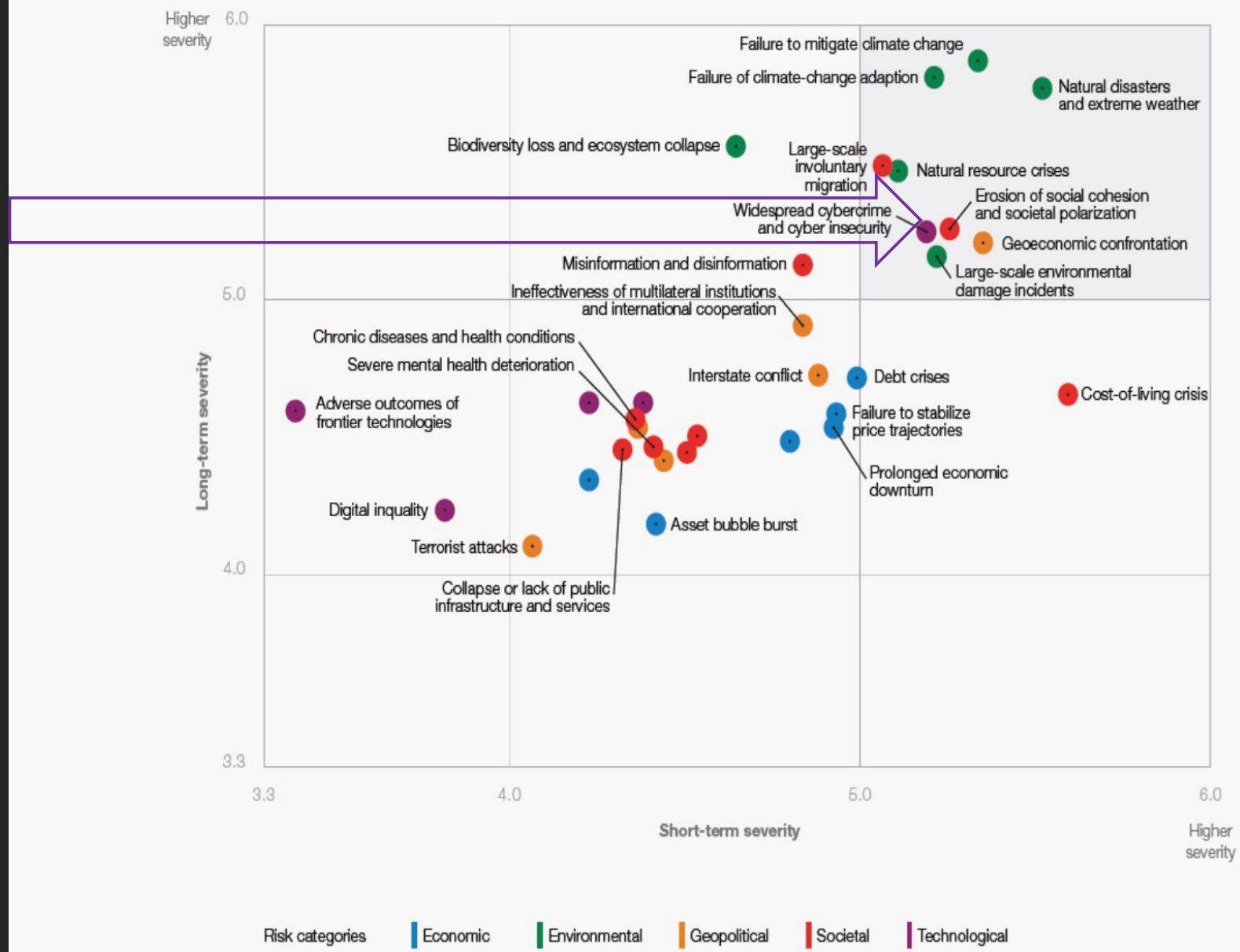
Area 3 - Sicurezza

La sicurezza è l'insieme delle misure di carattere tecnologico, organizzativo e procedurale volte a garantire la protezione dei sistemi informatici e dei dati in essi contenuti.



Perché affrontare il tema della Cyber Security?

Il Rapporto 2023 sui rischi globali, redatto dal World Economic Forum, inserisce il cybercrime e la cyber insecurity tra i principali rischi perché viviamo nell'era della trasformazione digitale, in cui i dati e la connettività svolgono un ruolo cruciale per l'innovazione e la prosperità di tutto il mondo, di conseguenza le minacce cyber rappresentano un grave ostacolo al progresso della società.



Source

World Economic Forum Global Risks Perception Survey 2022-2023.

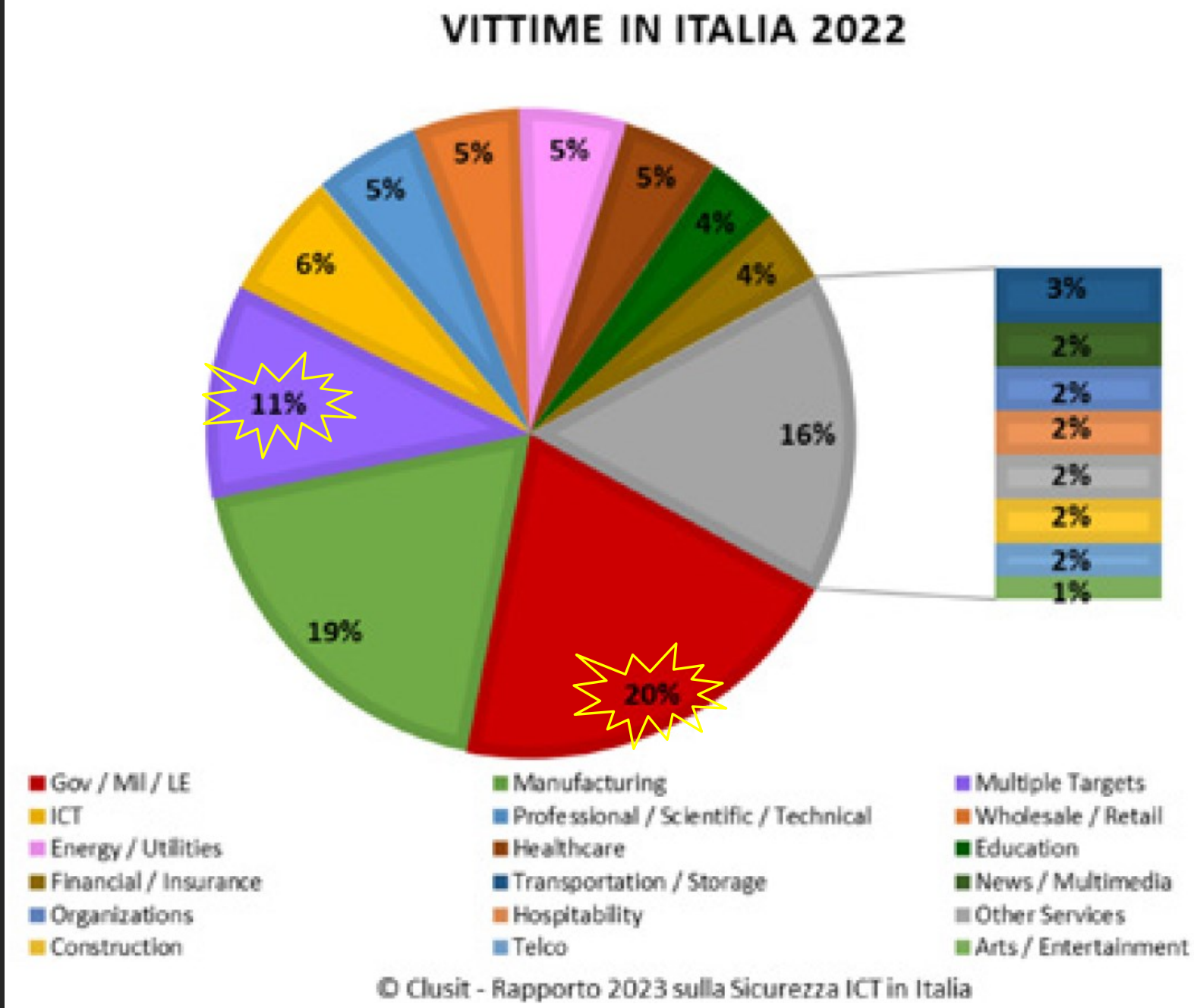
Note

Severity was assessed on a 1-7 Likert scale [1 – Low severity, 7 – High severity].

La Pubblica Amministrazione è sotto attacco?

La Pubblica Amministrazione non è esente dalla minaccia cyber.

Pertanto, il tema della cybersecurity è decisivo per la realizzazione di una completa transizione digitale, prodromica all'estensione e allo sviluppo dei servizi pubblici, perché è necessario che il processo sia resiliente a questa tipologia di minacce.



Le principali normative in tema di cyber security per la PA

Direttiva Ministeriale 16 gennaio 2002 "Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni." con cui si chiedeva a tutte le PA di avviare nell'immediato alcune azioni prioritarie tali da consentire il conseguimento di un primo importante risultato di allineamento ad una "base minima di sicurezza", attraverso:

1. una rapida autodiagnosi, sulla base dell'allegato 1, del livello di adeguatezza della Sicurezza informatica e delle telecomunicazioni (ICT), con particolare riferimento alla dimensione organizzativa operativa e conoscitiva della sicurezza
2. l'attivazione delle necessarie iniziative per posizionarsi sulla "base minima di sicurezza", definita nell'allegato 2, che consenta di costruire, con un approccio unitario e condiviso, le fondamenta della sicurezza della pubblica amministrazione

Nel 2004 è attivato «GOVCert», il primo CERT (Computer Emergency Response Team) Governativo, per fornire informazioni tempestive e supporto per gli eventi di sicurezza; appropriate informazioni e supporto nella gestione degli incidenti.

Direttive e Circolari in tema di Misure minime di sicurezza ICT per le Pubbliche Amministrazioni

Direttiva PCM 24 gennaio 2013 «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale»: definisce una prima struttura per la protezione cibernetica

→ Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico (Dicembre 2013)

Direttiva PCM 1 agosto 2015 «Direttiva impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici»: delega l'Agenzia per l'Italia Digitale (AgID) per la predisposizione di linee guida ad-hoc per la PA

→ Circolare AgID n. 2/2017 «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva PCM 1 agosto 2015)»

Direttiva PCM 17 febbraio 2017 «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali»: implementa la struttura per la protezione cibernetica e costituisce il CERT_PA e CERT_NAZIONALE, perché l'8 agosto 2016 è entrata in vigore la Direttiva 2016/1148 Network and Information Security (NIS) recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

→ Piano Nazionale per la Protezione Cibernetico e la Sicurezza Informatica (Marzo 2017)

Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione

La cd. «**Direttiva NIS**» del 6 luglio 2016 prevede misure in grado di rafforzare concretamente il livello di sicurezza della rete e dei sistemi informativi, obbligo di notifica degli incidenti rilevanti e stretta cooperazione a livello Ue.

La direttiva si basa su tre pilastri:

- **Prevenzione** gli operatori di servizi essenziali e i fornitori di servizi digitali devono mettere in atto misure per prevenire gli attacchi informatici
- **Rilevamento** gli stessi devono essere in grado di individuare tempestivamente gli attacchi informatici
- **Mitigazione** essi devono essere in grado di ripristinare rapidamente i propri servizi in caso di attacco informatico

A tal fine la direttiva:

1. fa obbligo a tutti gli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi;
2. istituisce un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi;
3. crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT») per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace;
4. stabilisce obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali;
5. fa obbligo agli Stati membri di designare autorità nazionali competenti, punti di contatto unici e CSIRT con compiti connessi alla sicurezza della rete e dei sistemi informativi.

Decreto Legislativo 18 maggio 2018 , n. 65
Attuazione della direttiva (UE) 2016/1148 («*Direttiva NIS*»)

La norma di attuazione ha recepito tutte le previsione della Direttiva NIS, in particolare:

1. Sono stati stabiliti le modalità e i criteri per identificare gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (FSD);
2. È stata definita la Strategia nazionale di Cybersicurezza (obiettivi, priorità e misure)
3. È stata individuata l'Autorità nazionale competente e il punto di contatto unico (*Agenzia per la Cybersicurezza Nazionale*)
4. È stato istituito presso l'Agenzia per la cybersicurezza nazionale, il CSIRT italiano, che svolge i compiti e le funzioni del Computer Emergency Response Team (CERT) nazionale
5. Sono stati definiti gli obblighi in materia di sicurezza per gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (FSD). Ogni OSE o FSD identifica e adotta misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi relativi alla sicurezza della rete e dei sistemi informativi che utilizza. Tenuto conto delle conoscenze più aggiornate in materia, tali misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente e tengono conto dei seguenti elementi: la sicurezza dei sistemi e degli impianti; trattamento degli incidenti; gestione della continuità operativa; monitoraggio, audit e test; conformità con le norme internazionali.
6. Gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (FSD) adottano misure per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi al fine di assicurare la continuità di tali servizi.
7. È reso obbligatorio che gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (FSD) notificano al CSIRT italiano senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti o sulla fornitura di un servizio.

Decreto-legge 21 settembre 2019 , n. 105 - Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica.

Il D.L. 21 settembre 2019 , n. 105, convertito con modificazioni dalla L. 18 novembre 2019, n. 133, «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica» delinea il Perimetro di sicurezza nazionale cibernetica composto da attori privati e pubblici che esercitano funzioni essenziali dello stato o assicurano un servizio essenziale alle attività fondamentali per l'interesse dello stato e gli adempimenti connessi.

Per far fronte alle previsioni contenute nel D.L. sono stati pubblicati 4 regolamenti attuativi e 1 DPR:

- DPCM 1 30 luglio 2020, n. 131, «Regolamento in materia di perimetro di sicurezza nazionale cibernetica», definisce le regole del Perimetro nazionale di sicurezza cibernetica e stabilisce i parametri con cui sono individuati i soggetti che si occupano di funzioni vitali per l'Italia. (Invio annuale elenco TIC)

DPR 5 febbraio 2021, n. 54, «Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge sul Perimetro di sicurezza nazionale cibernetica» affronta le procedure e i termini per le valutazioni da parte del CVCN e dei CV su prodotti in acquisizione da parte dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica

- DPCM 2 14 aprile 2021, 81, «Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici», Include la Tassonomia degli Incidenti (All. A), le Misure di Sicurezza (All. B) e Misure minime di sicurezza per la tutela delle informazioni (All. C)
- DPCM 3 15 giugno 2021, «Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica», Indicati nell'Allegato alla norma.
- DPCM 4 18 maggio 2022, 92, «Regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra Centro di Valutazione e Certificazione Nazionale, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell'interno e del Ministero della Difesa»

Con il D.L. 14 giugno 2021, n. 82 convertito nella legge 4 agosto 2021, n. 109, sono state emanate ulteriori «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale».

Codice in materia di protezione dei dati personali

Legge 31 dicembre 1996, n. 675 «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»

- *D.P.R., 28/07/1999 nº 318 "Misure minime di sicurezza per trattamento dati ex L.675/96» (abrogato dal D.Lgs. 30 giugno 2003, n. 196)*

Decreto Legislativo 30 giugno 2003, n. 196 *«Codice in materia di protezione dei dati personali»*

- *B. Disciplinare tecnico in materia di misure minime di sicurezza (abrogato con l'adeguamento al Regolamento (UE) 2016/679)*

Decreto Legislativo 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati (RGPD - Regolamento Generale sulla Protezione dei Dati).

- *RGPD - Articolo 32 Sicurezza del trattamento*

  Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.
- *RGPD - Articolo 33 Notifica di una violazione dei dati personali all'autorità di controllo*

  In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
- *RGPD - Articolo 34 Comunicazione di una violazione dei dati personali all'interessato*
- *RGPD - Articolo 35 Valutazione d'impatto sulla protezione dei dati*

Le misure che si possono applicare al Ministero dell'Interno

- Le Misure minime di sicurezza ICT per le pubbliche amministrazioni, di cui alla Circolare AgID n. 2/2017.

- Le Misure tecniche e organizzative, ai sensi del combinato disposto dell'art. 12 del D.lgv. 65/2018 (Direttiva NIS) e dell'art. 3, comma 2, lett. A, DPCM 30 luglio 2020, n. 131 (Regolamento in materia di perimetro di sicurezza nazionale cibernetica):

  Per il settore interno, il Ministero dell'interno, nell'ambito delle attribuzioni di cui all'art. 14 D.Lgs. 30 luglio 1999, n. 300: garanzia della regolare costituzione e del funzionamento degli organi degli enti locali e funzioni statali esercitate dagli enti locali, tutela dell'ordine e della sicurezza pubblica, difesa civile, politiche di protezione civile e prevenzione incendi, (…), tutela dei diritti civili, cittadinanza, immigrazione, asilo e soccorso pubblico.

- Le Misure in materia di sicurezza cibernetica, ai sensi dell'art. 68 del DPCM 6 novembre 2015, n. 5, Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva, per le informazioni gestite tramite i CIS abilitati in conformità al Quadro strategico nazionale di cui all'art. 3 del decreto del Presidente del Consiglio dei Ministri del 17 febbraio 2017, "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali".

- Le Misure tecniche e organizzative, ai sensi dell'art. 32 del Regolamento Generale sulla Protezione dei Dati, per i dati personali.

Implementazione

Misure minime di sicurezza ICT per *(tutte)* le Pubbliche Amministrazioni

Le Misure minime di sicurezza ICT per le pubbliche amministrazioni, di cui alla Circolare AgID n. 2/2017, sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti. https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

- Obiettivo → indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate al fine di contrastare le minacce più comuni e frequenti.
- Attuazione → Il responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, il dirigente allo scopo designato.
- Implementazione → le modalità debbono essere sinteticamente riportate nel modulo di implementazione
- Firma → Il modulo di implementazione dovrà essere firmato digitalmente con marcatura temporale dal responsabile dell'attuazione e dal responsabile legale della struttura. Deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.
- Scadenza → 31 dicembre 2017.

Misure minime di sicurezza ICT per *(tutte)* le Pubbliche Amministrazioni

Le misure consistono in controlli di natura tecnologica, organizzativa e procedurale e utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica.

Le misure sono ispirate ai CIS Critical Security Controls (SANS 20), versione 6.0 del 2015.

A seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'Amministrazione, le misure minime possono essere implementate in modo graduale seguendo tre livelli di attuazione.

- Minimo → è quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.
- Standard → è il livello, superiore al livello minimo, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e rappresenta la maggior parte delle realtà della PA italiana.
- Avanzato → deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

Misure minime di sicurezza ICT per *(tutte)* le Pubbliche Amministrazioni

Le misure minime, suddivise in gruppi, sono un importante supporto metodologico, oltre che un mezzo attraverso il quale le Amministrazioni, soprattutto quelle più piccole e che hanno meno possibilità di avvalersi di professionalità specifiche, possono verificare autonomamente la propria situazione e avviare un percorso di monitoraggio e miglioramento.

I gruppi di controlli
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI
ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE
ABSC 10 (CSC 10): COPIE DI SICUREZZA
ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID #			Descrizione		Min.	Std.	Alto
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	X
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	ID.AM-1		X	X
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ID.AM-1			X
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	ID.AM-1			X
	2	1	Implementare il "logging" delle operazione del server DHCP.	ID.AM-1		X	X
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	ID.AM-1		X	X
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	X
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1		X	X
	4	1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	ID.AM-1	X	X	X
		2	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	ID.AM-1		X	X
		3	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	ID.AM-1			X
1	5	1	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	ID.AM-1			X
	6	1	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	ID.AM-1			X

Misure tecniche e organizzative per gli Enti che rientrano del Perimetro

Ad operatori e fornitori che rientrano nel perimetro di sicurezza nazionale cibernetica sono richiesti alcuni obblighi, tra i quali:

- progettare misure tecniche capaci di gestire i rischi informatici e designare un responsabile della sicurezza delle informazioni;
- puntare sulla prevenzione di incidenti che violino la sicurezza delle proprie reti informatiche;
- contenere i danni di eventuali attacchi e garantire la continuità dei servizi;
- notificare alle autorità competenti gli incidenti che minano la continuità e la fornitura dei servizi o comportino la divulgazione di dati sensibili. Successivamente, dovranno inviare un report dettagliato di quanto avvenuto.

Definizioni

Cybersicurezza (Cybersecurity): l'insieme delle attività (..) necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico. (D.L. 14/7/2021, n. 82)

Dalla Cyber Security alla Cyber Resilience

LA SICUREZZA INFORMATICA RICHIEDE UN APPROCCIO *«OLISTICO»*

Storicamente le organizzazioni hanno adottato un approccio «*addizionale*» o «*a silos*» nei confronti della sicurezza informatica.
Successivamente, è mutato l'orientamento, diventando «*trans-disciplinare*», perché impatta con tutte le componenti (dati, persone, procedure, infrastrutture, asset, processi, procedure, sistemi di controllo, organizzazione e governance) e richiede un approccio «*olistico*».

IL NUOVO PARADIGMA DELLA SICUREZZA È LA *«CYBER RESILIENCE»*

La governance di un'organizzazione deve gestire la sicurezza informatica al pari degli altri asset perché da essa può dipendere il raggiungimento o il fallimento degli obiettivi.
Gli incidenti informatici sono complessi e inevitabili, pertanto agli obiettivi fondamentali («*disponibilità*», «*confidenzialità*» e «*integrità*») si affianca la «*resilienza*», ovvero la capacità di adattarsi al contesto e resistere alle minacce in modo da garantire l'erogazione dei servizi.

Le linee guida sulla gestione dei rischi e la prevenzione, mitigazione e notifica degli incidenti

Nell'ambito della Direttiva NIS e del d.lgs. del 18 maggio 2018 n.65, sono state predisposte le linee guida sulla gestione dei rischi e la prevenzione, mitigazione e notifica degli incidenti per l'implementazione degli articoli 12 «Obblighi in materia di sicurezza e notifica degli incidenti» e 13 «attuazione e controllo» del D. Lgs. 18 maggio 2018, n. 65.

- In particolare, l'art. 12 prevede che gli Operatori di Servizi Essenziali adottino misure tecniche organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle rete e dei sistemi informativi. Tali misure devono assicurare un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente nonché prevenire e minimizzare l'impatto dei incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuità operativa di tali servizi.
- Ai sensi del medesimo art. 12 gli operatori di servizi essenziali sono altresì tenuti a notificare al CSIRT (Computer Security Incident Response Team) e all'Autorità competente NIS gli incidenti con impatto rilevante sulla fornitura dei servizi essenziali.
- L'art. 13 affida alle Autorità competenti NIS il compito di valutare il rispetto da parte degli operatori di servizi essenziali degli obblighi previsti dall'art.12.

Gli indirizzi individuati nelle linee guida sono basati sul Framework Nazionale per la Cyber Security, documento che nella sua versione 2.0 pubblicata a febbraio 2019 recepisce tra le *informative reference* (linee guida, standard e normative) relative a ciascuna Subcategory anche le nuove disposizioni emanate a livello europeo, tra cui il GDPR e la NIS.

Lo scopo delle linee guida è quello di fornire indicazioni di carattere tecnico, organizzativo e procedurale per l'innalzamento dei livelli di sicurezza cibernetica di reti e sistemi, garantendo altresì la resilienza del Sistema-Paese.

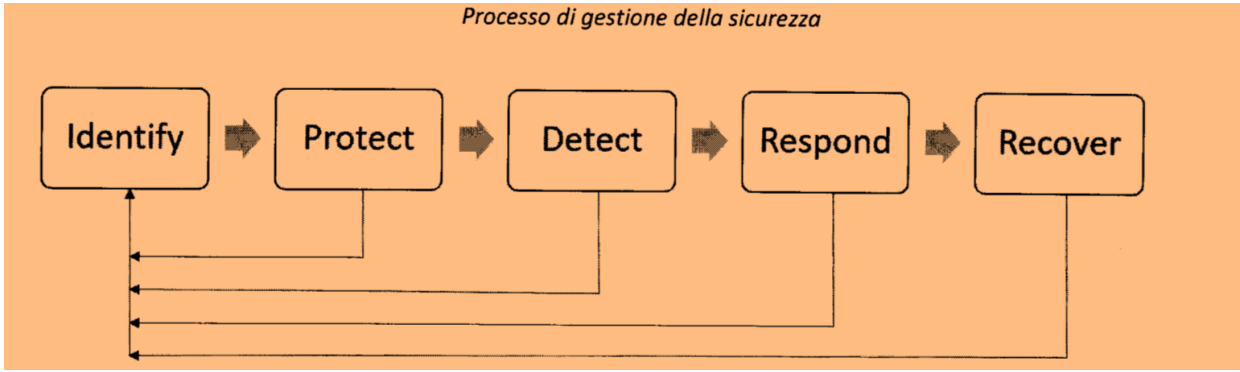
Framework Nazionale per la Cybersecurity e la Data Protection

Versione 2.0 Febbraio 2019 - https://www.cybersecurityframework.it/

Le indicazioni si basano sul Framework Nazionale per la Cybersecurity e la Data Protection *(ispirato al Cybersecurity Framework del NIST).*

Il core del Framework rappresenta la struttura del ciclo di vita del processo di gestione della cybersecurity, sia dal punto di vista tecnico che organizzativo. Il Framework è strutturato gerarchicamente in function, category e subcategory.

Le **Function**, concorrenti e continue, sono:



e costituiscono le principali tematiche da affrontare per operare una adeguata gestione del rischio cyber in modo strategico.

Il Framework quindi definisce, per ogni Function, **Category** e **Subcategory**, le quali forniscono indicazioni in termini di specifiche risorse, quali processi e tecnologiche da mettere in campo per gestire la singola Function.

Processo di Gestione della Sicurezza

	Function	Obiettivo
Gestione del rischio	IDENTIFY	La function IDENTIFY è legata alla comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati. Tale comprensione permette a un'organizzazione di definire risorse e investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali.
	PROTECT	La function PROTECT è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica.
Gestione dell'incidente	DETECT	La function DETECT è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica.
	RESPOND	La function RESPOND è associata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica.
	RECOVER	La function RECOVER è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente. L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle business operations.

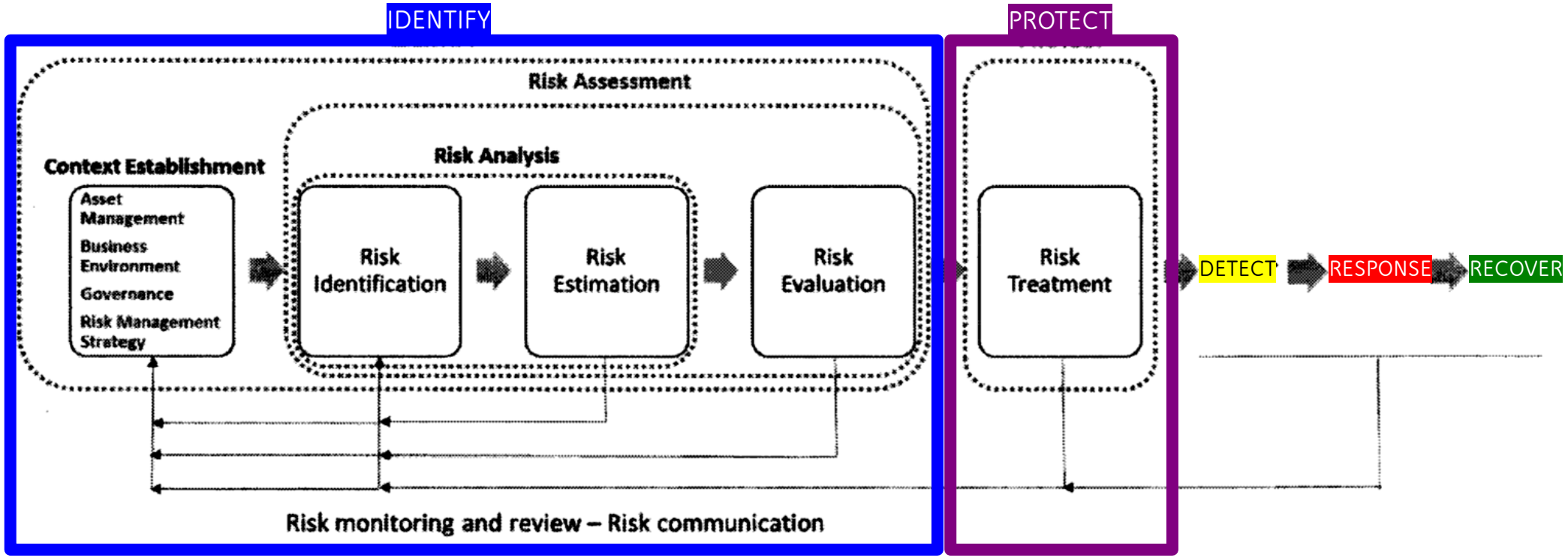
Processo di gestione dei rischi

Il processo di gestione dei rischi è incluso nel processo di gestione della sicurezza.
Le attività che ne fanno parte sono principalmente categorizzate nelle function «Identify» e «Protect», ma anche le restanti function contribuiscono all'efficacia dello stesso, fornendo informazioni per un miglioramento continuo.

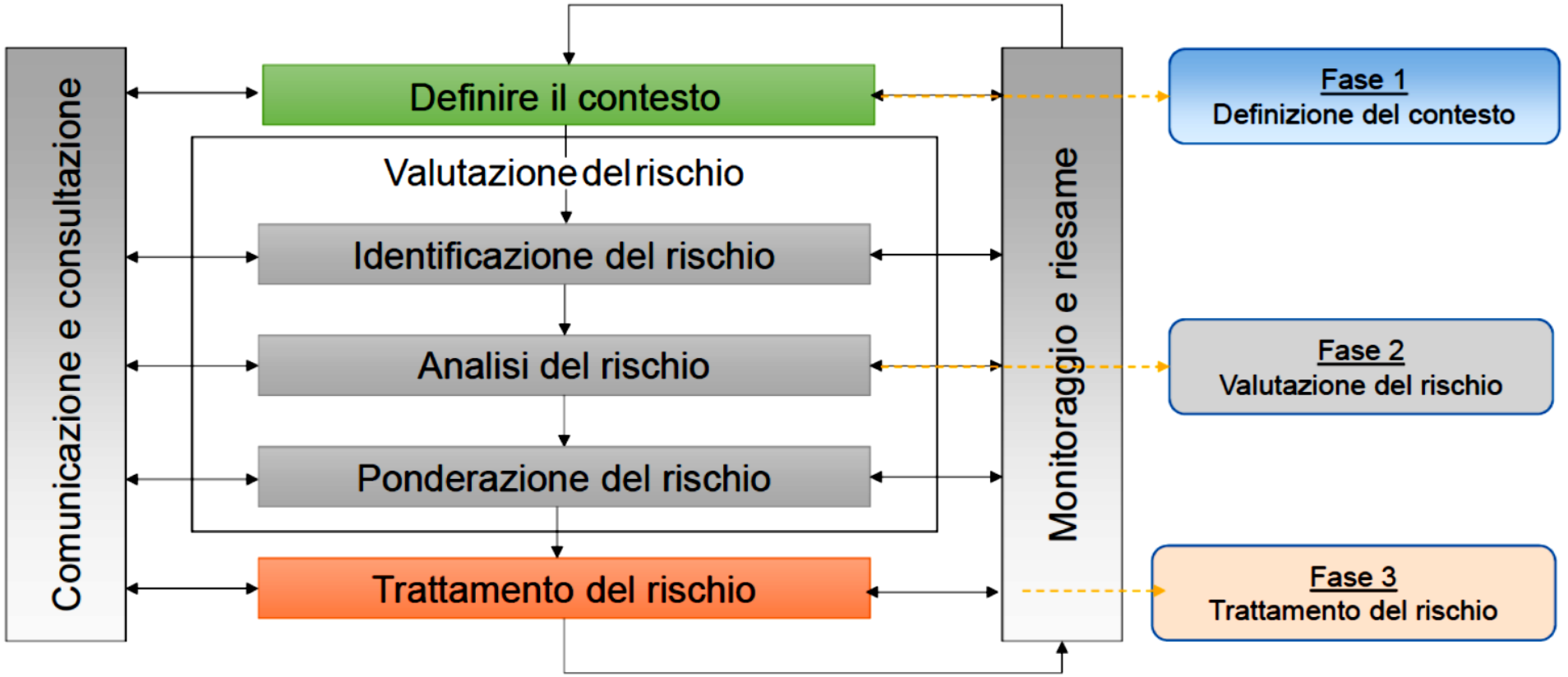
L'implementazione del processo dovrà fare riferimento ad una metodologia standard al fine di:

- individuare i principali rischi per la sicurezza delle reti e dei sistemi informativi tenendo conto delle minacce che insistono sugli asset;
- definire una metodologia di gestione dei rischi e utilizzare strumenti basati sugli standard di settore;
- verificare l'effettivo utilizzo di tali metodologie e strumenti di gestione del rischio da parte del personale;
- stabilire una priorità nelle azioni da condurre per ridurre l'impatto dei rischi e misurare l'efficacia del trattamento dei rischi.
- assicurarsi che i rischi residui, anche derivanti da vincoli realizzativi, siano minimizzati rispetto alla probabilità del verificarsi di incidenti;
- reiterare, monitorare e verificare il processo regolarmente.

Processo di gestione dei rischi



Metodologia di cybersecurity risk management



Macro-modello di calcolo del rischio

CARATTERISTICHE SERVIZI
A seconda delle caratteristiche primarie dei servizi erogati, è determinato il livello di criticità intrinseca (Profilo di Criticità) della PA. Le caratteristiche primarie e secondarie consentono di selezionare le Misure di Sicurezza da implementare (controlli di tipo amministrativo, sicurezza logica e fisica,) e dunque determinare le Vulnerabilità.

BENCHMARK
Il benchmark consente di valutare il fattore di Esposizione alla singola minaccia per il settore Pubblica Amministrazione.

IMPATTO
Consente di valutare gli impatti per ciascun servizio erogato dalla PA in caso di perdita di **Riservatezza (R), Integrità (I) e Disponibilità (D).** A partire dagli impatti sui singoli servizi erogati dalla PA, sarà poi calcolato l'impatto R,I,D sulla PA.

CYBER RISK = PROBABILITÀ DI ACCADIMENTO X IMPATTO

Macro-modello di calcolo del rischio

- Censimento dei servizi oggetto di analisi del rischio.
- Identificazione delle caratteristiche primarie e secondarie di ciascun servizio.
- Calcolo del Profilo di Criticità associato ad ogni servizio.
- Calcolo del Profilo di criticità associato alla PA in funzione dei profili di criticità dei servizi.

RISULTATI

- Per ciascun servizio, valutazione dell'impatto in termini di Riservatezza (R), Integrità (I) e Disponibilità (D) delle informazioni trattate dai servizi per ciascuna categoria di impatto: Economico/Finanziario, Operativo, Reputazionale e Legale/Compliance.
- Valutazione dell'impatto R,I,D della PA in funzione degli impatti sulle singole componenti R-I-D dei servizi.

RISULTATI

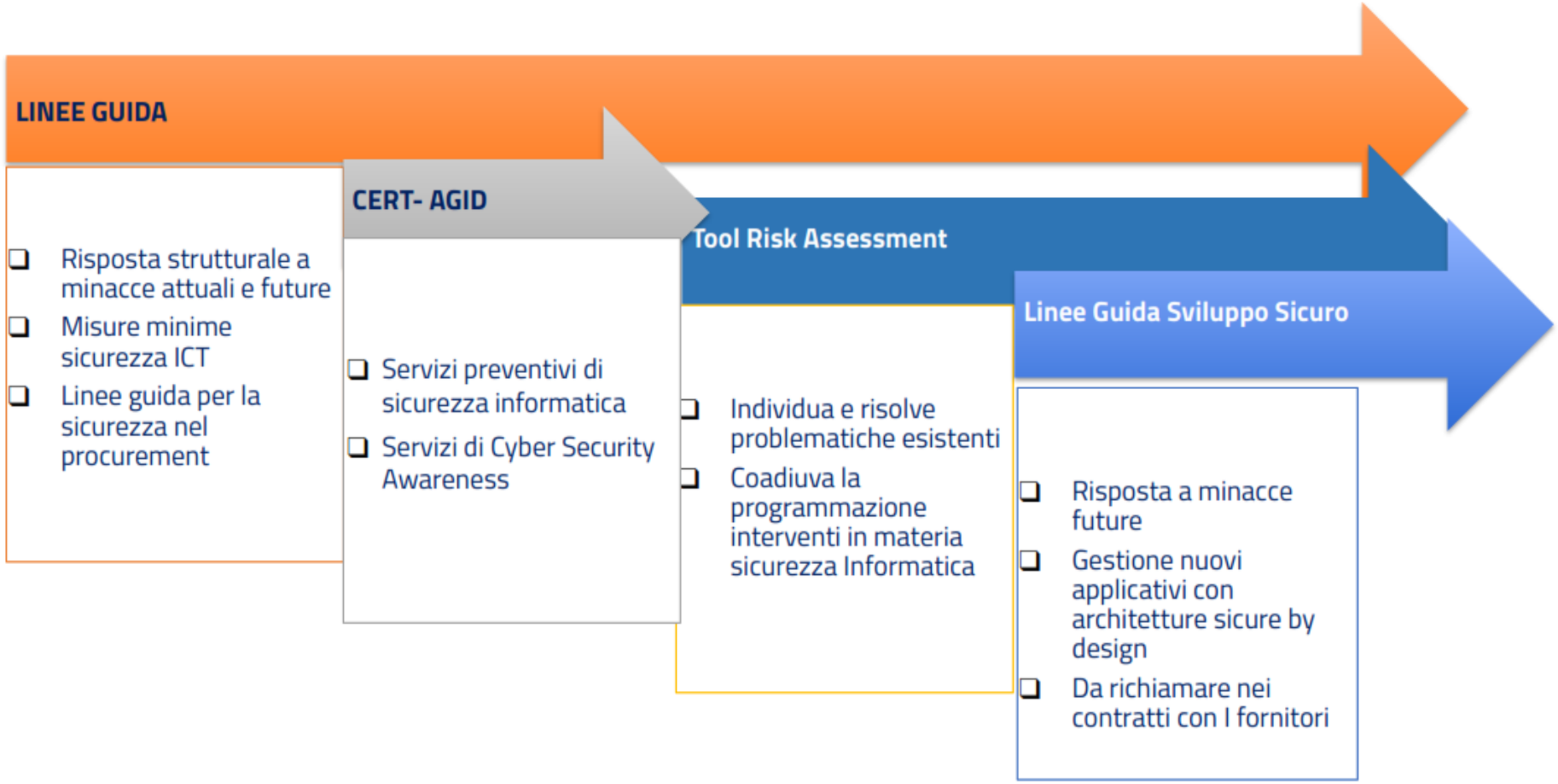
- Compilazione del questionario di Risk Assessment per la PA al fine di valutare il livello di vulnerabilità dei vari domini di sicurezza (accessi logici, sicurezza SW, gestione privacy, etc).
- Implementazione di un Risk Assessment report per la PA con indicazione delle componenti di rischio risultanti per ciascuna delle 32 minacce e relative opzioni di trattamento. Posizionamento della PA

REPORT

- Valutazione dei principali findings emersi dall'analisi del rischio.
- Definizione delle azioni di trattamento e mapping con le convenzioni attive.
- Implementazione di una matrice di prioritizzazione delle azioni di trattamento.
- Valutazione del Rischio Residuo.
- Definizione del Piano di Trattamento del Rischio

PIANO DI TRATTAMENTO

Azioni e strumenti di prevenzione messi a disposizione delle PP.AA. dall'AgID



Tool di valutazione e trattamento del rischio cyber

L'AgID ha elaborato un tool di autovalutazione del rischio cyber.

Il tool nasce per supportare le PP.AA. nel self-assessment di sicurezza informatica e migliorare la consapevolezza sulle materie di Cyber Security e permette di valutare le vulnerabilità e il livello di esposizione al rischio.

COME FUNZIONA IL TOOL?

FASE INIZIALE

Definizione del contesto in cui opera la PA

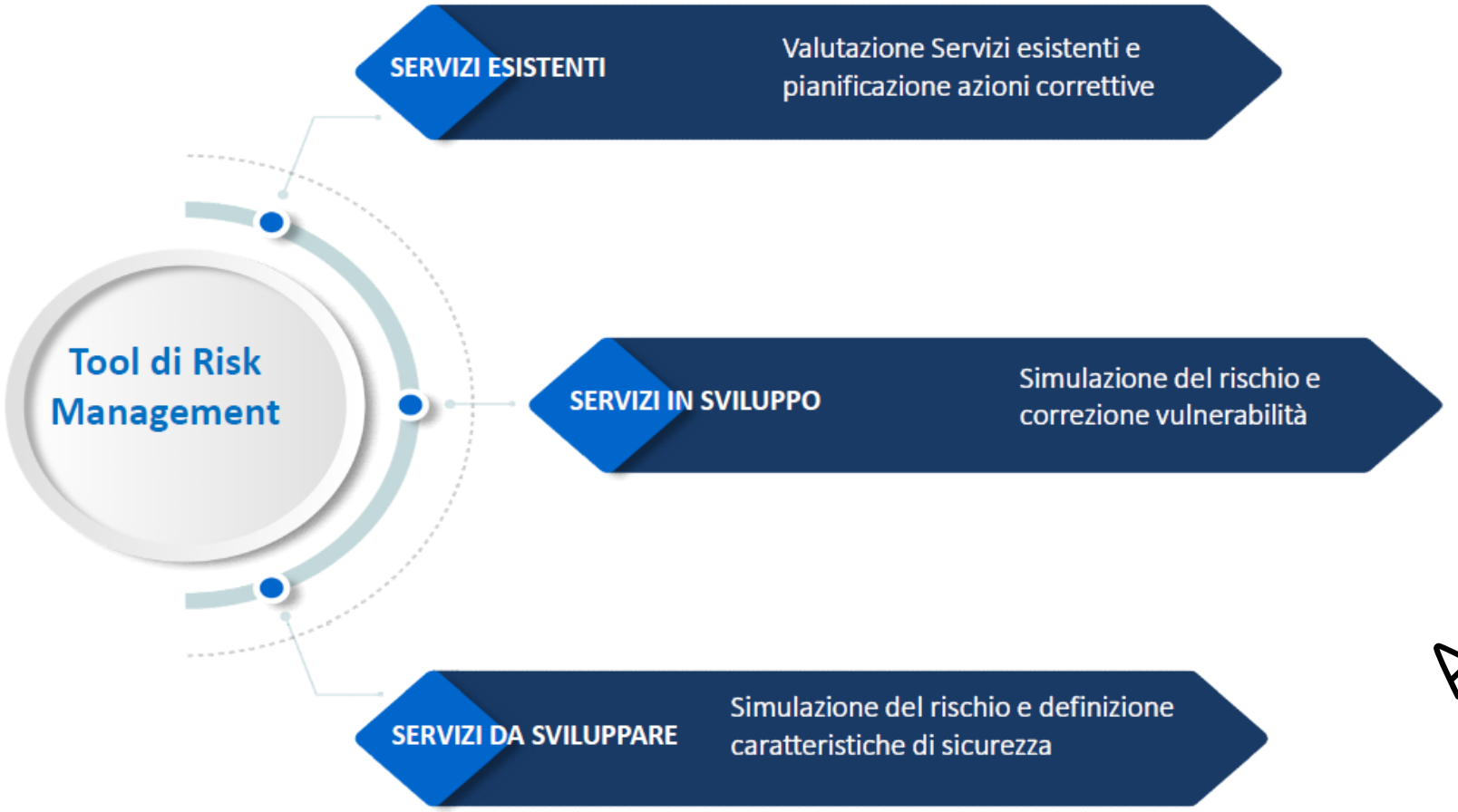
FASE DI ANALISI

- ❑ Identificazione dei rischi
- ❑ Simulazione degli effetti di mitigazione delle azioni
- ❑ Piano dei trattamenti

FASE OPERATIVA

VALUTAZIONE DELLE AZIONI DA METTERE IN CAMPO Orizzontale su tutta la PA o su singoli servizi

Tool di valutazione e trattamento del rischio cyber



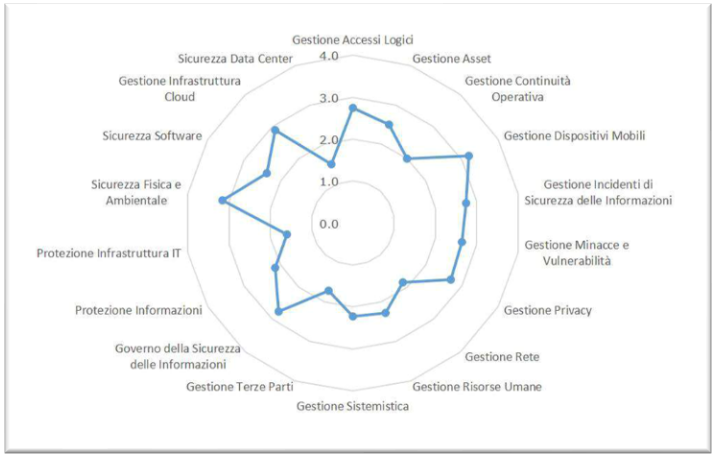
Ambiti di applicazione

Tool di valutazione e trattamento del rischio cyber

Al momento il tool non è fruibile perché è in fase di migrazione sul portale dell'Agenzia della Cybersicurezza Nazionale (www.acn.gov.it)

Inserimento delle informazioni

Grado di implementazione medio per ciascun dominio di sicurezza



Esempio di report – risultati analisi del rischio

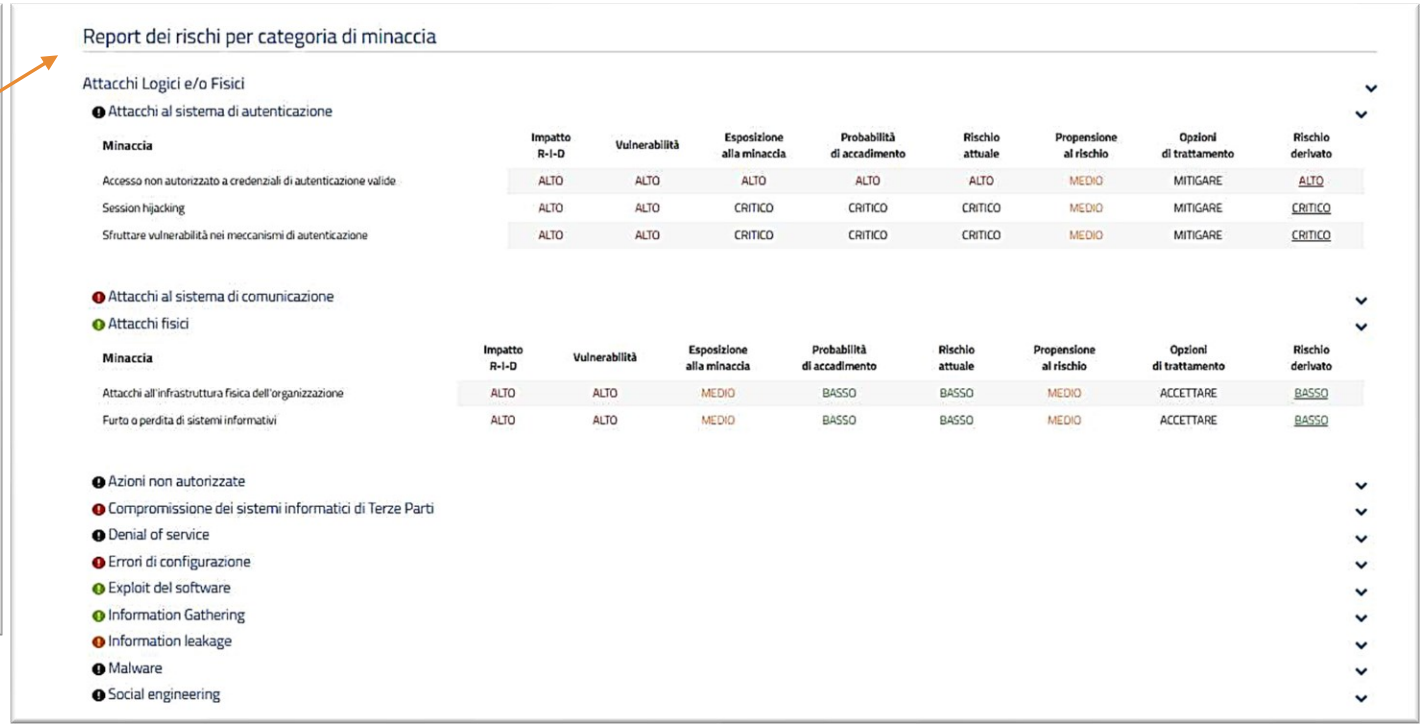
Per ciascuna categoria di minacce sono riportati i relativi livelli di rischio in base ai risultati dell'assessment

Distribuzione risposte per dominio di sicurezza

Gestione Accessi Logici	8/8
Gestione Asset	2/2
Gestione Continuità Operativa	2/2
Gestione Dispositivi Mobili	5/5
Gestione Incidenti di Sicurezza delle Informazioni	4/4
Gestione Infrastruttura Cloud	2/2
Gestione Minacce e Vulnerabilità	7/7
Gestione Privacy	18/18
Gestione Rete	9/9

Report dei rischi per categoria di minaccia

- Attacchi Logici e/o Fisici
- Minacce Ambientali
- Minacce Legali
- Utilizzo improprio e/o errori



Report dei rischi per categoria di minaccia

Attacchi Logici e/o Fisici

Attacchi al sistema di autenticazione

Minaccia	Impatto R-I-D	Vulnerabilità	Esposizione alla minaccia	Probabilità di accadimento	Rischio attuale	Propensione al rischio	Opzioni di trattamento	Rischio derivato
Accesso non autorizzato a credenziali di autenticazione valide	ALTO	ALTO	ALTO	ALTO	ALTO	MEDIO	MITIGARE	ALTO
Session hijacking	ALTO	ALTO	CRITICO	CRITICO	CRITICO	MEDIO	MITIGARE	CRITICO
Sfruttare vulnerabilità nei meccanismi di autenticazione	ALTO	ALTO	CRITICO	CRITICO	CRITICO	MEDIO	MITIGARE	CRITICO

Attacchi al sistema di comunicazione

Attacchi fisici

Minaccia	Impatto R-I-D	Vulnerabilità	Esposizione alla minaccia	Probabilità di accadimento	Rischio attuale	Propensione al rischio	Opzioni di trattamento	Rischio derivato
Attacchi all'infrastruttura fisica dell'organizzazione	ALTO	ALTO	MEDIO	BASSO	BASSO	MEDIO	ACCETTARE	BASSO
Furto o perdita di sistemi informativi	ALTO	ALTO	MEDIO	BASSO	BASSO	MEDIO	ACCETTARE	BASSO

Azioni non autorizzate

Compromissione dei sistemi informatici di Terze Parti

Denial of service

Errori di configurazione

Exploit del software

Information Gathering

Information leakage

Malware

Social engineering

Monitoraggio continuo del piano dei trattamenti

Misure minime di sicurezza

Allegato B – DPCM 14 aprile 2021, n. 81

Function	Misura
IDENTIFY	1. GESTIONE DEGLI ASSET (Asset Management) (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facility necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione. 2. GOVERNANCE (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity. 3. VALUTAZIONE DEL RISCHIO (Risk Assessment) (ID.RA): L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui. 4. STRATEGIA DELLA GESTIONE DEL RISCHIO (ID.RM): Le priorità e i requisiti dell'organizzazione e la tolleranza al rischio sono definiti e utilizzati per supportare le decisioni sul rischio operazionale. 5. GESTIONE DEL RISCHIO RELATIVO ALLA CATENA DI APPROVVIGIONAMENTO (ID.SC): Le priorità, i vincoli, le tolleranze al rischio e le ipotesi dell'organizzazione sono stabilite e utilizzate per supportare le decisioni di rischio associate alla gestione del rischio legato alla catena di approvvigionamento. L'organizzazione ha definito e implementato i processi atti a identificare, valutare e gestire il rischio legato alla catena di approvvigionamento.

Misure minime di sicurezza

Allegato B – DPCM 14 aprile 2021, n. 81

Function	Misura
PROTECT	1. GESTIONE DELLE IDENTITÀ, AUTENTICAZIONE E CONTROLLO DEGLI ACCESSI (PR.AC): L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate 2. CONSAPEVOLEZZA E ADDESTRAMENTO (PR.AT): Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti 3. SICUREZZA DEI DATI (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni. 4. PROCEDURE E PROCESSI PER LA PROTEZIONE DELLE INFORMAZIONI (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli asset. 5. MANUTENZIONE (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti. 6. TECNOLOGIE PER LA PROTEZIONE (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.

Misure minime di sicurezza

Allegato B – DPCM 14 aprile 2021, n. 81

Function	Misura
DETECT	1. ANOMALIE E EVENTI (DE.AE): Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato. 2. MONITORAGGIO CONTINUO PER LA SICUREZZA (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione. ... 3. PROCESSI DI RILEVAMENTO (DE.DP): Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.
RESPOND	1. PIANIFICAZIONE DELLA RISPOSTA (RS.RP): Procedure e processi di risposta sono eseguiti e mantenuti per assicurare una risposta agli incidenti di cybersecurity rilevati. 2. COMUNICAZIONE (RS.CO): Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine). 3. ANALISI (RS.AN): Vengono condotte analisi per assicurare un'efficace risposta e supporto alle attività di ripristino. 4. MITIGAZIONE (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i sui effetti e per risolvere l'incidente.
RECOVER	1. PIANIFICAZIONE DEL RIPRISTINO (RC.RP): I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity. 2. MIGLIORAMENTI (RC.IM): I piani di ripristino ed i relativi processi sono migliorati tenendo conto delle "lesson learned" per le attività future. 3. COMUNICAZIONE (RC.CO): Le attività di ripristino a seguito di un incidente sono coordinate con le parti interne ed esterne (es. le vittime, gli ISP, i proprietari dei sistemi attaccati, i vendor, i CERT/CSIRT).

Implementazione delle misure di sicurezza

Le misure devono essere implementate con tempi e priorità indicate nel Regolamento (DPCM 81).

Il DPCM prevede tre livelli di priorità:

ALTA interventi che permettono di ridurre sensibilmente uno dei tre fattori chiave del rischio cyber. Questi interventi sono prioritari e per loro natura sono da attuare indipendentemente dalla complessità realizzativa degli stessi

(entro sei mesi dalla data di trasmissione degli elenchi)

MEDIA interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber e che risultano generalmente anche di semplice implementazione

(entro trenta mesi dalla data di trasmissione degli elenchi)

BASSA interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber, ma la cui complessità realizzativa è generalmente considerata elevata (ad esempio cambiamenti organizzativi rilevanti e/o modifiche infrastrutturali significative.

Misure minime di sicurezza per la tutela delle informazioni (classificate)

Allegato C – DPCM 14 aprile 2021, n. 81

1. Trattamenti con l'ausilio di strumenti elettronici
   a) Identificazione degli utenti e gestione delle identità digitali;
   b) determinazione dei privilegi di accesso alle risorse da associare agli utenti e agli addetti o incaricati alla gestione o alla manutenzione;
   c) implementazione di un sistema di autenticazione e autorizzazione degli utenti secondo i privilegi individuati al punto precedente;
   d) protezione contro il software malevolo mediante l'impiego di software antimalware aggiornato;
   e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
   f) procedure di sicurezza per l'importazione e l'esportazione dei dati sui sistemi impiegati;
   g) procedure per la gestione della configurazione dei sistemi impiegati;
   h) procedure per la dismissione dei dispositivi di memorizzazione utilizzati sui sistemi impiegati;
   i) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
   j) adozione di tecniche di cifratura.

Processo di gestione degli incidenti

incidente, ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici

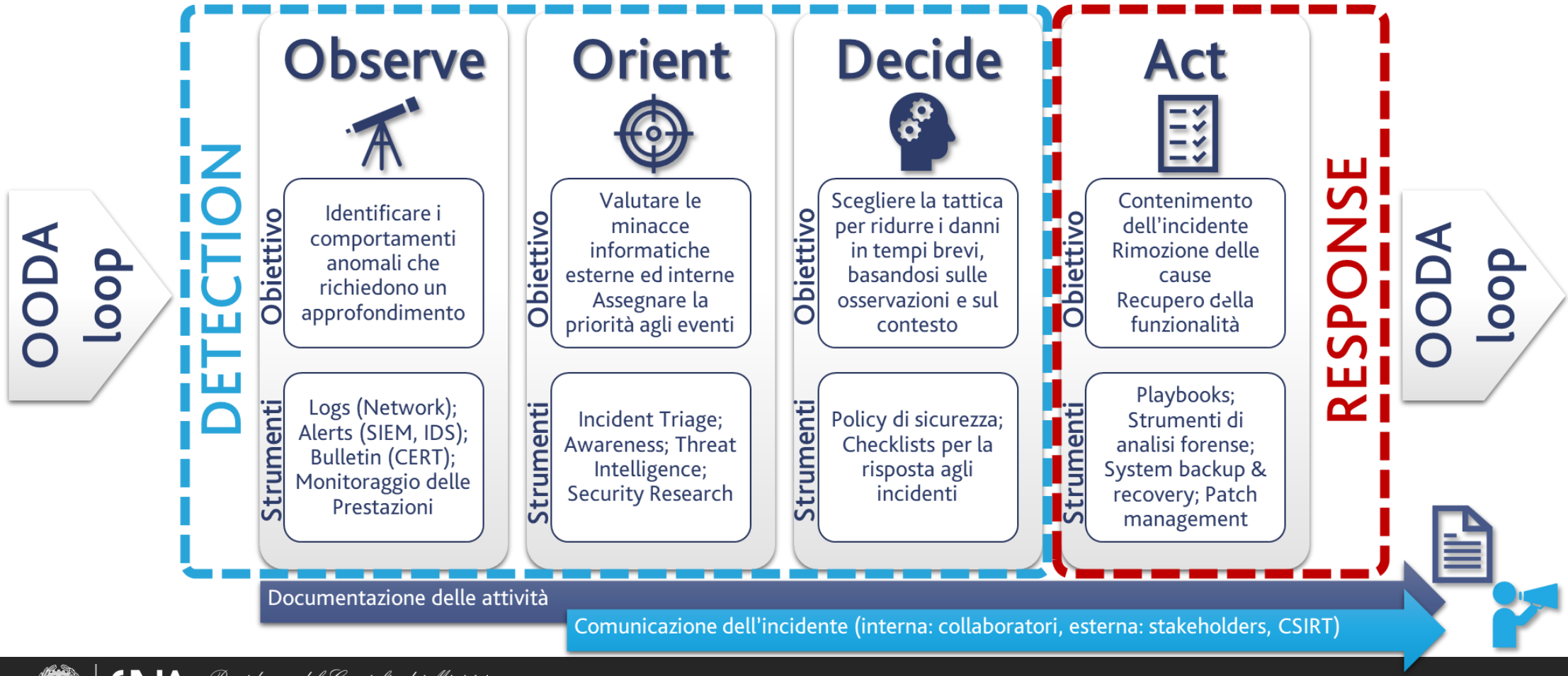
trattamento dell'incidente, tutte le procedure necessarie per l'identificazione, l'analisi e il contenimento di un incidente e l'intervento in caso di incidente

Prima: PREPARE
- PEOPLE: INCIDENT RESPONSE TEAM
- PROCESS: INCIDENT RESPONSE PLAN
- TECH: INCIDENT RESPONSE PLATFORM
- IMPROVEMENT PROGRAM

Durante: DETECT & RESPOND
- IDENTIFICAZIONE DELL'EVENTO
- CONTENIMENTO DEGLI EFFETTI
- RIMOZIONE DELLA MINACCIA
- RIPRISTINO DELL'OPERATIVITÀ

Dopo: FOLLOW UP
- DIGITAL FORENSICS
- ANALISI DELL'EVENTO
- LEZIONE DI APPRENDIMENTO
- CONDIVISIONE DEL CASO

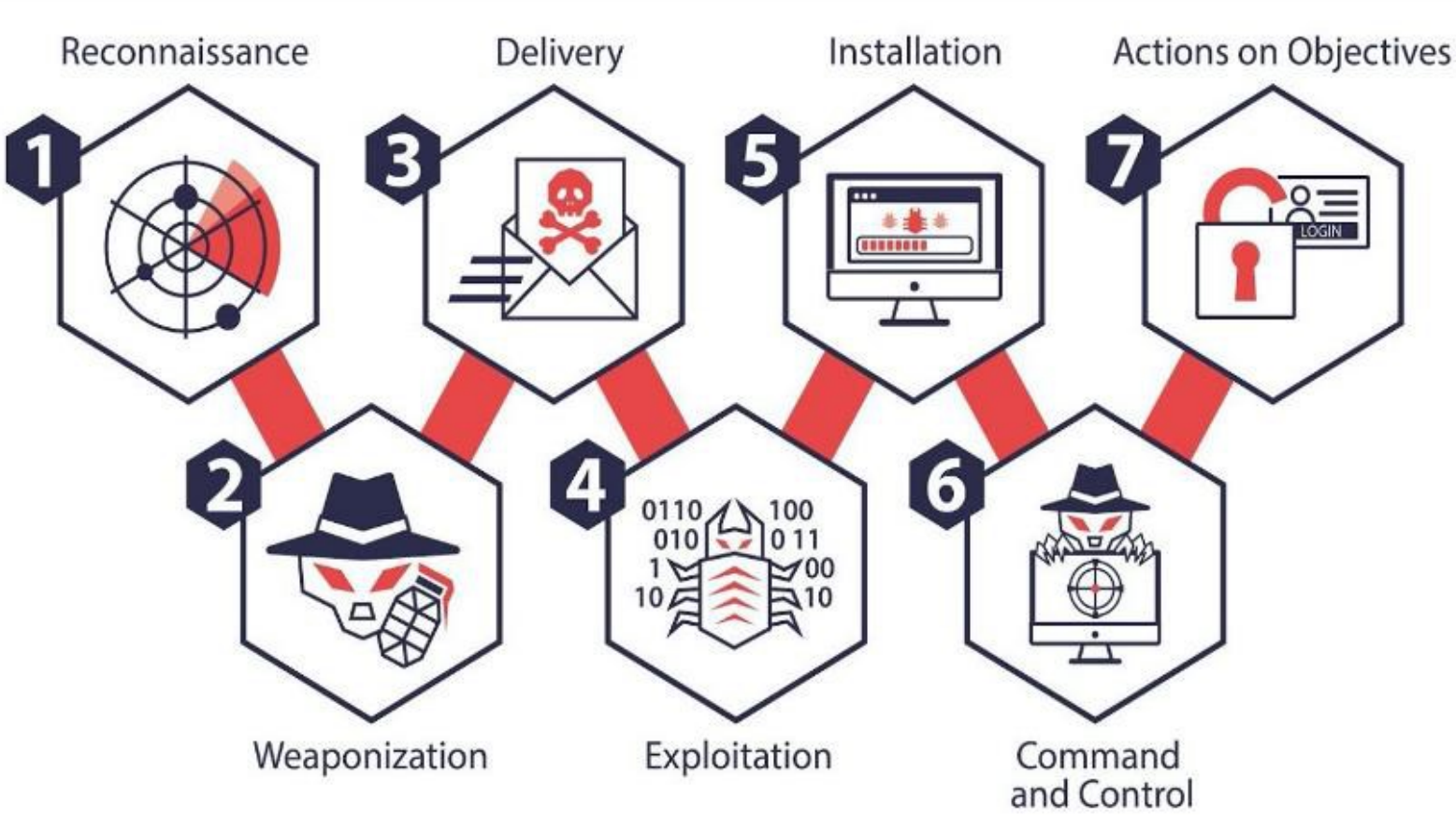
Processo di gestione degli incidenti



Cyber Kill Chain per la Detection

Rappresenta la sequenza di fasi di un attacco da parte di un attore malevolo

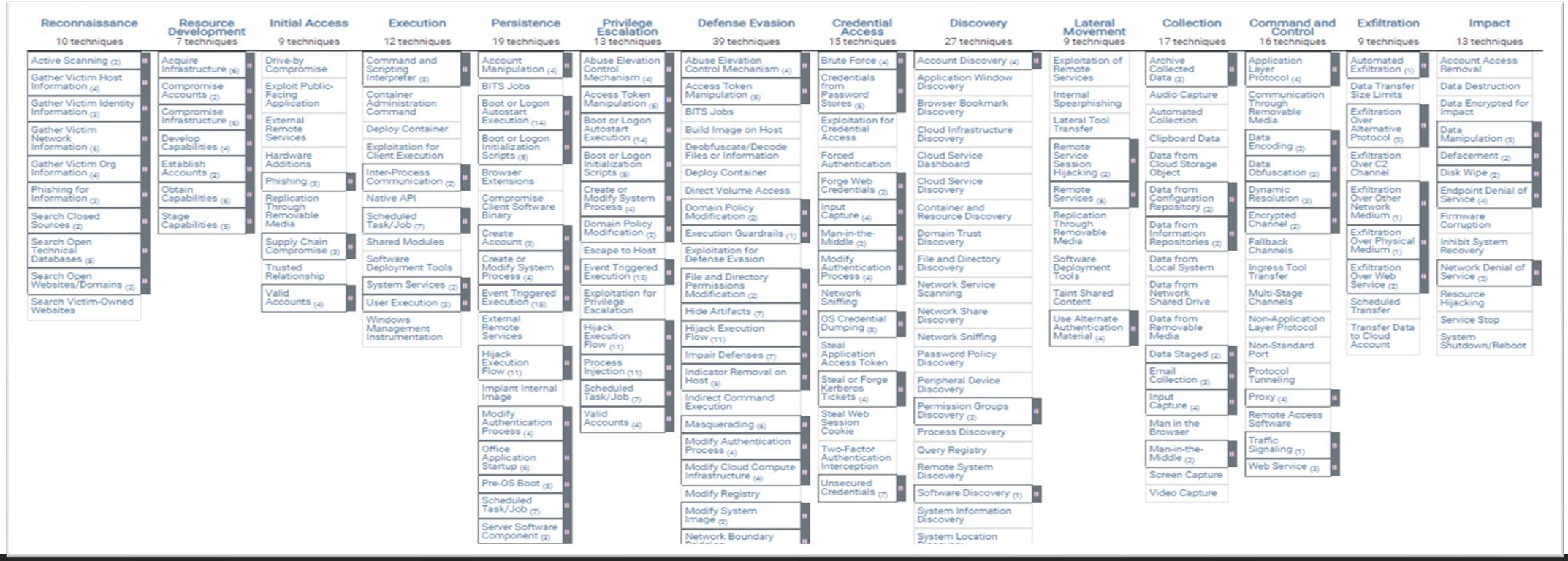
È utile per identificare le azioni prodromiche all'attacco



Prima si rileva l'attività malevola e prima si interrompere la catena di attacco

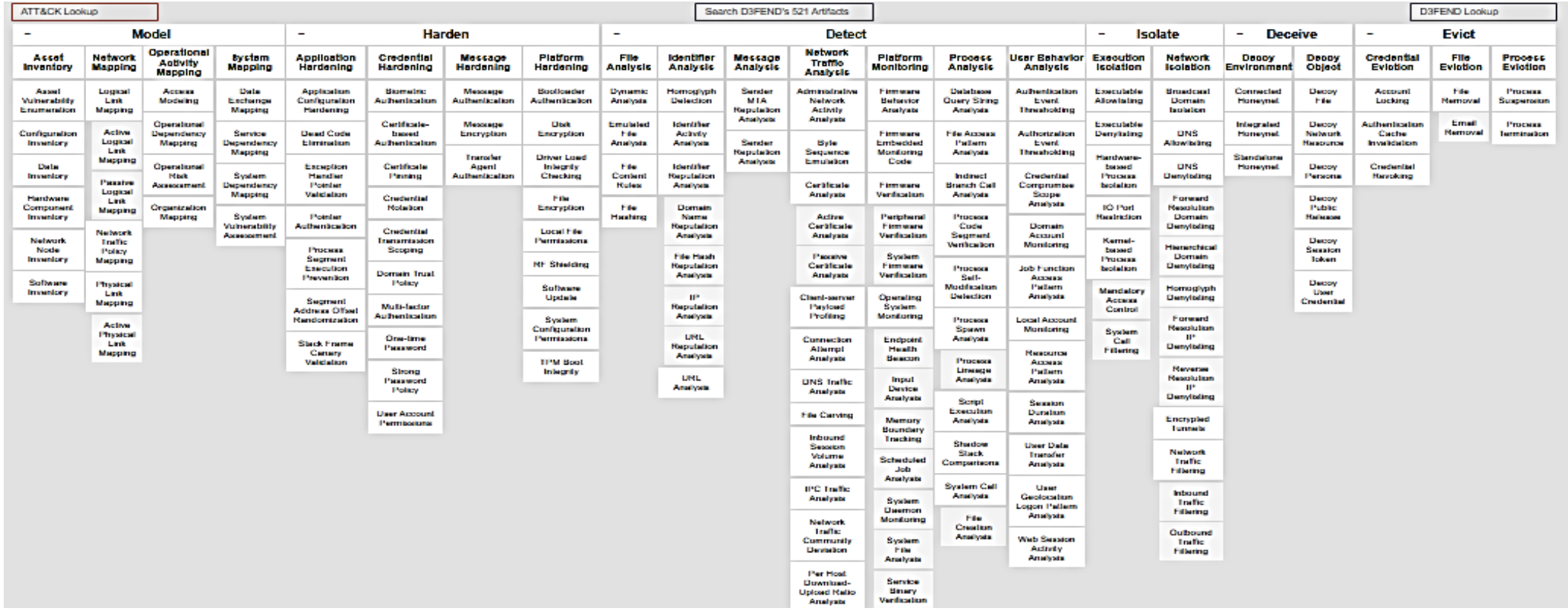
MITRE ATT&CK https://attack.mitre.org/

La matrice MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) è una risorsa di conoscenze di tattiche e tecniche di attacco basate su osservazioni del mondo reale.



MITRE DEFEND https://d3fend.mitre.org/

La matrice MITRE DEFEND è una risorsa di contromisure per la sicurezza informatica



Procedura di notifica degli incidenti

Dal 1° gennaio 2022, i soggetti inclusi nel perimetro, al verificarsi di uno degli incidenti avente impatto su un bene ICT di rispettiva pertinenza individuati nelle tabelle di cui all'allegato A del DPCM 14 aprile 2021, n. 81, procedono alla notifica al CSIRT italiano e per conoscenza all'Autorità competente NIS, senza giustificato ritardo.

Gli incidenti devono essere notificati obbligatoriamente:

- entro 6 ore quelli indicati nella tabella 1 allegato A DPCM 14 aprile 2021, n. 81
- entro 1 ora quelli indicati nella tabella 2 allegato A DPCM 14 aprile 2021, n. 81

I predetti termini decorrono dal momento in cui i soggetti inclusi nel perimetro sono venuti a conoscenza, a seguito delle evidenze ottenute, mediante le attività di monitoraggio, test e controllo.

I soggetti inclusi nel perimetro possono notificare, su base volontaria, gli incidenti non indicati nelle tabelle 1 e 2, così come anche i soggetti non inclusi nel perimetro possono notificare gli incidenti sempre su base volontaria.

Ricordarsi di effettuare la notifica al Garante per la privacy, nel caso in cui l'incidente abbia comportato la violazione dei dati personali, e di segnalare i fatti alle autorità di Pubblica Sicurezza nelle ipotesi di reato.

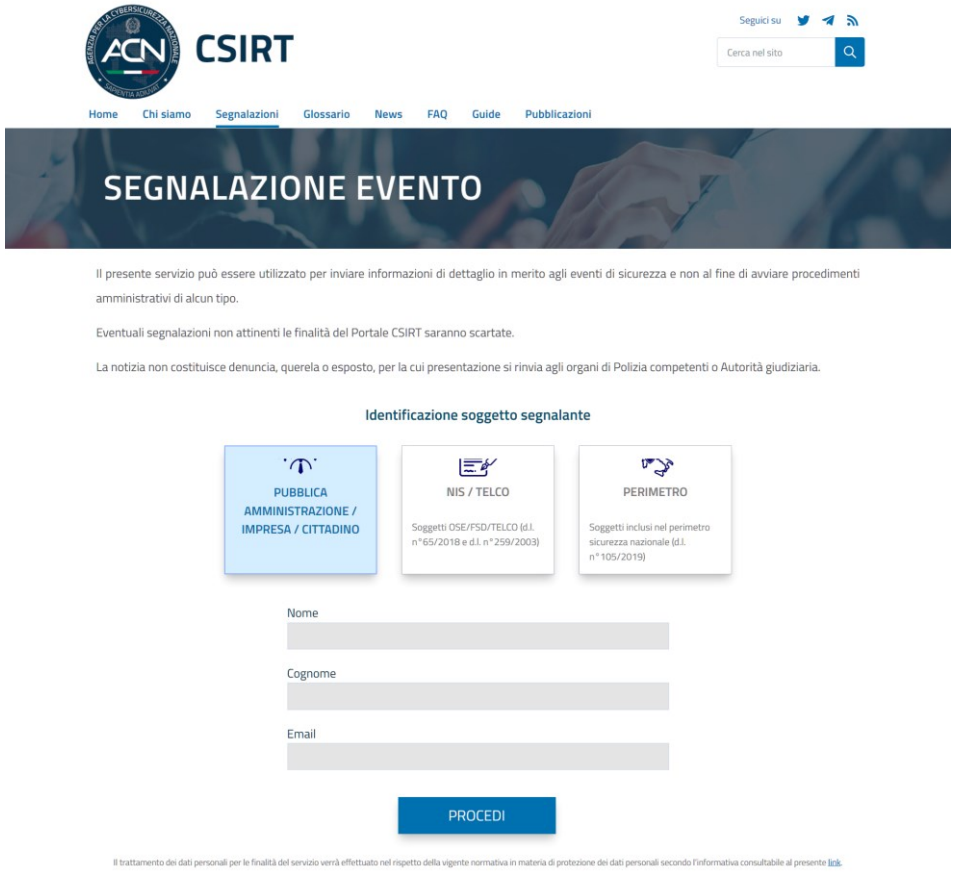
Tassonomia degli incidenti che debbono essere oggetto di notifica (All. A - DPCM 81)

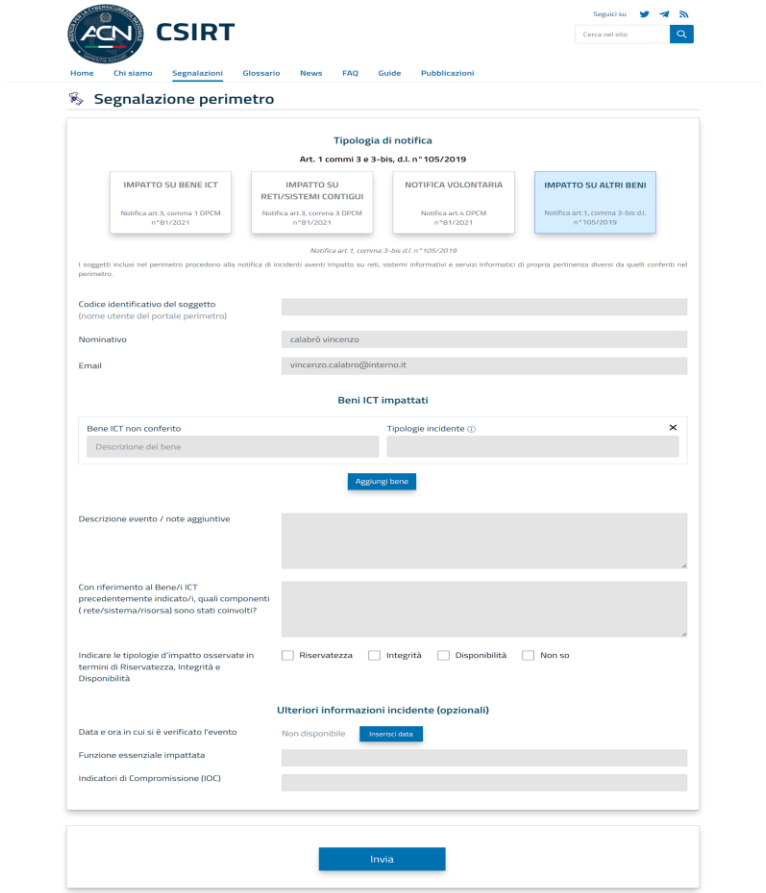
Tabella 1 (entro 6 ore)
Infezione (Initial exploitation): esecuzione non autorizzata di codice o malware
Guasto (Fault): violazione del servizio atteso, perdita di dati o delle chiavi
Installazione (Establish persistence): ottenimento di privilegi superiori, persistenza, evasione delle difese, command e control
Movimenti laterali (Lateral movement): esplorazione, raccolta credenziali, movimenti laterali
Azioni sugli obiettivi (Action on objects): raccolta e esfiltrazione dei dati

Tabella 2 (entro 1 ora)
Azioni sugli obiettivi (Action on objects): inibizione delle funzioni di risposta, compromissione dei processi di controllo, disservizio intenzionale
Disservizio (Failure): violazione del livello di servizio atteso, divulgazione di dati corrotti o esecuzione operazioni corrotte tramite il bene ICT, divulgazione non autorizzata di dati digitali relativi ai beni ICT

Come effettuare la segnalazione di incidente

https://www.csirt.gov.it → segnalazione evento





Decreto Legislativo 18 maggio 2018 , n. 65
Sanzioni amministrative

Salvo che il fatto costituisca reato,

1. l'operatore di servizi essenziali che non adotta le misure tecniche e organizzative adeguate e proporzionate per la gestione del rischio per la sicurezza della rete e dei sistemi informativi, ai sensi dell'articolo 12, comma 1, è soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro
2. l'operatore di servizi essenziali che non adotta le misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, ai sensi dell'articolo 12, comma 2, è soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro
3. l'operatore di servizio essenziale che non notifica al CSIRT italiano gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti, ai sensi dell'articolo 12, comma 5, è soggetto ad una sanzione amministrativa pecuniaria da 25.000 euro a 125.000 euro
4. l'operatore di servizio essenziale che non ottempera agli obblighi, ai sensi dell'articolo 13, comma 2, è soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro.
5. l'operatore di servizio essenziale che non osserva le istruzioni, ai sensi dell'articolo 13, comma 4, è soggetto ad una sanzione amministrativa pecuniaria da 15.000 euro a 150.000 euro
6. il fornitore di servizio digitale che non notifica al CSIRT italiano gli incidenti aventi un impatto rilevante sulla fornitura di un servizio fornito, ai sensi dell'articolo 14, comma 4, è soggetto ad una sanzione amministrativa pecuniaria da 25.000 euro a 125.000 euro.
7. l'operatore di servizi essenziali dipendente da terze parti che fornisce servizi digitali per la fornitura di un servizio che è indispensabile per il mantenimento di attività economiche e sociali fondamentali, che ometta la notifica, ai sensi dell'articolo 14, comma 9, è soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro
8. il fornitore di servizi digitali che non osserva gli obblighi ai sensi dell'articolo 15, comma 2, è soggetto ad una sanzione amministrativa pecuniaria da 12.000 euro a 120.000 euro

Codice in materia di protezione dei dati personali

PRINCIPALI ADEMPIMENTI

- Misure di sicurezza adeguate
  Il titolare del trattamento deve adottare misure tecniche e organizzative adeguate al fine di garantire, ed essere in grado di dimostrare, la conformità del trattamento al Regolamento, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Le dette misure debbono essere periodicamente riesaminate e aggiornate.
- Valutazione d'impatto sulla protezione dati
- Nomina di un Responsabile della Protezione dei Dati

NOTIFICHE E SANZIONI

Rientra tra gli obblighi del titolare anche la notifica all'autorità di controllo (Garante) senza ingiustificato ritardo - e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza -, di ogni violazione della sicurezza dei dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche.

In caso di violazione sono previste:

- Sanzioni per mancata attuazione delle misure
- Risarcimento danni ai titolari dei dati

E-procurement di beni, sistemi e servizi ICT

Nel corso degli ultimi anni è stato registrato un incremento di attacchi veicolati tramite la supply chain, ovvero tramite la compromissione di terze parti, il che consente poi a criminali e spie di colpire i contatti (clienti, fornitori, partner) dell'obiettivo, ampliando notevolmente il numero delle vittime e passando più facilmente inosservati perché sfruttano la fiducia conquistata da questi ultimi.

Per prevenire questo minaccia:

1. Sono state adottate Linee Guida – La sicurezza nel procurement ICT, Determinazione Agid n. 220/2020 del 17 maggio 2020, per definire indicazioni tecnico-amministrative al fine di garantire, all'interno delle procedure per l'approvvigionamento di beni e servizi informatici delle pubbliche amministrazioni, la rispondenza di questi ad adeguati livelli di sicurezza.

2. Gli operatori di servizi essenziali e i fornitori di servizi digitali prima di acquisire un bene, sistema e servizio da impiegare all'interno del perimetro di sicurezza nazionale cibernetica lo devono sottoporre ad un Centro di Valutazione.

Elenco di beni, sistemi e servizi da sottoporre al Centro di Valutazione prima dell'acquisizione

Componenti hardware e software che svolgono funzionalità e servizi di rete di telecomunicazione (accesso, trasporto, commutazione)

Router	Gateway Wifi
Switch	Ponte radio
Repeater	Optical transmission board
Bilanciatori di carico	Multiservice Provisioning Platform (MSPP)
Traffic shaper	Automotive ECU switch (Ethernet, CAN, LIN)
Proxy	IoT Edge Gateway
Access Network per reti radiomobili 2G, 3G, 4G, 5G	Network Function Virtualization (NFV): • vSwitch • vRouter • Application Function (5G)

Componenti hardware e software che svolgono funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati

Firewall	Security Gateway
Hardware Security Module (HSM)	Intrusion Detection System (IDS)
Intrusion Prevention System (IPS)	Network Function Virtualization (NFV) • Authentication Server Function (5G) • Whitelisting dei processi
Virtual Private Network	Trusted Platform Module

Applicativi software per l'implementazione di meccanismi di sicurezza

Applicazioni informatiche per la sicurezza • Public Key Infrastructure (PKI) • Single Sign-On (SSO) • Controllo Accessi	Moduli software che implementano Web Service mediante API, per protocolli di comunicazione

Componenti hardware e software per acquisizione dati, monitoraggio, supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali

Sistemi SCADA (Supervisory Control And Data Acquisition)	Sistemi Artificial Intelligence (AI) e Machine Learning (ML) per gestione reti/sistemi
Software Defined Network (SDN) Controller	Manufacturing Execution Systems (MES)
Management and Orchestration (MANO)	5G Mobile Edge Computing (MEC)
IoT orchestrator	NFV: • Network Slice Selection • Function (5G) • Application Function (5G) • Policy Control Function (5G) • Unified Data Management (5G) • Session Management Function (5G)

Prossimi sviluppi

- Con il d.P.R. 19 novembre 2021, n. 231 è stata istituita la Direzione centrale per la Polizia scientifica e sicurezza cibernetica presso il Dipartimento della Pubblica Sicurezza, per assolvere i compiti derivanti dall'essere il vertice amministrativo ed operativo della Polizia di Stato specializzata nel reprimere i cyber crime, nonché al ruolo di Autorità generale di contrasto affidatole dalla normativa europea NIS e dalla normativa sul Perimetro di sicurezza nazionale cibernetica, al cui interno opereranno:
  - Servizio polizia postale e per la sicurezza cibernetica per prevenire e contrastare gli attacchi informatici a infrastrutture critiche
    - i Centri Operativi per la Sicurezza Cibernetica (COSC) e le relative sezioni (SOSC)
    - il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) coordina i NOSC
  - Servizio per la sicurezza cibernetica del Ministero dell'Interno assicura la sicurezza delle reti, dei sistemi e delle infrastrutture
    - il Computer Emergency Response Team (CERT), incaricato di supportare le articolazioni ministeriali in caso di incidenti o attacchi informatici contro infrastrutture e reti dell'Amministrazione
    - il Centro Valutazioni (CV), incaricato di valutare, controllare e certificare le fornitura di beni e servizi ICT da impiegare nei sistemi e nelle infrastrutture informatiche del Ministero dell'Interno inclusi nel Perimetro di Sicurezza Nazionale Cibernetica
- Il 17 Gennaio 2022 sono state pubblicate due importanti Direttive dell'UE in tema di cyber resilience: la Direttiva CER (Critical Entities Resilience) e la Direttiva NIS2 (Network and information system security).

I Controlli Essenziali di Cybersecurity 1/2

Tematiche	Controlli Essenziali di Cybersecurity
Inventario dispositivi e software	1. Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro. 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 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.
Governance	5. Identificare e rispettare le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili
Protezione da malware	6. Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc…) regolarmente aggiornato.
Gestione password e account	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.

I Controlli Essenziali di Cybersecurity 2/2

Tematiche	Controlli Essenziali di Cybersecurity
Formazione e consapevolezza	10. Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti ICT (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, …). I vertici hanno cura di predisporre per tutto il personale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza.
Protezione dei dati	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.
Protezione delle reti	13. Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione).
Prevenzione e mitigazione	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.

Contatti

vincenzo.calabro@interno.it
www.vincenzocalabro.it

LinkedIn vincenzocalabro.it

Presidenza del Consiglio dei Ministri
SNA Scuola Nazionale dell'Amministrazione

who am i

Contatti

vincenzo.calabro@interno.it

www.vincenzocalabro.it

LinkedIn vincenzocalabro.it

Formazione

- laureato in ingegneria informatica (università la sapienza di roma) e sicurezza informatica (università di milano)
- specializzato in advanced cybersecurity (stanford university)
- certificato in cybersecurity engineering and software assurance e digital forensics (carnegie mellon university)

Esperienza professionale

- funzionario alla sicurezza cis (ministero dell'interno)
- consulente in sicurezza informatica e informatica forense
- professore a contratto di tecnologie per la sicurezza informatica
- relatore e autore sui temi della cybersecurity