POLIMI GRADUATE SCHOOL OF MANAGEMENT

Intelligenza artificiale: Come funziona, perché interessa, come si può utilizzare. I sistemi di intelligenza artificiale per la cyber security

LA GESTIONE DELLA SICUREZZA E DELLA PROTEZIONE DEI DATI

CENNI SULLE PRINCIPALI AZIONI POSTE IN ESSERE PRESSO IL MINISTERO DELL'INTERNO

AGENDA

1. CONTESTO ORGANIZZATIVO, TECNOLOGICO E NORMATIVO
2. CICLO DI VITA DELLA GESTIONE DELLA SICUREZZA
    - PRINCIPALI MINACCE
    - CONTROMISURE ADOTTATE
    - CRITICITÀ INCONTRATE
3. SVILUPPI IN CORSO
4. SINTESI

CHI SONO

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

Contatti

vincenzo.calabro@interno.it

www.vincenzocalabro.it

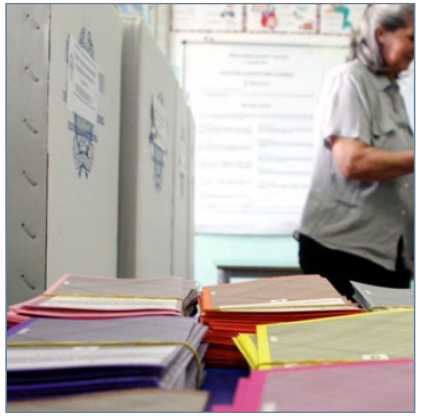
LinkedIn vincenzocalabro.it

CONTESTO ORGANIZZATIVO, TECNOLOGICO E NORMATIVO

Temi di competenza del Ministero dell'Interno

Cittadinanza e altri diritti civili

Elezioni e referendum



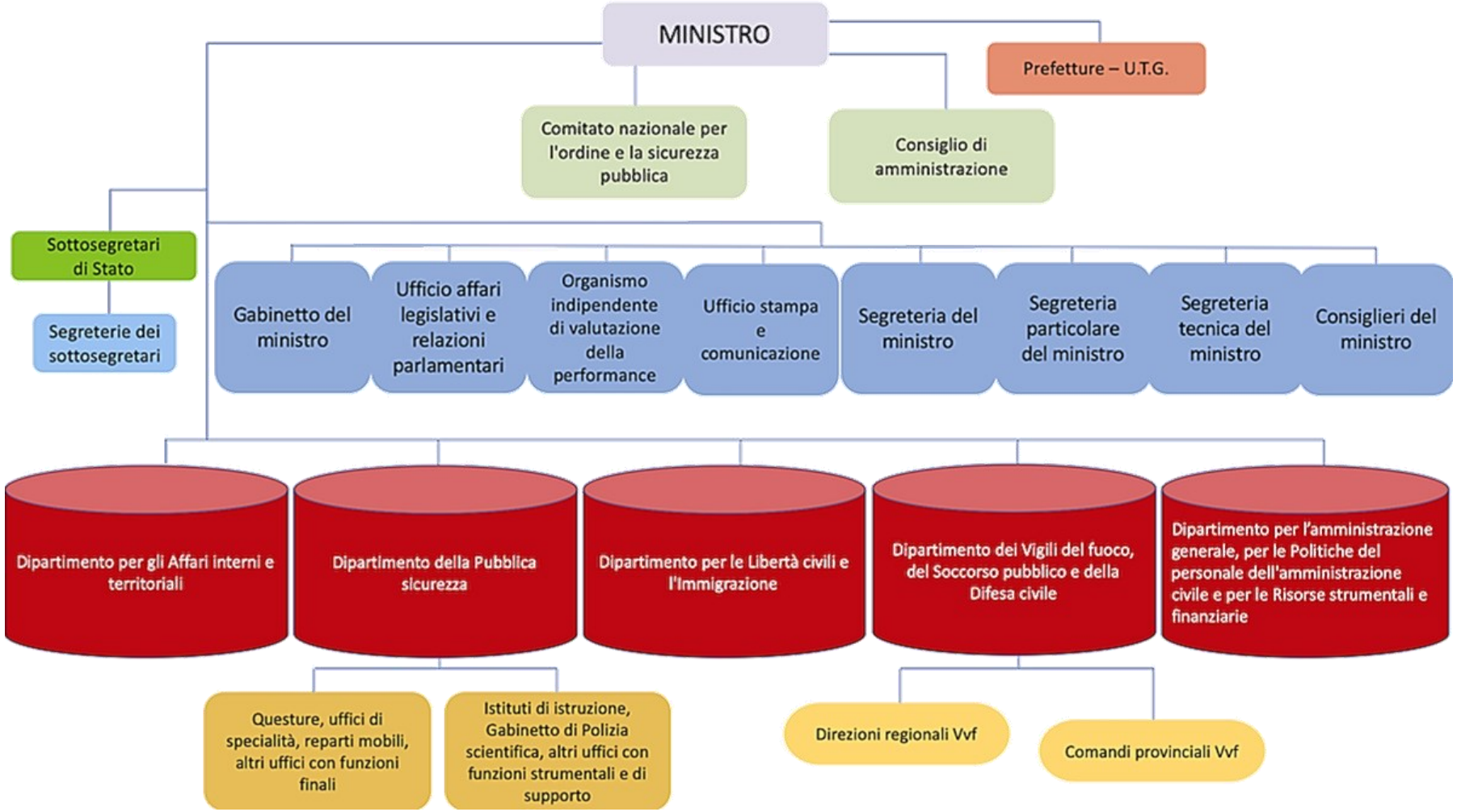
Prevenzione e soccorso

Sicurezza

Immigrazione e asilo

Territorio

Struttura organizzativa del Ministero dell'Interno



Inquadramento del Personale

Amministrazione civile

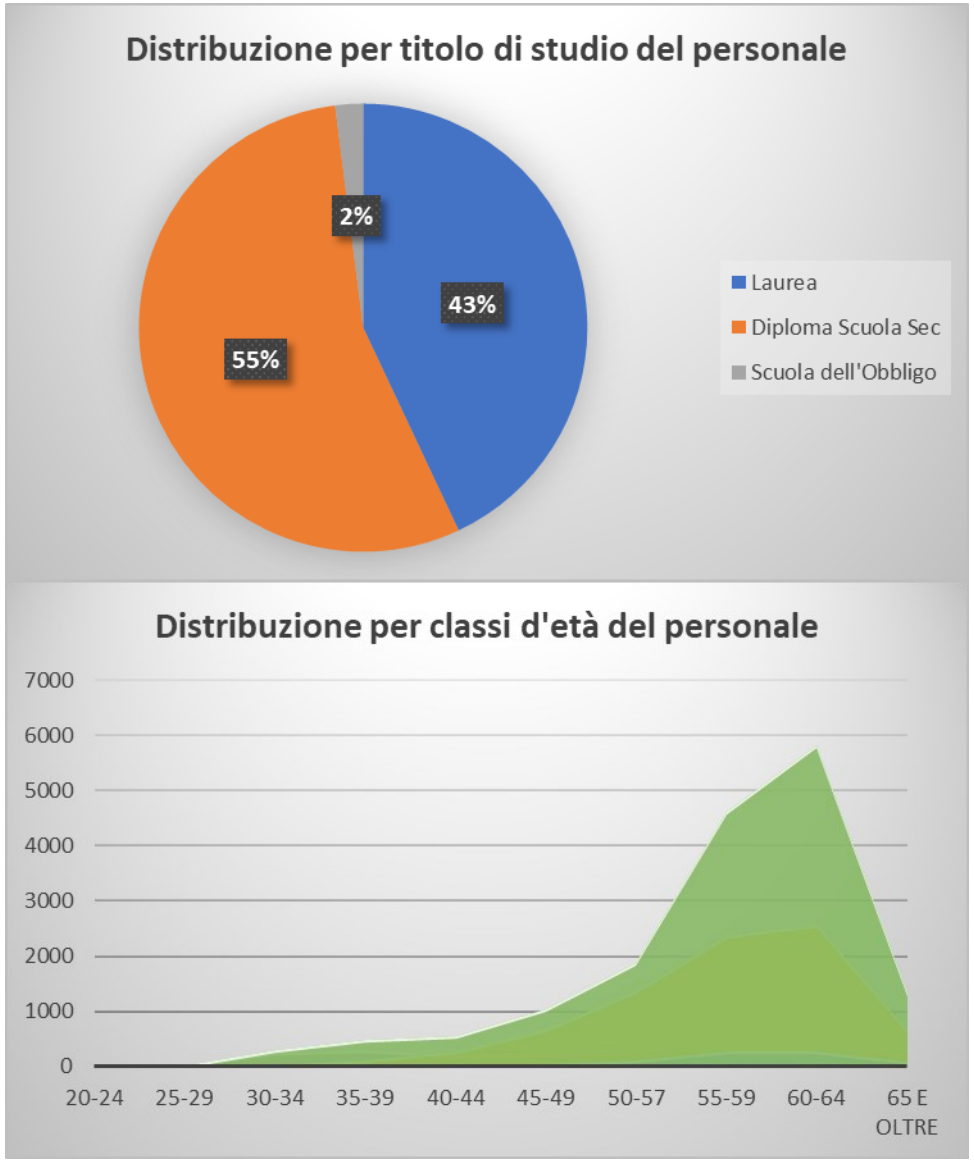
- **Corpo Prefettizio**
- **Personale Civile Dirigenziale**
- **Personale Civile non dirigenziale**

Polizia di Stato

- Carriera dei Funzionari
- Ruolo degli Ispettori
- Ruolo dei Sovrintendenti
- Ruolo degli Agenti e Assistenti
- Dirigente e Direttivo tecnico
- Ispettori, Sovrintendenti, Assistenti e Agenti tecnici

Corpo Nazionale dei Vigili del Fuoco

- Dirigenti e Direttivi con funzioni tecnico-operative
- Personale non dirigente e non direttivo con funzioni tecnico-operative
- Personale che espleta attività tecniche, amministrativo-contabili e tecnico-informatiche
- Personale Volontario



CONTESTO ORGANIZZATIVO, TECNOLOGICO E NORMATIVO

BD interne

- Protocollo informatico
- Licenze Polizia Amministrativa
- Gestione del personale
- Portale web
- Banca Dati Antimafia
- Antiracket e antiusura
- Elettorale
- Amministrazioni locali
- Revisori dei conti
- Anagrafe Nazionale Popolazione Residente
- Cittadinanza
- Immigrazione
- Flussi stagionali
- Sistema Informativo Sanzionatorio Amministrativo (codice strada, assegni e altre dep.)
- Gestione ruoli
- ...

BD interoperabili

- Camera di commercio
- Sistema di indagine (S.d.i.)
- Casellario giudiziario
- Centrale dei Rischi (CR)
- Sistema Visti
- ...

DB esterne

- Sistema per la gestione integrata della contabilità economica e finanziaria
- Servizi Anticorruzione
- Servizi CONSIP
- Servizi INPS (DURC, Visite mediche)
- Anagrafe tributaria
- Cartelle esattoriali (Agenzia Riscossione)
- Patenti di servizio
- PRA – alienazione veicoli
- Sistema informativo motorizzazione
- Sistema informativo veicoli sequestrati
- Telemaco
- VerifichePA
- ...

Normativa in tema di sicurezza informatica e protezione dei dati applicabile al Ministero dell'Interno

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

Misure tecniche e organizzative, ai sensi dell'art. 32 del Regolamento Generale sulla Protezione dei Dati, **per il trattamento dei dati personali**

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**)

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"

CICLO DI VITA DELLA GESTIONE DELLA SICUREZZA

CICLO DI VITA DELLA GESTIONE DELLA SICUREZZA

Obblighi normativi

+

Misure tecniche e organizzative per ridurre il rischio

→

Sicurezza Informatica e Protezione dei Dati

- Confidenzialità
- Integrità
- Disponibilità
- Resilienza

→

Security is a process, not a product → Continuous Improvement Process

TIMELINE DELLE PRINCIPALI NORMATIVE IN TEMA DI GESTIONE DELLA SICUREZZA E DELLA PROTEZIONE DEI DATI

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

- Misure minime di sicurezza per trattamento dati

Direttiva Ministeriale 16 gennaio 2002 «Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni»

- Allegato 2: iniziative per posizionarsi sulla "base minima di sicurezza"

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

- Disciplinare tecnico in materia di misure minime di sicurezza

Direttiva PCM 1 agosto 2015 «Direttiva impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici»

- Circolare AGID 2/2017 Misure Minime di Sicurezza ICT per la Pubblica Amministrazione

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.»

DPCM 1 30 luglio 2020, n. 131, «Regolamento in materia di 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»
DPCM 3 15 giugno 2021, «Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica»
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»

PRINCIPALI MINACCE E CONTROMISURE ADOTTATE

Prima della connessione della rete Ministeriale alla rete Internet

PRINCIPALI MINACCE	CONTROMISURE ADOTTATE
Insider Threats • Accesso abusivo/non autorizzato • Sottrazione di dati • Cancellazione di dati • Diffusione di malware • Danneggiamento dei sistemi	• Credenziali personali • Log management • Backup sicuri • Antivirus endpoint • Lettera di Responsabilità
Danni Accidentali/Involontari • Guasti hardware • Errata configurazione dei sistemi • Malfunzionamento dei software	• Ridondanza dei dischi • Hardening dei sistemi • Aggiornamento dei sistemi

Criticità riscontrate:

- Condivisione delle credenziali d'accesso
- Sfiducia negli strumenti ICT
- Scarsa responsabilità sul dato digitale

PRINCIPALI MINACCE E CONTROMISURE ADOTTATE

Dopo la connessione della rete Ministeriale alla rete Internet

PRINCIPALI MINACCE	CONTROMISURE ADOTTATE
Minacce dal WEB/Posta elettronica • Phishing • Diffusione Malware • Diffusione dei dati • Furto identità (mail)	• Anti-spam/Anti-phising • Proxing con filtraggio traffico • Implementazione di policy e finalità di utilizzo • Formazione sul corretto utilizzo dei servizi web
Minacce sul portale WEB • Defacement • Denied of service	• Controllo integrità dei dati • Ridondanza e bilanciamento
Accesso abusivo dalla Rete	• DMZ e monitoring

Criticità riscontrate:

- Resistenza all'accettazione delle policy WEB
- Eccessiva fiducia nei sistemi di sicurezza (anti-spam, anti-phishing, anti-malware)
- Inconsapevolezza del proprio ruolo per la sicurezza dei dati

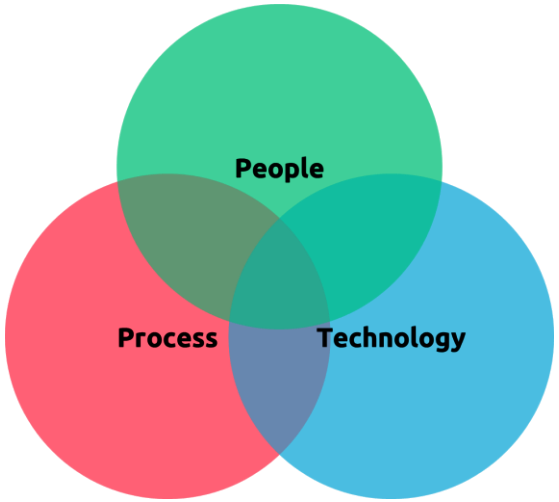
MISURE MINIME DI SICUREZZA ICT E TRATTAMENTO DATI

Sono emanate alcune misure minime di sicurezza, un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti.

- Misure adeguate di sicurezza (Legge 675/1996)
- Misure minime di sicurezza per trattamento dati personali (DPR 318/1999)
- Disciplinare tecnico in materia di misure minime di sicurezza (D.LGS. 196/2003)
- Misure minime di sicurezza ICT per le pubbliche amministrazioni (Circolare AgID n. 2/2017)

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

Misure minime di sicurezza Dati Personali
SISTEMA DI AUTENTICAZIONE INFORMATICA
SISTEMA DI AUTORIZZAZIONE
AGGIORNAMENTO DELLA LISTA DEGLI INCARICATI E DEI PROFILI DI AUTORIZZAZIONE
ATTIVAZIONE DI STRUMENTI ANTI-INTRUSIONE E ANTI-MALWARE
AGGIORNAMENTO DEI SOFTWARE
BACKUP DEI DATI
DOCUMENTO PROGRAMMATICO SULLA SICUREZZA



Misure minime di sicurezza ICT - 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

PRINCIPALI MINACCE E CONTROMISURE ADOTTATE

Con l'entrata in vigore del Codice in materia di protezione dei dati personali sono adottate le seguenti misure

PRINCIPALI MINACCE	CONTROMISURE ADOTTATE
Gestione debole delle credenziali	Single Sign-On (SSO) Complessità delle password Scadenza obbligatoria Diversificazione dei ruoli
Obsolescenza dei software	Deployment delle versioni più aggiornate dei sistemi oper.
Obsolescenza dei sistemi antivirus	Deployment degli aggiornamenti con cadenza settimanale
Esfiltrazione dei dati sensibili	Segmentazione dei dati e utilizzo della crittografia
Perdita dei dati sensibili	Backup specifici e differenziati

Criticità riscontrate:

- Difficoltà nella gestione delle credenziali
- Onerosità nella gestione dei dati sensibili

PRINCIPALI MINACCE E CONTROMISURE ADOTTATE

Con l'avvio dei servizi web e del lavoro a distanza sono adottate le seguenti misure per contrastare le minacce

PRINCIPALI MINACCE	CONTROMISURE ADOTTATE
Distributed Denial of Service (DDoS) Botnet	Content Delivery Network (CDN) Adozione del cloud
Advanced Persistent Threat (APT)	Cyber Threat Intelligence
Movimenti Laterali Insider Threat	User Behavior Analytics (UBA)
Smart Working Phishing Social Enginnering	Identity Access Management (IAM) Multi Factor Authentication (MFA) Approccio Zero Trust

Criticità riscontrate:

- Differenziazione tra le funzionalità in presenza e a distanza
- Insofferenza all'accettazione del Multi Factor Authentication

PRINCIPALI MINACCE E CONTROMISURE ADOTTATE

Con la pubblicazione delle Misure Minime di Sicurezza ICT per la Pubblica Amministrazione sono intraprese ulteriori azioni

PRINCIPALI MINACCE	CONTROMISURE ADOTTATE
Dispositivi non autorizzati	Inventario dei dispositivi (active directory) NO DHCP
Software non autorizzati	Inventario dei software (sccm) Distribuzione Configurazioni Standard
Software vulnerabili	Implementazioni policy aggiornamento
Utenze con permessi «admin»	Riduzione Utenze Privilegiate
Malware	Implementazione sistema anti-malware centralizzato
Ransomware	Backup sicuri e copie shadow

Criticità riscontrate:

- Malcontento di alcuni utenti per la riduzione privilegi
- Fondi insufficienti per aggiornare i sistemi obsoleti

DALLA SICUREZZA INFORMATICA ALLA CYBER RESILIENCE

SICUREZZA INFORMATICA

- Storicamente è stato adottato un approccio «addizionale» o «a silos» nei confronti della sicurezza informatica.

APPROCCIO OLISTICO

- Poi è mutato l'orientamento, diventando «trans-disciplinare», perché la sicurezza impatta con tutte le componenti di un'organizzazione (dati, persone, procedure, infrastrutture, asset, processi, procedure, sistemi di controllo, organizzazione e governance) e richiede un approccio «olistico».

GOVERNANCE DELLE SICUREZZA

- Successivamente, ci si è resi conto che 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.

CYBER RESILIENCE

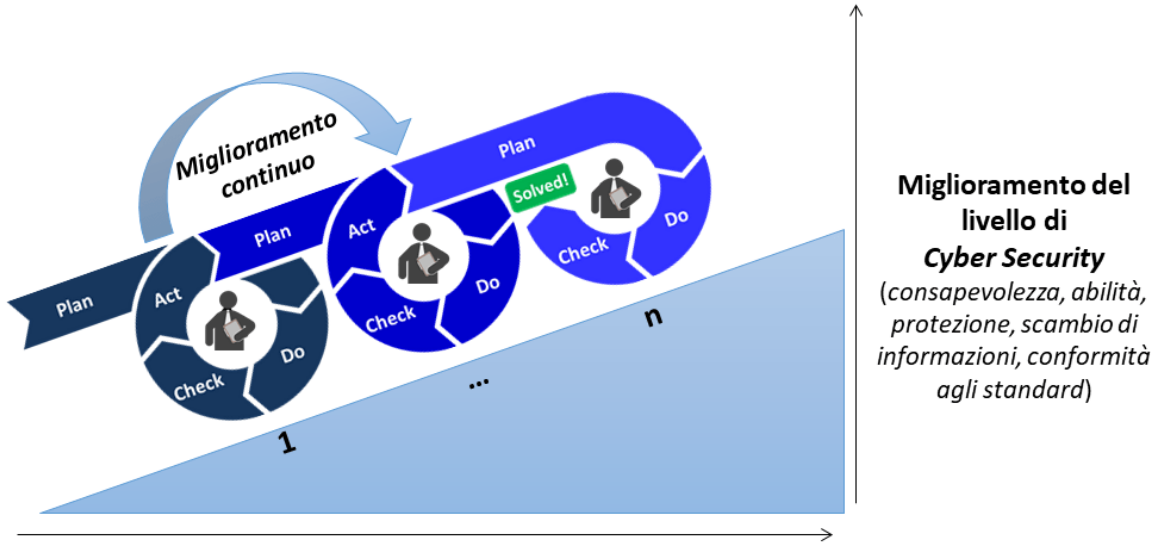
- Gli incidenti informatici sono complessi e inevitabili, pertanto agli obiettivi fondamentali («disponibilità», «confidenzialità» e «integrità») si affianca la «resilienza», ovvero la capacità di adattarsi al contesto e resistere alle minacce in modo da garantire l'erogazione dei servizi (continuità operativa).

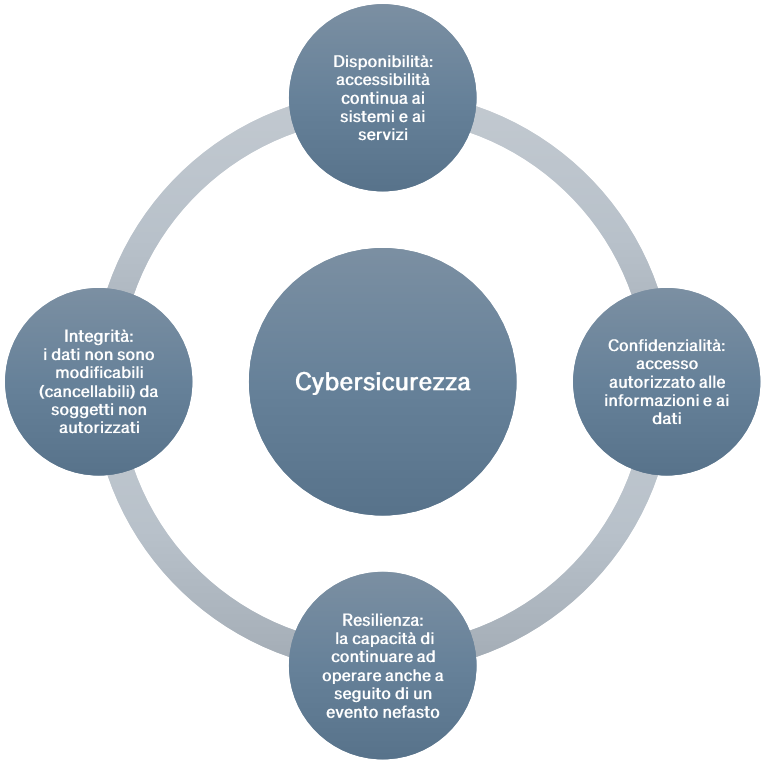
SVILUPPI IN CORSO

NUOVO APPROCCIO AL SICUREZZA INFORMATICA

L'esperienza maturata in ambito cyber ed il livello di maturità raggiunto ha consentito di individuare 6 obiettivi da perseguire:

1. **Improvement:** la sicurezza è un processo di miglioramento continuo
2. **Accountability:** la sicurezza ha una responsabilità certa
3. **Assessment:** non si può gestire ciò che non si può misurare
4. **Awareness:** la sicurezza è un obiettivo di tutta l'organizzazione
5. **Sharing:** la sicurezza trae benefici dalla condivisione delle informazioni e lo scambio di dati
6. **Resilience:** la sicurezza, oltre a garantire la riservatezza, l'integrità e la disponibilità dei dati, deve assicurare la resilienza agli attacchi, ovvero la capacità a erogare servizi





MISURE TECNICHE E ORGANIZZATIVE PER GLI ENTI CHE RIENTRANO DEL PERIMETRO

Il Regolamento in materia di perimetro di sicurezza nazionale cibernetica (DPCM 30 luglio 2020, n. 131, art. 3, comma 2, lett. A):

- **Include per il settore interno**, il Ministero dell'interno, nell'ambito delle attribuzioni di cui all'articolo 14 del decreto legislativo 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.

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

- **progettare misure tecniche per gestire i rischi informatici**
- **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**

MISURE TECNICHE E ORGANIZZATIVE PER GLI ENTI CHE RIENTRANO DEL PERIMETRO

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 art. 12 e 13 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.

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.

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

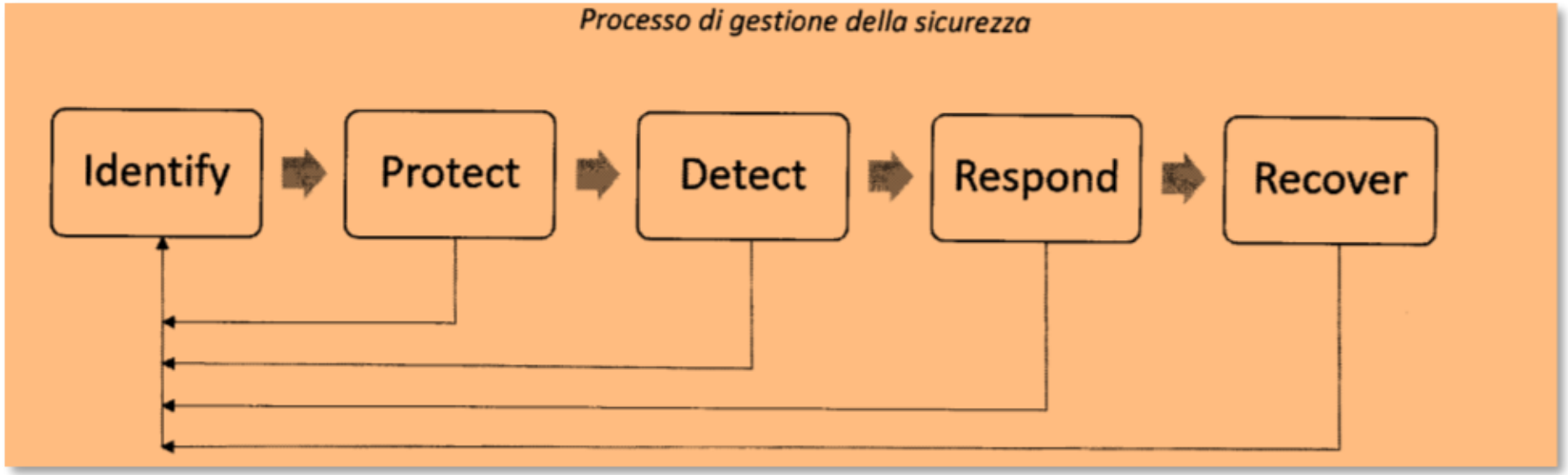
Le indicazioni si basano sul Framework Nazionale per la Cybersecurity e la Data Protection
(ispirato al Cybersecurity Framework del NIST)

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, costituiscono le principali tematiche per operare un'adeguata gestione del rischio cyber.

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



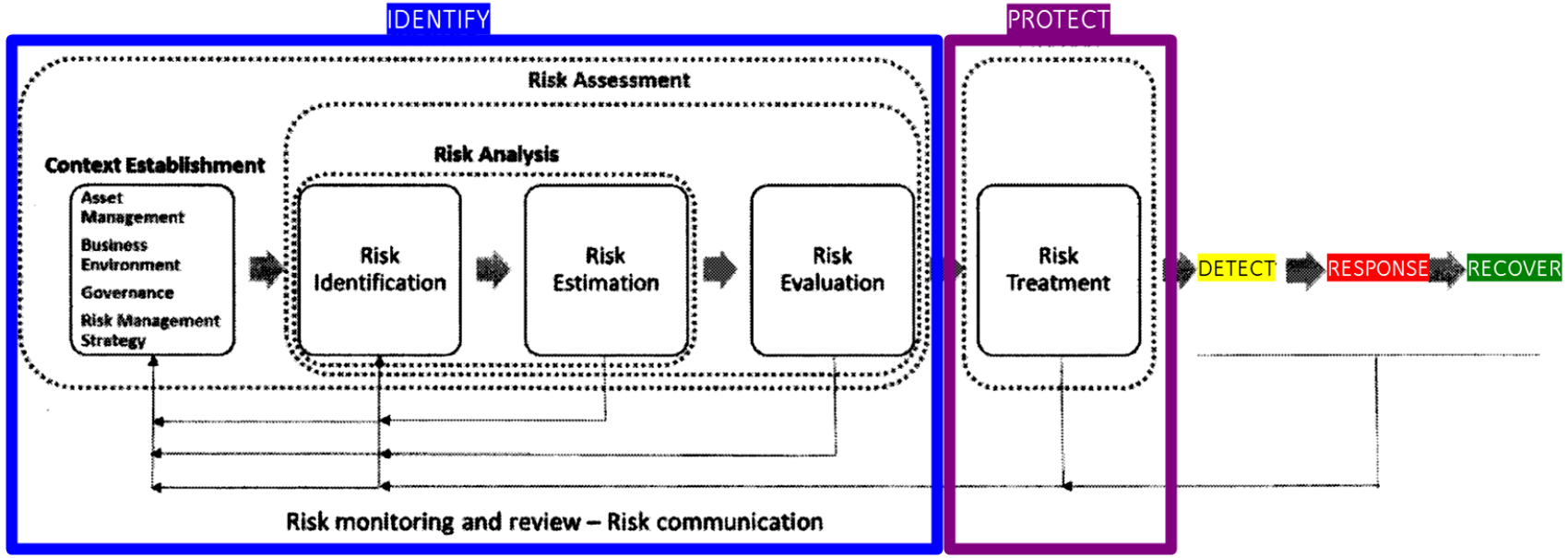
PROCESSO DI GESTIONE DELLA SICUREZZA

	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.

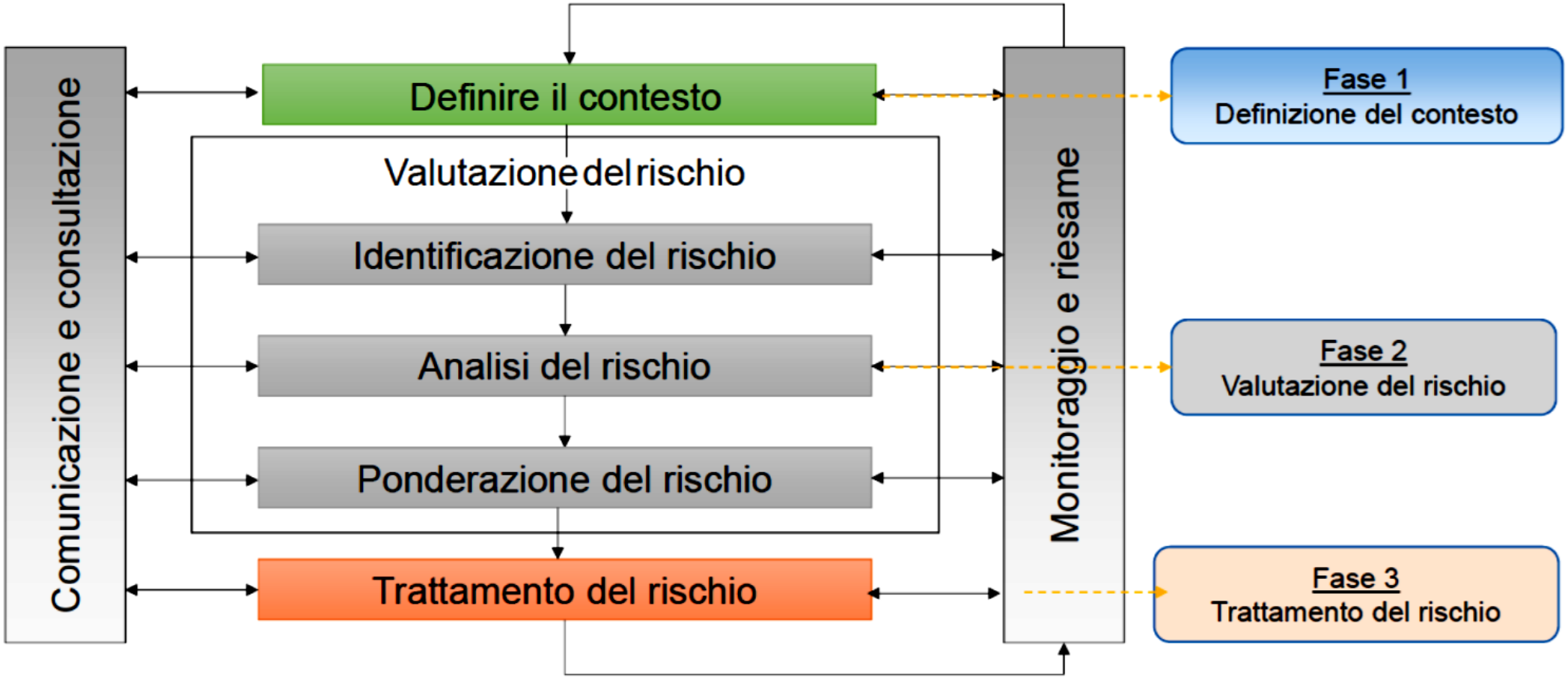
PROCESSO DI GESTIONE DEI RISCHI

L'implementazione del processo deve 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.



METODOLOGIA DI CYBERSECURITY RISK MANAGEMENT



MACRO-MODELLO DI CALCOLO DEL RISCHIO

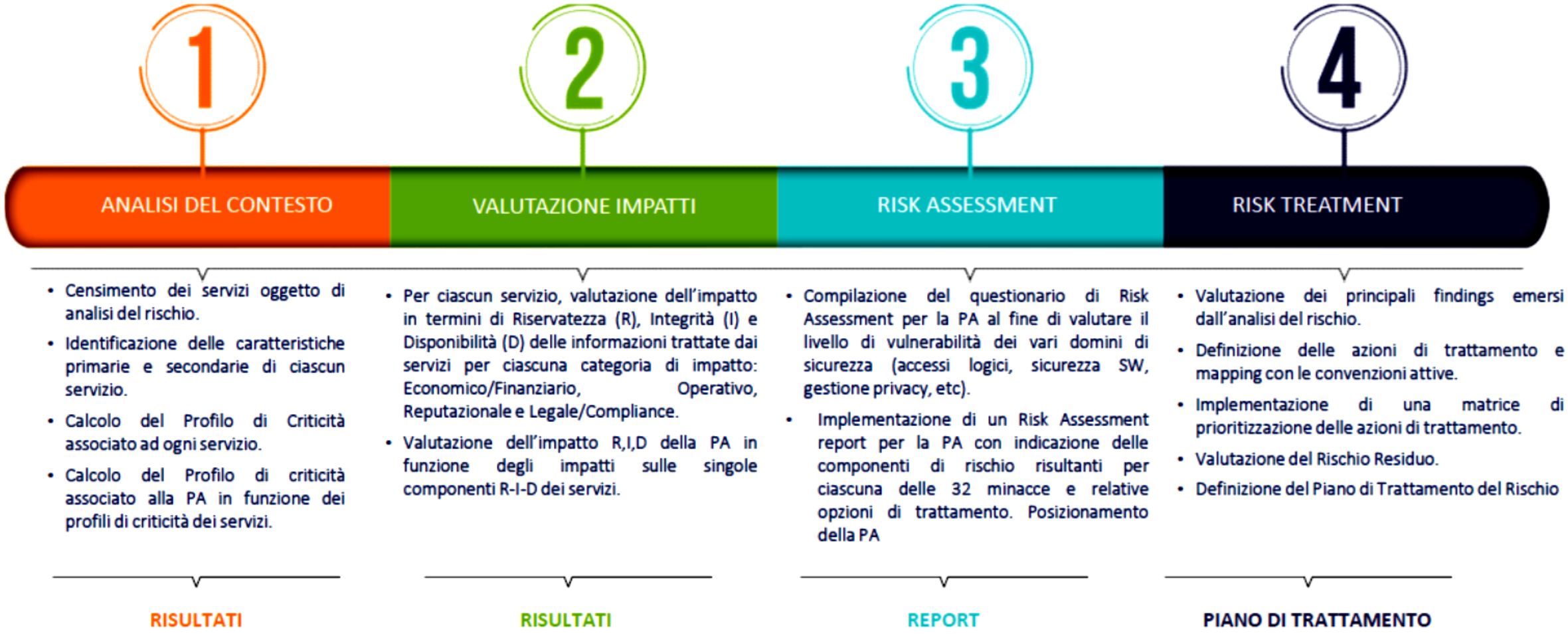
CARATTERISTICHE SERVIZI
A seconda delle caratteristiche primarie dei servizi erogati, è determinato il livello di criticità intrinseca (Profilo di Criticità) della PA. Le caratteristiche primarie e secondarie consentono di selezionare le Misure di Sicurezza da implementare (controlli di tipo amministrativo,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

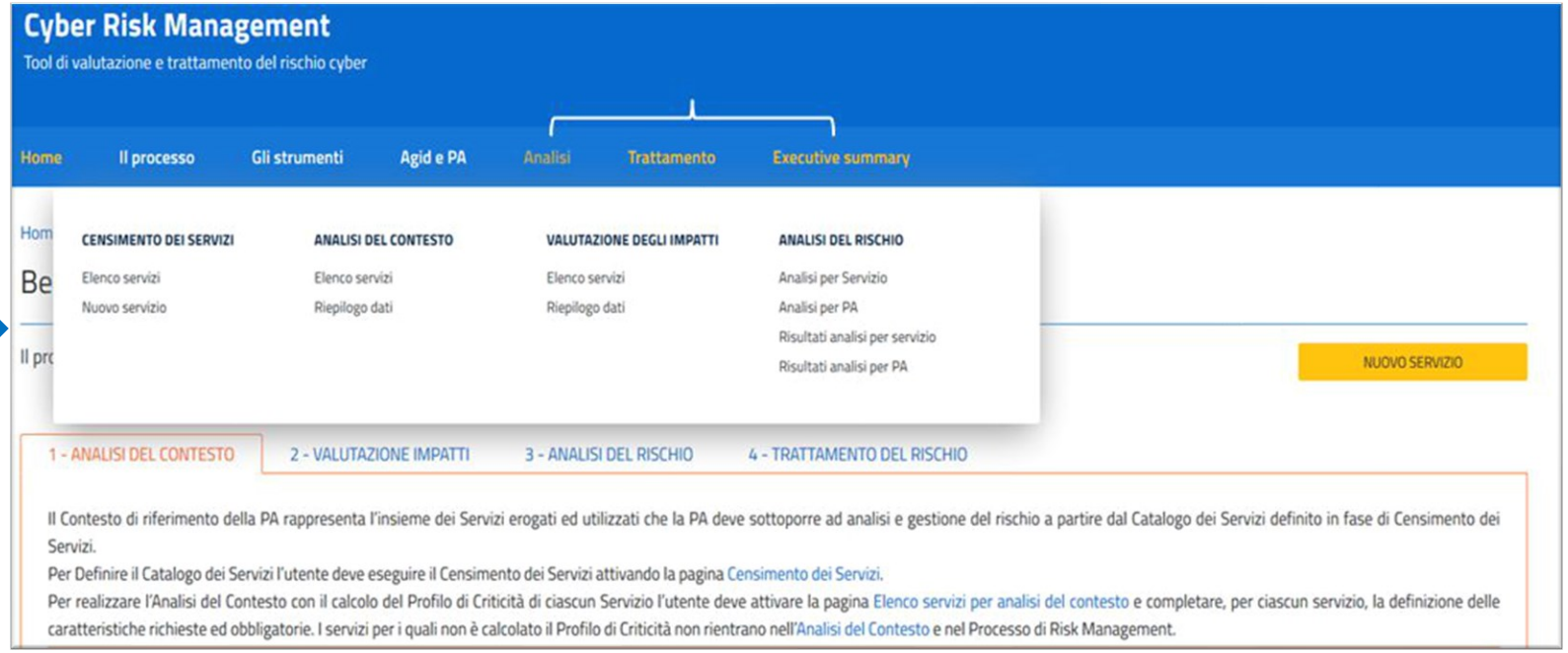
MACRO-MODELLO DI CALCOLO DEL RISCHIO



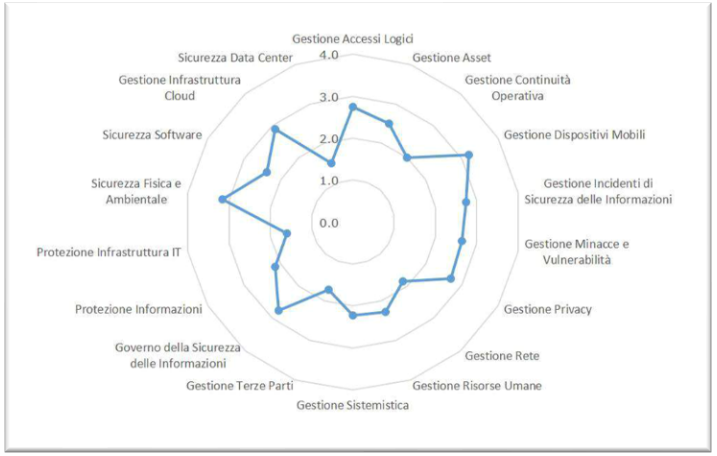
TOOL DI VALUTAZIONE E TRATTAMENTO DEL RISCHIO CYBER

Al momento il tool non è fruibile perché è in fase di migrazione sul portale dell'Agenzia della Cybersicurezza Nazionale

Inserimento delle informazioni

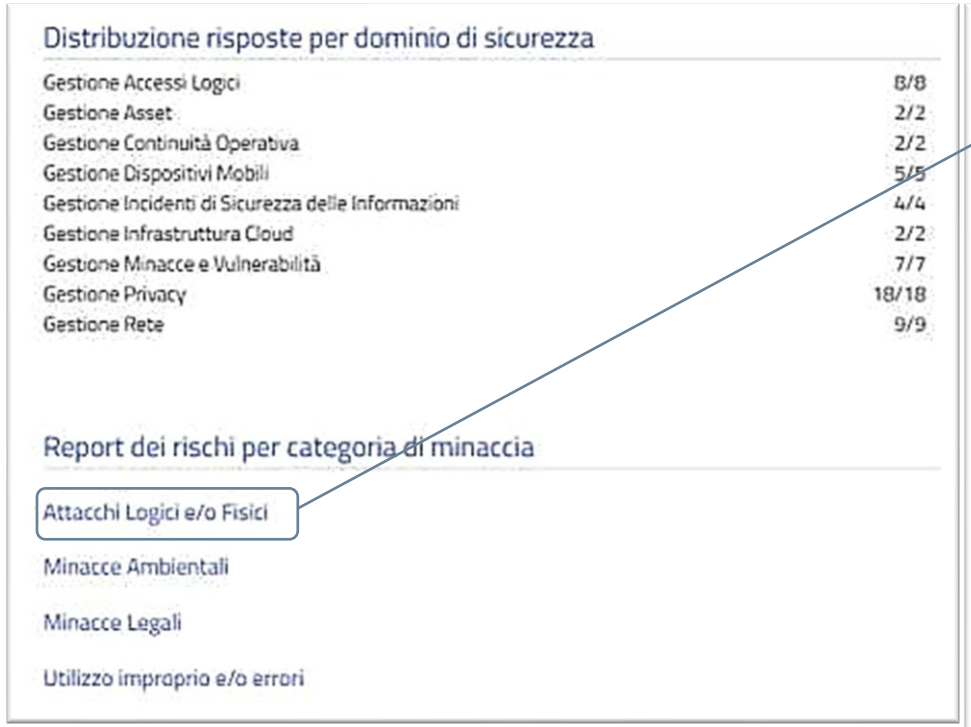


Grado di implementazione medio per ciascun dominio di sicurezza



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

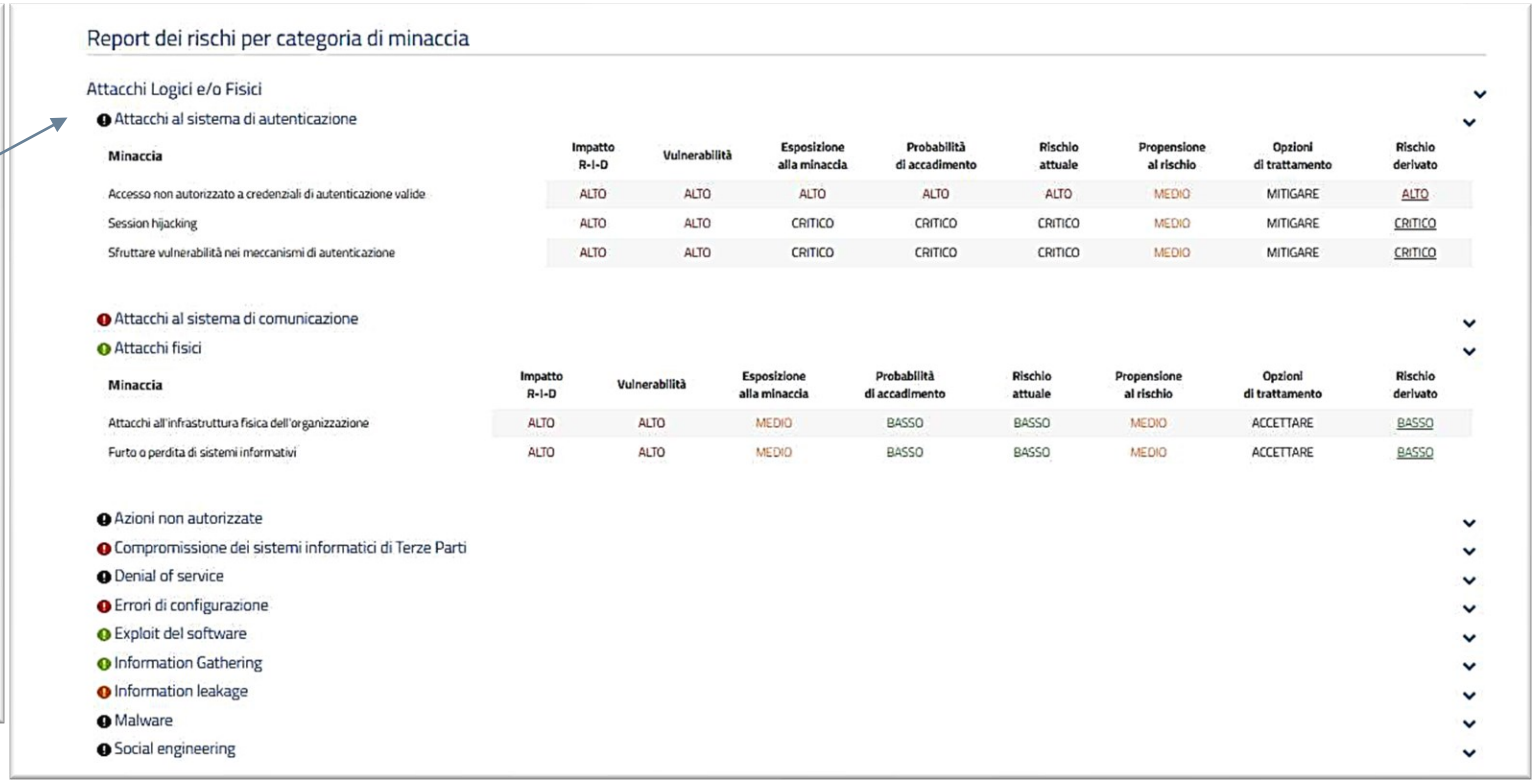
Report dei rischi per categoria di minaccia

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

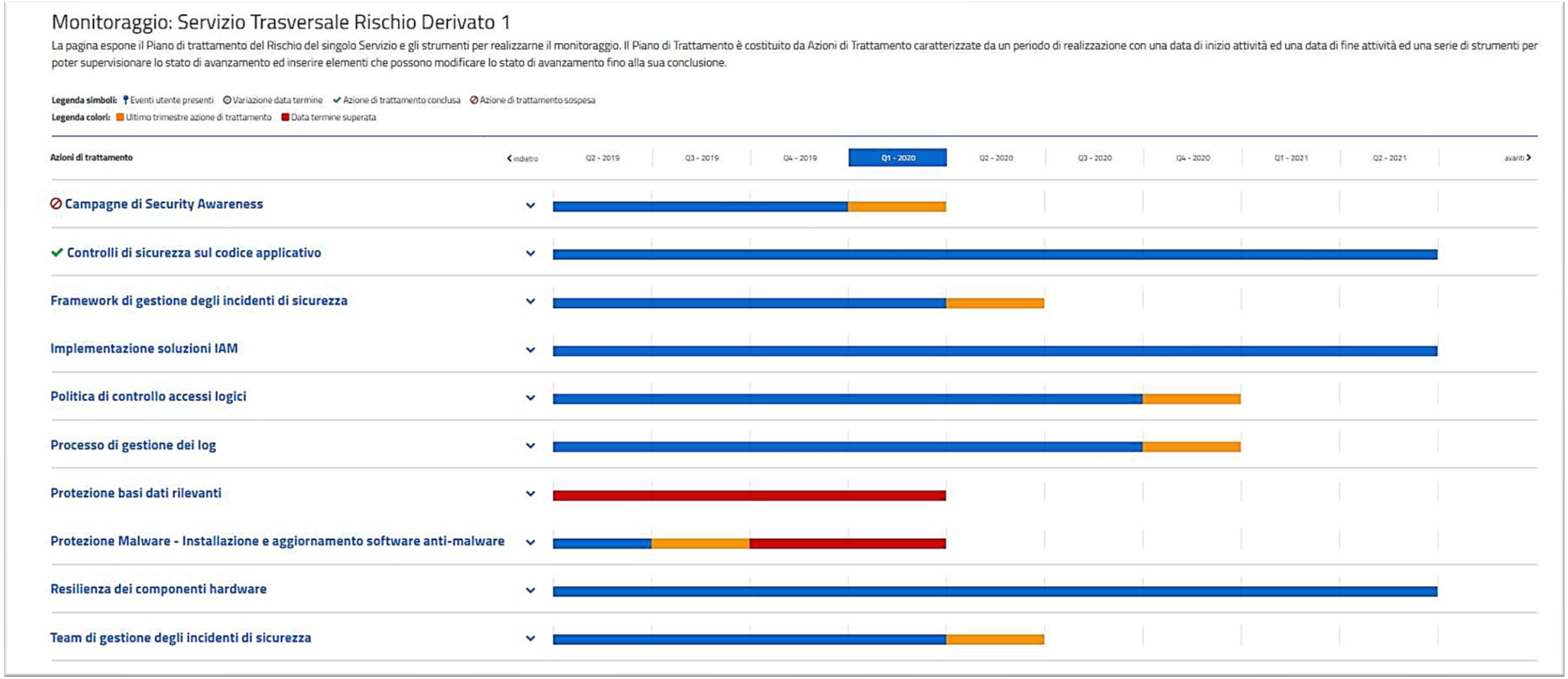
Information Gathering

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.

PROCESSO DI GESTIONE DEGLI INCIDENTI

Prima: PREPARE

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

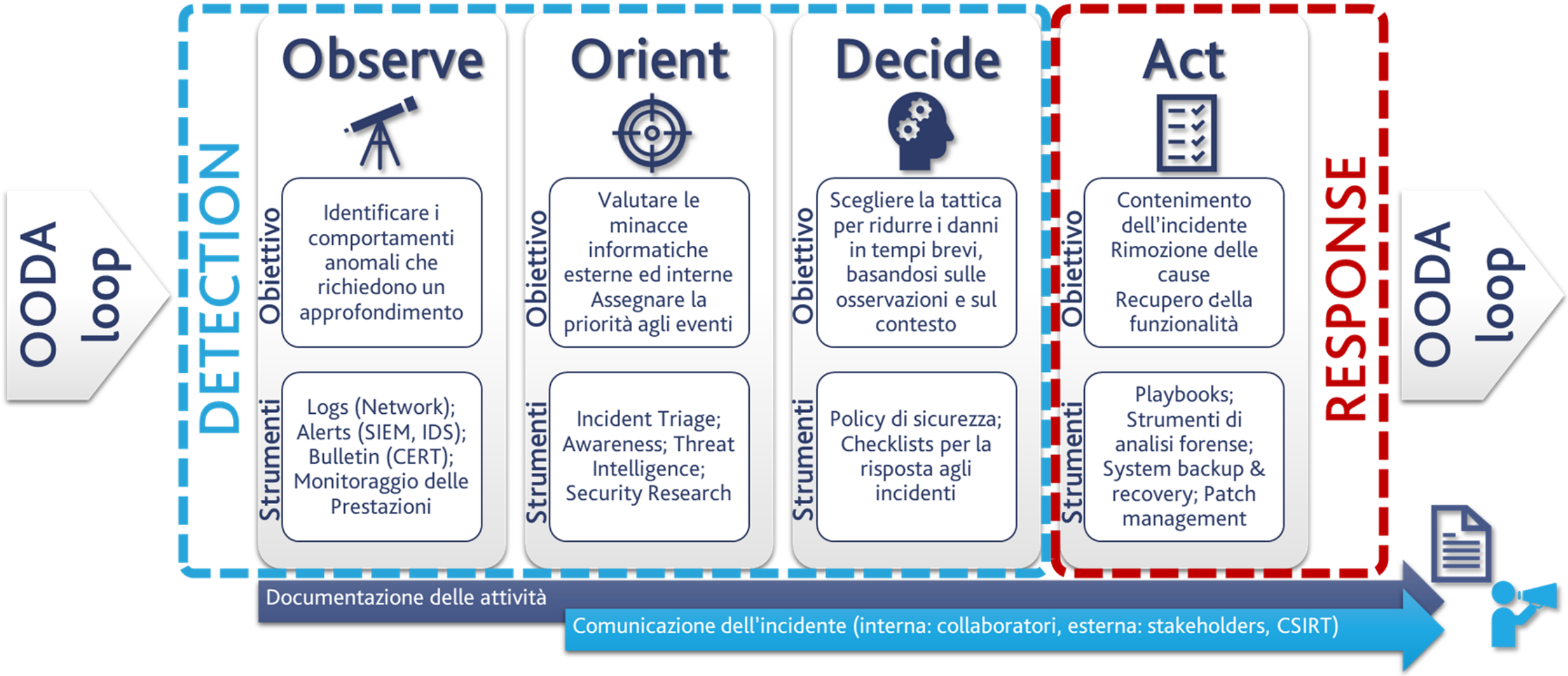
Durante: DETECT & RESPOND

- 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

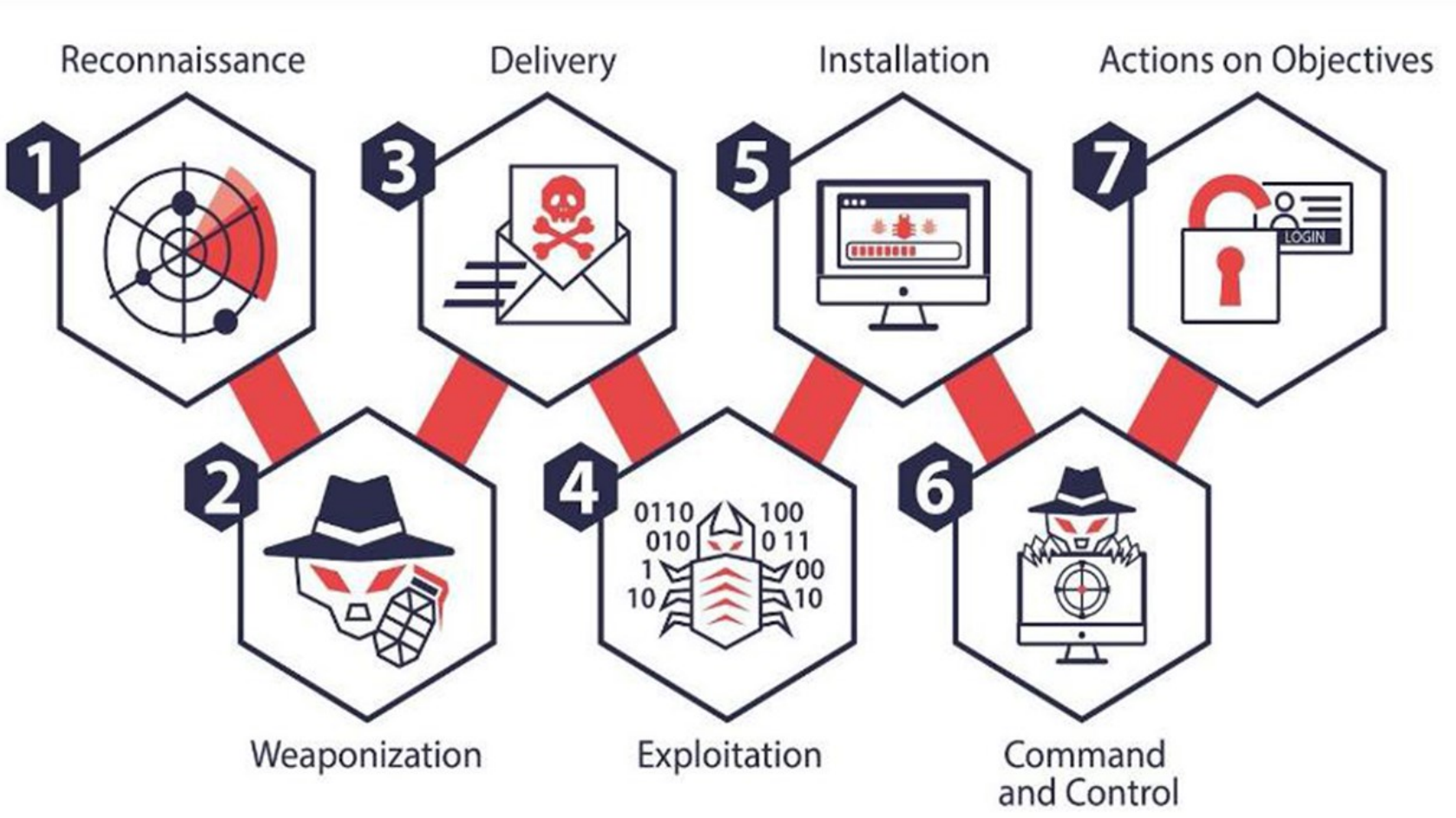
PROCESSO DI GESTIONE DEGLI INCIDENTI



CYBER KILL CHAIN PER LA DETECTION

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

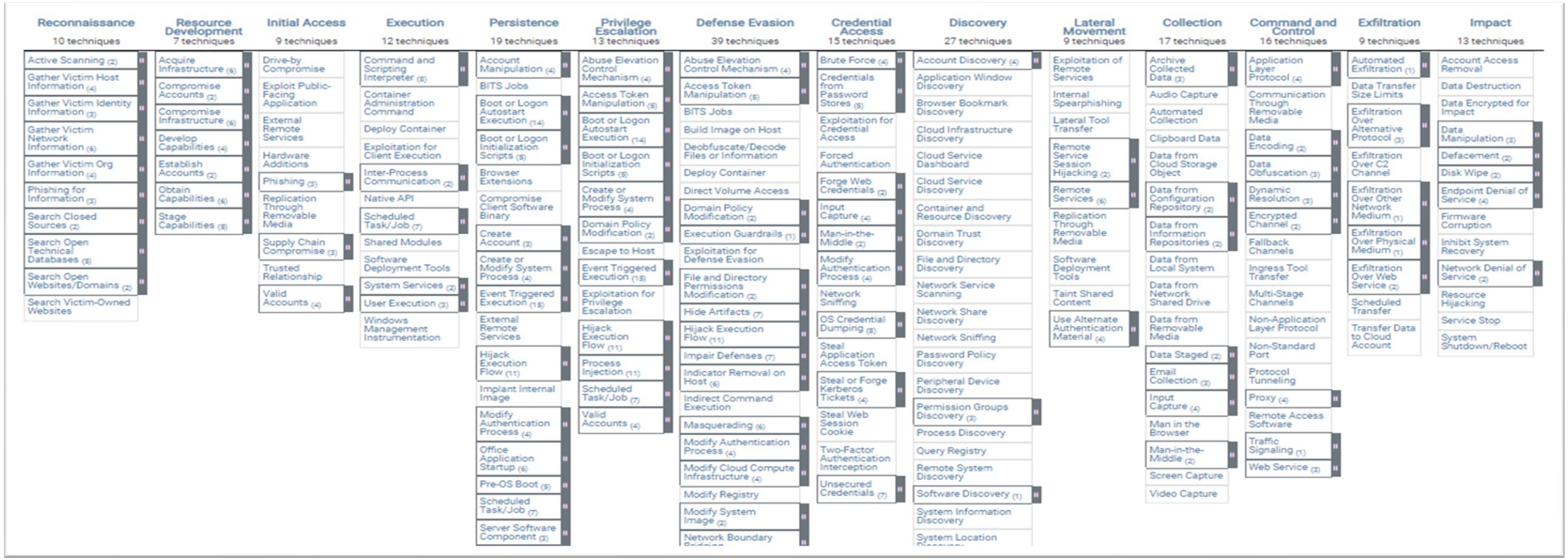
È utile per identificare le azioni prodromiche all'attacco



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

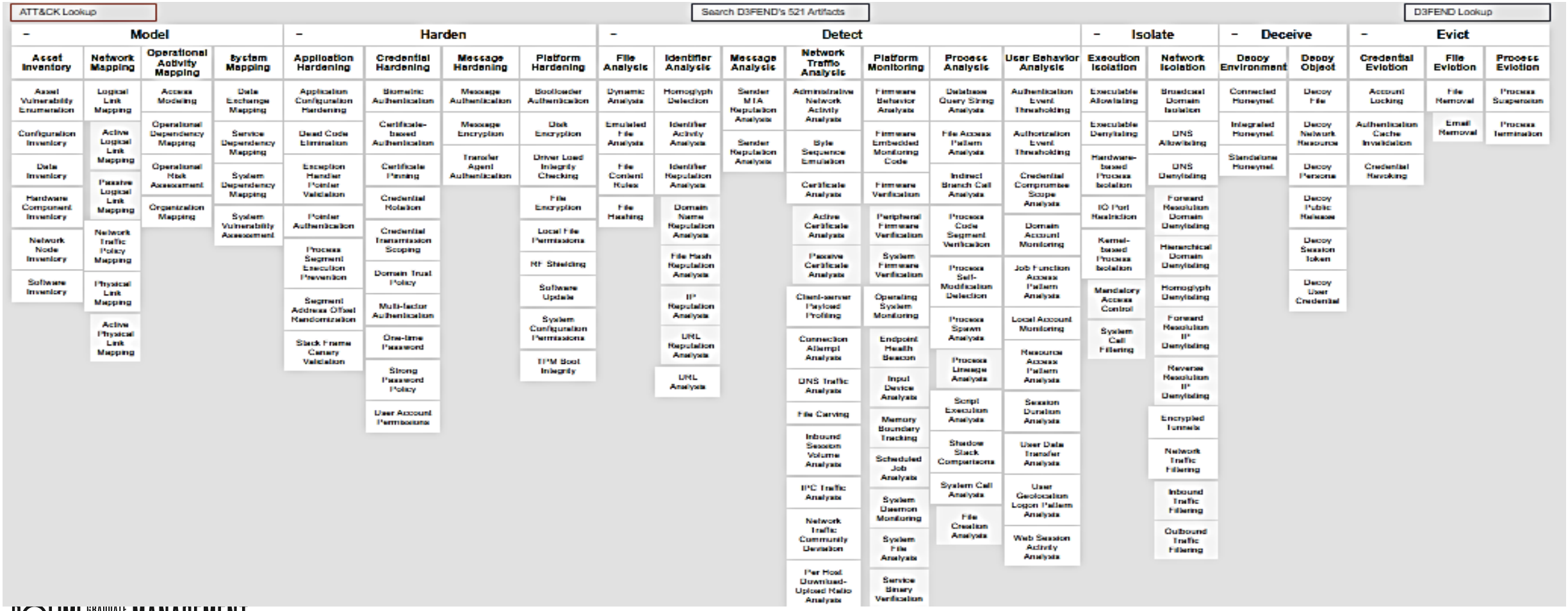
MITRE ATT&CK HTTPS://ATTACK.MITRE.ORG/

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



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).

PRINCIPALI MINACCE E CONTROMISURE ADOTTATE

Con l'entrata in vigore del Regolamento in materia di perimetro di sicurezza nazionale cibernetica è stato avviato un percorso

PRINCIPALI MINACCE	CONTROMISURE ADOTTATE
Minacce cyber in generale	Analisi e valutazione dei rischi Implementazione delle misure per ridurre i rischi cyber Implementazione di un sistema di monitoraggio proattivo Implementazione di policy per la segnalazione degli incidenti Formazioni specialistica per il personale ICT
Phishing	Formazione e informazione
Social engineering	Formazione e informazione
Continuità operativa	Formazione e informazione Piano di business continuity

Criticità riscontrate:

- Resistenza al cambiamento: dall'adempimento e/o applicazione di linee guida, alla gestione del rischio
- Carenza di personale specializzato
- Coinvolgimento di tutto il personale
- Segmentazione delle infrastrutture ICT
- Risorse insufficienti

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) – aggiornamento della precedente direttiva
- la **Direttiva NIS2** (Network and information system security) – ulteriori adempimenti per innalzare il livello di cyber resilience

SINTESI

• Adeguamento completo alle misure minime di sicurezza	→ Linee guida AGID e ACN - DPCM Perimetro
• Adozione di un modello risk-based per la gestione della sicurezza	→ Tool di valutazione e trattamento del rischio cyber
• Coinvolgimento di tutto il personale per:	
• Rafforzare la struttura che riporta al vertice amministrativo	→ Emanare regolamenti e policy ad-hoc
• Incrementare la consapevolezza (prevenzione)	→ Formazione e informazione sulle minacce cyber
• Innalzare il livello di sicurezza (reazione)	→ Simulazione di attacchi phishing e social engineering
• Velocizzare il tempo di risposta (risoluzione)	→ Sistema per la segnalazione di anomalie/incidenti Formazione specialistica per il personale ICT
• Acquisizione di beni e servizi «security by design»	→ Linee guida AGID e ACN – DPCM Perimetro Cento di Valutazione Supply chain ICT

THANK YOU

POLIMI GRADUATE SCHOOL OF MANAGEMENT

CONTACT INFORMATION

LEGAL NOTES