La Direttiva NIS 2

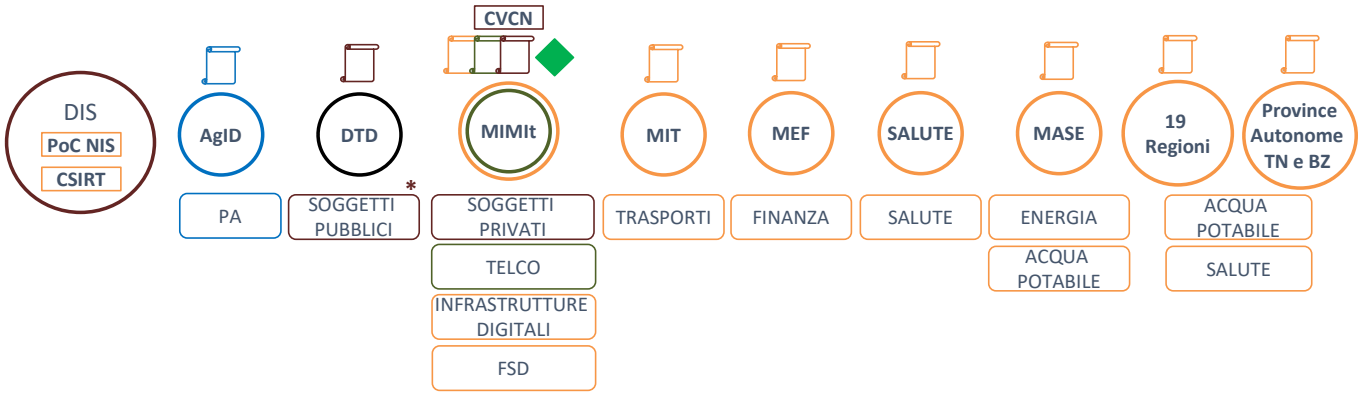
16 settembre 2024

Agenzia per la Cybersicurezza Nazionale

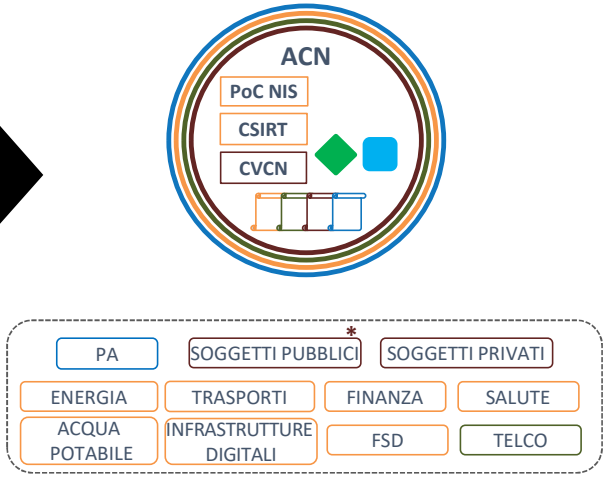
Funzioni principali dell'Agenzia

Razionalizzazione introdotta dal DL 82/2021

DPCM 17 febbraio 2017



DL 82/2021



Direttiva NIS (D.Lgs. 65/2018)
Disponibilità dei servizi nel mercato unico europeo
- ○ Autorità competente NIS
- ▱ Attività di verifica, di vigilanza e di ispezione NIS
- ▢ Operatori di Servizi Essenziali (OSE) e Fornitori di Servizi Digitali (FSD)

Telco (DM MiSE 12 dicembre 2018)
- ○ Autorità
- ▱ Attività di verifica, di vigilanza e di ispezione Telco
- ▢ Operatori Telco

Cybersecurity Act (Regolamento UE 2019/881)
- ◆ Autorità di certificazione di cybersicurezza (EU CSA)

Perimetro di sicurezza nazionale cibernetica (L. 133/2019)
- ○ Coordinamento
- ▱ Attività di verifica, di vigilanza e di ispezione PSNC
- ▢ Soggetti Perimetro

* Salvo per Ministeri Interno e Difesa

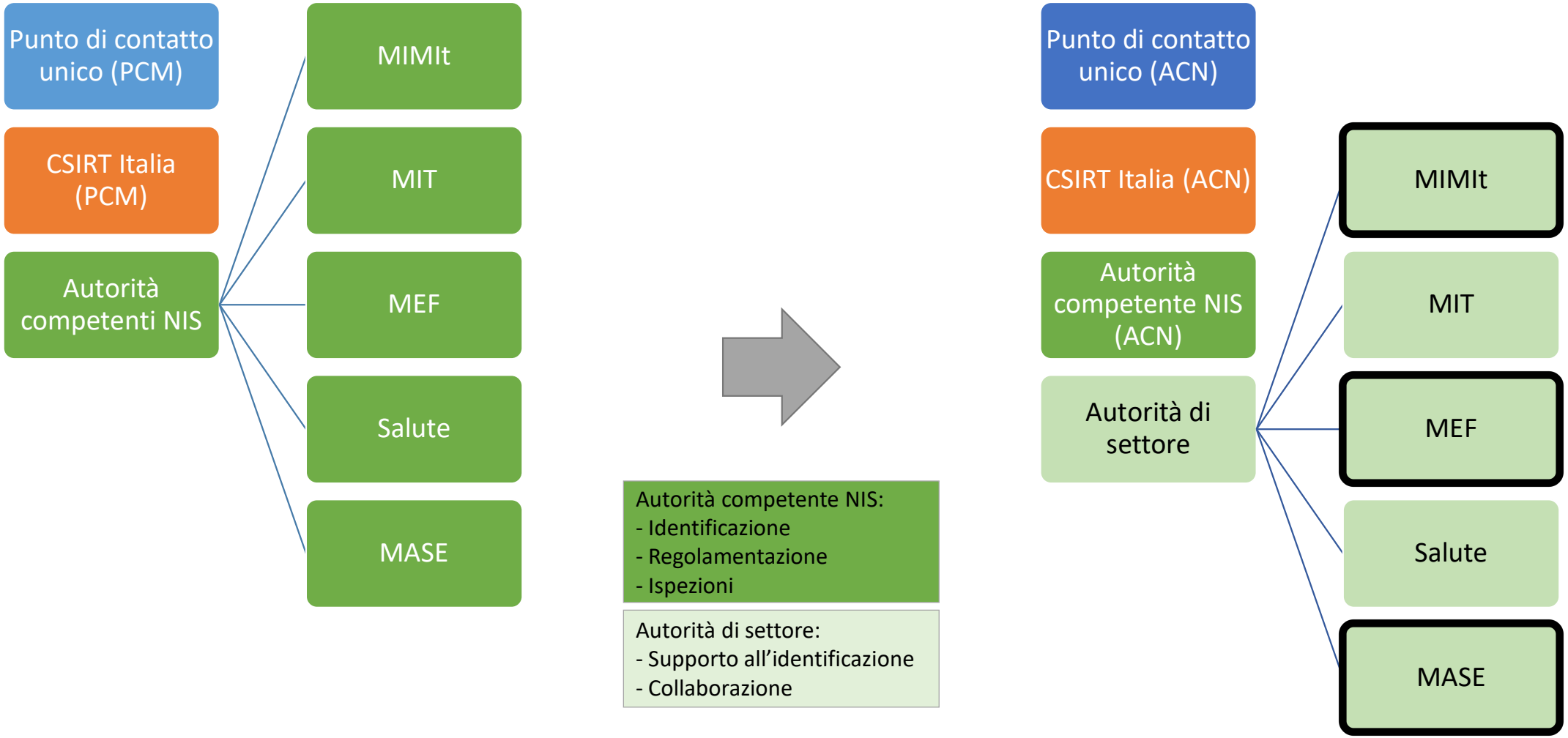
Codice dell'Amministrazione Digitale (D.Lgs. 82/2005) e Cloud per la PA (co. 4 art. 33-speties del DL 179/2012)
- ○ Misure di sicurezza e Cloud per la PA
- ▱ Attività di verifica, di vigilanza e di ispezione

Regolamento UE 2021/887
- ■ Centro nazionale di coordinamento (EU NCC)

DIS – Dipartimento delle informazioni per la sicurezza
AgID – Agenzia per l'Italia digitale
DTD – Dipartimento per la trasformazione digitale
MIMIt – Ministero delle Imprese e del Made in Italy
MIT – Ministero delle infrastrutture e dei Trasporti
MEF – Ministero dell'economia e delle finanze
MASE – Ministero dell'ambiente e della sicurezza energetica
ACN – Agenzia per la cybersicurezza nazionale

CVCN – Centro di valutazione e certificazione nazionale
CSIRT – Computer Security Incident Response Team
PoC NIS – Punto di contatto unico NIS

Modifiche introdotte dal DL 82/2021 in relazione al DLgs 65/2018



Servizio Regolazione

Missioni del Servizio Regolazione

Regolamentazione e normativa cyber

Cooperazione con omologhi europei

Sostenere il ruolo di ACN come **punto di riferimento per i profili regolatori** della vigente disciplina in materia di cybersicurezza, di derivazione comunitaria e nazionale.

Garantirne il rispetto anche attraverso l'**esercizio dei poteri sanzionatori**.

Rapporto con i soggetti vigilati

Misure di Sicurezza Obblighi di notifica

Settori vigilati

Settori	PSNC	NIS2	Altre normative	Raccordo
PA centrale	Governativo, Interno, Previdenza	PA Centrale	CAD Regolamento Cloud	CER
PA locale	Interno	PA Locale		CER
Difesa	Difesa			
Spazio e aerospazio	Spazio e aerospazio	Spazio		CER
Energia	Energia	Elettrico, Teleriscaldamento, Petrolio, Gas, Idrogeno	NCCS	CER
Telco	Telecomunicazioni	Servizi e reti di comunicazione elettronica pubblici	EECC	
Infrastrutture e servizi digitali	Infrastrutture e servizi digitali	Infrastrutture e servizi digitali, MS(S)P	Regolamento Cloud	eIDAS
Economia e Finanza	Economia e finanza	Bancario, Infrastrutture dei mercati finanziari		DORA
Trasporti	Trasporti	Trasporto aereo, ferroviario, per vie d'acqua, su strada, TPL	Regolamento 2015/1998	CER
Tecnologie e ricerca	Tecnologie critiche	Ricerca		CER
Salute		Assistenza, Laboratori di analisi, Farmaceutico		CER
Ambiente		Acqua potabile, Acque reflue, Gestione rifiuti		CER
Servizi postali		Servizi postali e di corriere		
Fabbricazione		Fabbricazione (dispositivi medici, computer e elettronica, apparecchiature elettriche, macchinari, mezzi di trasporto), nonché Fabbricazione, produzione e distribuzione di sostanze chimiche		
Alimentare		Produzione, trasformazione e distribuzione di alimenti		CER

Direttiva NIS2

(Principi generali)

Direttiva NIS2 – 2022/2555

Estensione ambiti di applicazione

- **18 settori: 11 settori altamente critici** (originariamente 8) e **7 settori critici** (originariamente 0)
- **Intera infrastruttura ICT** (originariamente solo reti e sistemi serventi i servizi essenziali)

Processo di identificazione dei soggetti

- **Soggetti** distinti tra entità **essenziali e importanti**
- **Identificazione automatica** sulla base di criteri oggettivi (da **media imprese in su**, salvo eccezioni)
- Il Governo ha anche la facoltà di identificare ulteriori soggetti

Rafforzamento degli obblighi

- Misure di sicurezza specifiche e **proporzionate rispetto al rischio** posto al sistema informativo e di rete
- Approccio **multi-rischio** (coordinamento con Direttiva CER)
- Processo di notifica più dettagliato
- Poteri di esecuzione, ispettivi e sanzionatori rafforzati (**allineamento alle sanzioni GDPR**)

Nuovi strumenti

- **Divulgazione coordinata delle vulnerabilità (CVD)**
- **Cyber crisis liaison organisation network** (CyCLONe) e Autorità nazionale competente per la gestione delle crisi informatiche
- Revisione tra pari e mutua assistenza
- Estensione Strategia

Recepimento entro il 17 ottobre 2024

Ambito di applicazione

[1] Possibile identificazione governativa come essenziali
[2] Possibile identificazione governativa come importanti o essenziali

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
SETTORI ALTAMENTE CRITICI				
Energia (+)	19 tipologie di soggetto	Essenziali	Importanti[1]	Fuori ambito[2]
Trasporti	10 tipologie di soggetto			
Settore bancario	DORA Lex specialis			
Infrastrutture dei mercati finanziari				
Settore sanitario (+)	5 tipologie di soggetto			
Acqua potabile	1 tipologia di soggetto			
Acque reflue	1 tipologia di soggetto			
Infrastrutture digitali (+)	9 tipologie di soggetto			
Gestione dei servizi TIC (b2b)	2 tipologie di soggetto			
Spazio	1 tipologia di soggetto			
SETTORI CRITICI				
Servizi postali e di corriere	1 tipologia di soggetto			
Gestione dei rifiuti	1 tipologia di soggetto			
Fabbricazione, produzione e distribuzione di sostanze chimiche	1 tipologia di soggetto			
Produzione, trasformazione e distribuzione di alimenti	1 tipologia di soggetto			
Fabbricazione	6 tipologie di soggetto			
Fornitori di servizi digitali (+)	4 tipologie di soggetto			
Ricerca	2 tipologie di soggetto			
ULTERIORI TIPOLOGIE DI SOGGETTI				
Pubblica Amministrazione centrale		Identificazione governativa		
Pubblica Amministrazione regionale e locale	11 categorie di PA			
Ulteriori tipologie di soggetti	5 tipologie e 2 criteri aggiuntivi			

Settori, sottosettori e tipologie di soggetti introdotti dalla NIS2

Panoramica degli obblighi

Recepimento entro il 17 ottobre 2024

Registrazione e aggiornamento dati	• In tempo utile per la trasmissione alla Commissione UE, **entro il 17 Aprile 2025**, delle statistiche sull'elenco dei soggetti essenziali/importanti
Responsabilità degli organi di amministrazione e direttivi	• Approvano e sovraintendono all'implementazione delle misure • **Sono responsabili delle violazioni**
Misure di sicurezza	• **Termini da definire a livello nazionale** • 10 ambiti • **Proporzionalità**
Notifica di incidenti	• **Termini da definire a livello nazionale** • Preallarme in 24 ore • Notifica in 72 ore
Certificazioni UE (uso di prodotti TIC certificati)	• Obbligo può essere imposto ai soggetti NIS2 a livello unionale con atto delegato della Commissione • Obbligo può essere imposto ai soggetti NIS2 a livello nazionale (Autorità)

Misure di sicurezza

Politiche di analisi dei rischi e di sicurezza dei sistemi informatici

Gestione degli incidenti

Continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi

Sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza […] dei rapporti […] con i suoi diretti fornitori o fornitori di servizi

Sicurezza dell'acquisizione, dello sviluppo e della manutenzione […], compresa la gestione e la divulgazione delle vulnerabilità

Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza

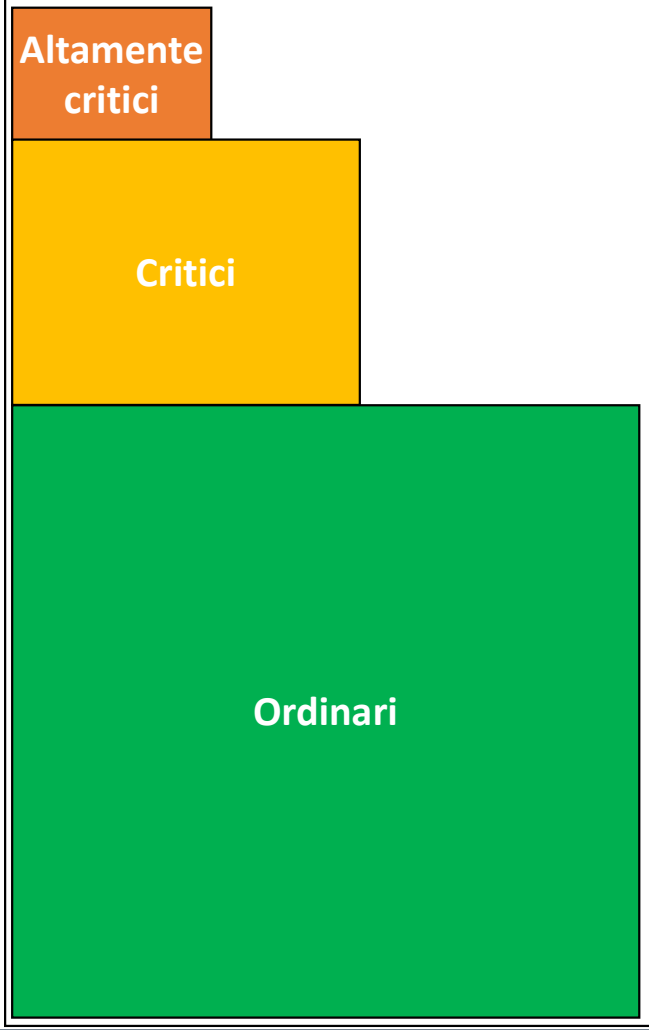
Pratiche di igiene informatica di base e formazione in materia di cybersicurezza

Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;

Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli assetti

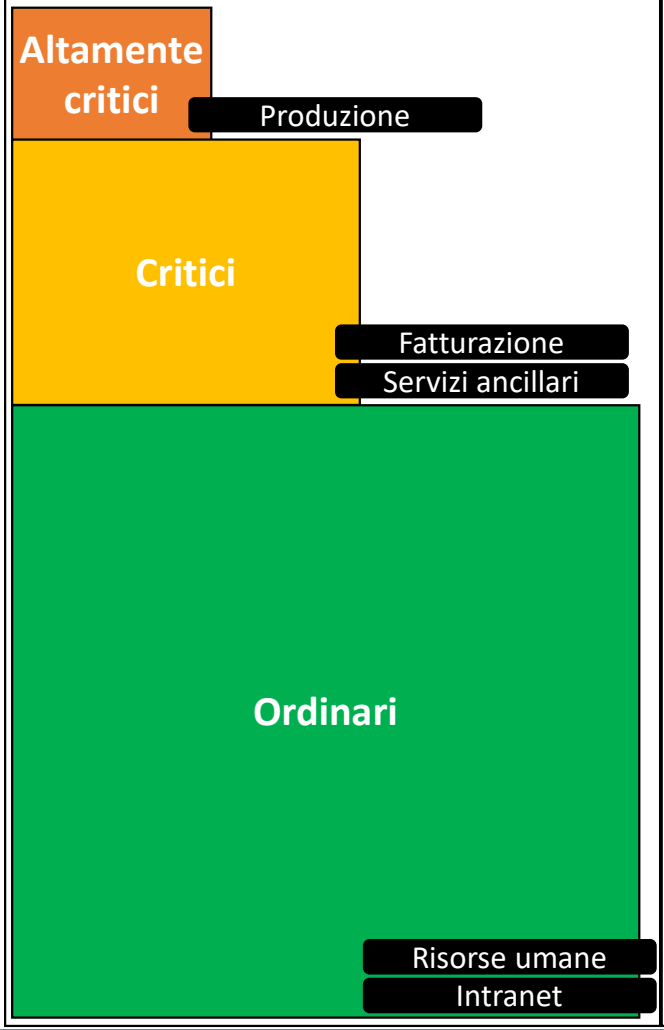
Uso di soluzioni di autenticazione a più fattori o di autenticazione continua […]

Approccio al principio di proporzionalità degli obblighi

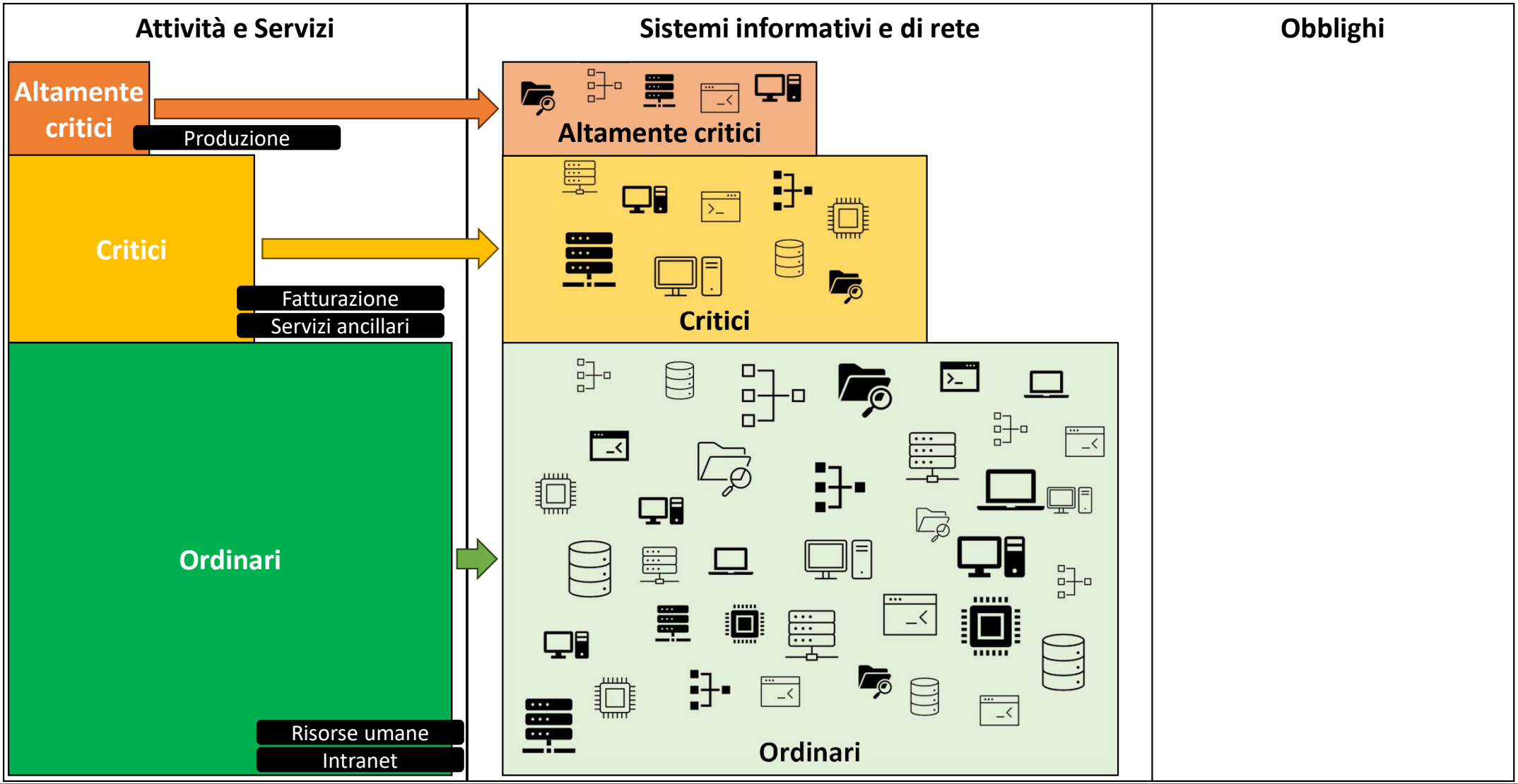
Attività e Servizi	Sistemi informativi e di rete	Obblighi
		

Approccio al principio di proporzionalità degli obblighi

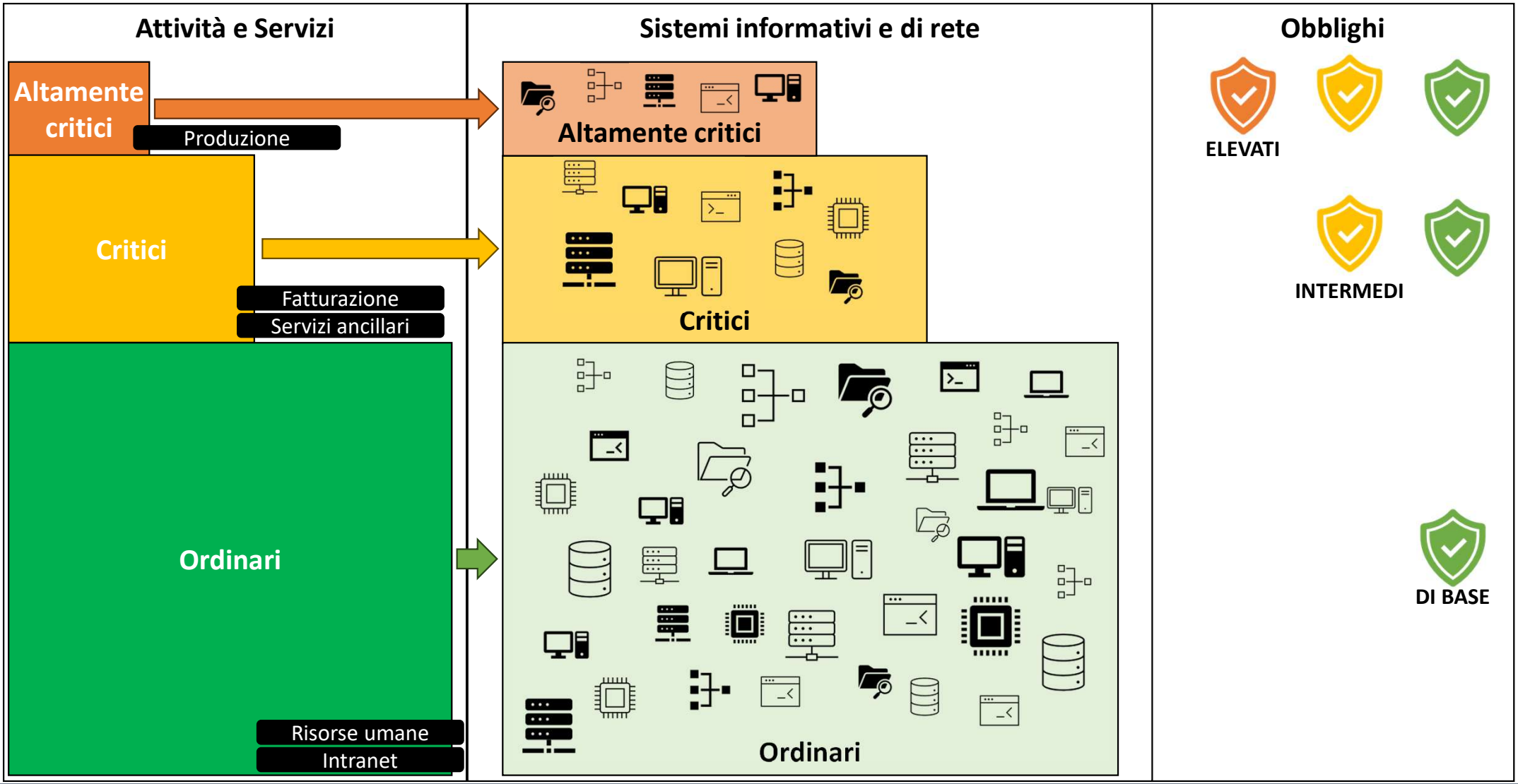
Attività e Servizi	Sistemi informativi e di rete	Obblighi



Approccio al principio di proporzionalità degli obblighi



Approccio al principio di proporzionalità degli obblighi



Tavoli settoriali

Coordinamento dell'Autorità di settore

- Ogni Autorità di settore NIS (1/2) coordina uno i più tavoli settoriali per i settori (e/o sottosettori) di competenza

Agenzia per la Cybersicurezza Nazionale (ACN)

- Partecipa ai tavoli settoriali nell'esercizio delle funzioni di Autorità nazionale competente NIS (1/2)

Tavoli di settore

- Camera di compensazione tra l'ambito governativo e i settori NIS (1/2) per una efficace attuazione della Direttiva
- Individuazione di criticità e condivisione di approcci in fase legislativa e regolamentare
- Monitoraggio dell'attuazione

Modalità

- Riunioni a cadenza, indicativamente, trimestrale (in fase legislativa e regolamentare)
- Interazioni con ACN per mezzo dell'Autorità di settore

Servizio Operazioni e gestione delle crisi cyber

già Servizio Operazioni
ridenominato con decreto del Direttore generale del 1° luglio 2024

Direttiva NIS2

(Le funzioni di prevenzione, gestione e risposta a incidenti cibernetici dell'ACN)

INDICE

DIRETTIVA NIS2

CSIRT ITALIA (*art. 10 Direttiva NIS2*)

Lo **CSIRT Italia** è il gruppo nazionale di risposta agli incidenti di sicurezza informatica operante all'interno dell'Agenzia per la cybersicurezza nazionale (ACN).

DIRETTIVA NIS2

CSIRT ITALIA – *Servizio Operazioni e gestione delle crisi cyber*

Il Servizio Operazioni e gestione delle crisi cyber è la **struttura operativa** dell'Agenzia incaricata delle attività di prevenzione, monitoraggio, rilevamento, analisi e risposta per prevenire e gestire eventi di natura cibernetica nonché della gestione di crisi cibernetiche e della pianificazione, organizzazione e condotta di esercitazioni cyber internazionali e nazionali. All'interno del Servizio opera lo **CSIRT Italia**.

Per assicurare lo svolgimento delle funzioni operative, lo CSIRT Italia svolge **compiti di natura *proattiva*** (monitoraggio, cyber threat intelligence, analisi specialistica sulle minacce ed early warning su eventi d'interesse), **di *natura reattiva*** (incident response, analisi malware, digital forensics ed analisi "post-mortem") e **servizi di *gestione rischio & governace***.

DIRETTIVA NIS2

CSIRT ITALIA – *Compiti (art. 11 Direttiva NIS2)*

I SERVIZI DI CSIRT ITALIA

Intervento in caso di incidente

Analisi dinamica dei rischi e degli incidenti

Monitoraggio degli incidenti a livello nazionale

Emissione di **allerte, annunci e divulgazione** riguardo rischi e incidenti

LE NOVITÀ INTRODOTTE DALLA NIS 2

Scansione, su richiesta**, di sistemi informatici e di rete** dei soggetti

Scansione proattiva e non intrusiva dei sistemi informatici e di rete **accessibili al pubblico**

Coordina il processo di **divulgazione coordinata delle vulnerabilità (CVD)**

DIRETTIVA NIS2

OBBLIGHI DI NOTIFICA – *Definizioni prioritarie (art. 6 Direttiva NIS2)*

INCIDENTE

Un **evento che compromette** la **disponibilità, l'autenticità, l'integrità o la riservatezza** di dati conservati, trasmessi o elaborati o dei servizi offerti da sistemi informatici e di rete o accessibili attraverso di essi. Ai sensi dell'art. 23, co.3 della Direttiva NIS, un **incidente è considerato significativo** se:

a) **ha causato** o **è in grado di causare una grave perturbazione operativa** dei servizi o **perdite finanziarie** per il soggetto interessato;

b) si è **ripercorso o è in grado di ripercuotersi** su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

NEAR-MISS

Un **evento che avrebbe potuto compromettere** la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti da sistemi informatici e di rete o accessibili attraverso di essi, **ma che è stato efficacemente evitato o non si è verificato**.

MINACCIA INFORMATICA

Qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone. La **minaccia** è considerata **significativa** se, in base alle sue caratteristiche tecniche, **si presume possa avere un grave impatto** sui sistemi informatici e di rete di un soggetto o degli utenti di tali servizi del soggetto **causando perdite materiali o immateriali considerevoli.**

DIRETTIVA NIS2

OBBLIGHI DI NOTIFICA – *Notifica obbligatoria al CSIRT Italia (art. 23 Direttiva NIS2)*

SOGGETTI | Soggetti essenziali e importanti individuati ai sensi dell'articolo 3 della Direttiva NIS2.

PERCHE' NOTIFICARE | L'obbligo di notifica obbligatoria degli incidenti al CSIRT Italia è prevista dall'articolo 23 della Direttiva NIS2.

COSA NOTIFICARE | La notifica obbligatoria va effettuata per gli incidenti aventi un impatto significativo sulla fornitura dei servizi del soggetto.

CON QUALI TEMPISTICHE | I soggetti trasmettono al CSIRT Italia:

a) senza ingiustificato ritardo, e comunque entro le 24 ore, un **preallarme**;
b) senza ingiustificato ritardo e, comunque entro le 72 ore, una **notifica** integrativa anche delle informazioni su gravità ed impatto dell'incidente e, ove disponibili, degli IoC;
c) su richiesta del CSIRT Italia, una **relazione intermedia** di aggiornamento;
d) entro 1 mese dalla notifica, una **relazione finale**, contenente anche indicazioni su tipo di minaccia, causa, misure adottate e in corso, eventuale impatto transfrontaliero;
e) in caso di incidente in corso al momento della trasmissione della relazione finale, una **relazione mensile** e quella finale entro 1 mese dalla conclusione sulla gestione dell'incidente.

Come effettuare la notifica al CSIRT Italia

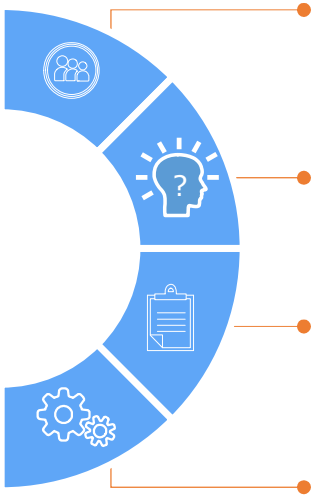
Sarà possibile effettuare una notifica attraverso il modulo disponibile sul sito internet CSIRT Italia.

Cosa aspettarsi da CSIRT Italia

A seguito della notifica sarà aperto un canale di comunicazione diretto, tramite il quale il CSIRT Italia offrirà al soggetto un supporto alle attività di incident handling.

DIRETTIVA NIS2

OBBLIGHI DI NOTIFICA – *Notifica volontaria al CSIRT Italia (art. 30 Direttiva NIS2)* 1° Ipotesi



SOGGETTI | Soggetti essenziali e importanti individuati ai sensi dell'articolo 3 della Direttiva NIS2.

PERCHE' NOTIFICARE | La notifica volontaria al CSIRT Italia è prevista dall'articolo 30 della Direttiva NIS2.

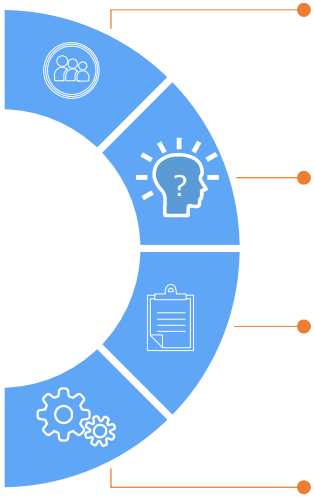
COSA NOTIFICARE | La notifica volontaria va effettuata per gli incidenti, le minacce informatiche e i quasi incidenti.

COSA FA LO CSIRT ITALIA | Lo CSIRT Italia tratta:

- le notifiche volontarie applicando la procedura prevista per quelle obbligatorie;
- Le notifiche obbligatorie con priorità rispetto a quelle volontarie.

DIRETTIVA NIS2

OBBLIGHI DI NOTIFICA – *Notifica volontaria al CSIRT Italia (art. 30 Direttiva NIS2)* 2° Ipotesi



SOGGETTI | Soggetti diversi da quelli essenziali e importanti, indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione della Direttiva NIS2.

PERCHE' NOTIFICARE | La notifica volontaria al CSIRT Italia è prevista dall'articolo 30 della Direttiva NIS2.

COSA NOTIFICARE | La notifica volontaria va effettuata per gli incidenti significativi, le minacce informatiche e i quasi incidenti.

COSA FA LO CSIRT ITALIA | Lo CSIRT Italia tratta:

- le notifiche volontarie applicando la procedura prevista per quelle obbligatorie;
- Le notifiche obbligatorie con priorità rispetto a quelle volontarie.

DIRETTIVA NIS2

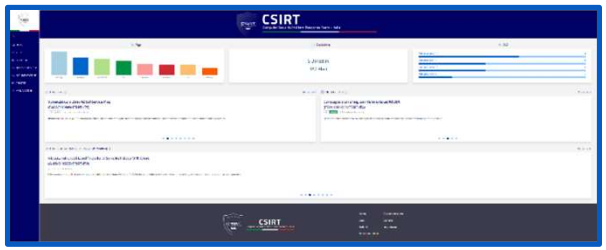
CSIRT ITALIA – Portali e caselle istituzionali

PORTALE PUBBLICO

- **Consultabile liberamente** all'indirizzo **https://www.csirt.gov.it**
- Condivisione **Alert, bollettini, monografie** e **Indicatori** relativi a minacce cyber
- Contenuti e informazioni ad accesso pubblico con **TLP WHITE**

PORTALE COLLABORATION

- Dedicato ai **soggetti NIS, PSNC** ed altri di interesse
- Contenuti ad accesso controllato con **TLP GREEN, AMBER, RED**
- Accreditamento tramite richiesta del soggetto (info@csirt.gov.it)



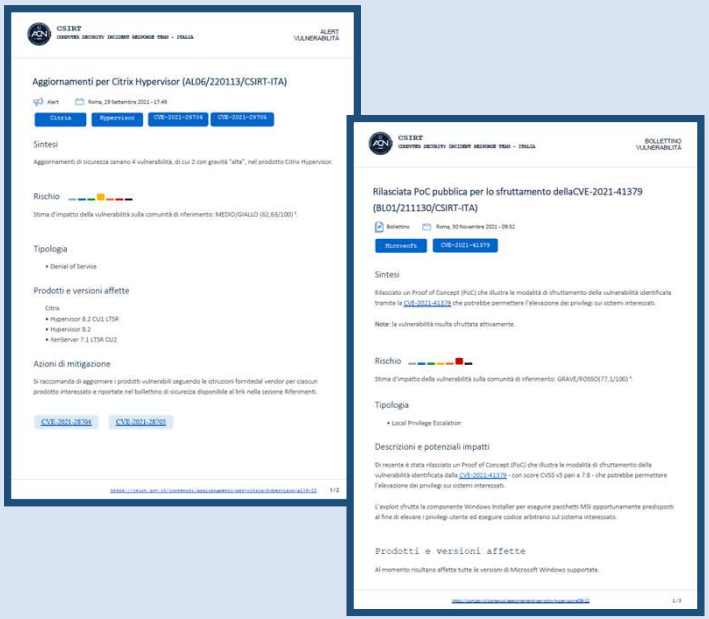
CASELLE DI POSTA ISTITUZIONALI

- Segnalazioni relative a **eventi** di **cybersicurezza**
- Comunicazioni punto-punto relative a **specifiche evidenze**
- **Interlocuzioni** di **natura tecnica** in materia di cybersicurezza

POSTA ELETTRONICA ORDINARIA:
info@csirt.gov.it
POSTA ELETTRONICA CERTIFICATA:
csirt@pec.acn.gov.it

DIRETTIVA NIS2

CSIRT ITALIA - Documentazione tecnica



Alert e bollettini su nuove campagne e vulnerabilità, contenenti gli indicatori di compromissione (IoC) e le azioni di mitigazioni consigliate

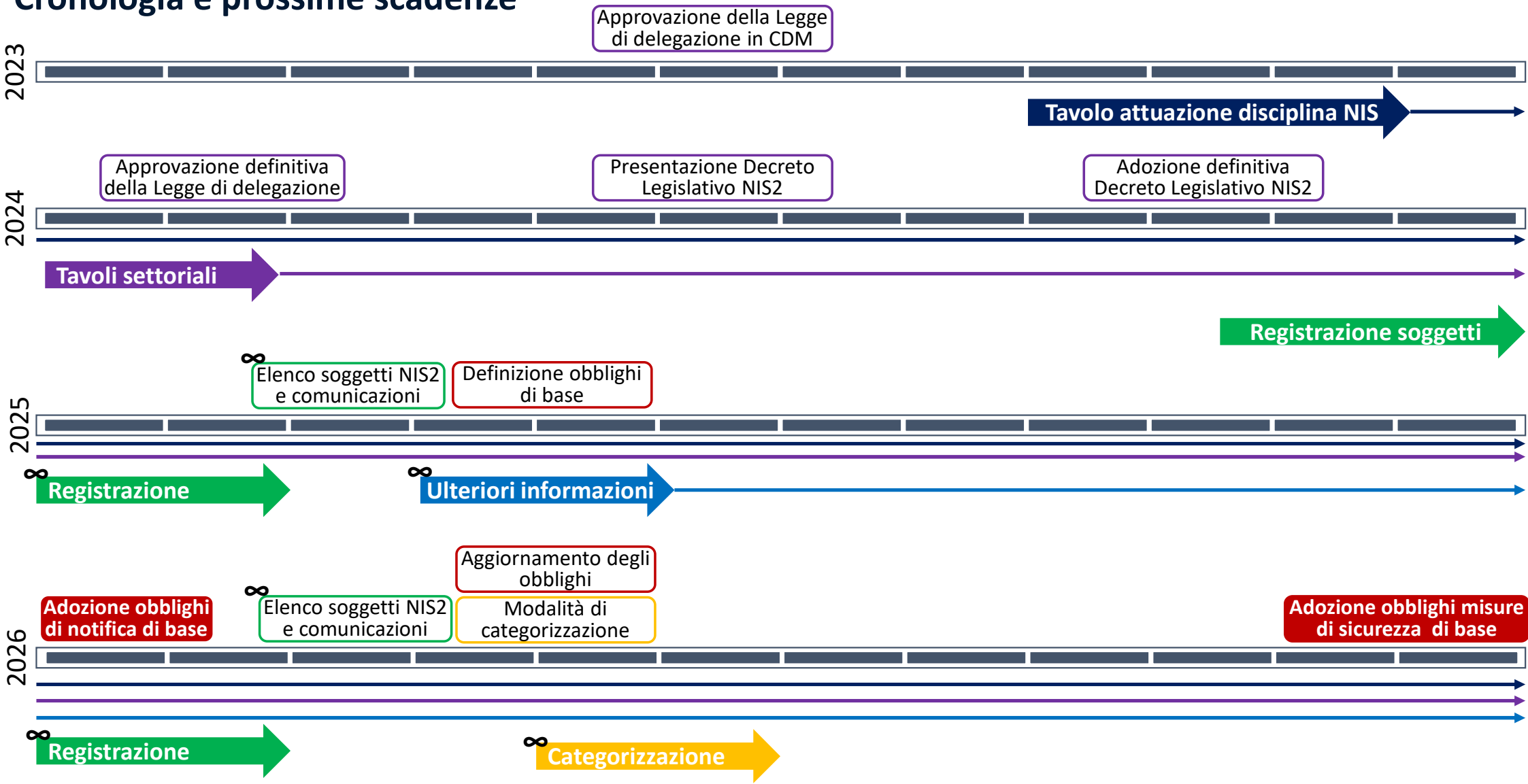
Pubblicazioni specialistiche su specifiche minacce, contenenti il dettaglio tecnico dei malware e delle TTP impiegate ed i relativi IoC

Report contenente l'analisi della postura di sicurezza degli asset esposti su Internet, usando lo stesso punto di vista di una minaccia esterna

Direttiva NIS2

(Cronologia)

Cronologia e prossime scadenze




AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT