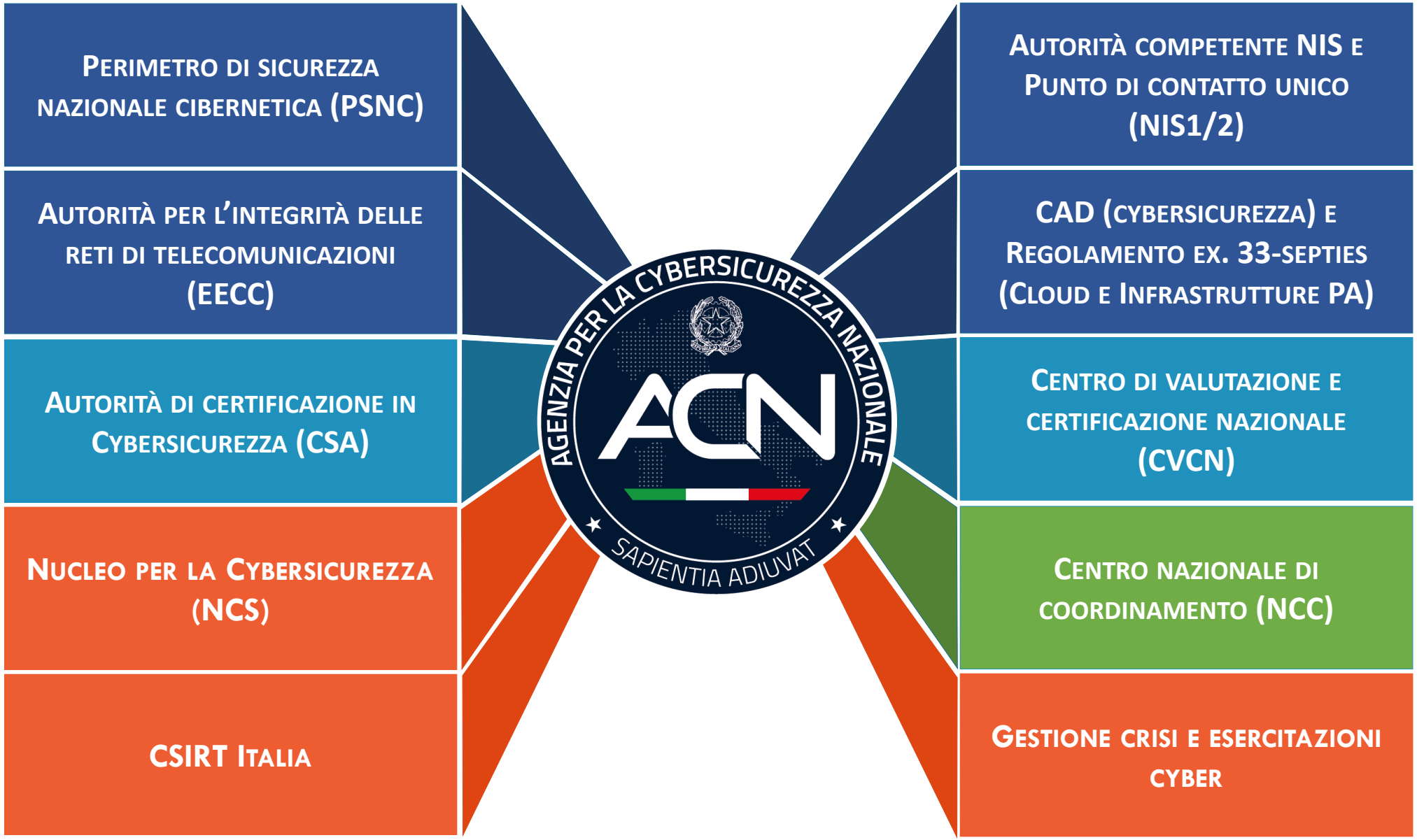
Verso la NIS2
per un livello comune elevato di cybersicurezza

09/05/2024

Principali funzioni e attività dell'Agenzia



Missioni del Servizio Autorità e Sanzioni

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**

Misure di Sicurezza Obblighi di notifica

Rapporto con i soggetti vigilati

Attività del Servizio Autorità e Sanzioni

PSNC – Perimetro di sicurezza nazionale cibernetica
NIS – Network and Information Systems

Attività nazionali
Attività europee/internazionali

D.L. 105/2019
Aggiornamento elenco soggetti
Impianto regolamentare (misure e notifiche)
Sanzioni

Tavolo Interministeriale

Direttiva 2016/1148 (NIS1) – D.Lgs. 65/2018
Aggiornamento elenco soggetti
Impianto regolamentare (misure e notifiche)
Sanzioni

Cyber Crisis Liaison Organisation Network (CyCLONe)

Gruppo di Cooperazione NIS (NISCG)

Recepimento Direttiva 2022/2555 (NIS2)

PSNC
Crisi Cyber
NIS
PA
Telco

Servizio Autorità e Sanzioni

D.Lgs. 82/2005 (CAD)
Linee guida ex. art 51 e 72 (cybersicurezza)

Classificazione dei dati e dei servizi

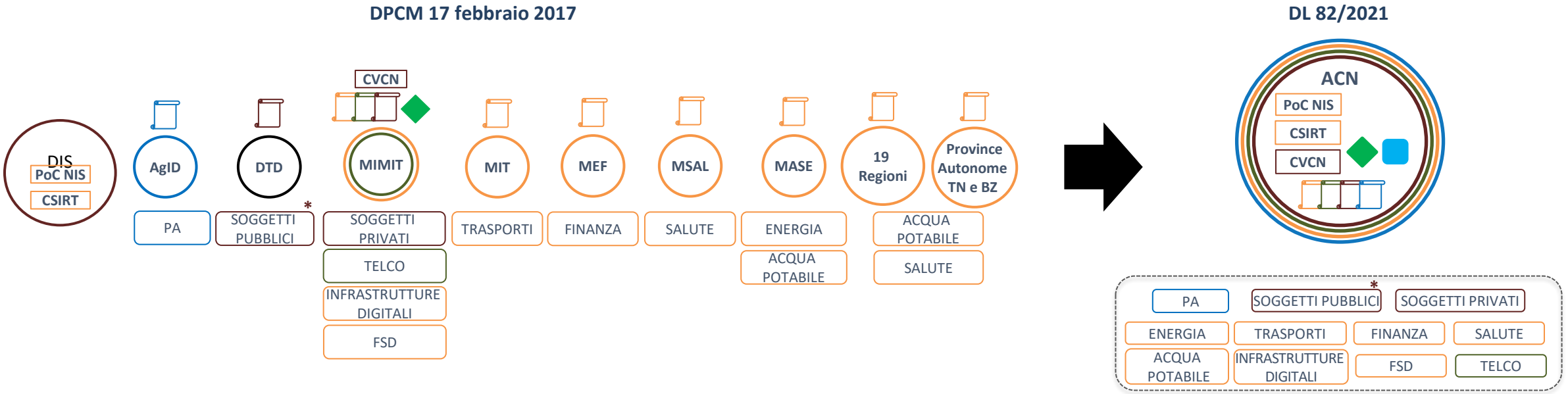
Regolamento Cloud ex 33-septies D.L. 179/2012
Impianto regolamentare
Misure infrastrutture digitali e servizi cloud

European Authorities for Secure Communications (ECASEC)

Direttiva 2018/1972 – D.Lgs. 207/2021
Articoli 40 e 41 (integrità delle reti)
Impianto regolamentare (misure e notifiche)
Sanzioni

Evoluzione del quadro normativo cyber

Razionalizzazione introdotta dal 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

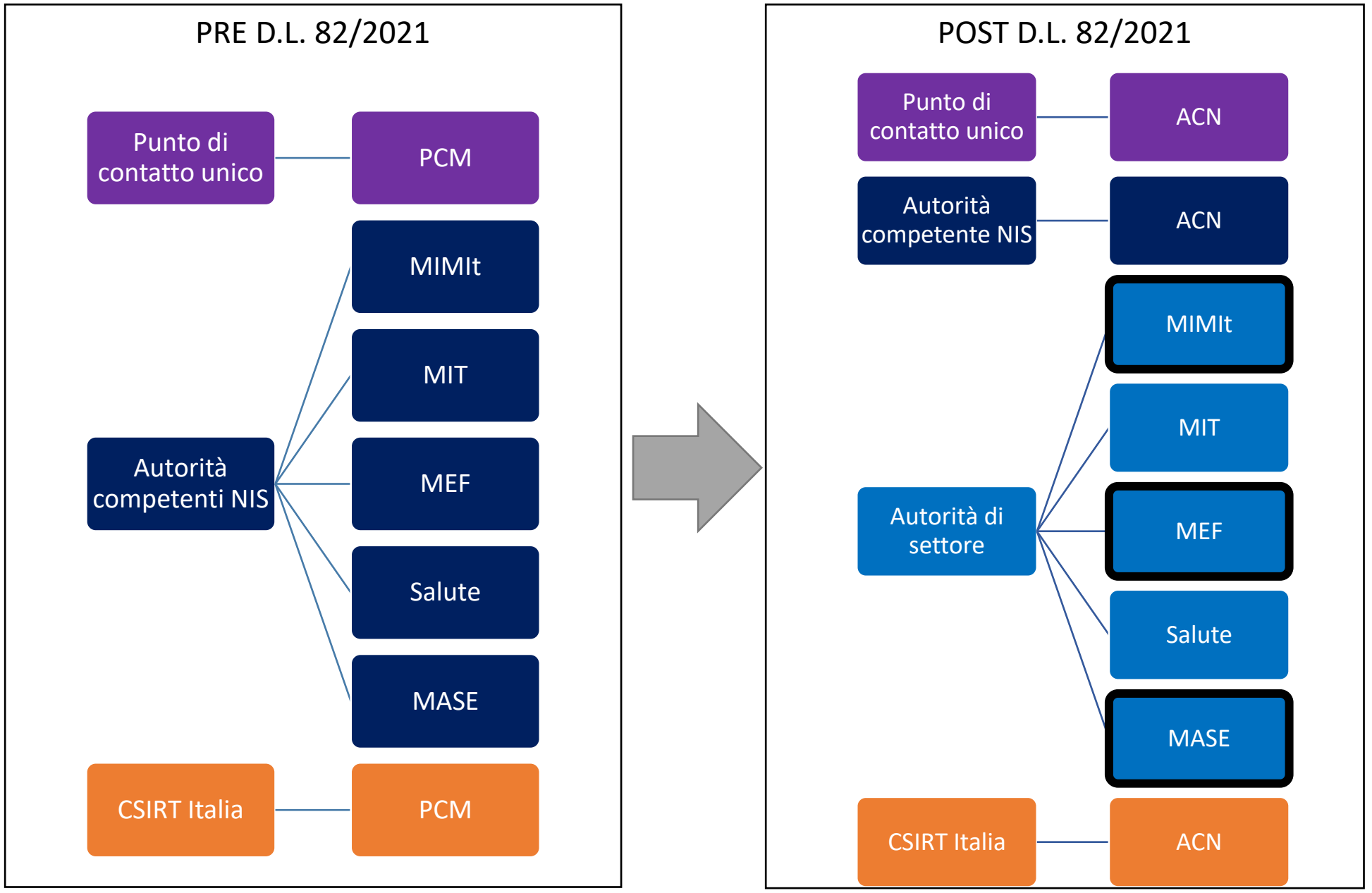
Codice dell'Amministrazione Digitale (D.Lgs. 82/2005) e Cloud per la PA (co. 4 art. 33-speties del DL 179/2012)
- ○ Misure di sicurezza e Cloud per la PA
- ▱ Attività di verifica, di vigilanza e di ispezione

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 D.L .82/2021 in relazione al D.Lgs. 65/2018



Autorità competente NIS
- Identificazione
- Regolamentazione
- Ispezioni e sanzioni

Autorità di settore
- Supporto all'identificazione
- Collaborazione

Direttiva NIS2

(Principi generali)

Direttiva NIS2 obiettivi e opportunità

Livello UE

- Aggiornamento delle misure per un livello comune elevato di cybersicurezza nell'UE
- Definizione di meccanismi di cooperazione tra gli Stati membri per una efficace risposta alle minacce cyber
- Elaborazione di modelli e procedure comuni sulla base degli orientamenti degli organismi europei

Livello nazionale

- Armonizzazione della legislazione cyber nazionale con la normativa UE
- Definizione di una governance nazionale per l'attuazione delle nuove misure di cybersicurezza
- Potenziamento della sicurezza informatica e della resilienza cibernetica delle PA

Tessuto produttivo

- Razionalizzazione delle attività di vigilanza per una semplificazione degli obblighi in capo ai soggetti
- Potenziamento della sicurezza informatica del tessuto produttivo nazionale
- Creazione di un «sistema imprese» cyber resiliente

Alcuni elementi fondanti della Direttiva NIS2

Recepimento entro il 17 ottobre 2024

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**)

Settori altamente critici (1/2)

SETTORE	SOTTOSETTORE O TIPO DI SOGGETTO	Soggetti NIS1 e CER	Grandi imprese	Medie imprese	Piccole e micro imprese
Energia	Energia elettrica; **teleriscaldamento e teleraffrescamento**; petrolio; gas; **idrogeno**	Essenziali	Essenziali	Importanti[1]	Fuori ambito[2]
Trasporti	Trasporto aereo; trasporto ferroviario; trasporto per vie d'acqua; trasporto su strada				
	TPL				
Settore bancario	Enti creditizi				
Infrastrutture dei mercati finanziari	Gestori delle sedi di negoziazione; controparti centrali				
Settore sanitario	Prestatori di assistenza sanitaria; **laboratori di riferimento dell'UE; soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali; soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici; soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica**				
Acqua potabile	Fornitori e distributori di acque destinate al consumo umano (esclusi i soggetti per cui tale attività non è essenziale)				
Acque reflue	Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali (escluse quelle per cui tale attività non è essenziale)				

[1] Possibile identificazione governativa come essenziali

[2] Possibile identificazione governativa come importanti o essenziali

Settori altamente critici (2/2)

<table>
<tr><th>SETTORE</th><th>SOTTOSETTORE O TIPO DI SOGGETTO</th><th>Soggetti NIS1 e CER</th><th>Grandi imprese</th><th>Medie imprese</th><th>Piccole e micro imprese</th></tr>
<tr><td rowspan="12">Infrastrutture digitali</td><td>Fornitori di servizi fiduciari qualificati</td><td rowspan="17">Essenziali</td><td colspan="3" rowspan="2">Essenziali</td></tr>
<tr><td>Fornitori di servizi DNS (esclusi gli operatori dei server dei nomi radice)</td></tr>
<tr><td>Registri dei nomi di dominio di primo livello (TLD)</td><td colspan="3">Essenziali</td></tr>
<tr><td>Fornitori di reti pubbliche di comunicazione</td><td colspan="2" rowspan="2">Essenziali</td><td rowspan="2">Importanti[1]</td></tr>
<tr><td>Fornitori di servizi di comunicazione elettronica accessibili al pubblico</td></tr>
<tr><td>Fornitori di servizi fiduciari non qualificati</td><td rowspan="6">Essenziali</td><td rowspan="6">Importanti[1]</td><td rowspan="6">Fuori ambito[2]</td></tr>
<tr><td>Fornitori di punti di interscambio internet</td></tr>
<tr><td>Fornitori di servizi di cloud computing</td></tr>
<tr><td>Fornitori di servizi di data center</td></tr>
<tr><td>Fornitori di reti di distribuzione dei contenuti (content delivery network)</td></tr>
<tr><td>Gestione dei servizi TIC (business-to-business)</td><td>Fornitori di servizi gestiti</td></tr>
<tr><td>Fornitori di servizi di sicurezza gestiti</td></tr>
<tr><td rowspan="2">Pubblica Amministrazione</td><td>Enti della pubblica amministrazione centrali e regionali</td><td colspan="3">Essenziali</td></tr>
<tr><td>Enti della pubblica amministrazione a livello locale</td><td colspan="3">Importanti[1]</td></tr>
<tr><td>Spazio</td><td>Operatori di infrastrutture terrestri</td><td>Essenziali</td><td>Importanti[1]</td><td>Fuori ambito[2]</td></tr>
</table>

[1] Possibile identificazione governativa come essenziali

[2] Possibile identificazione governativa come importanti o essenziali

Altri settori critici

SETTORE	SOTTOSETTORE O TIPI DI SOGGETTO	Soggetti NIS1 e CER	Grandi e medie imprese	Piccole e micro imprese
Servizi postali e di corriere		Essenziali	Importanti[1]	Fuori ambito[2]
Gestione dei rifiuti	Esclusi i soggetti per cui tale attività non è essenziale			
Fabbricazione, produzione e distribuzione di sostanze chimiche				
Produzione, trasformazione e distribuzione di alimenti				
Fabbricazione	Fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro, computer e prodotti di elettronica e ottica, apparecchiature elettriche, macchinari e apparecchiature n.c.a., autoveicoli, rimorchi e semirimorchi e altri mezzi di trasporto			
Fornitori di servizi digitali	Fornitori di mercati online, di motori di ricerca online e di **piattaforme di servizi di social network**			
Ricerca	Organizzazioni di ricerca			
	Istituti di istruzione che svolgono attività di ricerca critiche			

[1] Possibile identificazione governativa come essenziali

[2] Possibile identificazione governativa come importanti o essenziali

Direttiva NIS2

(Obblighi)

Panoramica degli obblighi

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)

Ambiti delle 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 fornitori […]

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

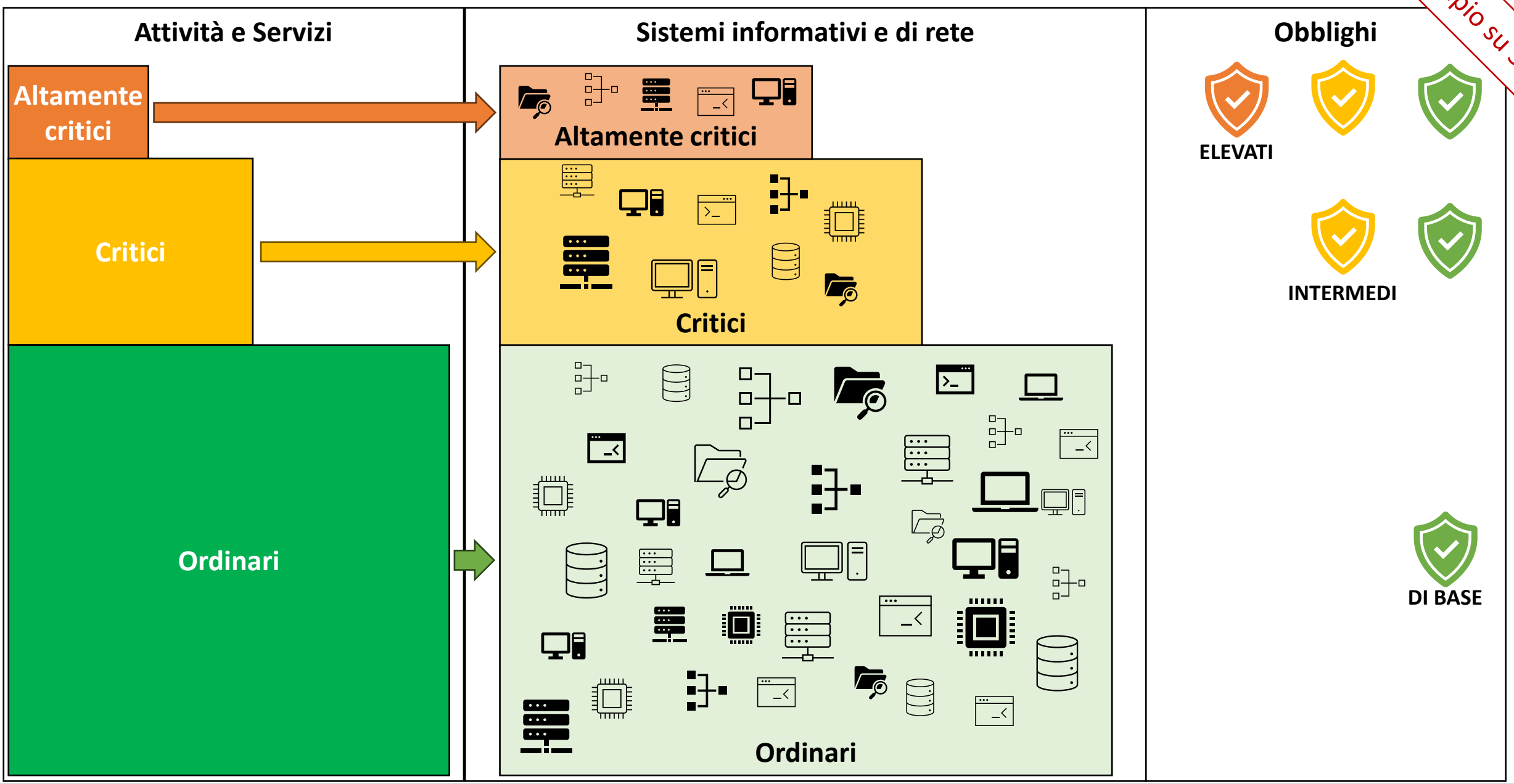
Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura

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

Esempio su 3 livelli



Approccio agli obblighi in materia di misure di sicurezza

Esempio su 3 livelli

PR.IP-9: Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro				
		SISTEMI ALTAMENTE CRITICI	**SISTEMI CRITICI**	**SISTEMI ORDINARI**
Business continuity	Requisiti	Alta affidabilità	Ridondanza a freddo	Piano di business continuity
	Termine	Entro 18 mesi	Entro 12 mesi	Entro 6 mesi
Backup dati offline	Requisiti	RPO max 12 ore	RPO max 48 ore	Raccomandato
	Termine	Entro 18 mesi	Entro 18 mesi	
Piano di DR	Requisiti	RTO max 72 ore	RTO max 5 giorni	Raccomandato
	Termine	Entro 24 mesi	Entro 24 mesi	
Soluzione di DR	Requisiti	RTO max 72 ore	Raccomandato	N/A
	Termine	Entro 36 mesi		
Sito di DR	Requisiti	Best practices	Raccomandato	N/A
	Termine	Entro 48 mesi		

Approccio agli obblighi in materia di notifica di incidente

Esempio su 3 livelli

	Pre-allarme e notifica		
	SISTEMI ALTAMENTE CRITICI	**SISTEMI CRITICI**	**SISTEMI ORDINARI**
Guasto	12h/24h	Volontario	Volontario
Sorpasso autorizzazioni	12h/24h	Volontario	Volontario
Persistenza	12h/24h	24h/72h	Volontario
Evasione	12h/24h	24h/72h	Volontario
Comando e controllo	12h/24h	24h/72h	Volontario
Esplorazione	12h/24h	24h/72h	Volontario
Accesso credenziali	12h/24h	24h/72h	Volontario
Lateral movement	12h/24h	24h/72h	Volontario
Raccolta	12h/24h	24h/72h	Volontario
Esfiltrazione	12h/24h	24h/72h	Volontario
Azioni sugli obiettivi	6h/12h	24h/48h	24h/72h
Disservizio	6h/12h	24h/48h	24h/72h

+ Linee guida per la definizione delle SLA relative ai guasti e ai disservizi

Direttiva NIS2

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

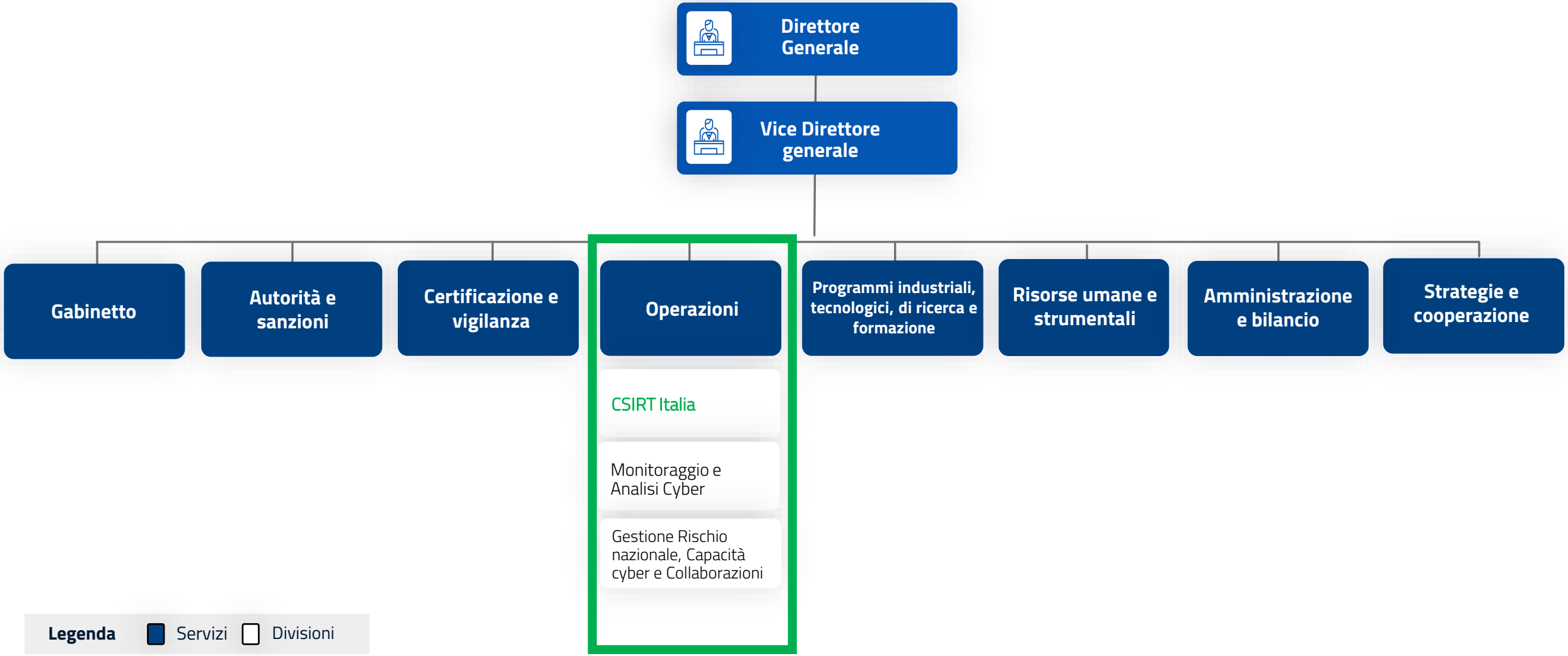
DIRETTIVA NIS2

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 – Struttura ACN



DIRETTIVA NIS2

CSIRT ITALIA – *Servizio Operazioni*

Il Servizio Operazioni è la **struttura operativa** dell'Agenzia incaricata delle attività di prevenzione, monitoraggio, rilevamento, analisi e risposta per prevenire e gestire eventi di natura cibernetica, all'interno della quale opera lo **CSIRT Italia**.

Per assicurare lo svolgimento delle funzioni operative, il servizio 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*.**

CSIRT: Computer Security Incident Response Team
MAC: Monitoraggio ed Analisi Cyber
GRICC: Gestione Rischio Nazionale, Capacità Cyber e Collaborazioni

DIRETTIVA NIS2

CSIRT ITALIA – *Sintesi servizi erogati*

CSIRT Italia

SERVIZI REATTIVI

- INCIDENT HANDLING SUPPORT 24/7
- REMEDIATION PLAN DEFINITION SUPPORT
- MALWARE & SUSPICIOUS ARTIFACT ANALYSIS
- DFIR TEAM (DEPLOYABLE IF NEEDED)

SERVIZI PROATTIVI

- EXPOSED ATTACK SURFACE MONITORING
- ACTORS, CAMPAIGNS & VULNERABILITY MONITORING
- EXPERT ANALYSIS ON CYBER THREATS
- EARLY WARNING ON EVENTS OF NATIONAL RELEVANCE

GESTIONE RISCHIO & GOVERNANCE

- INCIDENT SYSTEMIC IMPACT EVALUATION
- RISK MANAGEMENT
- FORECAST ANALYSIS AND THREAT TRENDS
- ACCREDITATION & CERTIFICATION

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

Principali novità

Monitora e analizza minacce, vulnerabilità e incidenti a livello nazionale e, su richiesta, secondo modalità definite **fornisce**, se del caso, **assistenza** ai soggetti essenziali e importanti interessati al monitoraggio

Può effettuare, secondo modalità e procedure definite, una **scansione proattiva e non intrusiva dei sistemi informatici e di rete accessibili al pubblico** di soggetti essenziali e importanti al fine di individuare se gli stessi siano vulnerabili o configurati in modo non sicuro ed informarne i soggetti

Emette preallarmi, allerte e bollettini nonché **divulga informazioni** su minacce, vulnerabilità e incidenti

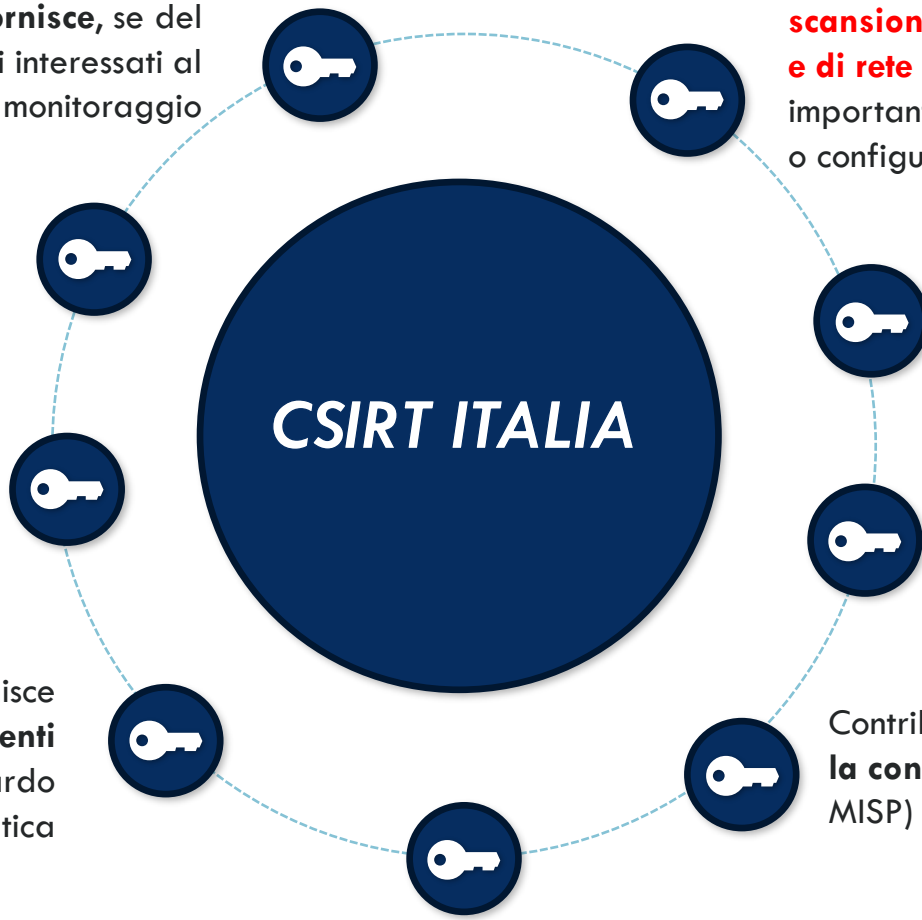
Partecipa alla **CSIRT Network**

Fornisce una risposta agli incidenti e assistenza ai soggetti essenziali e importanti interessati, se del caso

Agisce in qualità di **coordinatore ai fini del processo di divulgazione coordinata delle vulnerabilità** (c.d. CVD)

Raccoglie e analizza dati forensi, fornisce **un'analisi dinamica dei rischi e degli incidenti** nonché una **consapevolezza situazionale** riguardo la sicurezza informatica

Contribuisce allo **sviluppo di strumenti sicuri per la condivisione delle informazioni** (ad. es la MISP)



Effettua, **su richiesta** del soggetto essenziale o importante e secondo modalità e procedure definite, una **scansione proattiva dei suoi sistemi informatici e di rete** per rilevare vulnerabilità con potenziale impatto significativo

CSIRT ITALIA – *Focus CVD* (Coordinated Vulnerability Disclosure)

Processo tra la persona fisica o giuridica che segnala una vulnerabilità e il fabbricante o fornitore di servizi TIC o prodotti TIC potenzialmente vulnerabili, che può essere **coordinato dal CSIRT** quale intermediario fidato, il quale facilita, su richiesta di una delle parti, le interazioni tra tutti i soggetti interessati [Direttiva NIS2 Art. 12 e 11]

PERCHE' LA CVD

Minimizzare la finestra di esposizione delle vulnerabilità:

- quando viene scoperta una vulnerabilità è probabile che questa sia già sfruttata ai fini malevoli o che sia stata scoperta nello stesso periodo da attori che operano non in buona fede;
- concordare il momento in cui si rende nota al pubblico, al fine di
  - dare possibilità ai produttori di sviluppare i necessari aggiornamenti;
  - consentire ai soggetti vulnerabili di applicare le contromisure.

Incoraggiare la ricerca di vulnerabilità «a fin di bene»

- programmi di bug-bounty (solitamente all'estero) remunerano i ricercatori che trovano vulnerabilità anche per scoraggiare gli stessi a vendere le vulnerabilità ai criminali.

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.

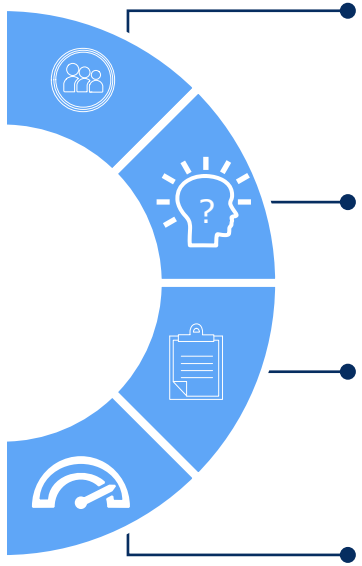
NEAR-MISS

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.**

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

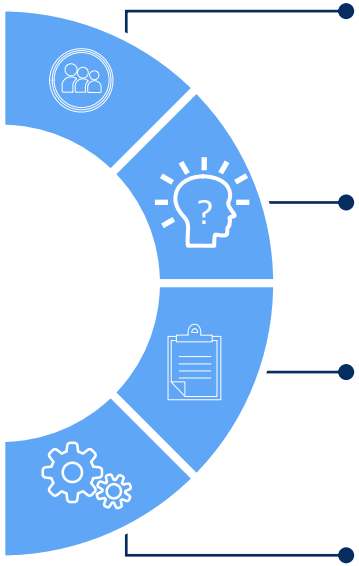
A seguito della notifica sarà aperto un canale di comunicazione diretto, tramite il quale il CSIRT Italia offrirà al soggetto un supporto alle attività di incident handling.

OBBLIGHI DI NOTIFICA – *Notifica destinatari servizi (art. 23 Direttiva NIS2)*

Se opportuno, i soggetti essenziali e importanti comunicano, senza ingiustificato ritardo:

- Ai **destinatari dei loro servizi,** gli **incidenti significativi** che possono ripercuotersi negativamente sulla fornitura di tali servizi.
- Ai **destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa,** qualsiasi **misura o azione correttiva** che tali destinatari sono in grado di adottare in risposta a tale minaccia.
- Ai **destinatari dei loro servizi** di cui al primo punto, anche la minaccia informatica significativa.

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.

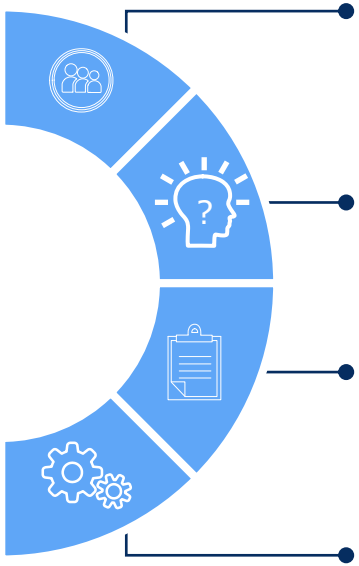
PERCHE' NOTIFICARE | La notifica volontaria al CSIRT Italia è prevista dall'articolo 30 della Direttiva NIS2.

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.

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

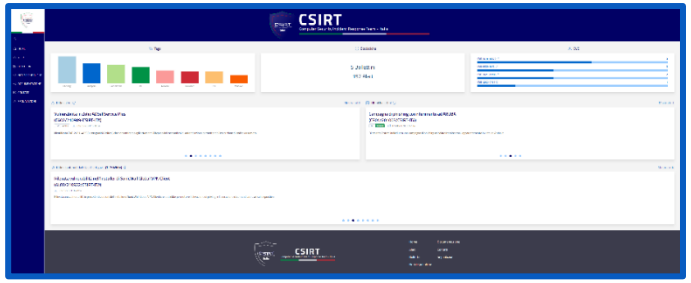
CSIRT ITALIA – Portali e caselle istituzionali

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)



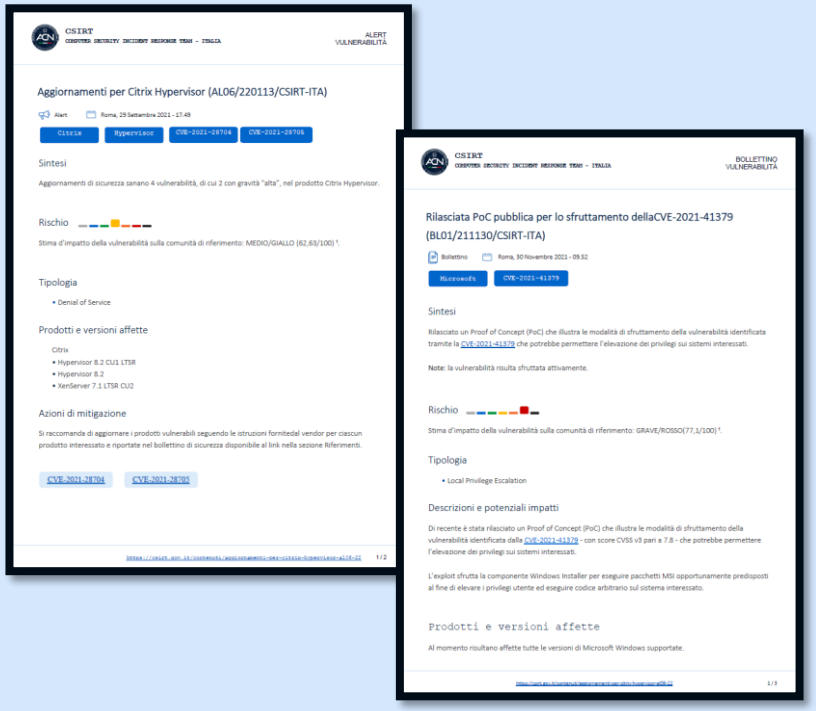
Caselle di posta istituzionali

- 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



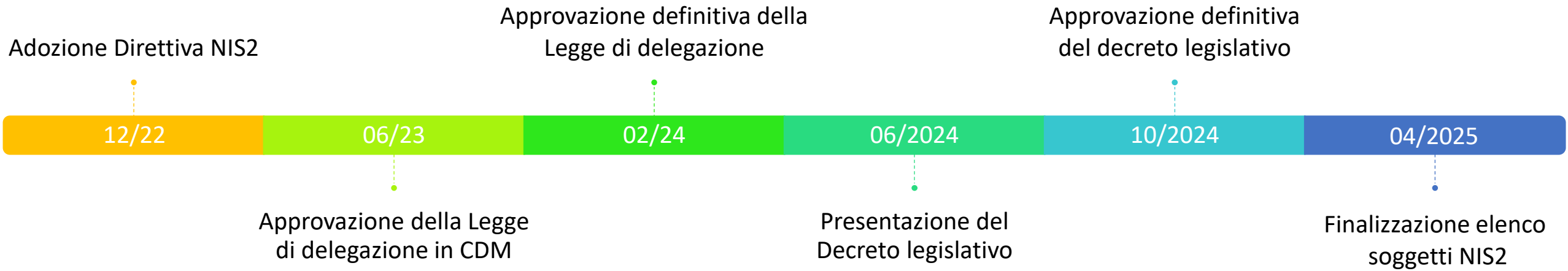
Alert e bollettini su nuove campagne e vulnerabilità, contenenti gli indicatori di compromissione (IoC) e le azioni di mitigazioni consigliate

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

Recepimento

Cronologia e prossime scadenze



Tavolo con le Autorità di settore NIS

Sensibilizzazione del tessuto industriale

Tavoli settoriali NIS


AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT