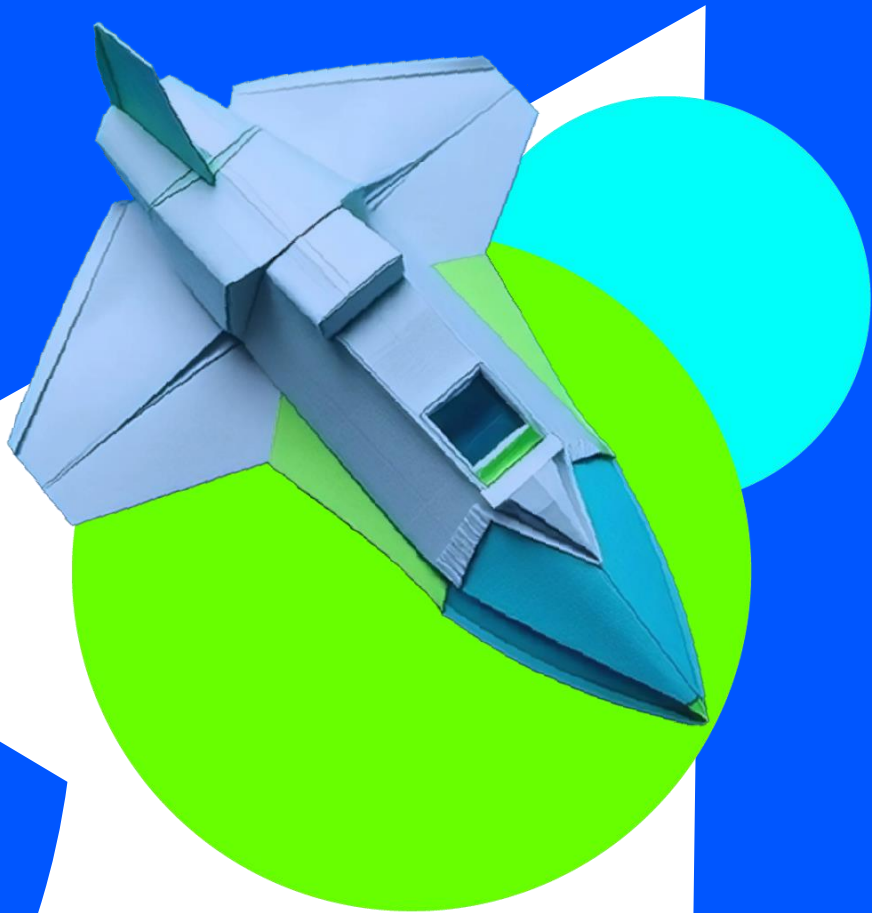


Lunedì 18 novembre 2024



In collaborazione con:





NIS2 per imprenditori:

Nuovi obblighi e strategie
per adeguarsi agli standard
di sicurezza

Relatori

Francesca Falcitelli

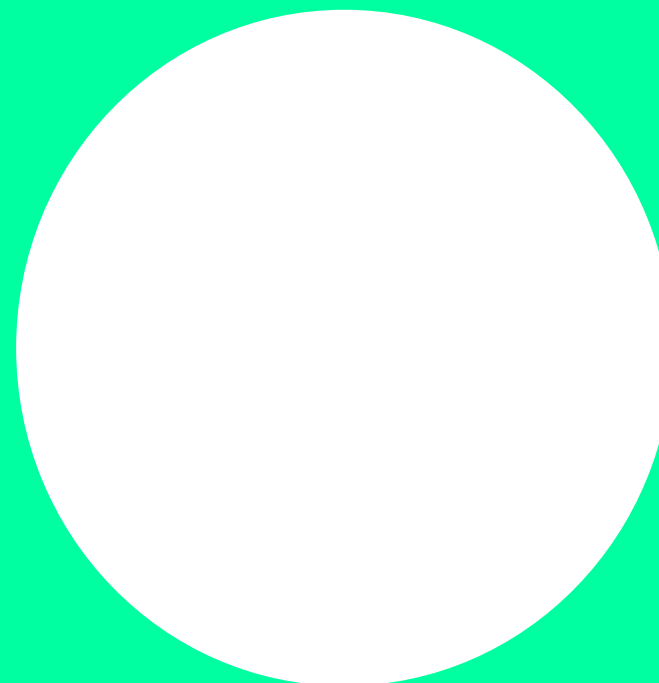
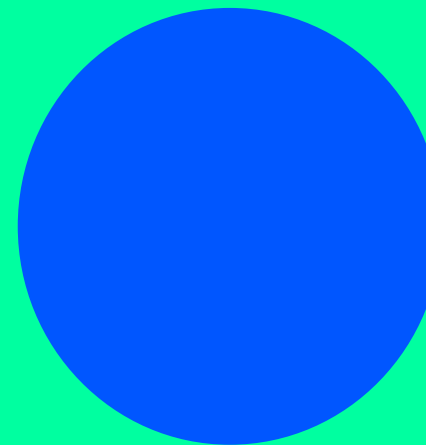
Sales & Marketing Manager – Nicma Company

Giulio Valeri

CEO – Software Solutions

Luana Lanfranchi

CEO & Founder - Eight Solutions Srl



Dalla NIS alla NIS2

Direttiva NIS 2016/1148 - recepita in Italia dal D.Lgs 65 del 2018 e abrogata dalle nuove disposizioni

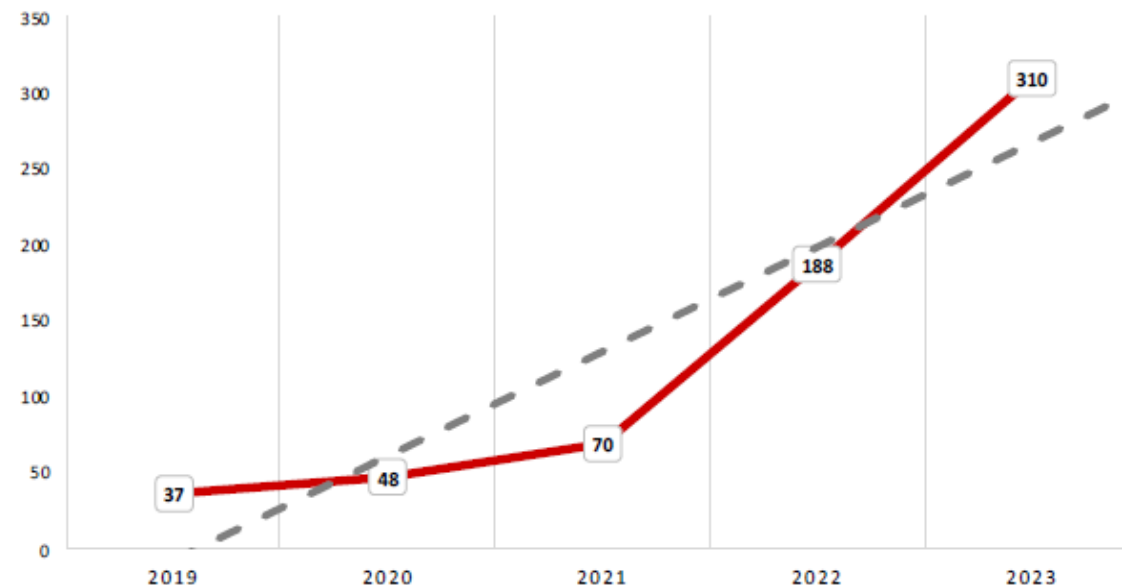
MOTIVAZIONI DELL'AGGIORNAMENTO A NIS2:

1. Digitalizzazione
2. Incremento degli attacchi in qualità e quantità
3. Situazione critica imprese e Pubblica Amministrazione

Incremento degli attacchi – Report CLUSIT

- Tendenza in rapido aumento in particolare ultimi due anni ovvero 2022 e 2023
- Incremento in Italia rispetto al trend mondiale 65% vs 12% (indice di protezione inadeguata)
- Tipologia di attaccanti in Italia:
 - ✓ **Cybercrime 64%**
 - ✓ **Hacktivism 36%**

Cyber attacchi in Italia 2019 - 2023



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Problematiche principali

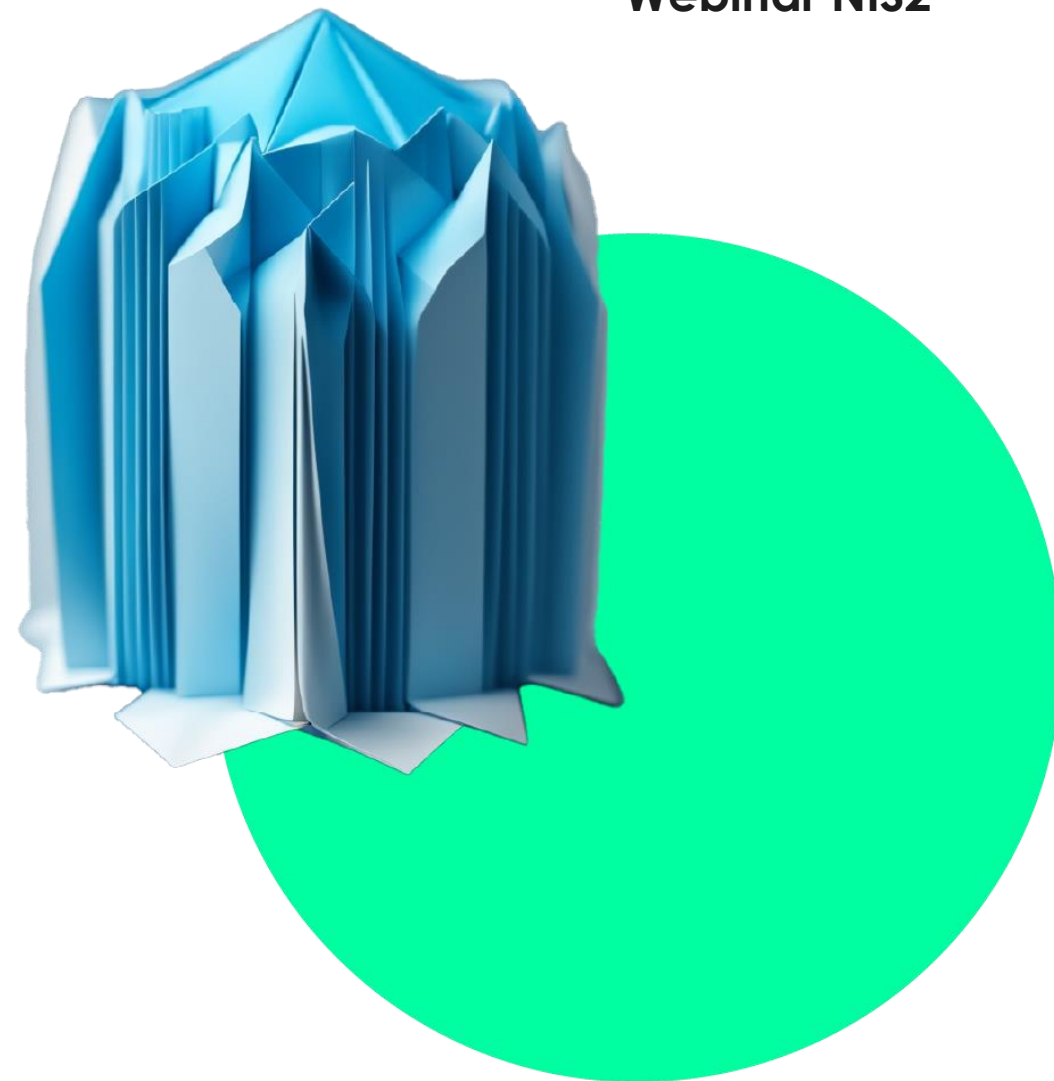
- Anche secondo il CLUSIT **la componente più vulnerabile è il fattore umano**
- **Mancanza di formazione e consapevolezza**
- **Lavoro da remoto**
- **Dispositivi mobile**

Mancanza di un sistema organizzato ed efficiente sul tema della Security

I dati del Rapporto CLUSIT sono rilevati dai DATA BREACH denunciati.

DATA BREACH (art. 4 par. 12 GDPR)

È la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.



NIS2 in Italia

- Il 27 dicembre 2022 è stata pubblicata sulla Gazzetta Ufficiale dell'Unione Europea la **Direttiva UE 2022/2555 c.d. Direttiva NIS 2**, con l'obiettivo di migliorare la capacità di prevenzione, risposta e resilienza agli incidenti di cybersecurity di operatori definiti come "Essenziali" e "Importanti", che forniscono beni e/o servizi di specifica rilevanza per la collettività.
- Il Consiglio dei Ministri ha approvato lo schema di Decreto legislativo per il recepimento della Direttiva in Italia, allineando così gli standard di sicurezza nazionali a quelli europei.
- La Direttiva doveva essere recepita dal diritto nazionale italiano entro il 17 ottobre 2024.
- **Decreto Legislativo di recepimento del 4 settembre 2024 n.138 - entrata in vigore il 16 ottobre 2024**

***Definizione di NIS - Network and Information Security
(Sicurezza delle informazioni)***

Interazioni tra NIS2 e GDPR (I)

1. Notifica di incidenti di sicurezza;
2. Valutazione del rischio e applicazione di misure di tecniche e organizzative;
3. Cooperazione e scambio di informazioni;
4. Accountability, policy e report;
5. Verifica della supply chain;
6. Obbligo di formazione del personale;



Interazioni tra NIS2 e GDPR (II)

1. Notifica di incidenti di sicurezza

- Entrambe le normative richiedono la **notifica di incidenti di sicurezza**, benché con focus diversi.
- **GDPR** - **notifica** di violazioni dei dati personali (Data Breach) **entro 72 ore** all'Autorità Garante e, a determinate condizioni, anche agli interessati.



Interazioni tra NIS2 e GDPR (II)

La Direttiva NIS2 richiede l'invio al CSIRT nazionale di:

1. **Pre-notifica entro 24 ore**
2. **Notifica entro 72 ore**
3. **Relazione finale entro 1 mese**



Interazioni tra NIS2 e GDPR (II)

CSIRT – COMPUTER SECURITY INCIDENT RESPONSE TEAM

Il **CSIRT Italia** è un organo informativo, di gestione e collaborazione, istituito presso **l'Agenzia per la Cybersicurezza Nazionale (ACN)**, con i **seguenti compiti** (definiti dal D.Lgs 18 maggio 2018, n. 65 e dal DPCM 8 agosto 2019 art. 4):

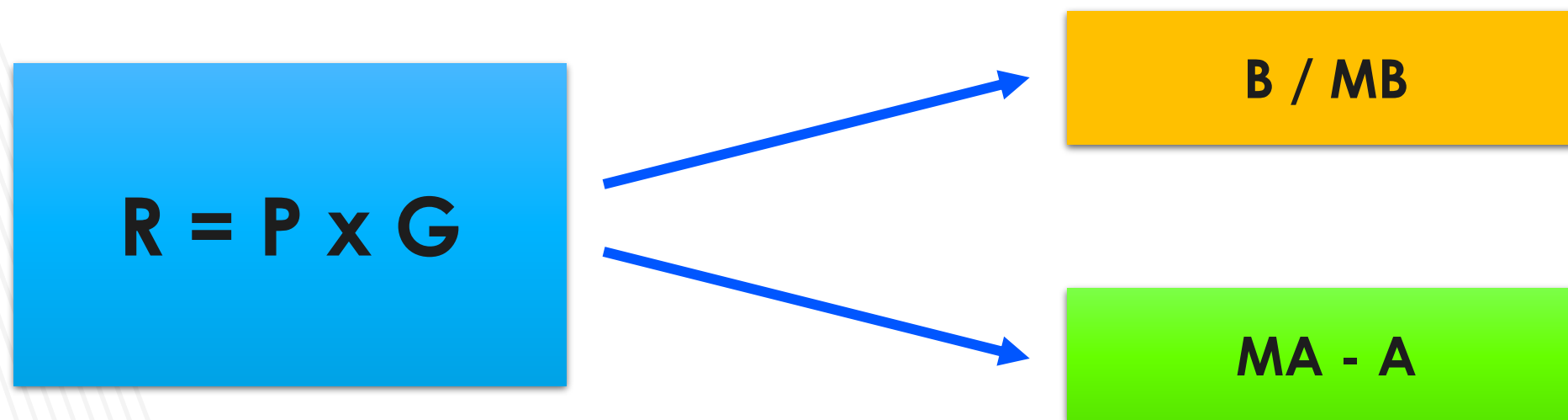
- ✓ **il monitoraggio degli incidenti a livello nazionale;**
- ✓ **l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi ed incidenti;**
- ✓ **l'intervento in caso di incidente;**
- ✓ **l'analisi dei rischi e degli incidenti;**
- ✓ **la sensibilizzazione situazionale;**
- ✓ **la partecipazione alla rete dei CSIRT.**

Interazioni tra NIS2 e GDPR (III)

2. ANALISI DEI RISCHI E ADEGUATE MISURE DI SICUREZZA:

- Sia il GDPR che la NIS2 enfatizzano l'importanza di valutare i rischi per la sicurezza e implementare misure tecniche e organizzative appropriate per mitigarli.
- Il GDPR si concentra sui rischi per i diritti e le libertà fondamentali delle persone, la NIS2 sui rischi per la sicurezza delle reti e dei sistemi informativi.
- **GDPR – approccio basato sul rischio.**
- **NIS2 – approccio c.d. «multirischio».**

GDPR: Approccio basato sul **rischio**



NIS2: definizione di multirischio

- **D.Lgs 138/2024 art.2 lett. dd) – «approccio multi-rischio»:** c.d. approccio all-hazards, l'approccio alla gestione dei rischi che considera quelli derivanti da tutte le tipologie di minaccia ai sistemi informativi e di rete, nonché al loro contesto fisico, quali furti, incendi, inondazioni, interruzioni, anche parziali, delle telecomunicazioni e della corrente elettrica e in generale degli accessi fisici non autorizzati



I danni Derivanti da una **violazione di sicurezza**

1. Perdita del controllo dei dati personali
2. Discriminazione (sociale e/o economica)
3. Furto d'identità
4. Furto di marchi e brevetti
5. Perdite finanziarie (es. danno reputazionale, pagamento di un riscatto, ecc...)
6. Decifratura non autorizzata dei dati personali
7. Compromissione del segreto professionale

Interazioni tra NIS2 e GDPR (IV)

3. COOPERAZIONE E SCAMBIO DI INFORMAZIONI

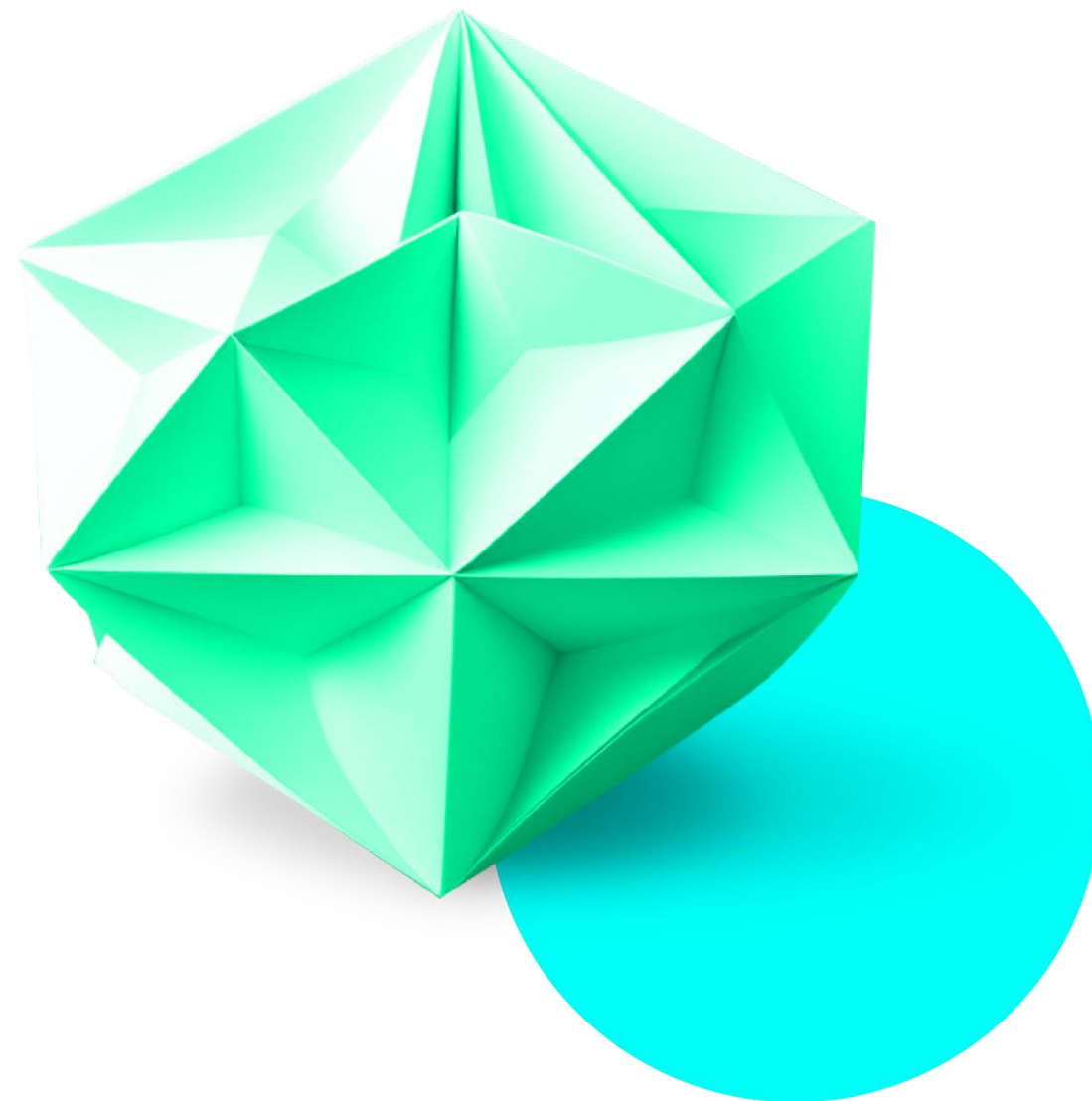
- **Entrambe** le normative promuovono la cooperazione e lo scambio **SICURO** di informazioni tra gli Stati membri per migliorare la resilienza di tutti i sistemi a livello europeo



Interazioni tra NIS2 e GDPR (V)

4. ACCOUNTABILITY, POLICY E REPORT

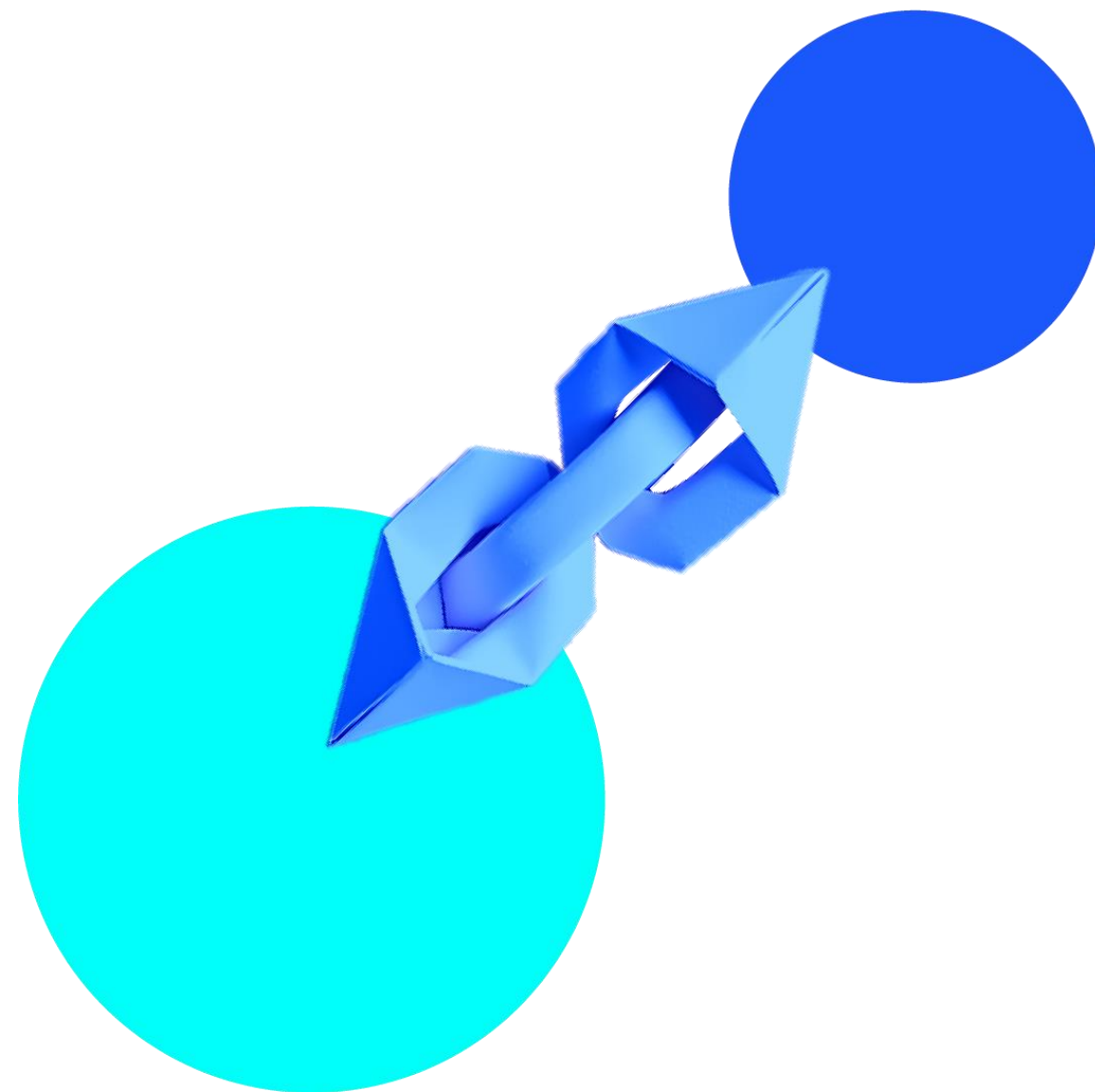
- **Comportamento «PROATTIVO»** della Governance ovvero la documentazione e dimostrazione delle attività svolte da parte dei titolari (es. attraverso procedure di sicurezza, formazione, disciplinari interni, ecc...)



Interazioni tra NIS2 e GDPR (VI)

5. VERIFICA DELLA SUPPLY CHAIN

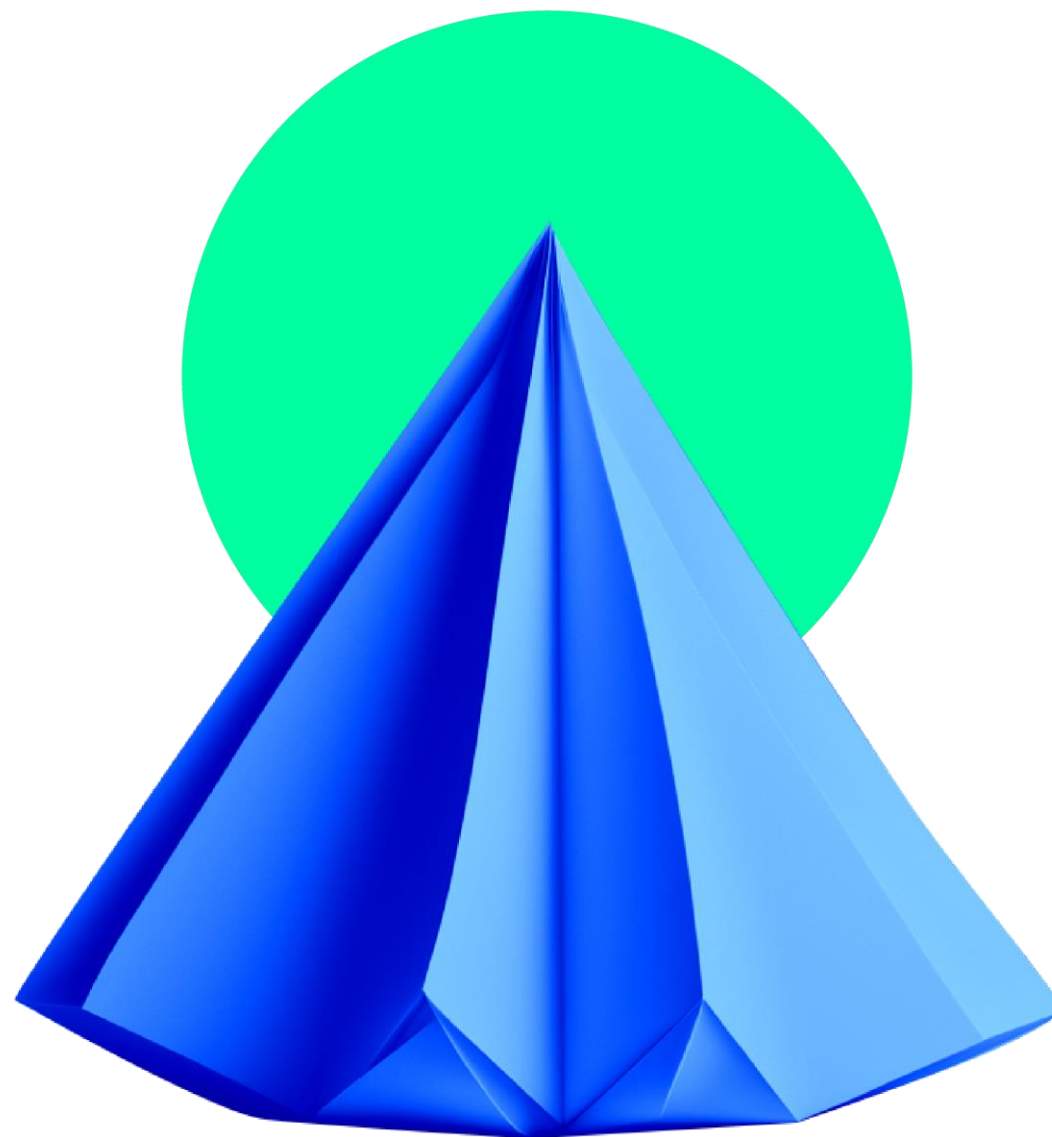
- **Verifica della sicurezza della propria catena di fornitura.**
 - ✓ La **NIS2** da un punto di vista informatico e procedurale;
 - ✓ il **GDPR** sotto tutti i profili (IT, legale, procedurale, tecnico, certificazioni, ecc...).



Interazioni tra NIS2 e GDPR (VII)

6. OBBLIGO DI FORMAZIONE

- **GDPR (art.29 – art.32)** in ambito Data Protection per tutti gli Autorizzati al trattamento;
- **D.LGS 138/2024** in materia di sicurezza ed igiene informatica, per gli organi direttivi, gli organi di amministrazione ed il personale dipendente dei soggetti essenziali e dei soggetti importanti (art.23).



Ambito di applicazione **DIRETTIVA NIS2**

(art. 3 D.Lgs 138/2024 –Allegati I-II-III-IV)

- **ALLEGATO I – descrive i settori ritenuti altamente critici + sotto settori e tipologie di soggetti** (es. energia elettrica, petrolio, gas, gestori di impianti di produzione e trasporto di idrogeno, trasporto aereo e ferroviario, settore sanitario, settore bancario, ecc....) – **c.d. SERVIZI ESSENZIALI.**
- **ALLEGATO II – descrive i settori ritenuti critici + sotto settori e tipologie di soggetti** (es. settore postale e di spedizioni, trattamento e gestione dei rifiuti, industrie chimiche, imprese alimentari, servizi digitali (social network, data center, ecc...) - **c.d. SERVIZI IMPORTANTI.**
- **ALLEGATO III – descrive le categorie di P.A. soggette al Decreto** (es. Amministrazioni centrali, regionali, provinciali, locali, ecc...) - **c.d. SERVIZI ESSENZIALI.**
- **ALLEGATO IV - descrive le ulteriori tipologie di soggetti a cui si applica il Decreto** (es. fornitori di trasporto pubblico locale, soggetti che svolgono attività di interesse culturale, società partecipate, società a controllo pubblico, ecc...).

Ambito di applicazione DIRETTIVA NIS2

(art. 3 D.Lgs 138/2024)

- Il Decreto si applica alle medie e grandi imprese descritte negli Allegati I e II.
- Per determinare se un soggetto è da considerarsi PMI o grande impresa si applica la **Raccomandazione 2003/361/CE** che divide:
 - ✓ **MEDIE IMPRESE** - sono imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di EUR oppure il cui totale di bilancio annuo non supera i 43 milioni di EUR.
 - ✓ **PICCOLA IMPRESA** - è un'impresa che occupa meno di 50 persone e realizza un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di EUR.
 - ✓ **MICROIMPRESA** - è un'impresa che occupa meno di 10 persone e realizza un fatturato annuo oppure un totale di bilancio annuo non superiori a 2 milioni di EUR.

LA NIS2 SI APPLICA ANCHE AI (PICCOLI) FORNITORI DEI SERVIZI ESSENZIALI ED IMPORTANTI

Ambito di applicazione DIRETTIVA NIS2

(art. 3 D.Lgs 138/2024)

- Il Decreto si applica, altresì, **al di là delle dimensioni**, a:
 - a) **Soggetti che sono identificati come critici ai sensi del D.Lgs n. 134/2024**, che recepisce la Direttiva UE 2022/2557 relativa alla resilienza dei soggetti critici (es. settore dell'energia elettrica - si tiene conto della valutazione dei rischi e dell'infrastruttura critica);
 - b) **Ai fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico;**
 - c) **Ai prestatori di servizi fiduciari (es. vigilanza privata);**
 - d) **Ai gestori di registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio;**
 - e) **Ai fornitori di servizi di registrazione dei nomi di dominio.**

I soggetti essenziali ed importanti

Dovranno:

- **Registrarsi sull'apposita piattaforma** (a partire dal 1 dicembre 2024 ed entro il 28 febbraio 2025) **messa a disposizione dall'ACN (Agenzia per la Cybersicurezza Nazionale)** la quale (entro aprile 2025) redigerà l'elenco ufficiale delle aziende e delle PA interessate.
- **Entro il 1 gennaio 2026** - adeguarsi all'art. 25 relativo alla notifica degli incidenti;
- **Entro il 1 gennaio 2026** - **Comunicare ed aggiornare annualmente (entro il 1 gennaio 2026) un elenco delle attività svolte e dei servizi erogati.**



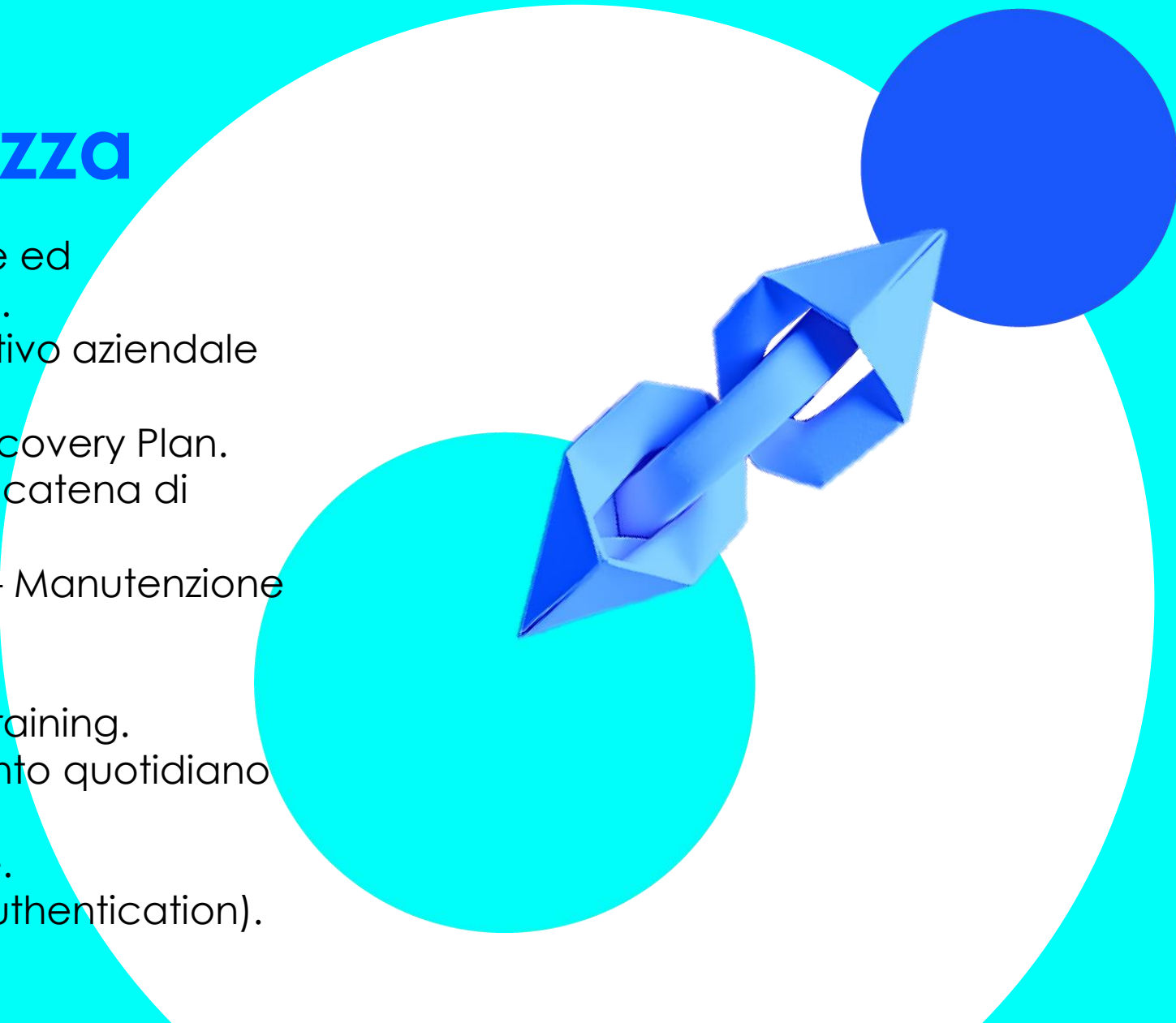
Gli adempimenti della Direttiva NIS2

1. Policy di analisi dei rischi e sicurezza dei sistemi informatici.
2. Sistemi di gestione degli incidenti.
3. Business Continuity e Disaster Recovery.
4. Sicurezza della Supply Chain.
5. Politiche di sicurezza, sviluppo e manutenzione dei sistemi – Monitoraggio delle vulnerabilità.
6. Internal Auditing (Audit interni).
7. Igiene informatica e Formazione.
8. Politiche relative alla Crittografia.
9. Policy per HR - Gestione degli accessi e degli Asset aziendali.
10. Policy sull'utilizzo dell'Autenticazione a più fattori.



La NIS2 tradotta in misure di **Sicurezza**

1. Adottare misure di sicurezza tecniche ed organizzative proporzionate al rischio.
2. Implementare un Modello Organizzativo aziendale per la gestione degli incidenti.
3. Business Continuity Plan e Disaster Recovery Plan.
4. Verifica dell'affidabilità della propria catena di fornitura.
5. Policy di Vulnerability Management – Manutenzione dei sistemi informativi.
6. Audit interni periodici di controllo.
7. Formazione, simulazioni periodiche, training.
8. Utilizzare la Crittografia come strumento quotidiano di sicurezza.
9. Policy condivise per le Risorse Umane.
10. Policy ed utilizzo MFA (Multi-Factor Authentication).



Le sanzioni (art.34)

- Le sanzioni per le imprese dei Servizi **Importanti** possono arrivare **fino a 7.000.000 euro o all'1,4% del fatturato annuo complessivo**, mentre per i Servizi **Essenziali** possono raggiungere i **10.000.000 euro o il 2% del fatturato annuo complessivo**, a seconda di quale importo sia maggiore.
- Le sanzioni per mancata registrazione sulla piattaforma ACN possono essere erogate **fino allo 0,1% del fatturato annuo globale**.





La tecnologia fatta di persone

Grazie per l'attenzione!

Contatti:

✓ www.nicma.com

✓ marketing@nicma.com

Webinar NIS2

18/11/2024

