NIS2: DA OBBLIGO NORMATIVO A OPPORTUNITA' DELLA CYBERSECURITY

Convegno Webinar gratuito organizzato dalla Fondazione dell'Ordine degli ingegneri Provincia di Perugia

Mercoledì, 21/05/2025

Da obbligo normativo a opportunità della cybersecurity

INTRODUZIONE ALLA NIS2

Soggetti -Autorità - Notifica - Sanzioni

OBBLIGHI INTRODOTTI DALLA NIS2

Timeline – Misure di sicurezza - Comunicazione - Formazione

SOLUZIONI PER LA COMPLIANCE ALLA NIS2

Assessment – Consulenza – Strumenti – Formazione - Documentazione

Sinapsi WE CONNECT DOTS Lusios FB

NIS2

SPEAKER

Avv. Filippo Bianchini

POWERED BY SINAPSI, LUSIOS, AVV.BIANCHINI

SINAPSI
WE CONNECT DOTS

Lusios

FB

Avv. Filippo Bianchini

- Avvocato cassazionista, iscritto al Foro di Perugia
- DPO e Valutatore privacy certificato UNI 11697 (a breve UNI EN 17740) – Lead Auditor 27001:2022 e 42001:2023 – CIPP/E
- Membro supplente dell'Autorità Garante per la protezione dei dati personali di San Marino
- Membro del Consiglio Direttivo di ASSO DPO e AIP-ITCS, fellow ISLC
- Docente nel Master Universitario Data Protection, Cybersecurity e Digital Forensics dell'Università degli Studi di Perugia e nel progetto Erasmus+ BuTH-AI, Building Trust In Human-Centric Artificial Intelligence della Link Campus University
- Membro dell'EDPB «Support Pool of Experts»
- Membro del Cybersecurity National Lab, nodo UniPg
- Componente UNI CT 510

POWERED BY SINAPSI, LUSIOS, AVV.BIANCHINI

NIS2

Introduzione alla sicurezza delle informazioni: perché la NIS2?

POWERED BY SINAPSI, LUSIOS, AVV.BIANCHINI

SINAPSI
WE CONNECT DOTS

Lusios

FB

Cronistoria

6 luglio 2016
Adozione della NIS

9 maggio 2018
Termine recepimento della NIS nella legislazione nazionale

7 luglio 2020
Commissione Europea avvia una consultazione sulla riforma della NIS

27 dicembre 2022
La Direttiva (UE) 2022/2555 NIS2 viene pubblicata nella GU UE ed entra in vigore il 16 gennaio 2023

1 ottobre 2024
Pubblicato in GU il Decreto Legislativo 4 settembre 2024, n. 138, che entra in vigore il 18 ottobre 2024

31 marzo 2025
Avvio ufficiale NIS2

Confronto NIS e NIS2: cosa è cambiato?

- Differente **classificazione** dei soggetti
- Ampliamento del **campo di applicazione**
- Istituzione di una **Rete Europea di Organizzazioni di Collegamento per le Crisi Informatiche**
- Obblighi diretti al **management**
- Disposizioni più precise sul processo di **segnalazione degli incidenti**
- Maggiore coordinamento nella **divulgazione** di nuove vulnerabilità
- Elenco di **sanzioni** amministrative

Definizioni più rilevanti della NIS2

- Sicurezza dei sistemi informativi e di rete
- Sicurezza informatica
- Incidente
- Quasi-incidente (*near-miss*)
- Incidente di sicurezza informatica su vasta scala
- Gestione degli incidenti
- Minaccia informatica
- Minaccia informatica significativa
- Prodotto TIC
- Servizio TIC

I soggetti obbligati

Fra i soggetti impattati da NIS2 rientrano anche le **piccole e micro-imprese** operanti in settori chiave e la **supply chain**

Soggetti essenziali (EE) Soglia dimensionale: varia a seconda del settore, ma in genere 250 dipendenti, ricavi annui di 50 milioni di euro o bilancio di 43 milioni di euro	**Soggetti importanti (IE)** Soglia dimensionale: varia a seconda del settore, ma generalmente 50 dipendenti, ricavi annui di 10 milioni di euro o bilancio di 10 milioni di euro
Energia	Servizi postali
Trasporti	Gestione dei rifiuti
Finanza	Prodotti chimici
Pubblica Amministrazione	Ricerca
Salute	Alimentari
Spazio	Industria Manifatturiera
Approvvigionamento idrico (acqua potabile e acque reflue)	Provider digitali (social network, motori di ricerca, marketplace online)
Infrastrutture digitali (fornitori di servizi cloud computing e gestione ICT)	

NIS2

I requisiti principali

Gestione del rischio

Responsabilità aziendale

Obblighi di comunicazione

Continuità del business

POWERED BY SINAPSI, LUSIOS, AVV.BIANCHINI

SINAPSI WE CONNECT DOTS Lusios FB

D.lgs. 138/2024 – Eccezioni al criterio del dimensionamento

Il Decreto si applica, infine, **indipendentemente dalle dimensioni**, all'**impresa collegata** a un soggetto essenziale e importante **se** essa soddisfa **almeno uno** dei seguenti requisiti:

- adotta decisioni o esercita una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale;
- detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale;
- effettua operazioni di sicurezza informatica del soggetto importante o essenziale;
- fornisce servizi TIC o di sicurezza, anche gestiti, al soggetto importante o essenziale.

Cosa si intende per impresa collegata?

Codice Civile (art. 2359)

Sono considerate **collegate** le società sulle quali un'altra società esercita un'influenza notevole. L'influenza si presume quando nell'assemblea ordinaria può essere esercitato almeno un quinto dei voti ovvero un decimo se la società ha azioni quotate in mercati regolamentati

Raccomandazione CE 2003/361 recepita dal D.M. 18/04/2005 (art. 3, par. 3)

Sono considerate «**collegate**» le imprese, fra le quali esista una tra le seguenti relazioni:

1. un'impresa detiene la maggioranza dei diritti di voto degli azionisti o soci di un'altra impresa;
2. un'impresa detiene voti sufficienti per esercitare un'influenza dominante nell'assemblea ordinaria di un'altra impresa;
3. un'impresa ha il diritto di esercitare una influenza dominante su un'altra impresa in virtù di un contratto concluso con quest'ultima o in virtù di una clausola statutaria dello statuto di quest'ultima;
4. un'impresa azionista o socia di un'altra impresa controllata da sola, in virtù di un accordo stipulato con altri azionisti o soci dell'altra impresa, la maggioranza dei diritti di voto degli azionisti o soci di quest'ultima.

Clausola di salvaguardia

Clausola di salvaguardia: art. 3, co. 12 del D.lgs. 138/2024 al fine di chiedere all'Autorità di settore NIS di disapplicare quanto previsto dall'art. 6, par. 2 dell'allegato della Raccomandazione della Commissione Europea n. 361 del 6.5.2003 recepita dal D.M. 18.4.2005.

Cosa prevede tale paragrafo?
L'art. 6, par. 2 della raccomanda zione 2003/361/CE disciplina i valori da tenere in considerazione nel calcolo del valore dei dati di bilancio, fatturato ed effettivi da considerare per le imprese associate e collegate.

Cosa fare?
L'utente, nel corso della registrazione alla piattaforma ACN, potrà richiedere l'applicazione della clausola di salvaguardai nel caso in cui ritenga che il calcolo per il criterio dimensionale non sia proporzionato, cioè quando il soggetto è indipendente dalle sue imprese collegate in termini di sistemi informativi e di rete che utilizza nella fornitura dei suoi servizi e in termini di servizi che fornisce (art. 3, co. 4).

Le Autorità competenti

L'Agenzia per la Cybersicurezza Nazionale (ACN)

CSIRT Italia

Autorità di settore NIS

La piattaforma ACN

Determinazione del Direttore generale dell'Agenzia per la cybersicurezza nazionale
Determinazione 38565/2024

Quali sono i criteri per designare il punto di contatto?

Quali sono le informazioni necessarie per la registrazione?

Di quali competenze e caratteristiche deve essere dotato il Punto di contatto?

Quali sono i criteri per designare il punto di contatto?

La notifica dell'incidente

La NIS2 prevede anche la possibilità di **notifica volontaria** di incidenti (art.30), minacce informatiche e quasi incidenti, che rappresenta un ulteriore strumento per migliorare la consapevolezza e la preparazione complessiva

Pre-notifica senza ingiustificato ritardo e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo

Notifica senza ingiustificato ritardo e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo che indichi una valutazione iniziale dell'incidente, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione

Relazione intermedia a richiesta del CSIRT sui pertinenti aggiornamenti della situazione

Relazione finale entro un mese dalla trasmissione della notifica dell'incidente

Le sanzioni

Soggetti essenziali
Massimo 10.000.000 € o 2% del totale del fatturato mondiale annuo per l'esercizio precedente

Soggetti importanti
Massimo 7.000.000 € o 1,4% del totale del fatturato mondiale annuo per l'esercizio precedente

NIS2

SPEAKER

Ing. Michele Mercanti

POWERED BY SINAPSI, LUSIOS, AVV.BIANCHINI

SINAPSI
WE CONNECT DOTS

Lusios

FB

Ing. Michele Mercanti

- Sistemista esperto ed auditor ISO 9001, ISO 14001, ISO 45001, legge 231
- Esperto ed auditor di terza parte di sistemi di gestione ISO 27001, ISO 27017 ed ISO 27018
- Analista di Sistema per sviluppo software e valutazione della sicurezza di sistemi informatici
- DPO certificato secondo UNI11697 da Accredia
- Consulente e Formatore in materia di Privacy e Whistleblowing

POWERED BY SINAPSI, LUSIOS, AVV.BIANCHINI

Timeline NIS2

Entro il 31 dicembre 2024

Aziende e Pubbliche Amministrazioni dovranno svolgere un *assessment* per comprendere se siano o meno soggette agli obblighi della Direttiva NIS2, seguendo il dettato dell'Art. 3 del D.Lgs. 138/2024 e verificando gli Allegati I, II, III e IV, nonché di ogni altro atto che verrà emanato

Dal 1° Gennaio al 28 Febbraio

Di ogni anno successivo alla data di entrata in vigore del Decreto, tutti i soggetti interessati, sia essenziali o importanti, dovranno registrarsi o aggiornare la propria registrazione sulla piattaforma digitale

Timeline NIS2

Entro il **17 gennaio 2025** dovranno registrarsi sulla piattaforma:

- I fornitori di servizi di sistema dei nomi di dominio
- I gestori di registri dei nomi di dominio di primo livello
- I fornitori di servizi di registrazione dei nomi di dominio
- I fornitori di servizi di *cloud computing*
- I fornitori di servizi di *data center*
- I fornitori di reti di distribuzione dei contenuti
- I fornitori di servizi gestiti
- I fornitori di servizi di sicurezza gestiti
- I fornitori di mercati online, di motori di ricerca online e di piattaforma di servizi di social network

POWERED BY SINAPSI, LUSIOS, AVV.BIANCHINI

Timeline NIS2

Entro il 31 marzo

Di ogni anno, l'Autorità Nazionale competente NIS (ACN) redige l'elenco dei soggetti essenziali e dei soggetti importanti sulla base delle registrazioni avvenute

Tra il 1° aprile e il 15 aprile 2025

Attraverso la piattaforma, l'ACN comunicherà ai soggetti registrati l'inserimento nell'elenco dei soggetti essenziali o importanti

Dal 15 aprile al 31 maggio

I soggetti che avranno ricevuto la comunicazione attraverso la piattaforma dovranno fornire le ulteriori informazioni richieste dalla normativa:

- Lo spazio di indirizzamento IP pubblico e i nomi di dominio in uso o nella disponibilità del soggetto
- L'elenco degli Stati Membri in cui forniscono servizi che rientrano nell'ambito di applicazione del Decreto
- Qualsiasi persona fisica responsabile di un soggetto essenziale, indicando il ruolo presso il soggetto, i suoi recapiti aggiornati, compresi indirizzi e-mail e numeri di telefono
- Un sostituto del punto di contatto, indicando il ruolo presso il soggetto e i suoi recapiti

Timeline NIS2

Dal 1° maggio al 30 giugno

Di ogni anno a partire dalla ricezione della prima comunicazione (ovvero quando l'ACN comunica ai soggetti registrati l'inserimento nell'elenco dei soggetti essenziali o importanti, tramite piattaforma digitale), i soggetti essenziali o importanti comunicano e aggiornano un elenco delle proprie attività e dei propri servizi, comprensivo di tutti gli elementi necessari alla loro caratterizzazione e della relativa attribuzione di una categoria di rilevanza

A partire dal 1° gennaio 2026

Si dovrà adempiere all'obbligo di notifica degli incidenti

Entro il 1° ottobre 2026

Si dovrà adempiere:

- Agli obblighi degli organi di amministrazione e direttivi
- Agli obblighi in materia di misure di sicurezza
- All'obbligo di raccolta e mantenimento di una banca dei dati di registrazione dei nomi di dominio laddove applicabile

Occorre, quindi, pianificare con attenzione le attività,
seguendo il dettato normativo previsto nel decreto di recepimento

NIS2: Cybersecurity come processo aziendale

Anche la Direttiva NIS2 come le altre nuove normative in termini di cybersecurity (DORA, GDPR, Direttiva sulla resilienza dei soggetti critici) sono costruite per implementare un sistema di gestione

Le caratteristiche dei sistemi di gestione sono:

- Tendere al miglioramento continuativo del sistema
- Definire risorse e policy
- Verificare nel tempo la performance
- Verificare l'efficacia delle soluzioni adattate
- Gestire il cambiamento

Misure di sicurezza per la minimizzazione del rischio

- Politiche in materia di analisi dei rischi e di sicurezza dei sistemi informativi e di rete
- Gestione degli incidenti ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli artt. 25-26
- Continuità operativa aziendale ivi inclusa la gestione di backup, il ripristino in caso di disastro e gestione delle crisi
- Supply chain security (sicurezza della catena di approvvigionamento) ivi inclusi gli aspetti relativi alla sicurezza riguardante i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi
- Sicurezza dell'acquisizione, dello sviluppo e manutenzione delle reti e dei sistemi informativi ivi comprese la gestione e divulgazione delle vulnerabilità

Misure di sicurezza per la minimizzazione del rischio

- Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica
- Pratiche di igiene di base e di formazione sulla sicurezza informatica
- Politiche e procedure riguardanti l'uso delle crittografia e ove opportuno della cifratura
- Sicurezza delle risorse umane, politiche di controllo degli accessi e gestione dei beni e degli asset
- Uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno

Procedura per gli obblighi di comunicazione: step principali

1. Stabilire per l'organizzazione quando un incidente è da considerare significativo: strutturazione dei criteri di gravità (Valutazione del Rischio Incidente)
2. Modalità di svolgimento dell'indagine: risorse e tempi modalità (strutture del report di incidente)
3. Chi effettua la comunicazione verso il management e verso il CSIRT Italia?
4. Chi gestisce le diverse fasi successive alla prima notifica?
5. Valutazione dell'impatto transfrontaliero dell'incidente
6. Valutazione dell'impatto economico e sociale dell'incidente
7. Valutazione della comunicazione ai fruitori dei servizi: va fatta? In quali casi? Con quali dettagli?
8. Chi è il punto di contatto per CSIRT Italia?
9. Quali sono le misure di mitigazione dell'incidente?
10. Il quasi-incidente va comunicato? Chi decide e con quali mezzi?
11. Al termine dell'incidente o del quasi-incidente, quali misure correttive bisogna adottare al fine di evitare il ripetersi degli stessi e migliorare la sicurezza del sistema?

Elementi formativi obbligatori: chi e come formare

1. Formazione del Top Management: deve seguire i corsi per migliorare la propria capacità di valutazione dei rischi per la cybersecurity
2. Obbligo del Top Management: deve garantire una adeguata formazione a tutta l'organizzazione

    I. Piano formativo anche pluriennale che investa tutte le funzioni aziendali con diversi gradi di profondità in funzione dei ruoli ricoperti
    II. Valutazione dell'efficacia del piano formativo
    III. Rivalutazione periodica del piano formativo

NIS2

SPEAKER

Ing. Alessia Micarelli

POWERED BY SINAPSI, LUSIOS, AVV.BIANCHINI

SINAPSI
WE CONNECT DOTS

Lusios

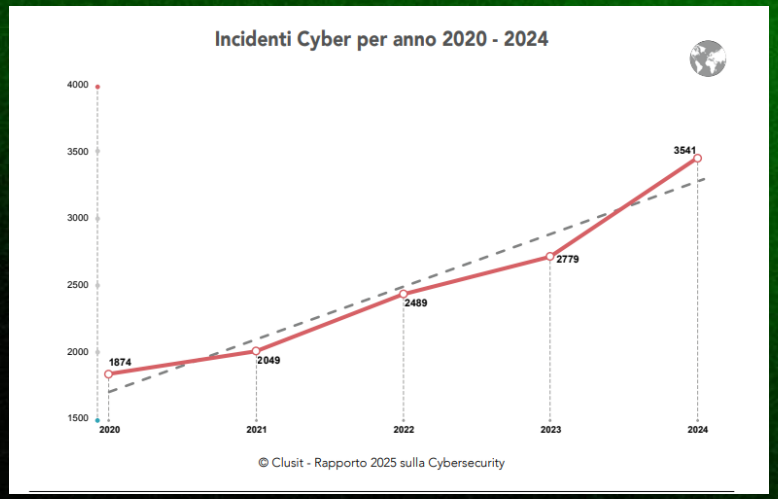
FB

Ing. Alessia Micarelli

- Ingegnere in Informatica e Telecomunicazioni
- Iscritta all'Ordine degli Ingegneri di Perugia
- Project Manager in ambito IT
- Project Manager in ambito cybersecurity
- Esperta di sistemi di gestione ISO 27001, ISO 27017 e ISO 27018
- PECB Certified NIS 2 Directive Lead Implementer

SCENARIO

TUTTE LE ORGANIZZAZIONI SONO POTENZIALI OBIETTIVI DI CYBER ATTACCHI……DAL SE AL QUANDO



GEN 20- DIC 24 – A livello globale

- Tot 12.732 INCIDENTI
- 2024 → 3.541 INCIDENTI

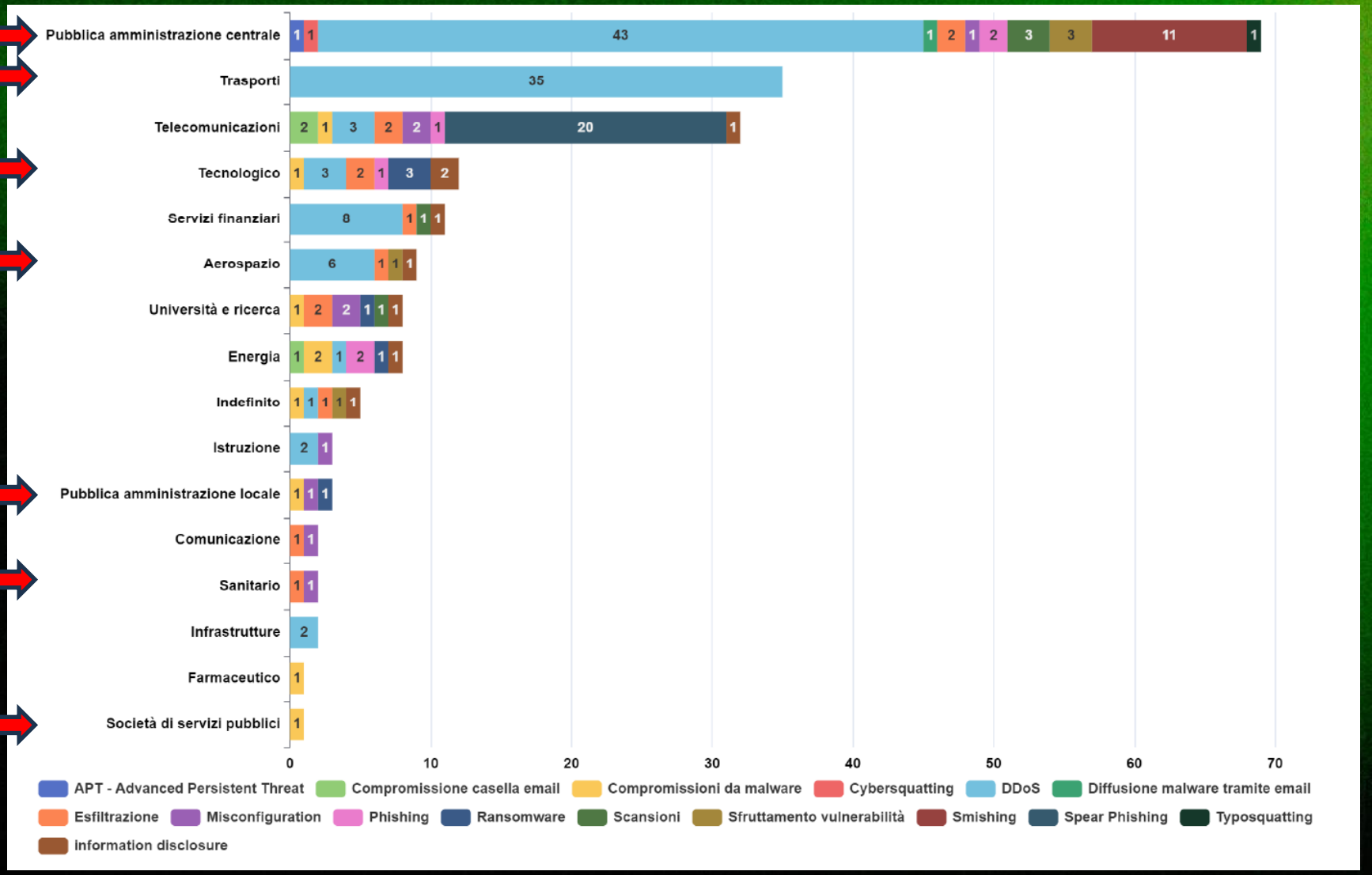
La realtà supera le previsioni

Fino al 2023 → Cybercrime, «normali» attività di intelligence economica, conflitto in Ucraina (guerra cibernetica diffusa)

2024 → AI Generativa (moltiplicatore di forza), aumentate tensioni (socioeconomico e geopolitico) → antagonismo digitale (attacchi DDoS)

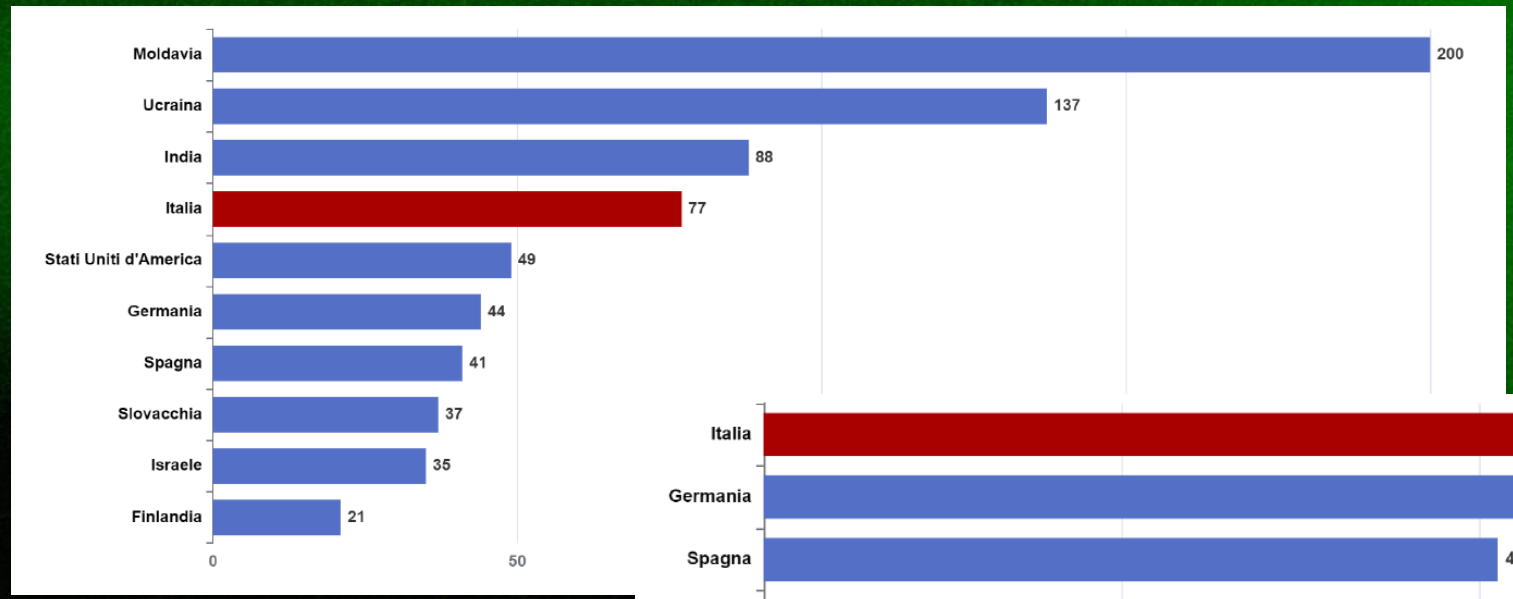
POWERED BY SINAPSI, LUSIOS, AVV. BIANCHINI

SCENARIO

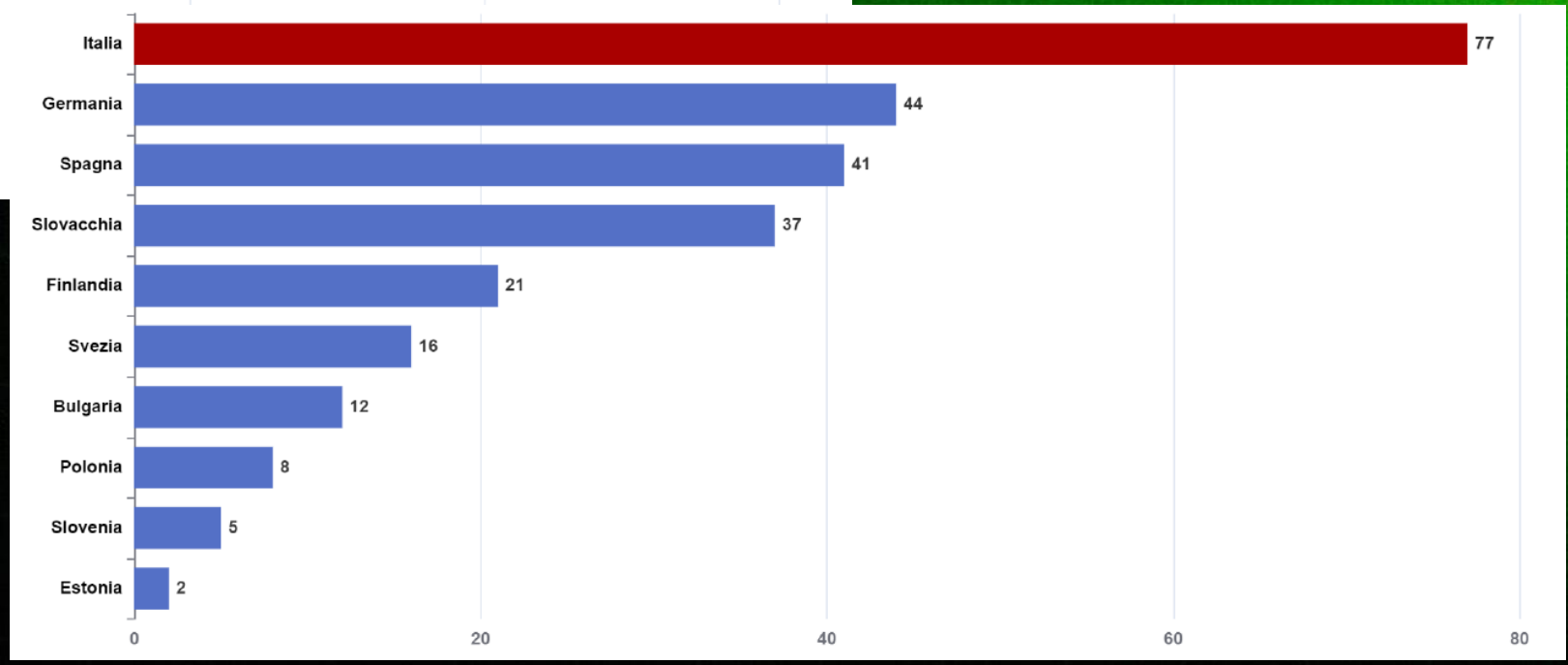


POWERED BY SINAPSI, LUSIOS, AVV. BIANCHINI

SCENARIO



rivendicazioni Ransomware



rivendicazioni DDoS

POWERED BY SINAPSI, LUSIOS, AVV. BIANCHINI

SCENARIO

SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 165° - Numero 153

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 2 luglio 2024 — SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DIREZIONE E REDAZIONE PRESSO IL MINISTERO DELLA GIUSTIZIA - UFFICIO PUBBLICAZIONE LEGGI E DECRETI - VIA ARENULA, 70 - 00186 ROMA
AMMINISTRAZIONE PRESSO L'ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - VIA SALARIA, 691 - 00138 ROMA - CENTRALINO 06-85081 - LIBRERIA DELLO STATO
PIAZZA G. VERDI, 1 - 00198 ROMA

La **Gazzetta Ufficiale, Parte Prima,** *oltre alla* **Serie Generale,** *pubblica cinque Serie speciali, ciascuna contraddistinta da autonoma numerazione:*
1ª Serie speciale: *Corte costituzionale (pubblicata il mercoledì)*
2ª Serie speciale: *Unione europea (pubblicata il lunedì e il giovedì)*
3ª Serie speciale: *Regioni (pubblicata il sabato)*
4ª Serie speciale: *Concorsi ed esami (pubblicata il martedì e il venerdì)*
5ª Serie speciale: *Contratti pubblici (pubblicata il lunedì, il mercoledì e il venerdì)*
La **Gazzetta Ufficiale, Parte Seconda,** "Foglio delle inserzioni", *è pubblicata il martedì, il giovedì e il sabato*

AVVISO ALLE AMMINISTRAZIONI

LEGGE 28 giugno 2024 , n. 90

LEGGE 90 del 2024

Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

- Misure di rafforzamento della cybersicurezza nazionale.
- Resilienza delle PA.
- Contratti pubblici di beni e servizi informatici per la tutela degli interessi nazionali strategici.
- Modifiche al Codice Penale e alle nome di prevenzione e contrasto dei reati informatici.
- Disposizioni in materia di coordinamento degli interventi in caso di attacchi ai sistemi informatici (ACN).

POWERED BY SINAPSI, LUSIOS, AVV. BIANCHINI

SCENARIO

DIRETTIVA NIS2 e D.Lgs 138/2024

NIS2 e D.Lgs 138/2024

Requisiti che le Organizzazioni devono soddisfare per innalzare il livello di cybersicurezza.

Nuovi obblighi:

- gestione del rischio
- comunicazione degli incident
- Business Continuity e Disaster recovery
- Formazione.

Soggetti essenziali ed importanti

Responsabilità dal tecnico al management.

POWERED BY SINAPSI, LUSIOS, AVV. BIANCHINI

DIFESA

ESPOSIZIONE AL RISCHIO

- PROLIFERARE DI MINACCE IN CONTINUA EVOLUZIONE (AI)
- ATTACK SURFACE SEMPRE PIU' AMPIA

Adozione di strategie avanzate per la gestione e quindi la riduzione dei rischi

GESTIONE PROATTIVA

Non solo **difesa** ma anche **prevenzione**!

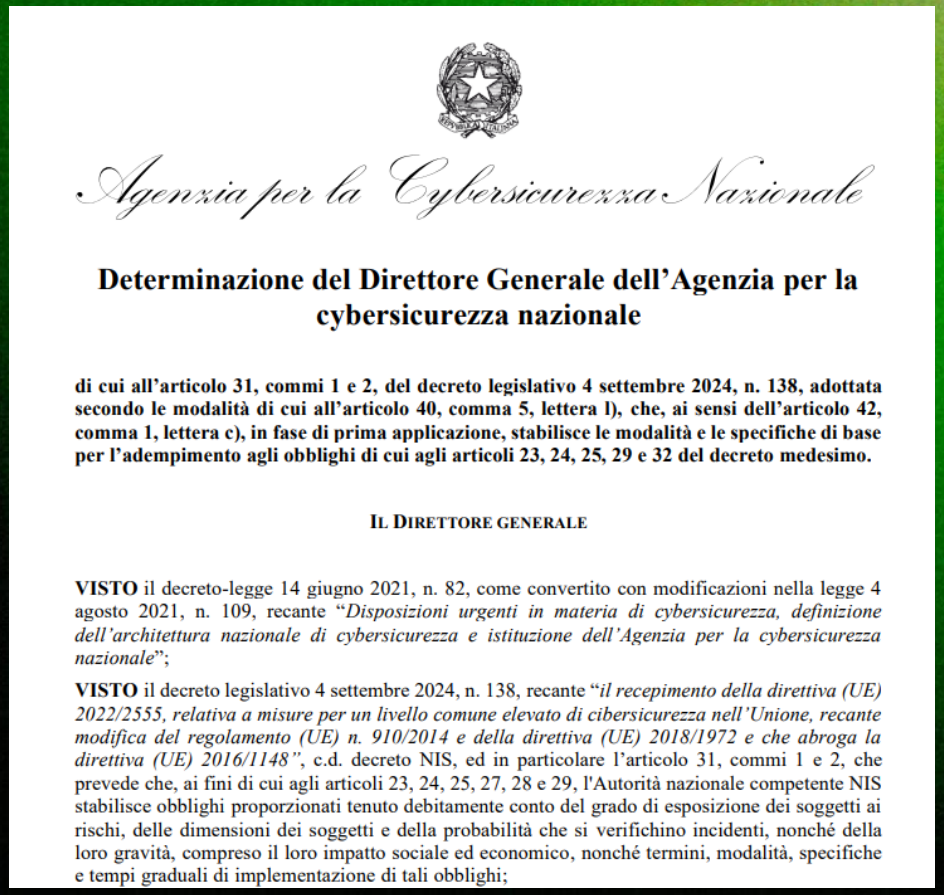
POWERED BY SINAPSI, LUSIOS, AVV. BIANCHINI

DETERMINAZIONI ACN

DETERMINA ACN n.164179 del 14 aprile 2025

MODALITA' E SPECIFICHE DI BASE PER L'ADEMPIMENTO AGLI OBBLIGHI DI CUI AGLI ART 23, 24, 25, 29 E 32.

Misure di sicurezza di base e Incidenti significativi



Agenzia per la Cybersicurezza Nazionale

Determinazione del Direttore Generale dell'Agenzia per la cybersicurezza nazionale

di cui all'articolo 31, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, lettera l), che, ai sensi dell'articolo 42, comma 1, lettera c), in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto medesimo.

IL DIRETTORE GENERALE

VISTO il decreto-legge 14 giugno 2021, n. 82, come convertito con modificazioni nella legge 4 agosto 2021, n. 109, recante "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*";

VISTO il decreto legislativo 4 settembre 2024, n. 138, recante "*il recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*", c.d. decreto NIS, ed in particolare l'articolo 31, commi 1 e 2, che prevede che, ai fini di cui agli articoli 23, 24, 25, 27, 28 e 29, l'Autorità nazionale competente NIS stabilisce obblighi proporzionati tenuto debitamente conto del grado di esposizione dei soggetti ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico, nonché termini, modalità, specifiche e tempi graduali di implementazione di tali obblighi;

SOLUZIONI

Il nostro team di esperti fornisce soluzioni complete per la totale e continuativa compliance alla Direttiva NIS 2 e al Decreto attuativo italiano D.Lgs 138/2024.

Inquadramento del soggetto
Tipologia e coinvolgimento

Assessment
Valutazione della postura cyber e Gap Analisys

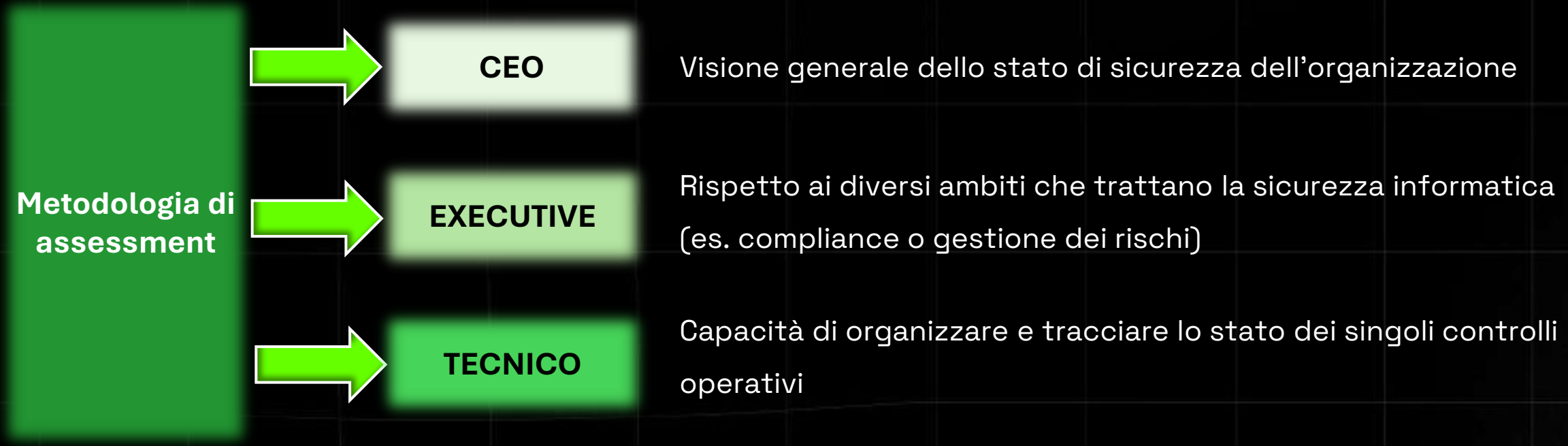
Report
Piani di sicurezza e Progetti di adeguamento

DPCM 81
MM Agid
Legge 90
GDPR

POWERED BY SINAPSI, LUSIOS, AVV.BIANCHINI

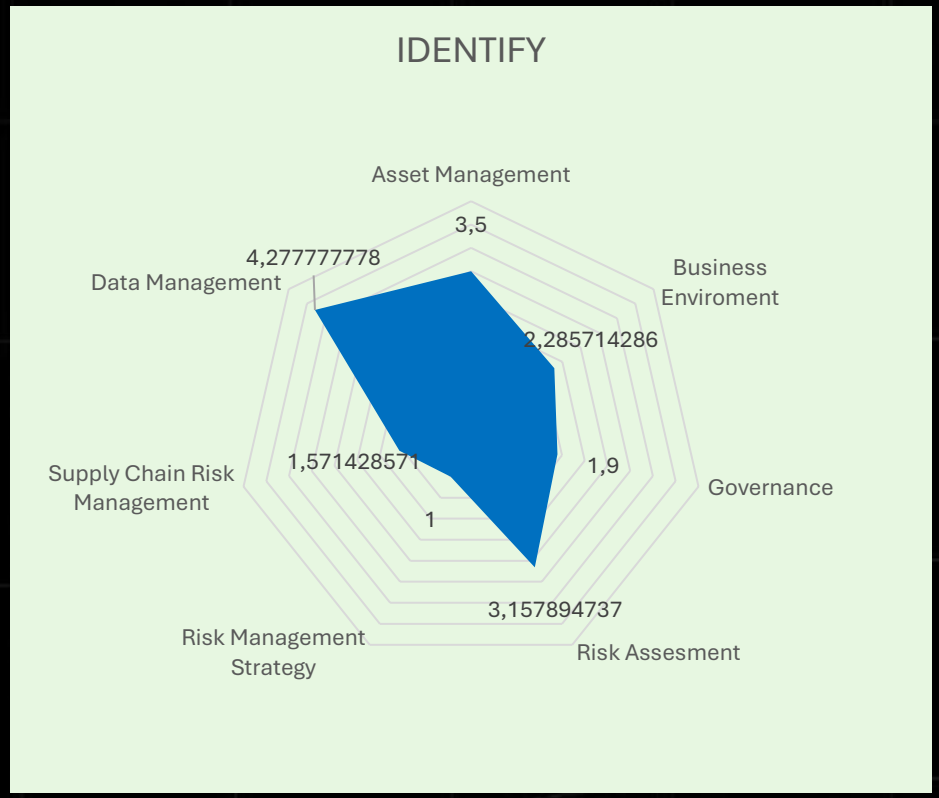
ASSESSMENT

Metodologia basata sul Framework Nazionale per la Cybersecurity e la Data Protection.



ASSESSMENT

Gap Analisys: stimare il grado di copertura di ciascun controllo e il livello di maturità implementativa del controllo stesso.



POWERED BY SINAPSI, LUSIOS, AVV.BIANCHINI

REPORT

PIANI DI SICUREZZA E/O DI POTENZIAMENTO: individuazione delle misure tecniche e organizzative da implementare per raggiungere un adeguato livello di capacità cyber (postura di cybersicurezza).

PROGETTO DI ADEGUAMENTO: declinazione tecnica del piano. Scelta delle tecnologie, degli strumenti, dei servizi e dei prodotti, con relative tempistiche di attuazione.

PIANI E PROGETTI

Continuità operativa aziendale ivi inclusa la gestione di backup, il ripristino in caso di disastro e gestione delle crisi

PIANO: …necessità di rafforzare il sistema di backup on-site e implementare un sistema di backup in cloud….

PROGETTO: acquisto di uno storage (marca, modello, dimensionamento, ecc…) per l'esecuzione di backup immutabile on-site. Sottoscrizione di un contratto (scelta del fornitore e dei parametri tecnici) per l'esternalizzazione del backup su cloud qualificato ACN. Tempi e costi.

PIANI E PROGETTI

Pratiche di igiene di base e di formazione sulla sicurezza informatica

PIANO: non è stato redatto il programma formativo né per gli organi di amministrazione e direttivi, né per i dipendenti dell'organizzazione.

PROGETTO: individuazione delle esigenze formative per le varie FA e redazione del programma , inclusa la parte di security awareness (campagne di phishing). Individuazione dei soggetti formatori e delle eventuali piattaforme. Tempi e costi.

SERVIZI - Security

SOC
Servizio 24/7/365 di Prevention, Detection and Response (PDR)

NOC
Servizio 24/7/365 per il monitoring proattivo delle infrastrutture e dei servizi critici

Advanced SIEM
Servizio di installazione, gestione e tuning di un sistema SIEM Avanzato

Incident Response
Servizi di IR atti alla preparazione, detection, contenimento, eradicazione e recovery di un attacco informatico (PARTNERSHIP SOPHOS)

Threat Intelligence
Servizio di raccolta informazioni e analisi delle minacce per fornire raccomandazioni strategiche

Security Awareness
Processi di sensibilizzazione degli utenti con campagne di phishing e smishing, reportistica e attività di formazione

Waf As A Service
Servizio gestito per la protezione completa di applicazioni web (DDoS, Botnet, OWASP ecc…)

ASM
Analisi continua della superfice di attacco VA/PT, analisi TLD

GAP/Risk Assessment
Servizi di analisi della compliance rispetto ai framework di riferimento (FNC – NIS2)
Servizi di analisi e gestione del rischio

POWERED BY SINAPSI, LUSIOS, AVV. BIANCHINI

NIS2

CYBER THREAT INTELLIGENCE (CTI)

CTI in configurazione ”Identity Intelligence:

- individuare, mitigare tempestivamente e prevenire i rischi legati alla compromissione delle credenziali personali
- ricerca approfondita e continua su Clear Web, Deep Web e Dark Web
- aiutiamo le organizzazioni a prevenire attacchi mirati.

IL FATTORE TEMPO È CRUCIALE: identificare tempestivamente le credenziali compromesse prima che diventino disponibili ad attori malevoli è determinante per ridurre i rischi e garantire la sicurezza.

SINAPSI
WE CONNECT DOTS
Lusios
FB

SERVIZI - IaaS

BaaS
Servizi di Backup gestito su Cloud Nextegy (Italia) con supporto immutabilità (WORM)
(Veeam, 365, Rubrik)

DRaaS
Definizione di piani di per garantire la disponibilità dei dati e dei servizi

S3 Object Storage
Servizi di object storage resiliente S3-compatibile con supporto all'immutabilità (WORM)

VPC
Servizi di Virtual Private Cloud gestiti per l'erogazione di servizi infrastrutturali su cloud Nextegy

VPS
Servizi di Virtual Private Server gestiti con servizi di sicurezza (SIEM, XDR, Backup, Patch Management, WAF)

Help-Desk
Servizio di Help-Desk gestito tramite portale di ticketing / supporto telefonico

Maintenance
Gestione e manutenzione Infrastrutture Sinapsi/Nextegy

POWERED BY SINAPSI, LUSIOS, AVV. BIANCHINI

SOLUZIONI

CONSULENZA

ASSESSMENT e GAP ANALISYS: interviste on-site o da remoto con il team IT, il DPO, il team legal, il Top management.

FORMAZIONE

PIANO DI FORMAZIONE strutturato per livelli e competenze: dai dipendenti al top management.

DOCUMENTAZIONE

POLICY E PROCEDURE: revisione e/o adattamento delle esistenti o stesura di nuove. Revisione peridodica.

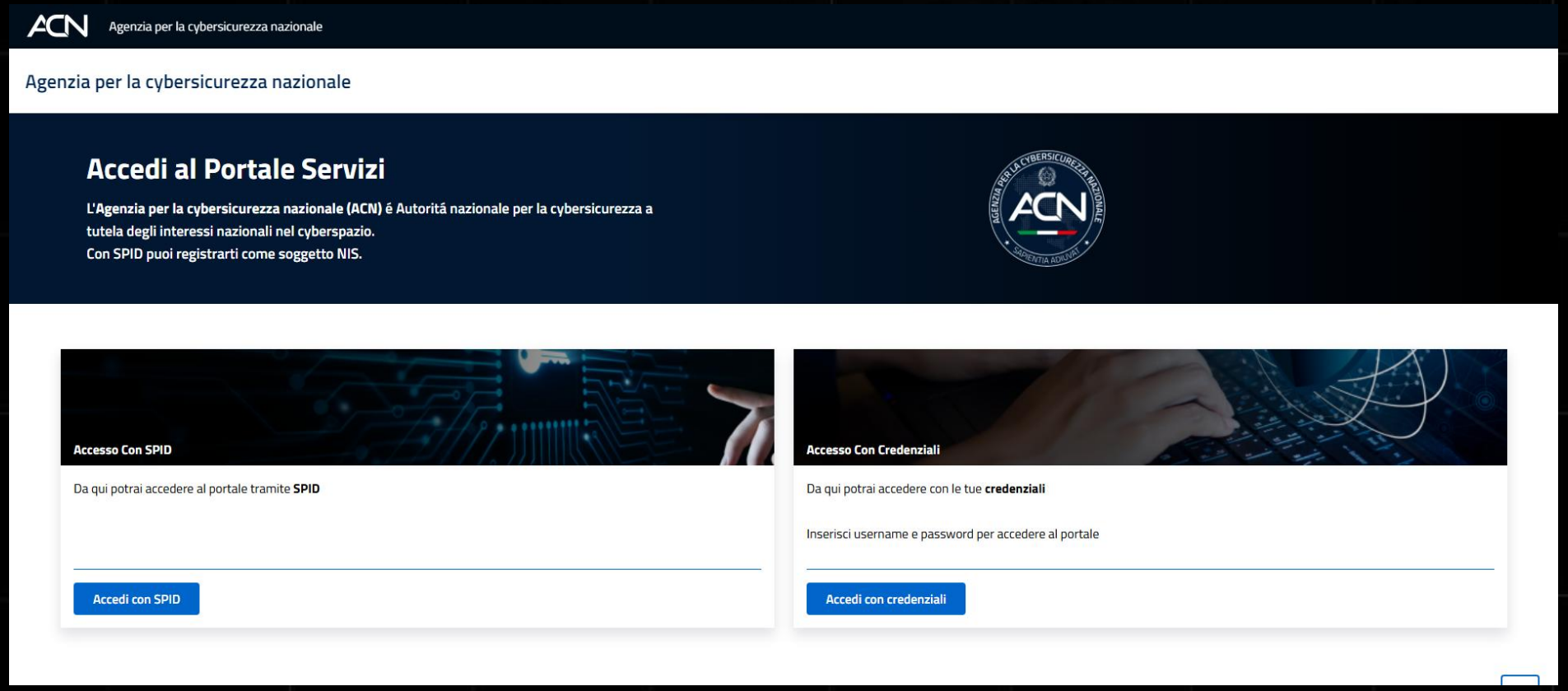
IMPLEMENTAZIONE

PIANI e PROGETTI redatti ad hoc insieme al cliente per raggiungere la compliance e migliorare la postura cyber.

POWERED BY SINAPSI, LUSIOS, AVV.BIANCHINI

AGGIORNAMENTO PORTALE ACN

1) IL PUNTO DI CONTATTO ACCEDE COL PROPRIO SPID AL PORTALE



NIS2

SERVIZIO DI APPROFONDIMENTO CON FINESTRE ONE-TO-ONE

Sarà possibile prenotare un appuntamento con i nostri esperti per approfondire le tematiche di vostro interesse.

Ing. Alessia Micarelli – alessia.micarelli@.sinapsi.email
Ing. Michele Mercanti – michele.mercanti@lusios.it
Avv. Filippo Bianchini - avv.filippobianchini@gmail.com

POWERED BY SINAPSI, LUSIOS, AVV.BIANCHINI

SINAPSI
WE CONNECT DOTS
Lusios
FB

Grazie per l’attenzione!

POWERED BY SINAPSI, LUSIOS, AVV.BIANCHINI