Strumenti di certificazione ed attestazione per ottemperare ai requisiti NIS2 e creare strategie di cybersecurity

Valentina Mussi | National Market Leader Cybersecurity e Digital , *Bureau Veritas Italia*
Maurizio Genna | ICT Product Manager, *Bureau Veritas Italia Bureau Veritas Italia*

RELATRICE

Valentina Mussi

National Market Leader
Cybersecurity e Digital

Bureau Veritas Italia

BUREAU VERITAS NEL MONDO

€5.9
miliardi

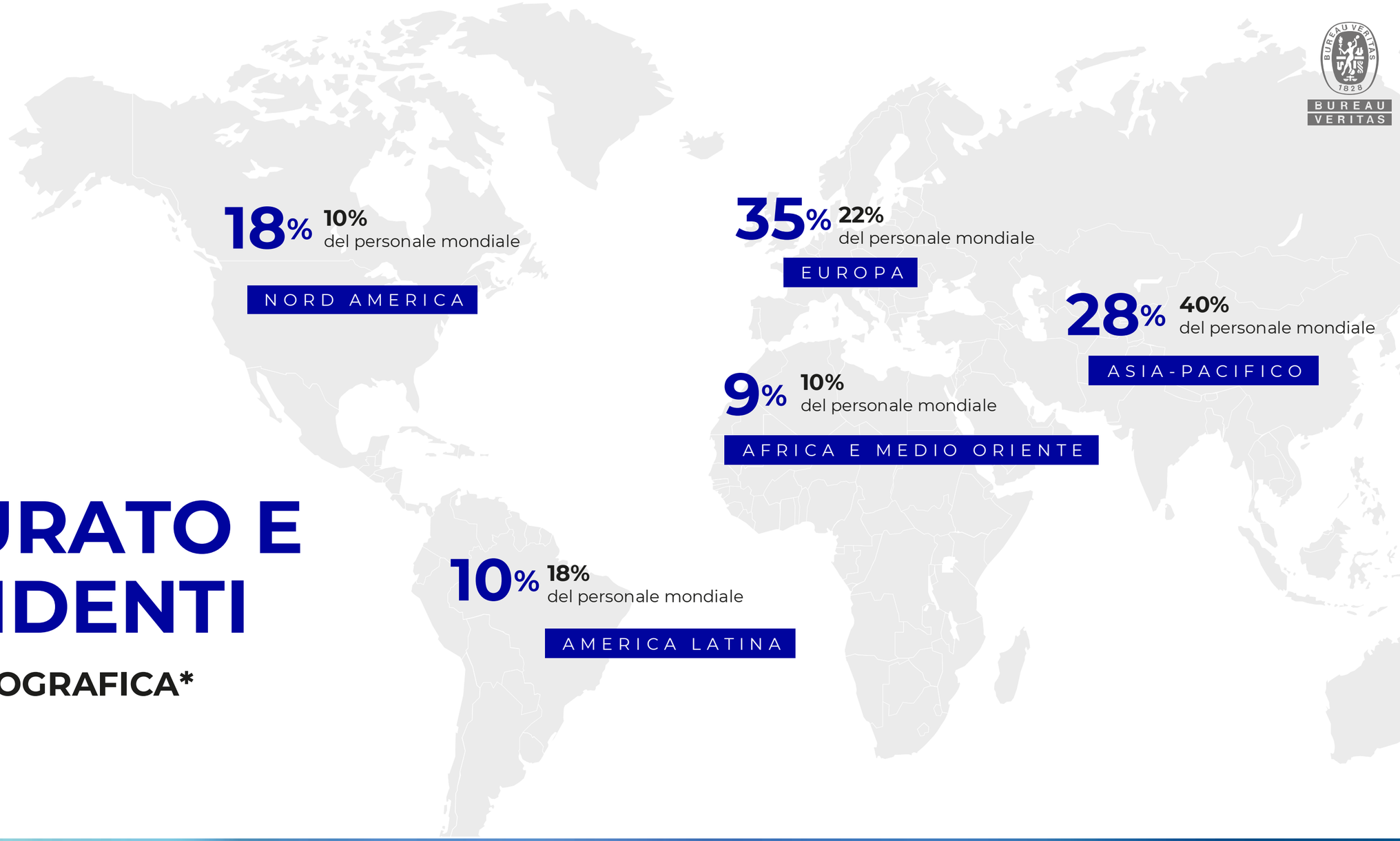
FATTURATO 2023

83.000
dipendenti*

400.000
clienti

~1.600
uffici e laboratori

IN 140 PAESI



18% 10% del personale mondiale

NORD AMERICA

35% 22% del personale mondiale

EUROPA

28% 40% del personale mondiale

ASIA-PACIFICO

9% 10% del personale mondiale

AFRICA E MEDIO ORIENTE

10% 18% del personale mondiale

AMERICA LATINA

FATTURATO E DIPENDENTI

PER AREA GEOGRAFICA*

* Al 31 Dicembre 2023

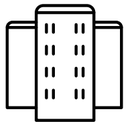
BUREAU VERITAS IN ITALIA

PRESENTE DAL 1839

VALORE DELLA PRODUZIONE

€ 182 milioni

UFFICI



21

DIPENDENTI

~ 1.000

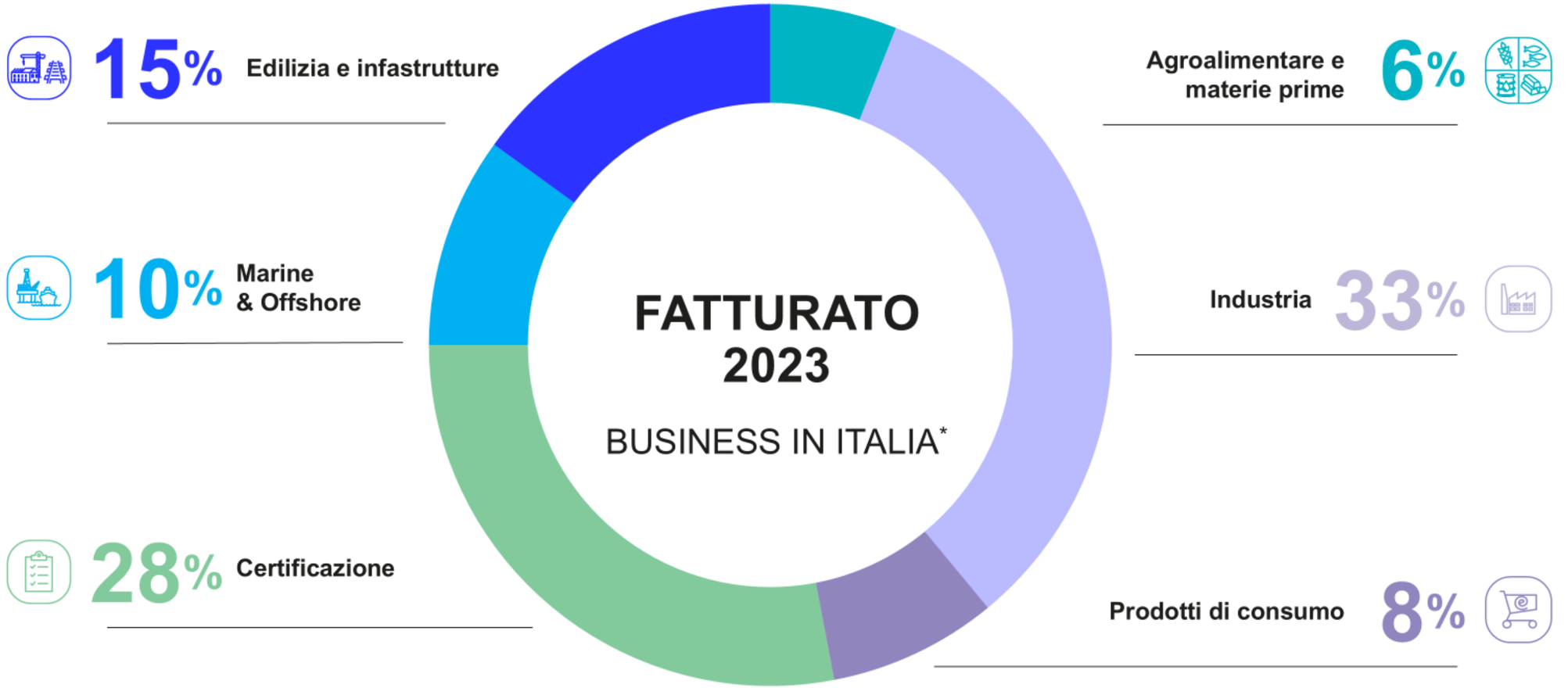
TECNICI E VALUTATORI

~ 900

CLIENTI

20.000

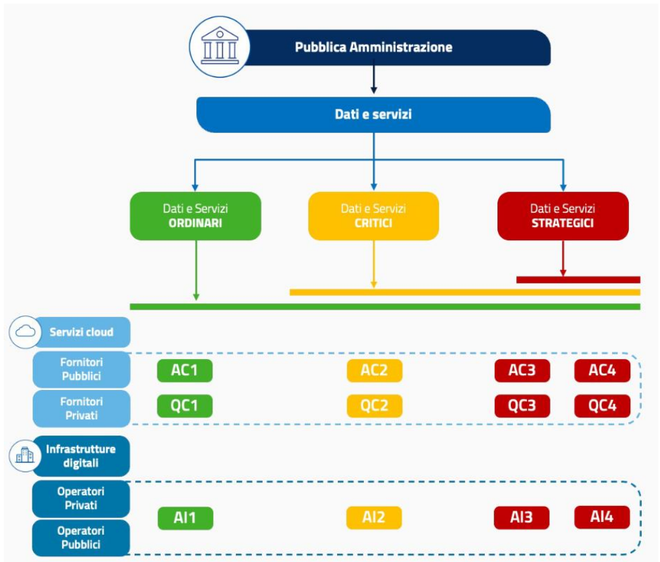
* Al 31 dicembre 2023



* Al 31 dicembre 2023
Le percentuali si riferiscono al valore del fatturato dell'attività di core business

BUREAU VERITAS ITALIA
CERTIFICAZIONI IN AMBITO CYBERSECURITY

- → **ISO 9001 – SISTEMA DI GESTIONE QUALITA'**
- → **ISO 27001 – SISTEMA DI GESTIONE SICUREZZA DELLE INFORMAZIONI**
- → **ISO 22301 – BUSINESS CONTINUITY**
- → **ISO 25000 – VALIDAZIONE DEL SOFTWARE**
- → **ANSI TIA 942-ISO 22237 e EN 50600 (data center)**
- → **ISO 42001 _ SISTEMA DI GESTIONE INTELLIGENZA ARTIFICIALE**
- → **IEC 62443 – CYBERSECURITY Linee guida per la cyber security industriale**



SERVIZI CLOUD vs PA (Qualifica QC1/QC2/QC3/QC4)

- → **ISO 27001 – SISTEMA DI GESTIONE INFORMATION TECNOLOGY**
- → **ISO 20000 – SERVICE MANAGEMENT** (Requisiti provider)
- → **ISO 9001 – SISTEMA DI GESTIONE QUALITA'**
- → **ISO 27017/27018 – CONTROLLI SICUREZZA SERVIZI CLOUD** (CSA star in sostituzione alla 27017-27018)

Inquadramento normativo NIS2 e Decreto 138/2024

Nis 2

La Direttiva Network and Information Security 2 è una normativa che mira a fissare un livello elevato e comune per la sicurezza informatica in tutti gli Stati membri dell'Unione Europea

A. Allargare il numero di soggetti destinatari delle prescrizioni in tema cyber security;

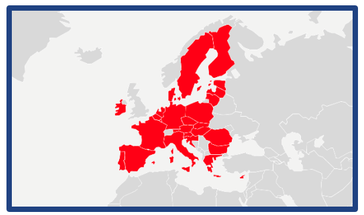
B. Ridurre le diverse incongruenze tra gli Stati per garantire un livello di sicurezza comune ed eliminare le differenze tra gli stessi;

C. Aumentare la consapevolezza collettiva.

D. La Direttiva NIS2 prevede un obbligo di notifica al CSIRT e alle autorità competenti, senza ritardo, di qualsiasi incidente che può avere un impatto significativo sulla fornitura del servizio. Inoltre, stabilisce che – quando è appropriato – la notifica debba avvenire anche a beneficio dei destinatari del servizio impattato dal cyber attacco, anche indicando le misure che detti destinatari sono in grado di adottare per reagire all'attacco.

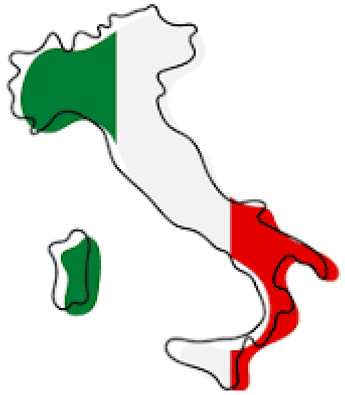
E. Rafforza la collaborazione fra aziende e organi istituzionali (ENISA, CSIRT, ACN in Italia) raccogliendo un database delle vulnerabilità, gestito da ENISA, per supportare la gestione delle crisi informatiche su larga scala.

IL decreto italiano e Gli attori coinvolti



DIRETTIVA EUROPEA NIS 2
(2022/2555)

DECRETO ITALIANO 138/2024



AGENZIA DI CYBERSICUREZZA NAZIONALE

TOP MANAGEMENT

AZIENDE

ORGANIZZAZIONE

ENTRO QUANDO?

I soggetti che si riconocono in uno dei settori/sottosettori/tipologie **DOVRANNO:**

REGISTRAZIONE PORTALE DI ACN

CONFERMA DA ACN + INDICAZIONE OBBLIGHI DI BASE CYBER

CLIENTE TRASMETTE INDIRIZZI IP + ELENCO STATI MEMBRI IN CUI SI EROGANO

TERMINE PER RAGGIUNGERE COMPLIANCE NIS 2

28 FEB ‘25

APR ‘25

MAG ‘25

GEN ‘26

OTT ‘26

Sanzione amministrativa pecuniaria fino a 0.1% del fatturato annuo su scala mondiale

→ **Tempo per adempimento agli obblighi segnalazione incidente**

→ **Tempo per adempimento agli obblighi di base in materia di sicurezza informatica**

- → **Entro il 17 gennaio 25:** 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, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network.
- → **Entro il 28 febbraio 25:** Tutti gli altri soggetti

Quali aziende sono interessate?

OPERATORI DI SERVIZI ESSENZIALI (I) E IMPORTANTI (II)

SETTORI AD ALTA CRITICITA' (I)	ALTRI SETTORI CRITICI (II)
ENERGIA: elettricità Gas, petrolio, Idrogeno	**SERVIZI POSTALI E CORRIERI**
SANITA' prest. sanitaria, laboratori, R&S, farmaceutica	**GESTIONE DEI RIFIUTI**
TRASPORTI	**CHIMICO:** fabbricazione, produzione distribuzione
BANCARIO E INFRASTRUTTURE FINANZIARIE	**FOOD:** Produzione, trasformazione e distribuzione Alimenti
ACQUA POTABILE E ACQUE REFLUE	**FABBRICAZIONE** disp. Medici, elettronica, macchinari, autoveicoli, rimorchi
INFRASTRUTTURE DIGITALI	Fornitori di **SERVIZI DIGITALI**
GESTIONE SERVIZI TIC	**R&D**
SPAZIO	

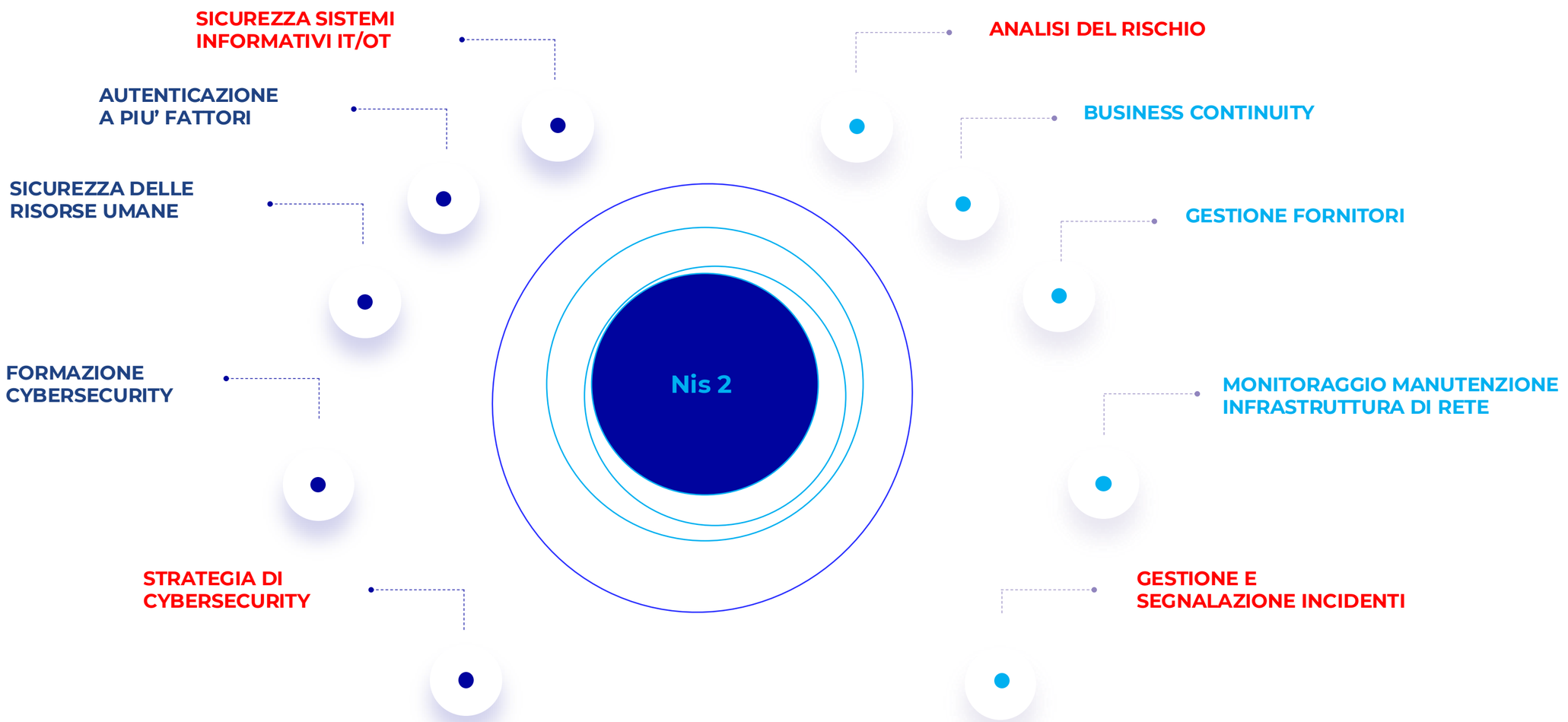
Medie/Grandi imprese

Dipendenti > 50; fatt annuo tot >10 mln

SUPPLYCHAIN
Indipendentemente dalla dimensione

che rappresentino **un elemento sistemico nella catena di approvigionamento, anche digitale** dei settori in tabella

OBIETTIVI NIS 2 - Quali misure adottare



Quali principali elementi di prescrizione

Governance	Vigilanza	Gestione del rischio	Supply chain	Segnalazione Incidenti
La **gestione della cyber sicurezza non è più un compito relegato esclusivamente alla funzione dei sistemi informativi**, ma diventa una **responsabilità diretta dell'organo di gestione aziendale**, come ad esempio il **Consiglio di Amministrazione.**	**Soggetti essenziali**: La normativa prevede un **regime di vigilianza completo** (ex ante- ex post) e sanzioni **fino a 10 mln di euro o pari al 2% del** fatt/anno/globale **Soggetti Importanti: regime di vigilanza leggero(ex post) e sanzioni fino a 7** mln di euro o pari al 1,4% del fatt/anno/globale	**«misure tecnico-organizzative "adeguate"»** per gestire i rischi per la sicurezza dei sistemi di rete e di informazione che i soggetti essenziali e importanti sono tenuti ad attuare	I soggetti identificati devono **garantire la cybersecurity lungo la supply chain** valutando il livello di maturità cyber dei fornitori	I soggetti identificati sono incaricati di inviare **un preallare entro 24 ore dell'incidente** e successiva **comunicazione entro 72 con aggiornamento delle informazion**i inviate precedentemente

→ **SANZIONI AMMINISTRATIVE**
→ **SOSPENSIONE MANAGEMENT**

Visione strategica

APPROCCIO MULTIDISCIPLINARE	Coinvolgimento diversi stakeholder aziendali (IT, OT, Operation, HR, C-Level)
TEMPISTICHE STRINGENTI	Le tempistiche richieste sono una grande prova per le aziende soprattutto per le PMI coinvolte che sono meno mature dal punto di vista Cyber
IMPLICAZIONI PER CYBER INDUSTRIALE (OT)	Una sfida importante quella della Cyber degli asset industriali dove ad oggi il livello di maturità e consapevolezza è ancora limitato
EFFORT RICHIESTO	Difficoltà nell'applicazione dei requisiti richiesti dalla normativa e nell'implementazione di azioni di mitigazione del rischio

QUALI STRUMENTI UTILIZZARE PER ESSERE COMPLIANCE A NIS 2?

RELATORE

Maurizio Genna

ICT Product Manager

Bureau Veritas Italia

Direttiva NIS 2: novità e adempimenti richiesti dalla nuova direttiva

LA UNI PDR CSF

Come dimostrare la compliance alla Nis 2?

Per esperienza pregressa, Direttive e Regolementi non danno mai indicazioni su come e strumenti da utilizzare per dimostrare la compliance ai requisiti (poche eccezioni in perimetri ristretti e settori definiti); allo sttao attuale gli unici strumenti di attestazione e certificazione erano:

1. Certificazione ISO 27001;
2. Attestazione secondo le Linee Guida NIST-ENISA-Schema Nazionale;
3. Ceritificazione ISA 62443 (OT).

NOVITA'

UNI , su input ACN e con la collaborazione e supervisione di Accredia, ha costituito a fine 2024 un tavolo tecnico finalizzato alla definzione di una UNI PdR per la gestione delle compliance alla NIS 2. Da capire , ora che è stata presentata, se verrà presa in carico da Accredia e se verrà indicata da ACN come strumento di riferimento per la conformità alla NIS 2. La UNI PDR è aperta alle integrazioni alla ISO 27001 (sia per chi ne è già in possesso, sia per chi ha intenzione di farla).

Come dimostrare la compliance alla Nis 2?

E’ in consultazione pubblica sul sito UNI la PdR (Prassi di Riferimento) “**Sistema di Gestione per la Cybersicurezza e la Sicurezza delle Informazioni armonizzato alla norma UNI CEI EN ISO/IEC 27001 e al Framework NIST CSF 2.0 – Requisiti**”.

Al tavolo di lavoro con ACCREDIA, CINI (Consorzio Interuniversitario Nazionale Informatica) ed UNINFO ha partecipato attivamente ASSOTIC, rappresentata dal nostro Gabriele Vitali della Service Line Certificazione.

Come e’ strutturata la UNI/PDR XX:2024?

- Sistema di Gestione per la Cybersicurezza e la Sicurezza delle Informazioni armonizzato alla **norma UNI CEI EN ISO/IEC 27001:2024** e al **Framework NIST CSF 2.0**
- Requisiti
- Adottata esclusivamente in ambito nazionale (se integrata con certificazione ISO 27001 puo’ essere utile anche per le Organizzazioni che hanno attività internazionali). Chi è già in possesso **della ISO 27001** potrà «attestare» il delta relativo ai **requisiti NIST**.
- Documento che introduce **prescrizioni tecniche** (elaborati dagli autori sotto la conduzione operativa di UNI)
- Basato su **Annex SL della Direttiva ISO/IEC parte 1**
- Contiene:
  - Parte di Sistema (I requisiti della PdR sono scritti in forma “additiva”)
  - Appendice A (prospetto tabellare per indicare la relazione tra NIST CSF 2.0 con i Requisiti della 27001 e relativo Annex A (controlli)
  - Appendice B (2 prospetti tabellari):
    - B.1 (Relazione tra Parte sistemica 27001 e NIST CSF 2.0
    - B.2 (Relazione tra Annex A 27001 e NIST CSF 2.0

UNI/PDR XX:2024

→ Esempio dell'Appendice A

Prospetto A – Relazione fra Punti e Controlli della norma UNI CEI EN ISO/IEC 27001:2024 e le Sottocategorie del Framework NIST CSF 2.0

Categorie e Sottocategorie NIST CSF 2.0	UNI CEI EN ISO/IEC 27001:2024		Attributi dei Controlli definiti dalla norma UNI CEI EN ISO/IEC 27002:2023						
	PUNTI PARTE SISTEMICA	CONTROLLI APPENDICE A	Capacità Operative	Domini di Sicurezza	Concetti di Cybersecurity				
			#Governance	#Governance_and_Ecosystem	#Identify	#Protect	#Detect	#Respond	#Recover
FUNZIONE GV									
GV.OC									
GV.OC-01	**4.1, 4.2, 4.3, 4.4, 5.2**	-							
GV.OC-02	**4.2, 4.3, 4.4**	-							
GV.OC-03	**4.1, 4.2, 4.3, 4.4**	5.31, 5.32, 5.33, 5.34		5.31, 5.32	5.31, 5.32, 5.33, 5.34	5.33, 5.34			
GV.OC-04	**4.2, 4.3, 4.4, 5.2, 7.4**	-							
GV.OC-05	**4.1, 4.2, 4.3, 4.4, 7.4, 8.1**	5.22		5.22	5.22				

UNI/PDR XX:2024

→ Esempio dell'Appendice B (B.1 + B.2)

Prospetto B.1 – Relazione fra i Punti della norma UNI CEI EN ISO/IEC 27001:2024 e le Sottocategorie del Framework NIST CSF 2.0

Norma UNI CEI EN ISO/IEC 27001:2024		Sottocategorie NIST CSF 2.0
Numero Punto	**Titolo Punto**	
4.1	Comprendere l'Organizzazione e il suo Contesto	GV.OC-01, GV.OC-03, GV.OC-05
4.2	Comprendere le Esigenze e le Aspettative delle Parti Interessate	GV.OC-01, GV.OC-02, GV.OC-03, GV.OC-04, GV.OC-05, GV.SC-04, GV.SC-05
4.3	Determinare il Campo di Applicazione del Sistema di Gestione per la Cybersicurezza e la Sicurezza delle Informazioni	GV.OC-01, GV.OC-02, GV.OC-03, GV.OC-04, GV.OC-05
4.4	Sistema di Gestione per la Cybersicurezza e la Sicurezza delle Informazioni	GV.OC-01, GV.OC-02, GV.OC-03, GV.OC-04, GV.OC-05, GV.RM-01, GV.RM-02, GV.RM-03, GV.RM-04, GV.RM-05, GV.RM-06, GV.RM-07

Prospetto B.2 – Relazione fra Controlli dell'Appendice A della norma UNI CEI EN ISO/IEC 27001:2024 e le Sottocategorie del Framework NIST CSF 2.0

Controlli in Appendice A della norma UNI CEI EN ISO/IEC 27001:2024	Attributi dei Controlli definiti dalla norma UNI CEI EN ISO/IEC 27002 :2023			Sottocategorie NIST CSF 2.0
	Capacità Operative Valore '#Governance'	**Domini di Sicurezza** Valore '#Governance_and_Ecosystem'	**Concetti di Cybersecurity** Valori '#Identify', '#Protect', '#Detect', '#Respond', '#Recover'	
5 Controlli Organizzativi				
5.1	#Governance	#Governance_and_Ecosystem	#Identify	GV.PO-01, GV.PO-02
5.2	#Governance	#Governance_and_Ecosystem	#Identify	GV.RR-02, GV.SC-02
5.3	#Governance	#Governance_and_Ecosystem	#Protect	GV.RR-02, PR.AA-05
5.4	#Governance	#Governance_and_Ecosystem	#Identify	PR.AT-01, PR.AT-02
5.5	#Governance		#Identify #Protect #Respond #Recover	RS.CO-03, RS.CO-02, RC.CO-03

Q&A

Contatti:

VALENTINA MUSSI
National Market Leader - Cybersecurity & Digital

valentina.mussi@bureauveritas.com

BUREAU VERITAS ITALIA

MAURIZIO GENNA
Product Manager ICT

maurizio.genna@bureauveritas.com

BUREAU VERITAS ITALIA

Vieni a trovarci al nostro stand!