REGIONE PIEMONTE

CSI your digital partner

WEBINAR
SICURI di essere SICURI?

NIS2: governance e formazione

SICURI DI ESSERE SICURI?

Cybersecurity e NIS 2 per un mondo digitale più protetto!

IV Stagione

Relatore Enzo Veiluva – Responsabile Cybersecurity e BU

Calendario eventi

maggio

NIS2: governance e formazione

giugno

NIS2: le misure di sicurezza

luglio

Il ruolo del CISO e le sfide all'interno delle organizzazioni

settembre

Cybersicurezza per tutti: formazione per non addetti ai lavori

ottobre

Analisi dei rischi cyber per tutti. Strumenti e metodologie per la NIS2

novembre

Gestione della supply chain: dal GDPR all'IA ACT, passando da NIS2 e DORA

Perchè un focus su NIS2

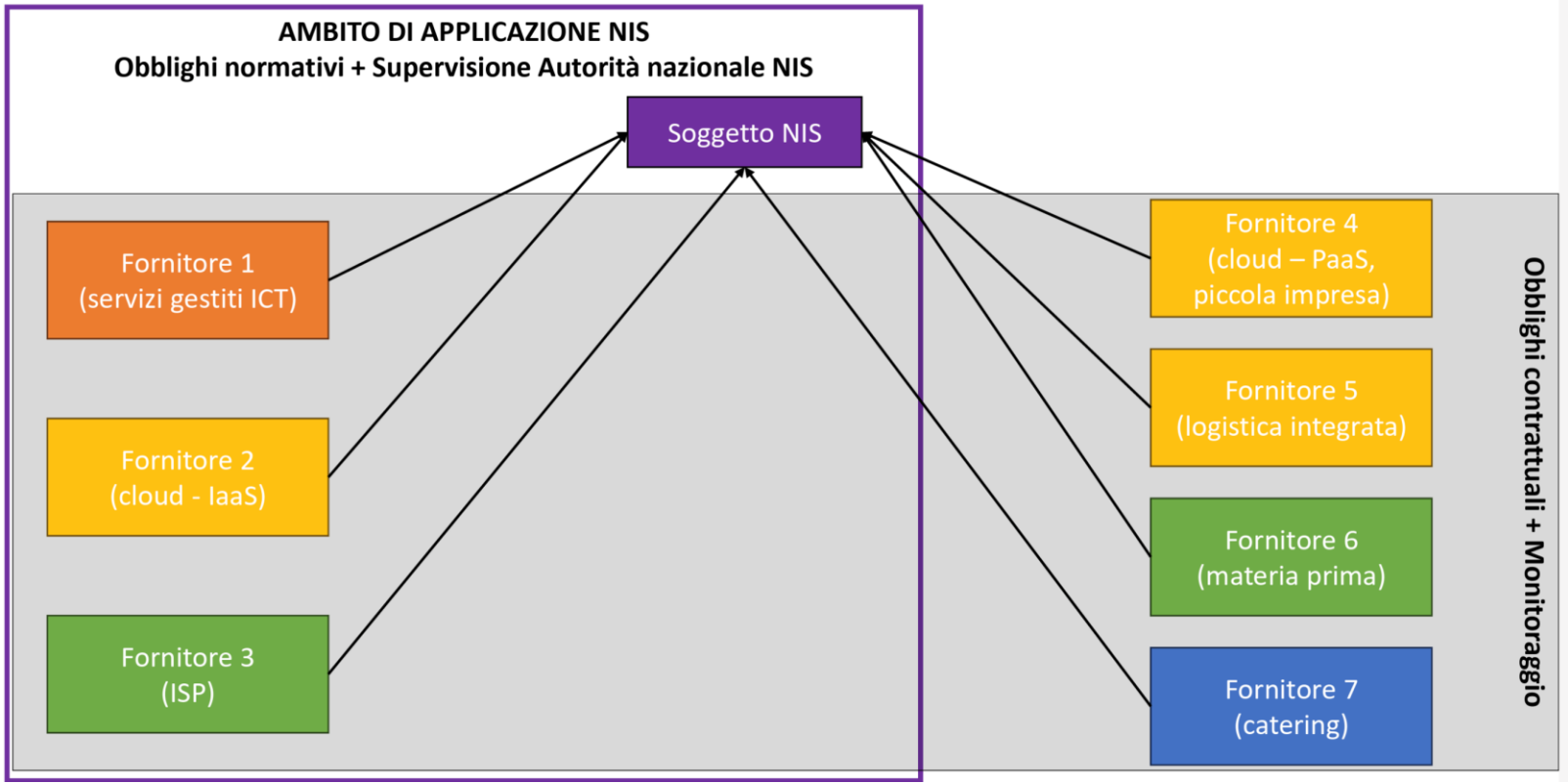
I NUMERI in ITALIA:

20.000 soggetti IMPORTANTI
5.000 soggetti ESSENZIALI

E’ nei restanti 23 Paesi d’Europa?

Perchè un focus su NIS2

Catena di approvvigionamento



Fonte ACN Presentazione del 26 marzo 2025

Notifiche di incidente

Fonte ACN Presentazione del 26 marzo 2025

Misure di sicurezza di base

41 misure di sicurezza → 10 ambiti di sicurezza NIS

- 36 per soggetti essenziali e importanti.
- 5 addizionali solo per i soggetti essenziali.

Struttura misura: codice + descrizione + requisiti

- Il codice identificativo e la descrizione della misura fanno riferimento al FNSC.
- I requisiti indicano ciò che è richiesto ai fini dell'implementazione.

116 requisiti → Proporzionalità

- 82 per soggetti essenziali e importanti.
- 34 addizionali solo per i soggetti essenziali.

Fonte ACN Presentazione del 26 marzo 2025

6 Categorie di misure

GOVERNO (GV)

IDENTIFICAZIONE (ID)

PROTEZIONE (PR)

RILEVAMENTO (DE)

RISPOSTA (RS)

RIPRISTINO (RC)

Ciò anche per consentire la **pianificazione delle sessioni di informazione** dedicata ai componenti degli organi di amministrazione e direttivi. Inoltre, la **presa d'atto telematica** prevista dall'**articolo 16 della Determinazione n. 136117 del 10 aprile u.s.** potrà essere effettuata **anche successivamente al termine del 31 luglio.**

Organi di amministrazione e direttivi (articolo 23)

Sono individuate precise responsabilità in capo agli organi di amministrazione del soggetto, i quali approvano e sovraintendono all'implementazione delle misure oltre a essere responsabili delle eventuali violazioni.

GOVERNANCE

ART. 23..
(Organi di amministrazione e direttivi)

1. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e importanti:

   a) **approvano le modalità di implementazione** delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24;

   b) **sovrintendono all'implementazione** degli obblighi di cui al presente capo e di cui all'articolo 7;

   c) **sono responsabili delle violazioni** di cui al presente decreto.

2. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e importanti:

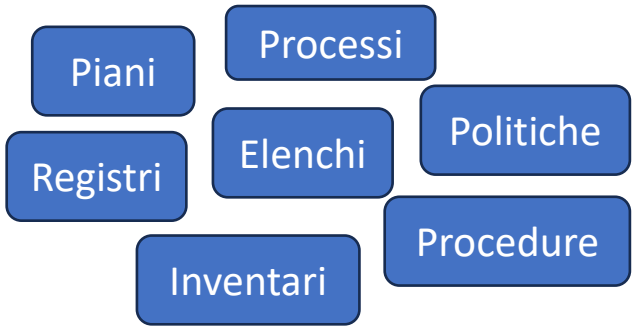
   a) sono tenuti a **seguire una formazione** in materia di sicurezza informatica;

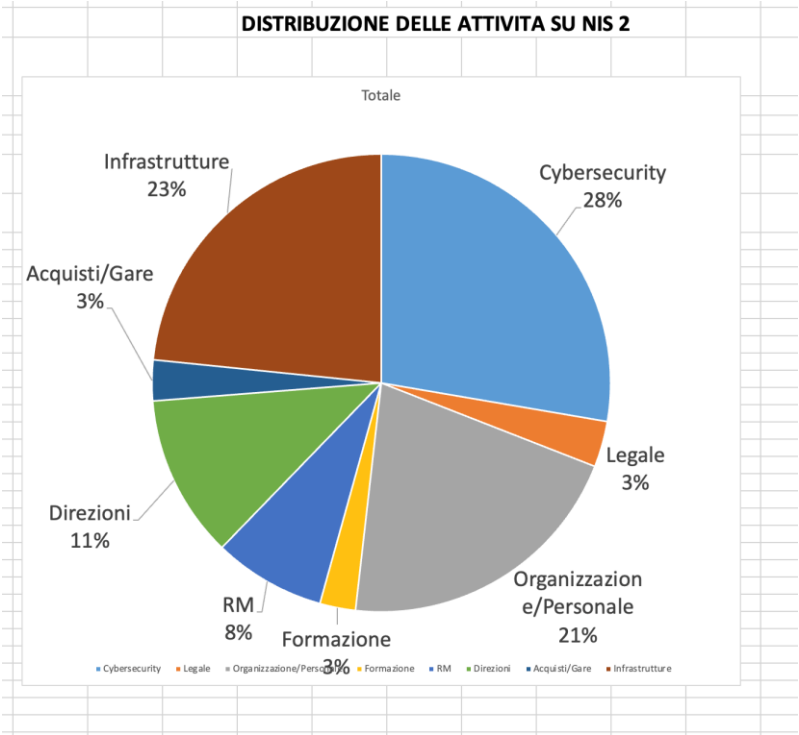
   b) promuovono l'offerta periodica di una **formazione coerente** a quella di cui alla lettera a) **ai loro dipendenti**, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di **individuare i rischi e valutare le pratiche di gestione dei rischi** per la sicurezza informatica e **il loro impatto** sulle attività del soggetto e sui servizi

CONCLUSIONI :
AL TERMINE DEGLI INTERVENTI

Governance vuol dire:

- *Assunzione di responsabilità*
- *Formazione*
- *Controllo e Monitoraggio*
- *Definizione Ruoli di Obiettivi*





In particolare, la prassi costituisce un ponte metodologico che consente ai soggetti già certificati ISO/IEC 27001 di estendere il proprio sistema di gestione ai controlli e alle misure richieste dal NIST CSF.

CSI
your digital partner

NIS2

UNA PROVA DA AFFRONTARE INSIEME

Grazie

enzo.veiluva@csi.it