Direttiva NIS

Agenda

1. CONTESTO DI RIFERIMENTO - LA DIRETTIVA NIS
2. NIS TIMELINE
3. NIS DIRECTIVE – APPROCCIO ITALIANO ALLA NIS
4. VALUTAZIONE DI OVERVIEW – FRAMEWORK NIS

Contesto di riferimento

LA DIRETTIVA EUROPEA NETWORK AND INFORMATION SECURITY (NIS)

- Il **17 Maggio 2016** Il Consiglio Europeo ha adottato la **Network and Information Security Directive ("NIS")** quale parte integrante della Cybersecurity Strategy della Commissione Europea. Tale Direttiva è entrata in vigore l' **8 Agosto 2016**.
- Gli Stati Membri hanno avuto 21 mesi per il recepimento a livello nazionale ed altri 6 mesi per individuare gli operatori (pubblici e privati) di servizi essenziali.
- In data 18 Maggio 2018 **l'Italia ha recepito la Direttiva NIS con il D.Lgs. 65/2018**.
- IL **9 Novembre 2018** sono stati identificati gli Operatori di Servizi Essenziali

Contesto di riferimento

LA DIRETTIVA EUROPEA NETWORK AND INFORMATION SECURITY (NIS)

Obiettivo della Direttiva

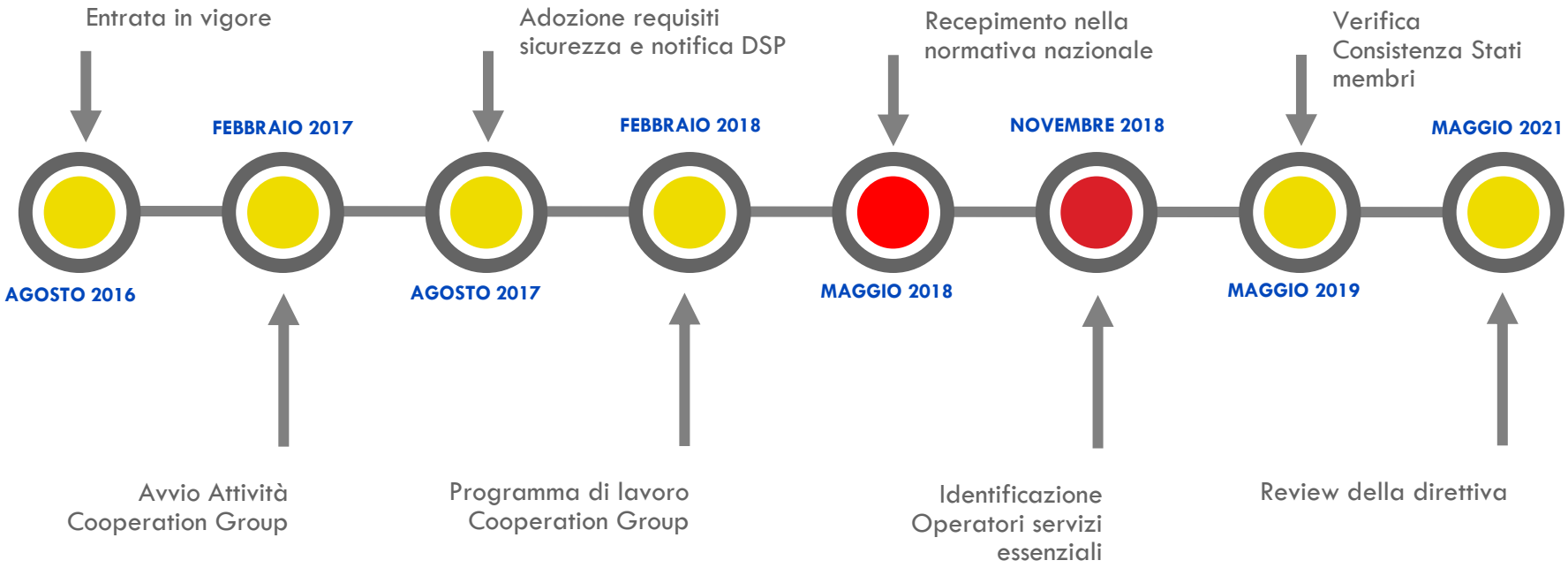
- Adottare **misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi** posti alla sicurezza delle reti e dei sistemi informativi, provvedendo a realizzare un effettivo **innalzamento dei livelli di sicurezza** connessi ai servizi essenziali e digitali.

Destinatari

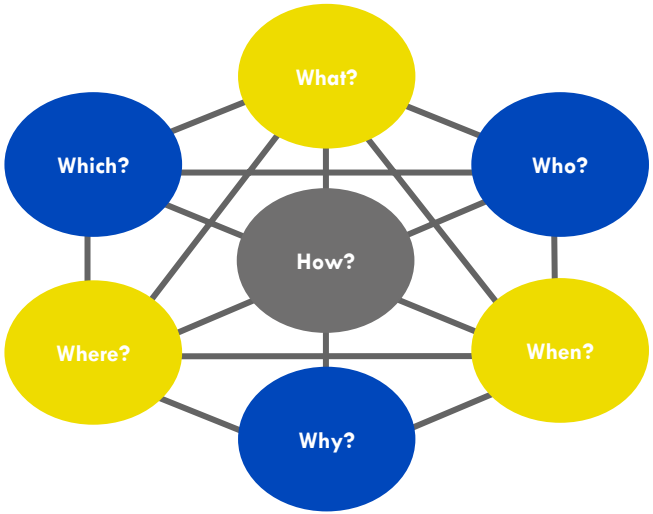
- La Direttiva si applica alle **organizzazioni pubbliche e private**, in particolare:
  - **Operatori (pubblici e privati) di servizi essenziali** (quali fornitori energetici, aziende di trasporto aereo, ferroviario e stradale, banche, infrastrutture per i mercati finanziari, ospedali, fornitori e distributori di acqua, fornitori di infrastrutture e servizi di Telecomunicazioni)
  - **Fornitori di servizi digitali** (quali online marketplaces, motori di ricerca e fornitori di servizi cloud).

NIS timeline

La direttiva *Network and Information Security* (NIS) è stata recepita nell'ordinamento Nazionale nel mese di maggio del 2018 entrando, come rappresentato dal diagramma riportato di seguito, nella sua fase operativa piena il 9 novembre del 2018.



NIS DIRECTIVE



What?

Cosa prevede a livello politico e giuridico la Direttiva NIS?
La Direttiva NIS prevede l'adozione di misure volte ad innalzare il livello di sicurezza delle reti e dei sistemi informativi.

Who?

Chi sono i referenti istituzionali?
I referenti istituzionali sono il MiSE, il MEF, il MIT, Il Ministero della salute, il Ministero dell'ambiente e della tutela del territorio e del mare, regioni e province autonome di Trento e Bolzano (sanità e distribuzione acqua) e il DIS e il CNAIPIC.

When?

Quando un operatore è da considerarsi responsabile nel framework della NIS?
Quando è responsabile nel framework NIS In tutti i casi in cui un servizio offerto si configura come servizio essenziale.

Why?

Perché un operatore è tenuto a implementare la NIS?
Perché, data la tipologia di servizi offerti, un incidente potrebbe avere un impatto significativo sul mantenimento di attività sociali ed economiche fondamentali, nonché avere impatti sulla sicurezza nazionale.

Where?

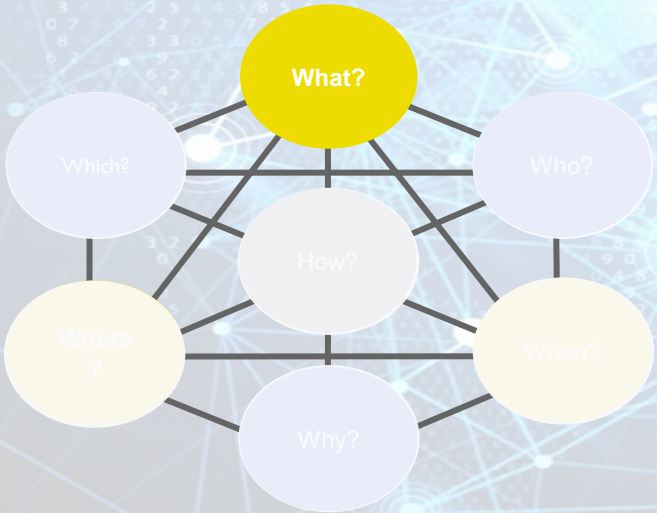
Dove è posizionato un OSE nel contesto italiano ed europeo?
Qualsiasi operatore, pubblico o privato, che occupa una posizione rilevante nel contesto italiano/europeo nella fornitura di servizi in settori differenti.

Which?

Quali sono i servizi essenziali forniti dagli OSE?
Servizi nei settori dei Sanitari, Bancario, Servizi Finanziari, Trasporti, Distribuzione Acqua, in generale nell'erogazione dei servizi al cittadino.

How?

Come si può implementare la direttiva NIS?
Recependo le linee guida generali del NIS Cooperation Group.



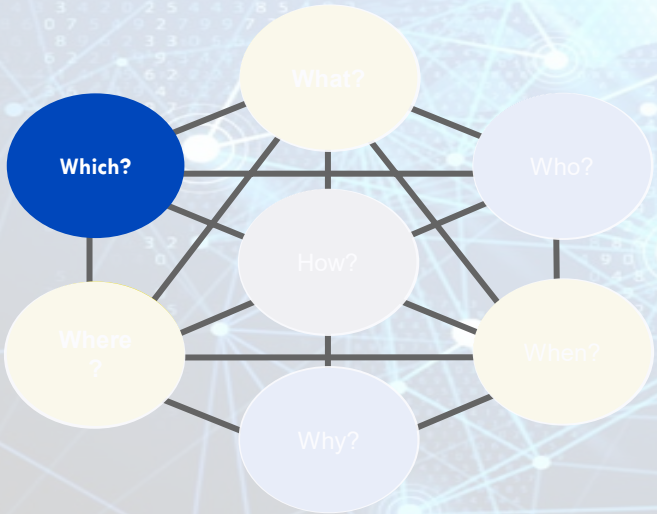
COSA PREVEDE LA DIRETTIVA NIS?

NIS DIRECTIVE

What?

L'obiettivo della Direttiva NIS è quello di promuovere l'**innalzamento dei livelli di sicurezza** connessi ai servizi essenziali e digitali

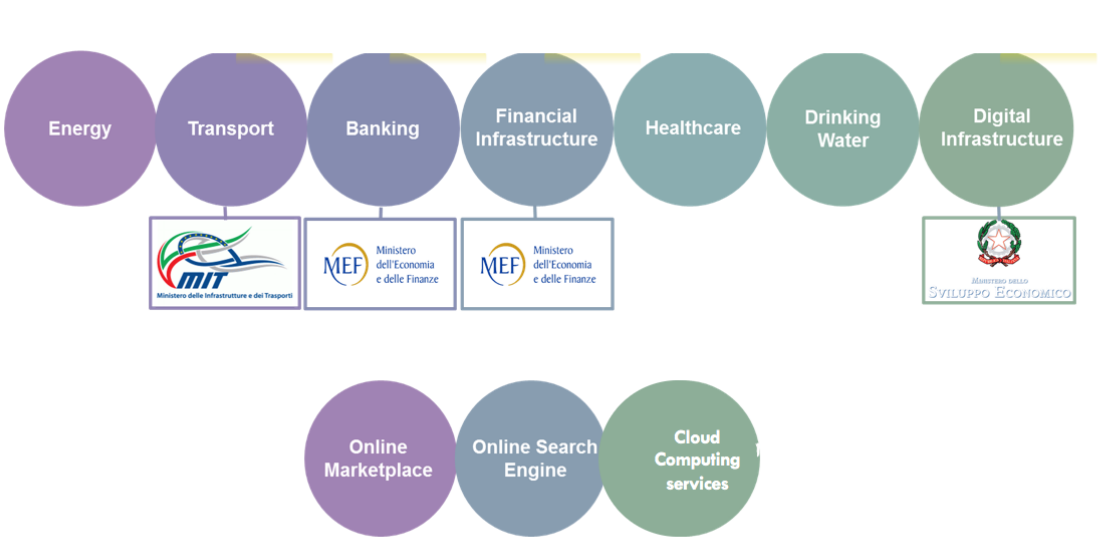
- *Adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi*
- *Adottare misure adeguate per prevenire e minimizzare l'impatto di incidenti e garantire la continuità dei servizi essenziali offerti*
- *Adempiere agli obblighi normativi di notifica, senza indebito ritardo, all'autorità competente, come CSIRT e CNAIPIC, degli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati*
- *Fornire all'autorità competente le informazioni necessarie a valutare la sicurezza delle reti e dei sistemi informativi, compresi i documenti relativi alle politiche di sicurezza*
- *Fornire all'autorità competente la prova dell'effettiva attuazione delle politiche di sicurezza*



QUALI SONO I SERVIZI ESSENZIALI?

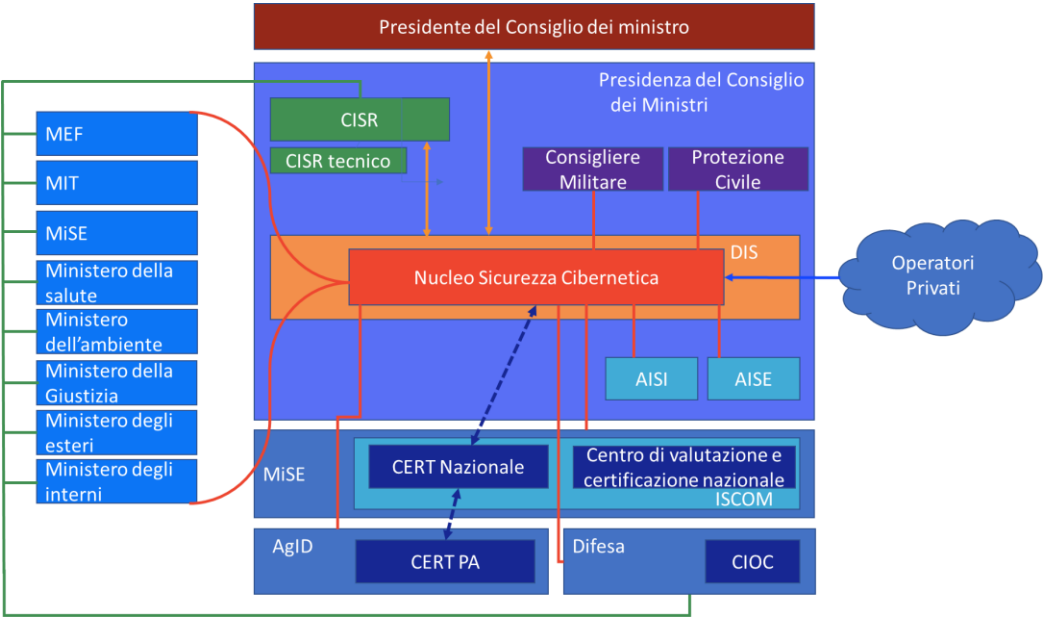
NIS DIRECTIVE

Which?



Servizi Essenziali

NIS DIRECTIVE



Contesto istituzionale italiano

- Il Presidente del Consiglio dei Ministri adotta, sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), la strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale.
- Le Autorità competenti NIS sono responsabili dell'attuazione del presente decreto.
- Il **Dipartimento delle informazioni per la sicurezza (DIS)** è designato quale punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi.
- I **Ministeri** si configurano come i Riferimenti Istituzionali degli Operatori per area di competenza.
- Le funzioni di CSIRT italiano sono svolte dal CERT nazionale unitamente al CERT-PA in collaborazione tra loro.
- Gli OSE (operatori di servizi essenziali), devono notificare eventuali incidenti significativi che hanno impatto sulla continuità dei servizi al **CSIRT** e **CNAIPIC.**

NIS DIRECTIVE

RISCHI, SANZIONI E SENSO DI RESPONSABILITA'

A quali sanzioni risulta esposto un operatore di servizi essenziali nei casi di non compliance alla Direttiva?

Le sanzioni in cui rischia di incorrere oscillano tra i **12.000 euro** ed i **150.000 euro,** nei seguenti casi:

1. Operatore di servizi essenziali che non adotta le misure tecniche e organizzative adeguate e proporzionate **per la gestione del rischio per la sicurezza della rete e dei sistemi informativi**
2. Operatore di servizi essenziali che non adotta le misure adeguate **per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi**
3. Operatore di servizio essenziale che non notifica al CSIRT italiano **gli incidenti aventi un impatto rilevante sulla continuita' dei servizi essenziali** forniti
4. Operatore di servizio essenziale **che non fornisce all'autorità competente NIS le evidenze richieste in termini di documentazione.**
5. Operatore di servizio essenziale **che non rispetta le indicazioni vincolanti ricevute dall'autorità competente NIS di riferimento.**
6. Operatore di servizi essenziali dipendente da terze parti che fornisce servizi digitali per la fornitura di un servizio che è indispensabile per il mantenimento di attività economiche e sociali fondamentali.

ALLEGATI ALLA NIS

NIS DIRECTIVE

COSA PREVEDE LA DIRETTIVA NIS? (1/2)

What?

La **DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO** stabilisce misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno.

Art. 14

REQUISITI

*"Gli Stati membri provvedono affinché gli operatori di servizi essenziali **adottino misure tecniche e organizzative adeguate** e proporzionate alla gestione dei **rischi posti alla sicurezza delle reti e dei sistemi informativi** che usano nelle loro operazioni.*

Tenuto conto delle conoscenze più aggiornate in materia, dette misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente.

*Gli Stati membri provvedono affinché gli operatori di servizi essenziali adottino **misure adeguate per prevenire e minimizzare l'impatto di incidenti** a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di **assicurare la continuità di tali servizi**"*

NOTIFICA

*Gli Stati membri provvedono affinché gli operatori di servizi essenziali **notifichino senza indebito ritardo all'autorità competente o al CSIRT gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati.** Le notifiche includono le informazioni che consentono all'autorità competente o al CSIRT di determinare qualsiasi impatto transfrontaliero dell'incidente. La notifica non espone la parte che la effettua a una maggiore responsabilità.*

Obiettivi

1. **Innalzamento dei livelli di sicurezza connessi ai servizi essenziali e digitali**
2. **Adozione di misure tecniche e organizzative adeguate e proporzionate alla gestione del rischio**
3. **Gestione dei rischi e segnalazione degli incidenti di una certa entità**

NIS DIRECTIVE

COSA PREVEDE LA DIRETTIVA NIS? (2/2)

What?

La **DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO** stabilisce misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno.

Art. 15

CONTROLLI

Gli Stati membri provvedono affinché le autorità competenti siano dotate dei poteri e dei mezzi per richiedere agli operatori di servizi essenziali di fornire:

- *Le **informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi**, compresi i documenti relativi alle politiche di sicurezza;*
- *La prova dell'effettiva attuazione delle politiche di sicurezza, come i **risultati di un audit sulla sicurezza svolto dall'autorità competente o da un revisore abilitato** e, in quest'ultimo caso, **metterne a disposizione dell'autorità competente i risultati, inclusi gli elementi di prova**.*

SANZIONI

Si va da un minimo di 12.000 euro ad un massimo di 150.000 euro per le violazioni poste in essere da parte degli operatori di servizi essenziali (la più grave, mancato rispetto di istruzioni vincolanti, fornite dall'Autorità NIS, al fine di porre rimedio a carenze individuate).

La reiterazione delle violazioni indicate all'art. 21 dello schema di Decreto comporta l'aumento della sanzione fino al triplo di quanto previsto.

NIS DIRECTIVE

QUALI SONO I SERVIZI ESSENZIALI?

Art. 5

I criteri per l'identificazione degli operatori di servizi essenziali di cui all'articolo 4, punto 4, sono i seguenti:

1. **Un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali**
2. **La fornitura di tale servizio dipende dalla rete e dai sistemi informativi**
3. **Un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio**

Art. 6

Nella determinazione della rilevanza degli effetti negativi di cui all'articolo 5, paragrafo 2, lettera c), gli Stati membri tengono conto almeno dei seguenti fattori intersettoriali:

a) il numero di utenti che dipendono dal servizio fornito dal soggetto interessato;

b) la dipendenza di altri settori di cui all'allegato II dal servizio fornito da tale soggetto;

c) l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza;

d) la quota di mercato di detto soggetto;

e) la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;

f) l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio.

PA, Ministero della Giustizia e Direttiva NIS

- Le pubbliche amministrazioni, anche in considerazione dei dati sensibili che trattano e che offrono servizi nei settori sopra elencati dalla normativa di trasposizione della Direttiva NIS (quindi, ad esempio, trasporti, sanità e distribuzione di acqua potabile) saranno comunque sottoposte alla normativa NIS, **se identificate quali operatori di servizi essenziali**.
- Le pubbliche amministrazioni rimangono comunque soggette a quanto disposto dalla **Circolare AgID n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni".**

Approfondimento

Libri di testo, risorse web e altri materiali di approfondimento

- Decreto legislativo 18 maggio 2018, n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione
- DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 8 agosto 2019. Disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT italiano.
- L.Gaiser, "La necessità di una strategia della presenza costante e della creazione di ecosistemi regionali per migliorare la sicurezza cibernetica delle infrastrutture critiche europee", Sicurezza, Terrorismo e Società, vol. 7, n. 1, 2018, pp. 103-116
- Sicurezza Nazionale, "La NIS in pillole", https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/06/La-NIS-in-pillole.pdf (14/06/2020)