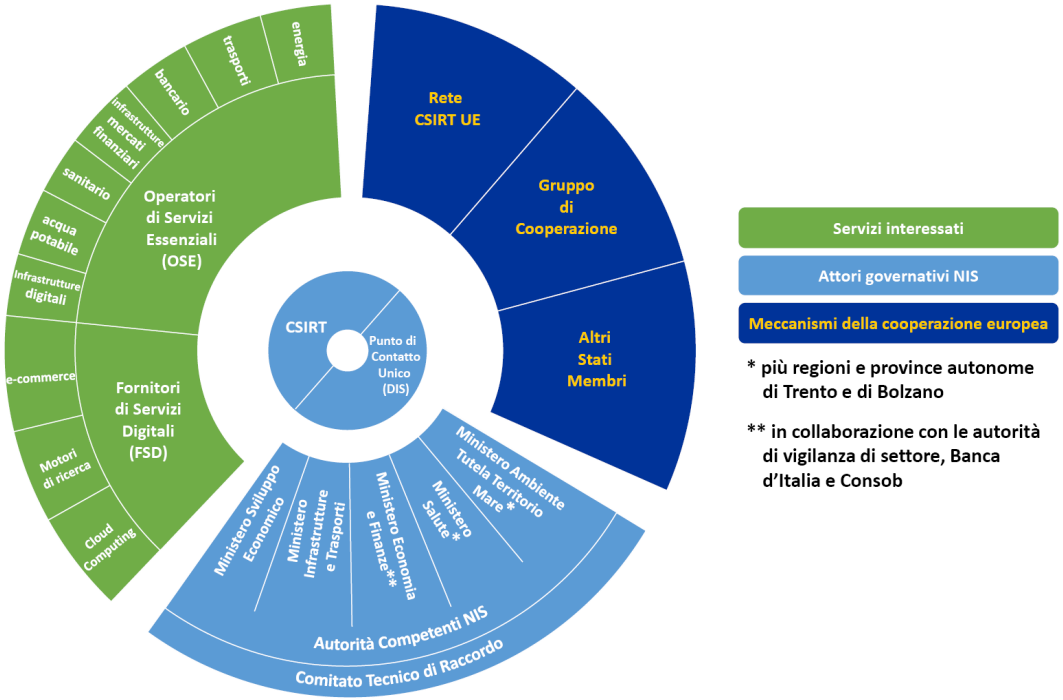
La NIS in pillole

- Con il **Decreto Legislativo 18 maggio 2018, n.65**, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018, l'Italia ha dato attuazione, recependola nell'ordinamento nazionale, alla Direttiva (UE) 2016/1148, cd. **Direttiva NIS**, intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi. Il decreto si applica agli **Operatori di Servizi Essenziali (OSE)** e ai **Fornitori di Servizi Digitali (FSD)**.
- Gli **OSE** sono i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori **sanitario**, dell'**energia**, dei **trasporti**, **bancario**, delle **infrastrutture dei mercati finanziari**, della **fornitura e distribuzione di acqua potabile** e delle **infrastrutture digitali**.
- Gli **FSD** sono le persone giuridiche che forniscono servizi di *e-commerce*, *cloud computing* o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale. Gli obblighi previsti per gli FSD non si applicano alle **imprese** che la normativa europea definisce "**piccole**" e "**micro**", quelle cioè che hanno meno di 50 dipendenti e un fatturato o bilancio annuo non superiore ai 10 milioni di Euro.



- Tanto gli **OSE** che gli **FSD**:
  - sono chiamati ad adottare **misure tecniche e organizzative adeguate e proporzionate** alla **gestione dei rischi** e a **prevenire** e **minimizzare l'impatto degli incidenti** a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio;
  - hanno l'**obbligo di notificare**, **senza ingiustificato ritardo**, gli **incidenti** che hanno un **impatto rilevante**, rispettivamente sulla continuità e sulla fornitura del servizio, al *Computer Security Incident Response Team* (CSIRT) italiano, informandone anche l'Autorità competente NIS di riferimento.

- Gli **FSD** sono tenuti ad applicare le prescrizioni dettate dal decreto di recepimento a partire dal **24 giugno 2018**, data di entrata in vigore del provvedimento, valutando la rilevanza degli incidenti sulla base dei criteri e delle soglie indicati nel Regolamento (UE) 2018/151 del 30 gennaio 2018 reperibile online all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018R0151&from=IT.

Un incidente a carico di un FSD è rilevante se si verifica almeno una delle seguenti condizioni
Indisponibilità del servizio fornito per oltre 5.000.000 di ore utente
Perdita di integrità, autenticità o riservatezza dei dati per oltre 100.000 utenti dell'UE
Rischio per la sicurezza e/o l'incolumità pubblica, o in termini di perdite di vite umane
Danni materiali superiori a 1.000.000 di EUR per almeno un utente nell'UE

- I **soggetti giuridici non identificati** come **OSE** e che **non** sono **FSD** possono inoltrare al CSIRT **notifiche volontarie** degli incidenti che abbiano un impatto rilevante sulla continuità dei servizi da loro erogati. Ciò poiché l'intento della Direttiva NIS e del relativo decreto di recepimento è quello di favorire la più ampia diffusione di una consapevole cultura nel campo della *cybersecurity* e di un conseguente accrescimento dei relativi livelli di sicurezza, anche attraverso un maggiore scambio di informazioni.
- Il ***Computer Security Incident Response Team*** **(CSIRT) italiano**:
  - definisce le procedure per la prevenzione e la gestione degli incidenti informatici;
  - riceve le notifiche di incidente, informandone il DIS, quale punto di contatto unico e per le attività di prevenzione e preparazione a eventuali situazioni di crisi e di attivazione delle procedure di allertamento affidate al Nucleo per la Sicurezza Cibernetica;
  - fornisce al soggetto che ha effettuato la notifica le informazioni che possono facilitare la gestione efficace dell'evento;
  - informa gli altri Stati membri dell'UE eventualmente coinvolti dall'incidente, tutelando la sicurezza e gli interessi commerciali dell'OSE o del FSD nonché la riservatezza delle informazioni fornite;
  - garantisce la collaborazione nella rete di CSIRT, attraverso l'individuazione di forme di cooperazione operativa, lo scambio di informazioni e la condivisione di *best practices*.

  Il CSIRT italiano sarà istituito presso la Presidenza del Consiglio dei ministri mediante unificazione del *Computer Emergency Response Team* (CERT) Nazionale e del CERT-PA, assumendone i compiti. Nelle more della definizione di funzionamento e organizzazione della nuova struttura (demandata ad un DPCM da adottare entro il 9 novembre 2018):
  - le funzioni del CSIRT italiano sono svolte dal CERT-N unitamente al CERT-PA, con una ripartizione di ruoli e responsabilità secondo le attuali *constituency* (Pubblica Amministrazione per il CERT-PA, settore privato per il CERT-N) e con l'introduzione di uno scambio informativo rafforzato e di specifiche procedure di gestione delle notifiche;
  - il CERT-N garantisce la cooperazione a livello europeo, anche nell'ambito della rete di CSIRT, in stretto raccordo con il CERT-PA.

- Le **Autorità competenti NIS**, quali responsabili dell'attuazione del decreto:
  - vigilano sulla sua applicazione ed esercitano le relative potestà ispettive e sanzionatorie, fatte salve le attribuzioni e le competenze degli organi preposti alla tutela dell'ordine e della sicurezza pubblica. Salvo che il fatto costituisca reato, la violazione da parte di OSE e FSD degli obblighi previsti dal decreto legislativo comporta l'irrogazione di sanzioni amministrative pecuniarie fino ad un massimo di 150.000 euro; la reiterazione determina l'aumento fino al triplo della sanzione prevista;
  - procedono ad identificare gli OSE entro il 9 novembre 2018 (consultando, laddove necessario, le Autorità competenti NIS degli altri Stati Membri), individuando anche le soglie in ragione delle quali un incidente è da considerarsi pregiudizievole per la sicurezza delle reti e dei sistemi informativi. Se un evento implica anche violazione di dati personali, le Autorità competenti NIS operano in stretta cooperazione con il Garante per la protezione dei dati personali. Al riguardo, sono in corso approfondimenti per propiziare un raccordo tra gli obblighi introdotti dal Decreto legislativo di recepimento della Direttiva NIS e quelli previsti dal nuovo Regolamento europeo per la protezione dei dati personali (GDPR);
  - possono predisporre linee guida per la notifica degli incidenti e dettare specifiche misure di sicurezza, sentiti gli OSE.

Autorità competenti NIS	Ambito di competenza
Ministero dello sviluppo economico	Settore dell'energia – Sottosettori energia elettrica, gas e petrolio
	Settore delle infrastrutture digitali
	Servizi digitali
Ministero delle infrastrutture e dei trasporti	Settore dei trasporti – Sottosettori trasporto aereo, trasporto ferroviario, trasporto per vie d'acqua e trasporto su strada
Ministero dell'economia e delle finanze in collaborazione con Banca d'Italia e Consob	Settore bancario
	Settore delle infrastrutture dei mercati finanziari
Ministero della salute, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità sanitarie territorialmente competenti)	Settore sanitario
Ministero dell'ambiente e della tutela del territorio e del mare, Regioni e Province autonome di Trento e di Bolzano (direttamente o per il tramite delle Autorità territorialmente competenti)	Settore della fornitura e distribuzione di acqua potabile

L'**elenco nazionale degli OSE** è istituito presso il Ministero dello sviluppo economico e viene aggiornato, almeno ogni due anni, a cura delle Autorità competenti NIS.

- Il **punto di contatto unico NIS** assicura, a livello nazionale, il coordinamento delle questioni relative alla sicurezza delle reti e dei sistemi informativi e, a livello europeo, il raccordo necessario a garantire la cooperazione transfrontaliera delle Autorità competenti NIS italiane con quelle degli altri Stati

membri, con il Gruppo di cooperazione istituito presso la Commissione europea - anche attraverso l'elaborazione di linee guida e lo scambio di informazioni e *best practices* - e la rete dei CSIRT UE. Rientra tra i compiti del punto di contatto unico NIS trasmettere a:

- Gruppo di cooperazione, entro il 9 agosto 2018 (e in seguito annualmente), una relazione sulle notifiche ricevute, contenente numero e natura degli incidenti e le azioni intraprese da OSE e FSD;
- Commissione UE, entro il 9 novembre 2018 (e in seguito ogni due anni), le informazioni per verificare l'attuazione della Direttiva NIS in Italia.

Quale punto di contatto unico NIS è stato designato il **Dipartimento Informazioni per la Sicurezza (DIS)**, in ragione del ruolo svolto nell'architettura *cyber* nazionale.

- Allo scopo di agevolare le Autorità competenti NIS nell'adempimento dei compiti loro affidati, verrà istituito, attraverso un apposito DPCM, un **Comitato tecnico di raccordo**.
  Il Comitato opererà presso la Presidenza del Consiglio dei ministri, riunendo i delegati dei Ministeri-Autorità competenti NIS e i rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano.

- A valle del recepimento della Direttiva NIS, sarà integrata di un apposito *addendum* la **Strategia nazionale di sicurezza cibernetica**, adottata dal Presidente del Consiglio dei ministri, sentito il Comitato Interministeriale per la Sicurezza della Repubblica (CISR).