Shipping 4.0
Tecnologie trasformative e opportunità per lo Shipping e il maritime cluster

DIH
Digital Innovation Hub
LIGURIA

Orietta Campironi, CIO Gruppo Messina
Genova 18 Ottobre 2018

Tecnologie trasformative e opportunità per lo Shipping e il maritime cluster

Il mutamento di paradigma e l'impatto della rivoluzione 4.0 ha travalicato i confini della produzione industriale, e il settore dello Shipping sta affrontando una nuova disruption.

Il potenziale delle tecnologie acceleratrici di innovazione nel processo di trasformazione digitale può essere sostanziale per creare nuovo valore nei processi core e nelle attività commerciali, operative e di pianificazione in ambito Container Shipping, Porti, Terminal e Logistica Terrestre.

IoT, Advanced Analytics, AI, Cybersecurity, sono alcuni dei trend tecnologici, considerati da Gartner tra i Top 10 del 2018, che le aziende stanno contemplando nelle iniziative ″Shipping 4.0″, con un approccio olistico di trasformazione verso Smart Shipping e Smart Ports.

DX, un fenomeno ineluttabile

"Entro il 2021, il mercato digitale avrà completamente ridisegnato lo scenario economico mondiale."

*"Gli investimenti mondiali in tecnologie per la trasformazione digitale arriverà a sfiorare i **1.300 miliardi di dollari nel 2018**, in crescita del 16,8% sul 2017, e i **1.700 miliardi nel 2019**, in crescita del 42% sempre rispetto al 2017.*

*… **dei 1.700 miliardi previsti nel 2019**, la parte più consistente, **1.300 miliardi** di dollari, sarà spesa negli Acceleratori dell'Innovazione(*) che animeranno un processo di discontinuità in tutti i settori industriali."*

(IDC, feb2018)

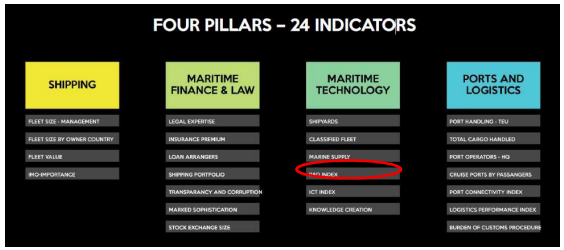
(*)IDC identifica gli Acceleratori dell'Innovazione principalmente nelle seguenti tecnologie: IoT, robotica, AI, sistemi cognitivi, realtà aumentata e virtuale, 3D Printing, blockchain.

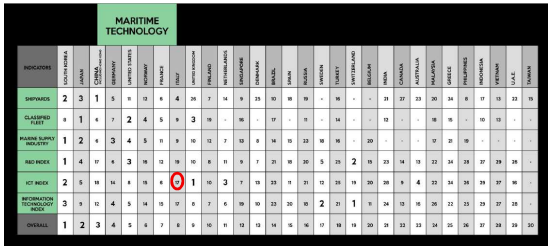
Una nuova disruption per lo Shipping, paragonabile per impatti e conseguenze operative a quella della «containerizzazione».

Una opportunità per semplificare e facilitare le interazioni, la connettività, la intermodalità, per migliorare la customer experience, per generare ecosistemi con forti integrazioni, per ridurre i tempi e i costi nella catena logistica, per avere flussi operativi seamless, per crescere in efficienza, trasparenza e sicurezza.

"Leading Maritime Nations of the World" 2018.
(Menon Economics and DNV GL)

Benchmarking studio su capability e performance su 30 nazioni, 24 indicatori per 4 pillar
Italia si colloca al 10 posto globalmente e al 17 nel ICT index del pillar Tecnologico





***Ranking europeo DESI 2018*:**
Italia, 26 su 29

Roland Berger – 2018 Global Investigation of Startup working un AI:
Italia, 19 su 20
(A livello mondiale per numero di startup attive (22))

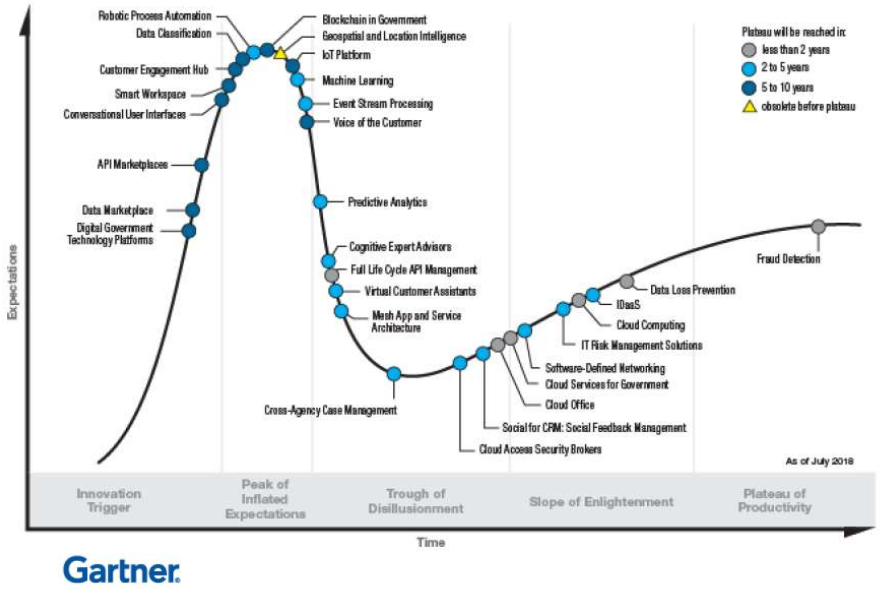
Technology Trends

Nonostante le posizioni di coda nelle classifiche europee e mondiali, ci sono isole di eccellenza che colgono ciò che offre la tecnologia integrandolo nei propri processi, servizi e prodotti, per diventare leading edge. E' un elevato potenziale che va integrato, connesso, con uno sforzo di ecosistema.

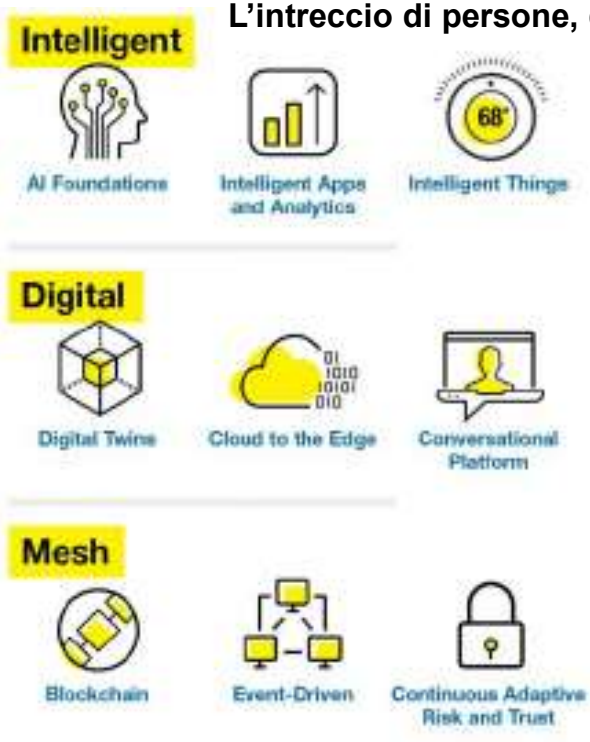
Alcune tecnologie hanno cominciato a diffondersi ampiamente e si è cristallizzata la consapevolezza che possano avvantaggiare le imprese in diversi modi (procedono verso la Slope of Enlightenment):

IoT, AI, cloud, sono piattaforme «democratizzate».

Gartner Hype Cycle 2018 - Emerging technologies



The Intelligent Digital Mesh
L'intreccio di persone, device, contenuti e servizi



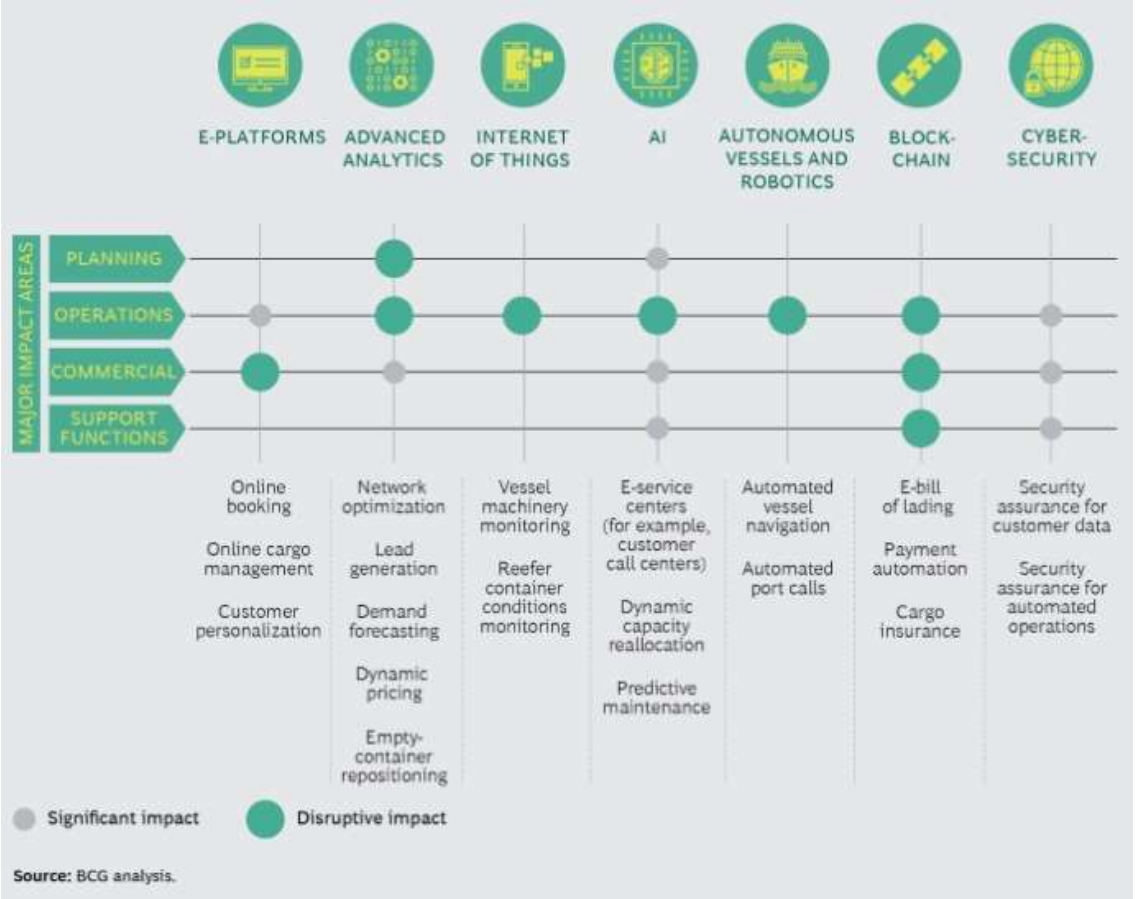
Gartner Top 10 Strategic Technology Trends for 2018

…che stanno trasformando lo shipping

Gruppo Messina
1921 Ignazio Messina & C.

I principali trend digitali che creeranno valore aggiunto, contribuendo all' incremento delle performance nei processi ed attività delle aree Commerciali, Operative, di Pianificazione, e nei processi ICT, Finance, Legal

The Digital Imperative in Container Shipping, Feb '18



…che stanno trasformando lo shipping

Gruppo Messina
1921 Ignazio Messina & C.

Offrire maggiori benefici al cliente e distribuire maggior valore attraverso nuove piattaforme digitali di business, **sviluppando azioni chiave**:

- ❑ nuovi modelli di business e di offering:
  - online booking platform, high-margin services (intermodali e wharehousing), real-time cargo tracking and cargo condition monitoring
- ❑ digitalizzazione delle core operation (attività e tecnologie), creando valore
  - Revenue Management e dynamic pricing, attraverso analytics
  - Costi di sistema (cargo routing, empty-container repositioning), attraverso analytics e AI
  - iERP con focus su centralità dati e capacita di aggregarli ed analizzarli
  - Control Tower Fleet Monitoring, ottimizzazione prestazioni e manutenzione predittiva, attraverso la elaborazioni di milioni di dati da sensori a bordo (posizione, velocità, dati meteo, bunker, ..)
  - Piattaforme di collaborazione multimodali, tra carrier, terminal, e compagnie intermodali (es. per document Management)
- ❑ costruzione interna della digital foundation e della digital vision
  - Strategia, agilità, nuova organizzazione, nuove competenze
  - Scegliere tecnologie e impiantarle secondo strategia, non per stratificazione
  - Tecnologia evolve esponenzialmente, le organizzazioni logaritmicamente; Agile è epicentro del cambiamento, lanciare digital sprint
  - Infrastrutture liquide, tecnologie elastiche, la sfida è organizzativa
  - Investire su incremento competenze del capitale umano

…. e le Port Operations

- Prevalgono ancora molte procedure manuali e **paper-based**
- **Ecosistema articolato** con vari partner (Autorita' portuali, terminals, compagnie di navigazione, quelle di trasporto terrestre e di logistica, ..), e le tecnologie devono agevolare le loro interazioni promuovendo efficienza in tutto l'ecosistema
- **Smart-technology** per riconfigurare le funzioni essenziali di base e velocizzare ed ottimizzare le operazioni per tutti i partner coinvolti
- Le specifiche necessita dei Porti (tipologia e obiettivi) guidano la definizione della strategia tecnologia

- **Sensoristica** per ridurre costi di **ispezioni** e supportare **manutenzioni preventive** (autorità portuali e operatori dei terminal)
- «Black Box» che raccolgono **dati** e attraverso **analytics e AI** individuare colli di bottiglia ed intraprendere azioni correttive durante la **movimentazione merci**
- Sistemi **GPS** basati su controllo traffico per fornire le migliori **opzioni di avvicinamento** in aree congestionate
- Sistemi di **gate automation** per velocizzare flussi di ingresso e uscita…

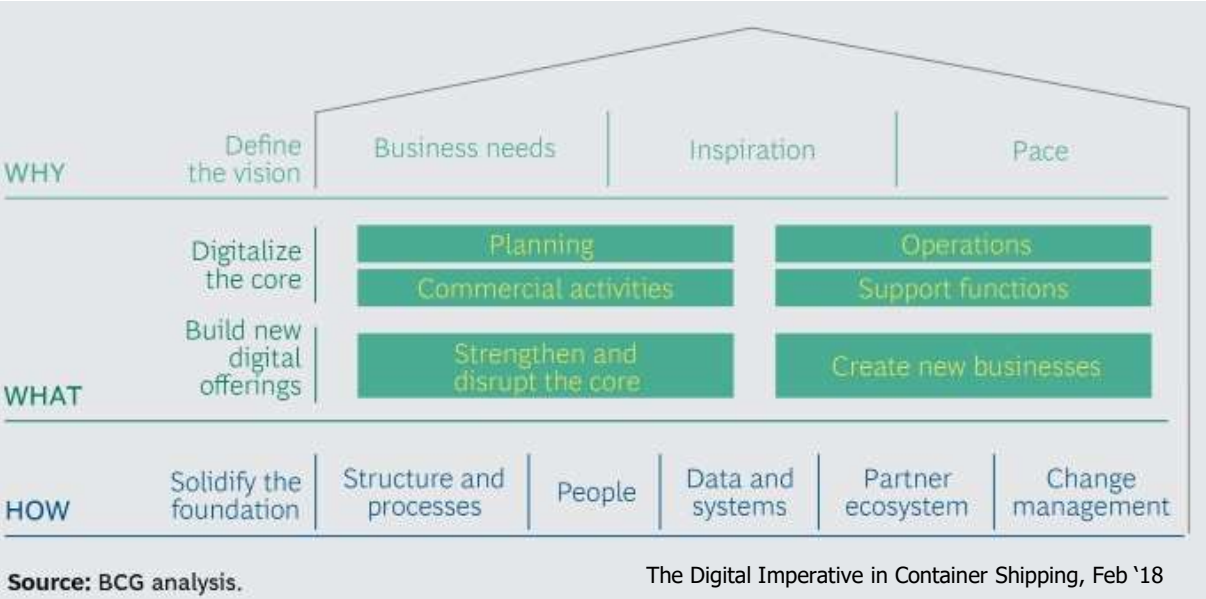
EXHIBIT 3 | A Port's Individual Needs Drive the Technology Strategy

TYPE	FOCUS	APPLICABLE SOLUTIONS
Emerging port	Ease of doing business	• Port community systems • Single-window customs • X-ray scanning • Biometric access control systems
Local trade hub	High productivity	• Smart cargo-handling systems • Equipment management and control • Gate automation • Safety management solutions
Intermodel gateway	Optimized traffic across transport modes	• Truck appointment systems • Traffic-monitoring systems • Integrated rail and barge platforms
City-based port	Minimized impact on surroundings	• Asset health monitoring • Environment and energy • Management systems • Port-wide platforms

Source: BCG analysis.

Un approccio olistico per la trasformazione digitale

Un approccio strutturato, a cominciare dalla definizione della digital vision, per generare commitment, indirizzare i business needs, guardando anche realistici esempi ispiratori, ed integrando non solo tecnologie e nuove capability ma anche nuovi mindset.



The Digital Imperative in Container Shipping, Feb '18

Si digitizzano informazioni, si digitalizzano processi e ruoli, e si trasforma digitalmente il business e la strategia.

La trasformazione digitale incomincia dal cambiamento della organizzazione.

- Visione
- Commitment per rapida adozione
- Foundation
- Open innovation
- Testare e scalare rapidamente

Iniziative a volore aggiunto per il cluster maritime

1. E-platform (booking on line, cargo management on line)
    - Accordo operativo Maersk – Alibaba per booking online
2. Advanced Analytics (demand forecasting, dynamic pricing, riposizionamento containers)
    - Descriptive, predictive, i piu utilizzati, prescriptive in aumento e automated, in fase pilota
    - Per il revenue management, per ottimizzare dinamicamente i processi esistenti.
    - Per ottimizzare i costi di sistema (riprogettare rete, routing merce, riposizionamento dei contenitori)
3. IoT (vessel monitoring, container tracking/monitoring, gate automation)
    - Tracking della merce durante tutte le fasi del trasporto, per aver informazioni di stato e posizione (per cliente, programmazione interna, assicurazioni)
    - Esempio di convergenza IoT e AI, per identificazione evoluta di veicoli, contenitori e conducenti gia' in avvicinamento ai gate e durante tutta la permanenza in area operativa
    - Accordo operativo Maersk e AT&T per il tracking dei trasporti

Soluzioni a volore aggiunto per il cluster maritime

4. AI (dynamic capacity reallocation, manutenzione e gestione predittiva degli asset, Customer Service Center)
    - Accordo operativo Maersk e Microsoft per iniziativa di deep learning (30 terabyte mensili generati dalla rete di trasporto, da processare per individuare trend e pattern predittivi)
    - Accordo operativo Maersk con Sea Machines Robotics per trial visione artificiale, riconoscimento oggetto e prevenzione incidenti
5. Blockchain (E-Bill of lading, cargo insurance, payment automation)
    - Ottimizzare e proteggere il processo di scambio di documentazione (es, B/L, documenti ferroviari)
    - Accordo operativo Maersk- IBM
    - Piattaforma CargoChain (information sharing platform per la global supply chain), esempio di convergenza tra Blockchain e IoT, tracking della spedizione e disponibilità in tempo reale dei documenti su blockchain
6. Cybersecurity (security assurance per customer data e automated operations)
    - La interconnessione di oggetti e sistemi richiede sicurezza agli access point, ampliando il concetto di sicurezza perimetrale.
    - Misure adottate dalla Commissione europea e direttive di sicurezza NIS (a terra e a bordo); precedentemente il basso grado di interconnessione e la frammentazione della catena logistica, hanno protetto dalle minacce cyber

Cybersecurity

Cybersecurity è una delle tecnologie abilitanti, ma non appare ai primi posti per adozione. Sicurezza durante le operazioni in rete su sistemi aperti.

- Introduzione **dispositivi IoT e vulnerabilità** (capacità elaborativa, usati come sensori o attuatori, non sempre sicuri by design) – (es. manipolazione di parametri critici di calibrazione e serie minacce a sistemi critici, o in caso di attuatori minacce alla sicurezza fisica)
- Salto tecnologico e culturale riguardo alla sicurezza, rispetto ai sistemi informativi tradizionali – **Linee guida Enisa** per la sicurezza IoT (2017)
- **Nuovo paradigma**, pratiche e controlli tradizionali non sono sufficienti. Dispositivi IoT con capacita' limitate di elaborazione, memoria e potenza. Sono oggetti di un ecosistema, dispositivi, comunicazione, interfacce, persone.
- Integrare e rendere interoperabili **differenti soluzioni di autenticazione** sui dispositivi, adozione lenta di **standard e normative** vs emergere continuo di **nuove tecnologie**
- Time-to-market e contenimento costi vs **sicurezza by design**; funzionalità e usabilità vs sicurezza
- Correzione dei sistemi IoT lungo il **ciclo di vita** (interfaccia utente non consente tradizionali forme di update e spesso sono parte di contesto diversificato con molti attori)

- Iniziative di sicurezza e **regolamentazione** in ambito IOT, **consapevolezza** necessità cybersecurity, linee guida per progettazione e sviluppo (**sicurezza by design**), gestione **ciclo di vita** e **responsabilità**
- Costo totale di un Data Breach nel 2018, in "Age of AI and IOT ", con collezione di grandissimi volume di dati,
  Costi diretti e indiretti (oltre per fermo macchina, furti brevetti, costi di notifica, perdita di fiducia verso clienti e partner…) e tempi di individuazione.
  - Piattaforme di End point detection and response
  - Vulnerability Management
  - Awareness e protezione delle persone

Fattori di successo e sfide

Risultati di Survey 2017 condotta da Futurenautics Maritime in associazione con Ericsson (711 individui, ship operators, suppliers, industry stakeholders del cluster marittimo di Europa, Asia, Middle East, Americhe)

L'aneddotica convinzione che il settore dello Shipping fosse conservativo nei confronti delle disruption, ed in particolare della trasformazione digitale, è risultata superata.

Top 5 Key Factors in Successful Digital Initiatives

1. **Integrate** technologies with existing information systems
2. Form **strategic alliances** with other companies that have key products, services and/or technologies
3. Provide customers with significant value by establishing an ongoing **digital connection** with them
4. Develop digital technologies to operate **reliably**
5. Have a clear and unified **strategy** that rethinks entire products and services and the business processes that support them.

Top 5 Biggest Challenges to Digital Transformation in Shipping & Maritime

1. Lack of data and understanding of how digital trends **affect** the industry and organization's competitiveness
2. Lack of internal **leadership or talent** (functional or technical) for digital projects
3. Lack of senior **management involvement** or desire to change current practices
4. Fears over **security** of digital operations, cyber security and resilience
5. Lack of **funding** for digital initiatives

Esperienze maturate nel cammino verso l'innovazione

1. Riconoscere il valore di una idea, dovunque si origini, e portarla a maturazione velocemente
2. Sviluppare apertura mentale e capacità di diffondere e far circolare conoscenze e idee
3. Formare, stimolare, incoraggiare, valorizzare potenziale e sviluppare la cultura dell'errore come valore formativo e di apprendimento
4. Investire per incrementare le competenze del capitale umano
5. Definire dei KPI e misurarli; cicli brevi e implementazioni veloci; Lanciare digital sprint e raccogliere successi
6. Adottare i principi Agile, per flessibilità e disponibilità al cambiamento (strutture, processi e competenze IT, collaborazione LOB, IT e partner piuttosto che negoziazione, accordi per iterazioni con valutazione; «individuals and interactions over process and tools»)
7. Orchestrare competenze interne con quelle diversificate di altri generatori di idee esterni alla organizzazione (startup, centri di eccellenza e di ricerca) sapendo selezionare quelli coerenti con le proprie strategie di business

Direttiva NIS

La Direttiva europea NIS
(Network and Information Security)

- La Direttiva è stata adottata dal Parlamento Europeo il 6 luglio 2016 ed è entrata in vigore l'8 agosto 2016.
- Gli Stati membri della UE hanno avuto tempo sino al 9 maggio 2018 per recepire la Direttiva in leggi nazionali, in vigore dal 10 maggio 2018, ed ulteriori sei mesi per identificare gli operatori di servizi essenziali (OES)
- Per quanto riguarda l'**Italia**, il 18 maggio 2018 il Consiglio dei Ministri ha approvato il Decreto Legislativo n.65/2018 per attuare la Direttiva NIS. Tale decreto è stato pubblicato il 9 giugno 2018 in Gazzetta Ufficiale ed è **in vigore dal 24 giugno 2018**.

Si rivolge a due gruppi:

- gli **operatori di servizi essenziali**, ossia organizzazioni pubbliche o private operanti nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari e della fornitura e distribuzione di acqua potabile,
- i **fornitori di servizi digitali**, cioè motori di ricerca, servizi Cloud e siti web di e-commerce.

Le **piccole imprese e micro imprese** (meno di 50 (o 10) dipendenti ed un fatturato e/o bilancio annuale inferiore a 10 (o 2) milioni di Euro) **non rientrano** nel campo di applicazione della Direttiva

I requisiti della Direttiva NIS

Sia gli operatori di servizi essenziali, sia i fornitori di servizi digitali, devono:

- Adottare **misure tecniche ed organizzative** appropriate per proteggere la rete ed i sistemi di informazione;
- Tenere conto dell'evoluzione delle minacce e considerare i **rischi potenziali** che i sistemi devono affrontare;
- Adottare misure adeguate alla **prevenzione ed al contenimento dell'impatto** degli incidenti di sicurezza, e garantire la continuità del servizio;
- Comunicare all'autorità di vigilanza di competenza qualsiasi **incidenti di sicurezza** che abbia un impatto significativo sulla continuità del servizio.

Conseguenze della non conformità alla Direttiva

La maggior parte degli Stati membri dell'UE ha recepito la Direttiva NIS nella legislazione nazionale ed ha definito le proprie norme relative alle sanzioni per la non conformità.

L'Italia ha stabilito sanzioni amministrative pecuniarie fino ad un massimo di €150.000, che possono triplicare in caso di reiterazione di reato.

Autorità competenti e CSIRT

Autorità competenti: monitorano l'applicazione della Direttiva e formano gruppi di risposta ad incidenti della sicurezza informatica (CSIRT)

L'Italia ha scelto di designare quali autorità competenti NIS i **5 Ministeri** (Sviluppo Economico, Infrastrutture e Trasporti, Economia, Salute e Ambiente), ciascuno responsabile per uno o più settori che rientrano nelle aree di loro competenza.

Inoltre, il Dipartimento delle Informazioni per la sicurezza (**DIS**) è stato designato come **punto unico di contatto** con l'Unione Europea e come coordinatore con le autorità competenti degli altri Stati Membri

Entro il **9 novembre 2018**, le Autorita' competenti provvederanno ad identificare gli OSE dei rispettivi settori (il MIT per i Trasporti)

CSIRT (Computer Security Incident Response Team): ente che si concentra principalmente sul governo e sulle infrastrutture critiche.

- Riceve le notifiche di incidente, e ne informa il DIS, come punto di contatto unico per la prevenzione e preparazione ad eventuali situazioni di crisi;
- Definisce le procedure per prevenire e gestire gli incidenti informatici;
- Fornisce un supporto al soggetto che ha notificato l'incidente per una gestione efficace dell'incidente;
- Costituisce una piattaforma per la cooperazione su problematiche di sicurezza informatica.

Per l'Italia, il CSIRT è istituito presso la Presidenza del Consiglio dei Ministri e sostituisce il CERT Nazionale (che opera presso il Ministero dello Sviluppo Economico) ed il CERT-PA (che opera presso l'Agenzia per l'Italia Digitale).