


1. 290-192A5_01 - Network e information systems



FIASS
FORMAZIONE
INTERMEDIARI
ASSICURATIVI

Corso e-learning IVASS

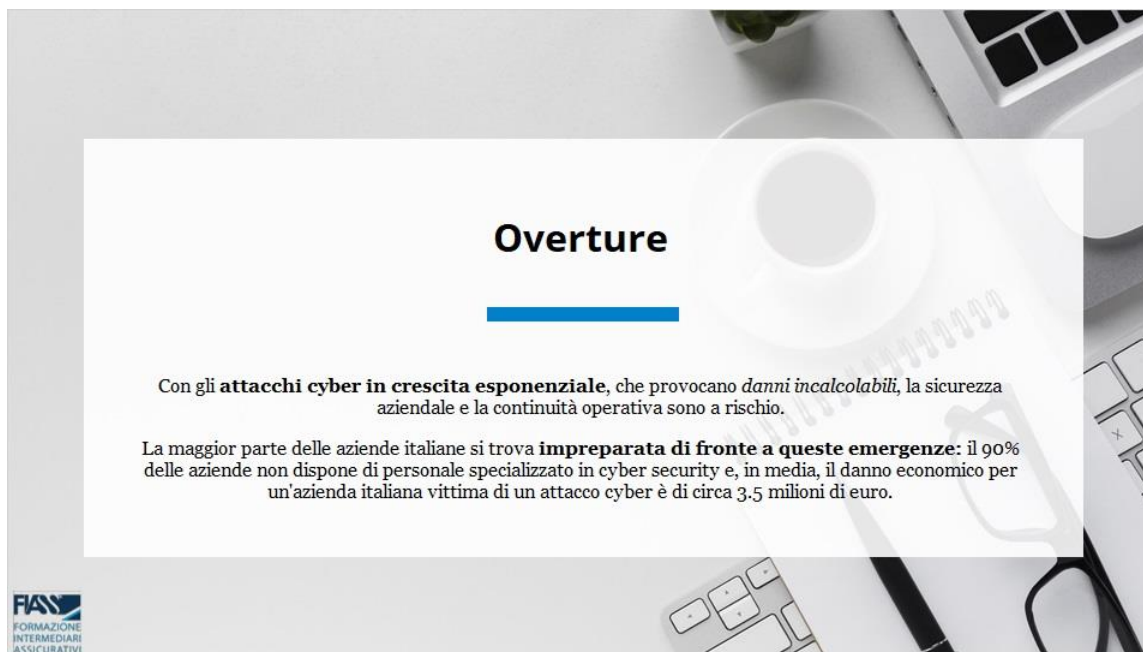
Network & Information Systems

La NIS 2 e le opportunità del mondo delle assicurazioni

FORMAZIONE E-LEARNING AI SENSI DEL REG. IVASS VIGENTE

Video Lezione: **1/3** | Docente: **Laura Lucchi** | Durata Modulo: **un'ora circa** | CM: **290-192A5_01**

1.2 Overture



Overture

Con gli **attacchi cyber in crescita esponenziale**, che provocano **danni incalcolabili**, la sicurezza aziendale e la continuità operativa sono a rischio.

La maggior parte delle aziende italiane si trova **impreparata di fronte a queste emergenze**: il 90% delle aziende non dispone di personale specializzato in cyber security e, in media, il danno economico per un'azienda italiana vittima di un attacco cyber è di circa 3,5 milioni di euro.

FIASS
FORMAZIONE
INTERMEDIARI
ASSICURATIVI

1.3 L'allarme cybersecurity: crescita esponenziale di attacchi e impatti globali



L'allarme cybersecurity: crescita esponenziale di attacchi e impatti globali

La crescente interconnessione e digitalizzazione della società ha reso istituzioni, imprese e cittadini sempre più esposti alle **minacce informatiche**. Gli attacchi informatici hanno raggiunto **picchi senza precedenti**, sia per frequenza che per gravità: negli ultimi 5 anni, il numero di attacchi registrati a livello globale è cresciuto del 60% secondo i dati del **rapporto Clusit 2023**.

Ad aggravarsi sono state anche le **conseguenze sociali ed economiche degli incidenti causati dagli attacchi cyber**: sempre secondo il Clusit, l'80% degli attacchi rilevati nel 2022 hanno avuto impatti gravi o molto gravi, a differenza di cinque anni fa quando ammontavano a una quota del 52% del totale.



1.4 Rischi cyber per le aziende: minacce, vulnerabilità e dipendenze critiche

Rischi cyber per le aziende: minacce, vulnerabilità e dipendenze critiche

Le aziende corrono diversi rischi legati alla cyber sicurezza, tra cui:


Attacchi informatici: Aumento degli **attacchi ransomware e phishing** che possono compromettere i **dati sensibili** e **interrompere le operazioni aziendali**.

Vulnerabilità nella catena di fornitura: La dipendenza da **fornitori esterni** può introdurre vulnerabilità significative. È cruciale valutare la **sicurezza dei fornitori** e **integrare requisiti di cyber sicurezza nei contratti**.

Lock-in tecnologico: Un'eccessiva **dipendenza da un singolo fornitore** può rendere difficile e costoso cambiare tecnologia o fornitore in caso di problemi.



1.5 Shodan.io: dati privati, telecamere di sicurezza, computer esposti



Shodan.io:
dati privati, telecamere di sicurezza, computer esposti

Shodan è un **motore di ricerca** specializzato che scandaglia Internet alla **ricerca di dispositivi connessi, dai server ai dispositivi IoT**. Per gli **assicuratori**, Shodan rappresenta sia un'opportunità che una minaccia potenziale.



1.6 Shodan: opportunità e minacce


Shodan: opportunità e minacce

Opportunità:

- **Valutazione del rischio:** Shodan può essere utilizzato per *identificare vulnerabilità* nelle reti dei clienti, permettendo una più accurata valutazione dei rischi cyber.
- **Due diligence:** può aiutare a verificare le misure di sicurezza dichiarate dai clienti.

Minacce:

- **Esposizione:** le stesse informazioni *possono essere sfruttate da attori malevoli* per individuare obiettivi vulnerabili.
- **Responsabilità:** se non adeguatamente gestite, queste informazioni potrebbero aumentare la responsabilità degli assicuratori.



1.7 17 ottobre 2024 - Direttiva NIS 2



17 ottobre 2024 - Direttiva NIS 2

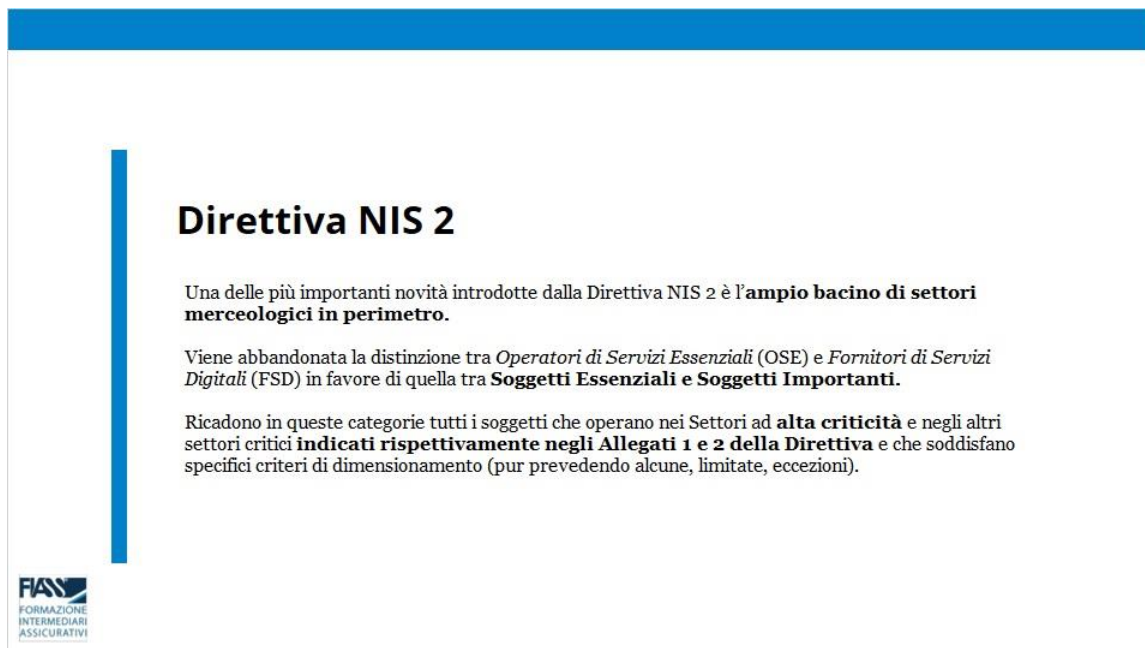
Pilastro della Cyber resilience europea

La **Direttiva NIS 2** rappresenta un'importante **legislazione dell'Unione Europea in materia di cyber sicurezza**, mirata a *migliorare la protezione contro gli incidenti di sicurezza informatica*.

Essa si applica a una **vasta gamma di organizzazioni**, sia *pubbliche che private*, che gestiscono **servizi essenziali per la società**, come energia, trasporti, sanità e servizi digitali.



1.8 Direttiva NIS 2




Direttiva NIS 2

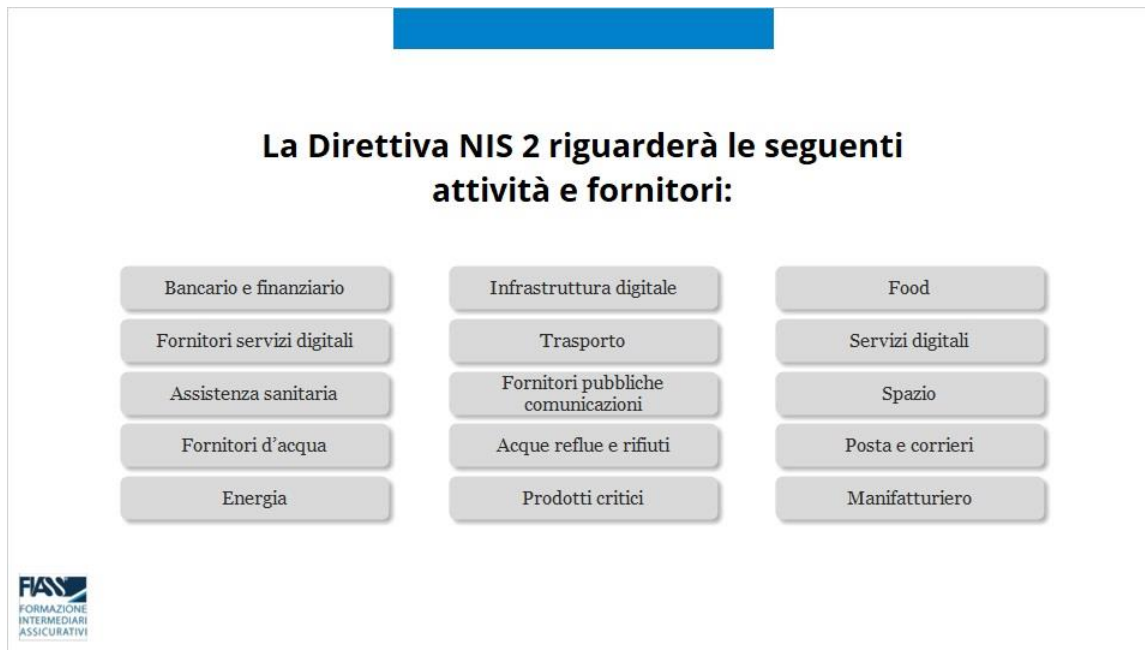
Una delle più importanti novità introdotte dalla Direttiva NIS 2 è l'**ampio bacino di settori merceologici in perimetro**.

Viene abbandonata la distinzione tra *Operatori di Servizi Essenziali (OSE)* e *Fornitori di Servizi Digitali (FSD)* in favore di quella tra **Soggetti Essenziali e Soggetti Importanti**.

Ricadono in queste categorie tutti i soggetti che operano nei Settori ad **alta criticità** e negli altri settori critici **indicati rispettivamente negli Allegati 1 e 2 della Direttiva** e che soddisfano specifici criteri di dimensionamento (pur prevedendo alcune, limitate, eccezioni).



1.9 La Direttiva NIS 2 riguarderà le seguenti attività e fornitori:



1.10 Cosa si intende rafforzare la Cyber sicurezza?



1.11 Applicazione italiana della direttiva



Applicazione italiana della direttiva

Nell'**applicazione italiana** della direttiva si è aggiunto il settore

↓

RICERCA

FIASS
FORMAZIONE
INTERMEDIARI
ASSICURATIVI

1.12 Governance nella NIS2



Governance nella NIS2

Definizione di Governance

La governance si riferisce ai **processi e alle strutture** attraverso cui le **organizzazioni** dirigono e controllano le loro attività.

Nella NIS2, la governance implica che gli **organi di gestione**, come il Consiglio di Amministrazione, siano direttamente coinvolti nella **supervisione delle misure di sicurezza informatica**.

FIASS
FORMAZIONE
INTERMEDIARI
ASSICURATIVI

1.13 I punti essenziali di NIS2



I punti essenziali di NIS2

1. **Analisi dei rischi e politiche di sicurezza dei sistemi informativi.**
2. Gestione degli incidenti (prevenzione, individuazione e risposta).
3. Continuità operativa e gestione delle crisi.
4. Sicurezza della catena di approvvigionamento.
5. Sicurezza nell'acquisizione, sviluppo e manutenzione della rete.
6. Politiche e procedure (test e audit) e formazione.
7. Uso della crittografia, della cifratura e di soluzioni MIA.
8. Sicurezza delle risorse umane, controllo dell'accesso e gestione attivi.

1.14 Analisi dei Rischi e Politiche di Sicurezza nei Sistemi Informativi



Analisi dei Rischi e Politiche di Sicurezza nei Sistemi Informativi

L'analisi dei rischi e le politiche di sicurezza **sono fondamentali per la protezione dei sistemi informativi aziendali**. Questi processi consentono di **identificare, valutare e mitigare le minacce che possono compromettere la riservatezza, l'integrità e la disponibilità delle informazioni**.

1.15 Definizione di rischio informatico



Definizione di rischio informatico

Il rischio informatico è definito come la **possibilità che eventi negativi**, come la **perdita di dati o violazioni della sicurezza**, si verifichino a **causa di vulnerabilità nei sistemi informatici o azioni malevole**. È essenziale per le aziende comprendere queste minacce per sviluppare **strategie efficaci di prevenzione e risposta**.



1.16 Fasi dell'analisi del rischio

Fasi dell'analisi del rischio

Identificazione degli Asset

Questa fase prevede l'**individuazione di tutti gli asset critici** dell'organizzazione, inclusi *hardware, software, dati e personale*.

È essenziale comprendere **quali risorse sono a rischio per poterle proteggere adeguatamente**.



1.17

Valutazione delle minacce e delle vulnerabilità

Una volta **identificati gli asset**, si procede a **valutare le minacce potenziali** (come attacchi informatici, errori umani o guasti tecnici) e **le vulnerabilità esistenti nei sistemi**.

Questo può includere l'analisi di configurazioni errate, bug software o pratiche di sicurezza inadeguate.

Analisi dell'impatto

Si effettua una **Business Impact Analysis (BIA)** per determinare l'**impatto potenziale di un attacco informatico sull'organizzazione**.

Questo include la valutazione delle perdite economiche, reputazionali e operative.



1.18

Valutazione del Rischio

Utilizzando *matrici di valutazione*, si assegna un **punteggio a ciascuna minaccia** in base alla **sua probabilità e all'impatto previsto**. Questa fase aiuta a prioritizzare i rischi da affrontare.

Modalità di Analisi del Rischio

- **Approccio Qualitativo:** si basa su *giudizi esperti* per valutare i rischi senza l'uso di dati numerici precisi. È utile in contesti dove le informazioni quantitative sono scarse.
- **Approccio Quantitativo:** utilizza *dati numerici per calcolare il rischio* in termini monetari o probabilistici, permettendo una valutazione più precisa delle perdite potenziali.
- **Valutazione Semi-Quantitativa:** *combina elementi qualitativi e quantitativi*, utilizzando scale o intervalli per esprimere la gravità dei rischi in modo più strutturato



1.19

Pianificazione delle Contromisure

Sulla base della valutazione dei rischi, si sviluppano **strategie di mitigazione per ridurre o eliminare i rischi identificati**. Queste possono includere *l'implementazione di misure di sicurezza, politiche interne e formazione del personale*.

Monitoraggio e Revisione

L'analisi del rischio **non è un processo statico**; richiede **monitoraggio continuo e revisione periodica** per *adattarsi a nuove minacce e cambiamenti nell'ambiente operativo*. Questo assicura che le misure di sicurezza rimangano efficaci nel tempo.



1.20 Fine



Fine

Prima parte



Per domande al docente usa il tasto **Help Desk** o scrivi a info@fiass.it



Se hai problemi di visualizzazione o salvataggio consulta il **"Modulo Guida ai Corsi FIASS"**

