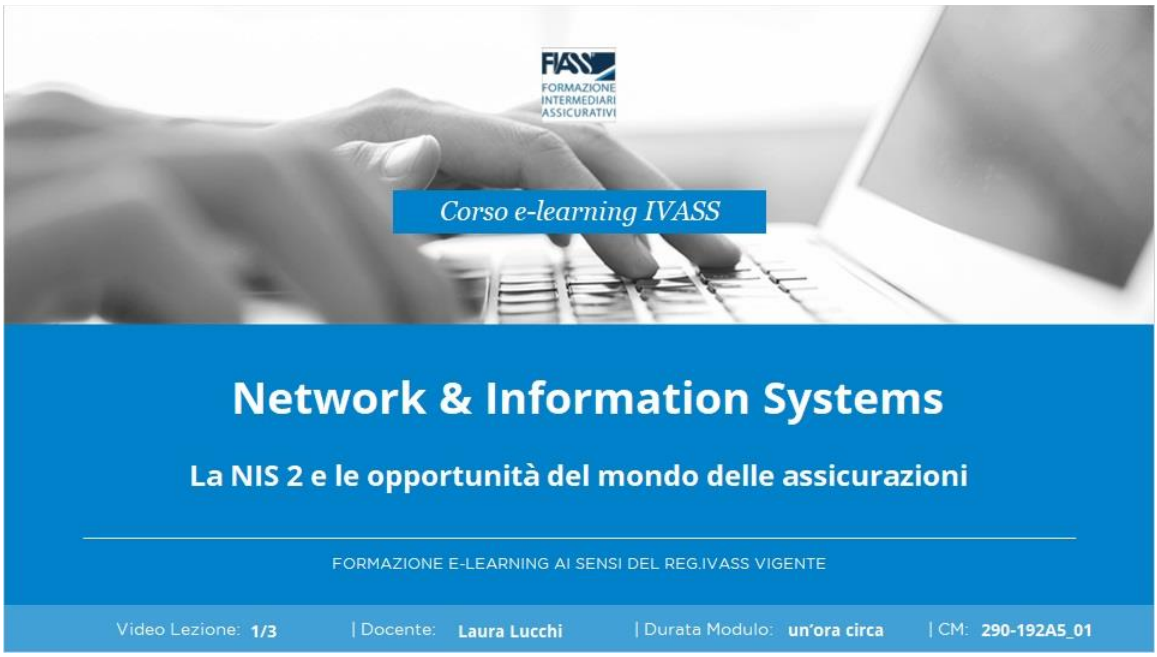
1. 290-192A5_01 - Network e information systems



1.2 Overture

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.

FIASS FORMAZIONE INTERMEDIARI ASSICURATIVI

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.

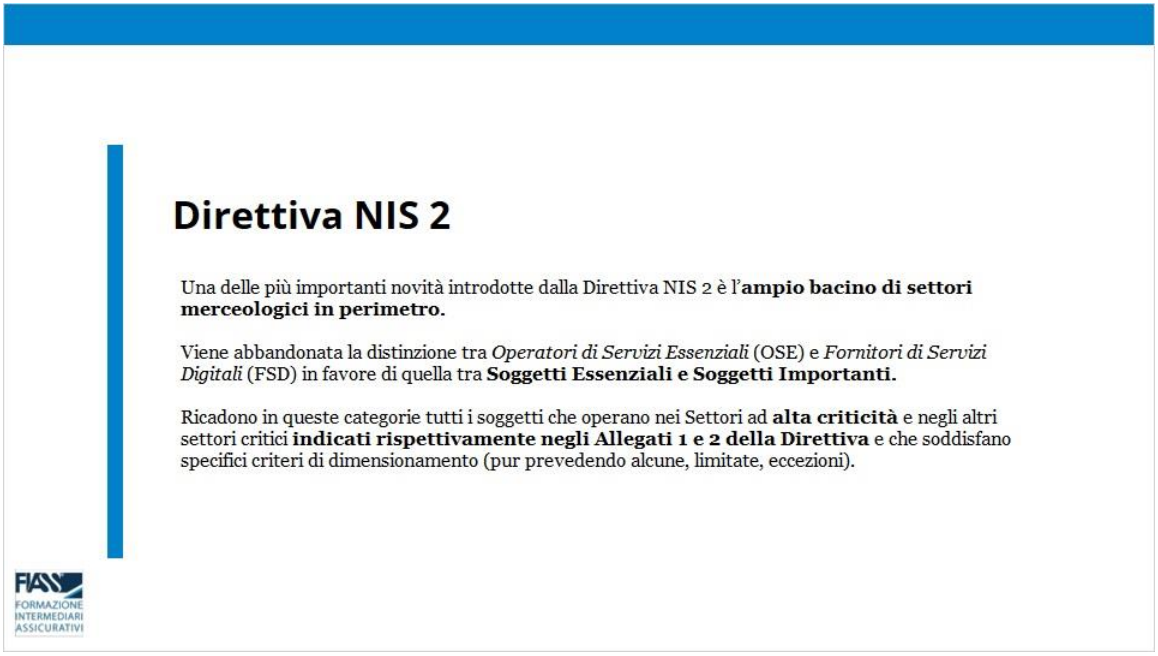
FIASS FORMAZIONE INTERMEDIARI ASSICURATIVI

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

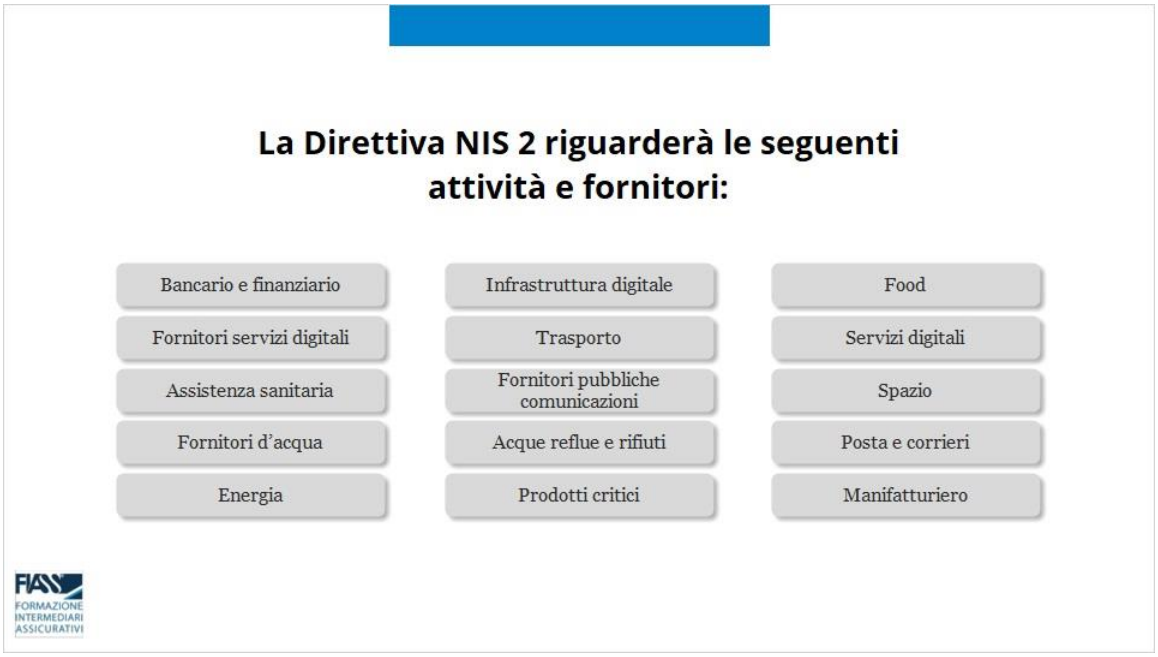
1.6 Shodan: opportunità e minacce

1.7 17 ottobre 2024 - Direttiva NIS 2

1.8 Direttiva NIS 2



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

1.12 Governance nella NIS2

1.13 I punti essenziali di NIS2

1.14 Analisi dei Rischi e Politiche di Sicurezza nei Sistemi Informativi

1.15 Definizione di rischio informatico

1.16 Fasi dell'analisi del rischio

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.

FIASS FORMAZIONE INTERMEDIARI ASSICURATIVI

1.18

Valutazione del Rischio

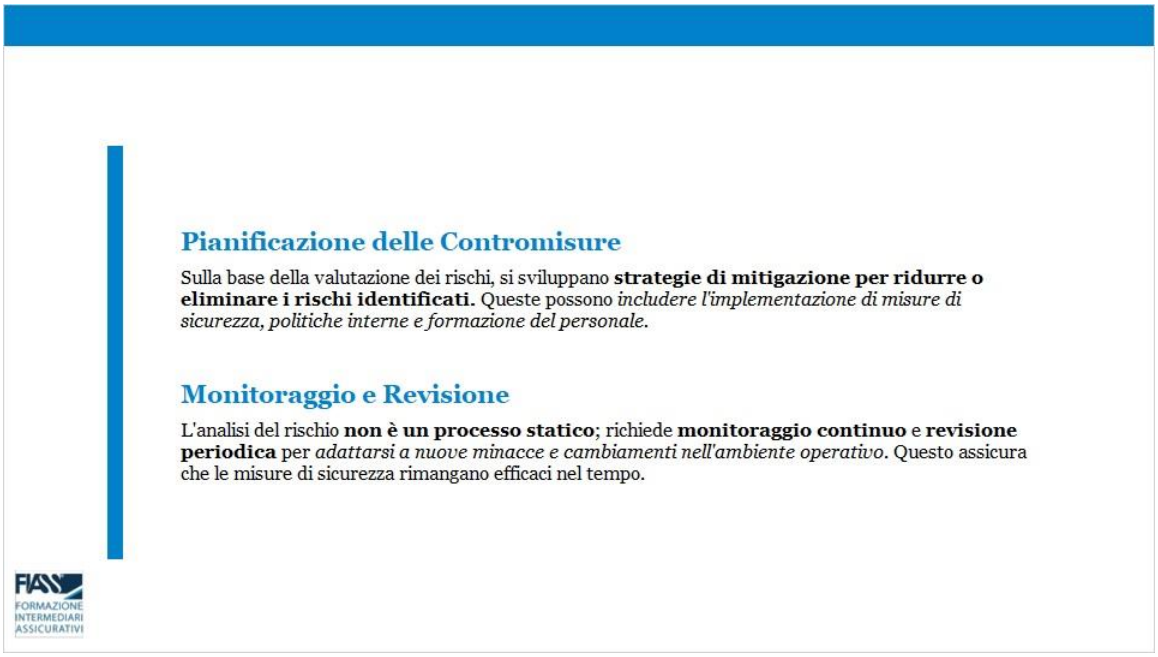
Utilizzando *matrici di valutazione*, si assegna un **punteggio a ciascuna minaccia** in base alla **sua probabilità e all'impatto previsto.** Questa fase aiuta a prioritizzare i rischi da affrontare.

Modalità di Analisi del Rischio

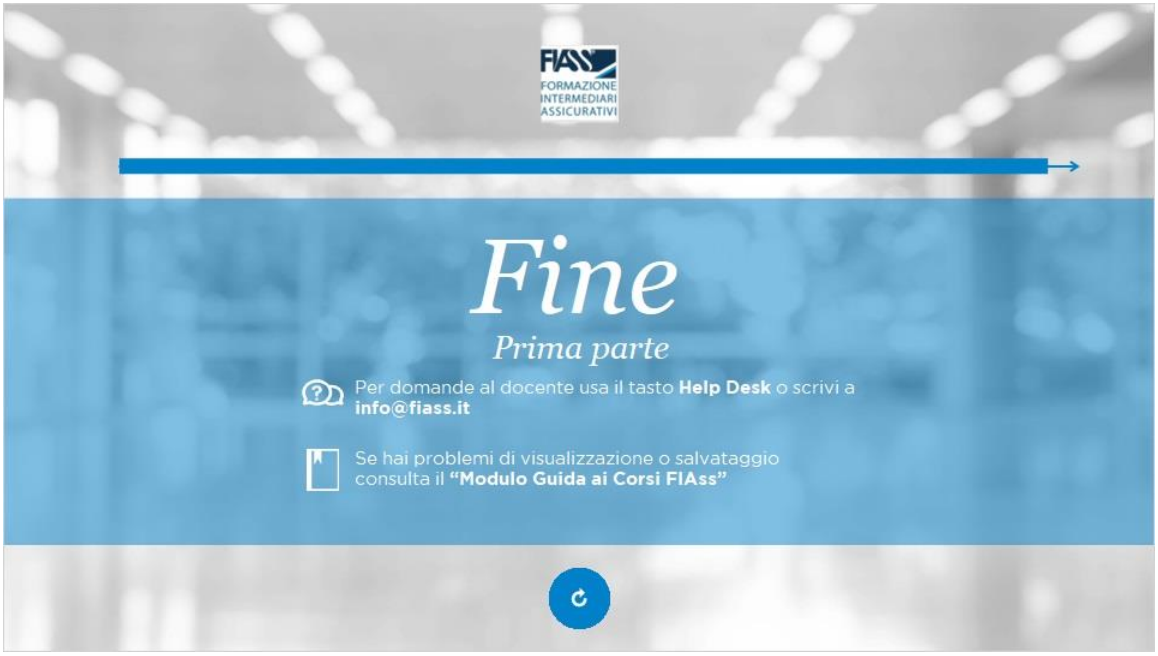
- **Approccio Qualitativo:** si basa su *giudizi esperti* per valutare i rischi senza l'uso di dati numerici precisi. È utile in contesti dove le informazioni quantitative sono scarse.
- **Approccio Quantitativo:** utilizza *dati numerici per calcolare il rischio* in termini monetari o probabilistici, 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

FIASS FORMAZIONE INTERMEDIARI ASSICURATIVI

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.
FIASS
FORMAZIONE INTERMEDIARI ASSICURATIVI

1.20 Fine


FIASS
FORMAZIONE INTERMEDIARI ASSICURATIVI
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"