


## 1. 290-192A5\_03 - Network e information systems



**FIASS**  
FORMAZIONE  
INTERMEDIARI  
ASSICURATIVI

*Corso e-learning IVASS*

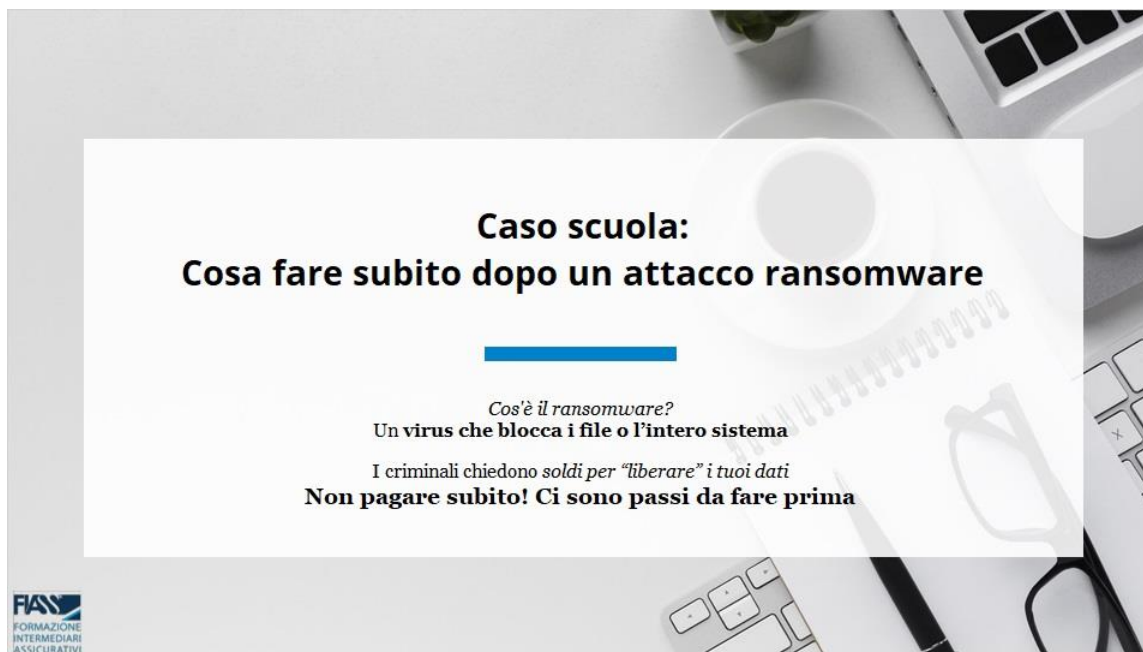
### Network & Information Systems

**La NIS 2 e le opportunità del mondo delle assicurazioni**

FORMAZIONE E-LEARNING AI SENSI DEL REG. IVASS VIGENTE

Video Lezione: **3/3** | Docente: **Laura Lucchi** | Durata Modulo: **un'ora circa** | CM: **290-192A5\_03**

### 1.2 Caso scuola: Cosa fare subito dopo un attacco ransomware



### Caso scuola: Cosa fare subito dopo un attacco ransomware

*Cos'è il ransomware?*  
**Un virus che blocca i file o l'intero sistema**

*I criminali chiedono soldi per "liberare" i tuoi dati*  
**Non pagare subito! Ci sono passi da fare prima**

**FIASS**  
FORMAZIONE  
INTERMEDIARI  
ASSICURATIVI

### 1.3 Passo 1 Spegner i sistemi colpiti



#### Passo 1 Spegner i sistemi colpiti

- ✓ **Isolare i computer infettati** scollegandoli dalla rete.
- ✓ Evita che il **ransomware si diffonda** ad altri dispositivi.
- ✓ **Non spegnere completamente i server**: mettili in modalità sicura.

### 1.4 Passo 2 Informare il team IT e la sicurezza



#### Passo 2 Informare il team IT e la sicurezza

- ✓ **Notifica subito il team IT o il responsabile della sicurezza.**
- ✓ Attivare il **protocollo di risposta agli incidenti.**
- ✓ Coinvolgi anche un **esperto esterno se necessario.**

### ***1.5 Passo 3 Non pagare subito il riscatto***



#### **Passo 3 Non pagare subito il riscatto**

- ✓ Pagare **non garantisce** il recupero dei dati!
- ✓ Potrebbe **incoraggiare** altri attacchi.
- ✓ Esplora altre soluzioni: **backup**, strumenti di **decriptazione**.



### ***1.6 Passo 4 Controllare i backup***



#### **Passo 4 Controllare i backup**

- ✓ Verifica se **esistono backup recenti e sicuri**.
- ✓ I **backup non devono essere stati compromessi** dall'attacco.
- ✓ Se il **backup è sicuro**, puoi **ripristinare i dati senza pagare**.



## 1.7 Passo 5 Contatta le autorità competenti



### Passo 5 Contatta le autorità competenti

- ✓ Segnala l'attacco alla **Polizia Postale** o altre autorità.
- ✓ Molti paesi hanno **squadre specializzate** contro il cybercrimine.
- ✓ Potrebbero esserci risorse per aiutarti a **recuperare i dati**.

## 1.8 Passo 6 Comunicazione



### Passo 6 Comunicazione

- ✓ **Informa i tuoi dipendenti:** cosa è successo e cosa fare.
- ✓ **Notifica anche i clienti o partner,** se necessario.
- ✓ **La trasparenza aiuta a ricostruire la fiducia.**

## 1.9 Prevenire attacchi futuri




### Prevenire attacchi futuri

**Aggiorna i sistemi e fai backup regolari.**  
**Forma i dipendenti** su come evitare e-mail sospette.  
**Installa software antivirus** e firewall più robusti.

**FIASS**  
FORMAZIONE  
INTERMEDIARI  
ASSICURATIVI

## 1.10 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.

**FIASS**  
FORMAZIONE  
INTERMEDIARI  
ASSICURATIVI



## 1.11 Gestione della Supply Chain



### Gestione della Supply Chain

I fornitori terzi possono rappresentare una **grande minaccia per la resilienza aziendale**.

Il controllo della **supply chain** prevede la valutazione dei fornitori, la verifica dei loro processi di sicurezza e la stipula di accordi di livello di servizio (SLA)\* che definiscono le responsabilità in materia di sicurezza.

**Un controllo rigoroso dei fornitori aiuta a mitigare il rischio di attacchi che sfruttano le loro vulnerabilità.**



\*Uno SLA (Service Level Agreement) è un **contratto tra un fornitore di servizi e un cliente che definisce il servizio da fornire e il livello di prestazioni previsto**. Uno SLA descrive anche come le prestazioni verranno misurate e approvate e cosa succede se i livelli di prestazioni non vengono soddisfatti.

## 1.12 Stabilire relazioni con i fornitori

### Stabilire relazioni con i fornitori

**Selezione dei Fornitori:** scegliere **fornitori che dimostrano un adeguato livello di sicurezza informatica**. Ciò include la **verifica delle certificazioni di sicurezza e delle politiche di gestione dei rischi**.

**Consapevolezza dei Rischi:** comunicare ai fornitori i **rischi specifici legati alla sicurezza della supply chain** e richiedere che adottino **misure adeguate per mitigarli**.

**Sensibilizzazione dei Fornitori:** collaborare con i fornitori per **sensibilizzarli** riguardo all'**importanza della sicurezza informatica nella supply chain**.



## 1.13 Implementazione di misure tecniche e organizzative

### Implementazione di misure tecniche e organizzative

**Misure di Sicurezza:** adottare **misure tecniche** come l'autenticazione multifattoriale, la crittografia dei dati e sistemi di monitoraggio per **proteggere le informazioni scambiate con i fornitori**.

**Procedure di Controllo:** stabilire **procedure operative standard** per la gestione della sicurezza nella supply chain, inclusa la **revisione regolare delle pratiche di sicurezza dei fornitori**.



## 1.14 Monitoraggio continuo della catena di fornitura

### Monitoraggio continuo della catena di fornitura

**Audit e verifiche:** condurre **audit periodici sui fornitori** per garantire che rispettino gli **standard di sicurezza richiesti**. Questo può includere controlli sulla **conformità alle politiche di cybersecurity**.

**Aggiornamenti Regolari:** **monitorare continuamente le minacce emergenti** e **aggiornare le misure di sicurezza in base ai risultati delle valutazioni dei rischi**.



## 1.15 Pianificazione della continuità operativa

### Pianificazione della continuità operativa

**Piani di Continuità (BIA):** sviluppare **piani di continuità operativa** che includano **strategie specifiche** per gestire interruzioni nella supply chain dovute a incidenti informatici.

**Collaborazione con i Fornitori:** assicurarsi che **anche i fornitori abbiano piani di continuità operativa in atto** e che siano allineati con quelli dell'organizzazione.



## 1.16 Reporting e Comunicazione

### Reporting e Comunicazione

**Procedure di Segnalazione:** stabilire **chiare procedure per la segnalazione degli incidenti** legati alla supply chain, sia internamente che verso le autorità competenti, in conformità **con le scadenze stabilite dalla NIS2**.

**Comunicazione Trasparente:** mantenere una **comunicazione aperta con tutti gli stakeholder** riguardo ai **rischi identificati** e alle **misure adottate per mitigarli**.

Adottando queste contromisure, un'organizzazione può **migliorare significativamente la sicurezza della propria supply chain**, riducendo il rischio di incidenti informatici e garantendo la conformità ai requisiti della direttiva NIS2.





## 1.17 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.  
Sicurezza delle risorse umane, controllo dell'accesso e gestione attivi.

## 1.18 Deadline nazionali & attività annuali

### Deadline nazionali & attività annuali

#### **DAL 01/01 AL 28/02**

I soggetti previsti si devono registrare o aggiornare la propria registrazione sulla piattaforma digitale dell'Autorità nazionale competente ACN.

#### **ENTRO 31/03 DI OGNI ANNO**

L'Autorità redige l'elenco dei soggetti essenziali e importanti sulla base delle registrazioni ricevute attraverso la piattaforma.

#### **TRA IL 1° E 15/04 DI OGNI ANNO**

Attraverso la piattaforma, l'ACN comunica ai soggetti registrati l'inserimento, la permanenza o l'espulsione nell'elenco dei soggetti importanti o essenziali.

#### **DAL 15/04 AL 31/05 DI OGNI ANNO**

Le aziende notificate devono aggiornare le informazioni su: IP pubblici, nomi di dominio, stati membri di distribuzione e responsabili della sicurezza.

## 1.19 I rischi e le sanzioni

### I rischi e le sanzioni

La **Direttiva NIS2** si applica a un *ampio spettro di aziende e organizzazioni*, suddivise in due categorie: **essenziali e importanti**.

Le *aziende essenziali* offrono **servizi cruciali per la società e l'economia**, mentre le *aziende importanti*, pur non fornendo servizi essenziali, **sono rilevanti per il contesto economico e sociale**.

Per le *aziende essenziali*, le **sanzioni** in caso di non conformità possono arrivare **fino a 10 milioni di euro o al 2% del fatturato globale annuo precedente**.

Per le *aziende importanti* le **sanzioni** possono raggiungere i **7 milioni di euro o un massimo di almeno l'1,4% del fatturato annuo globale**.



## 1.20 Il trasferimento del rischio

### Il trasferimento del rischio

Per trasferire il rischio agli assicuratori e garantire la conformità alla direttiva NIS2, è fondamentale seguire una **serie di passaggi strategici e operativi**. Ecco come procedere:

#### 1. Valutazione dei Rischi

**Identificazione dei Rischi:** iniziare con una **valutazione dettagliata dei rischi informatici** e operativi che l'organizzazione affronta. Questo include la valutazione delle vulnerabilità della rete, dei sistemi informativi e delle pratiche di gestione della supply chain.

#### 2. Analisi dell'Impatto:

valutare l'**impatto potenziale** di ciascun rischio identificato, considerando sia le **conseguenze finanziarie** che quelle **reputazionali**.

#### 3. Valutazione dei risk appetite

e motivazioni certificate.



## 1.21 Sviluppo di una strategia di risk management

### Sviluppo di una strategia di risk management

**Definizione della Politica di Gestione del Rischio:** stabilire una **politica chiara** che delinei come l'organizzazione intende **gestire i rischi identificati**, inclusi quelli legati alla cybersecurity.

**Integrazione delle Polizze Cyber:** considerare l'**integrazione di polizze assicurative specifiche per la cybersecurity** nel portafoglio assicurativo esistente. Queste polizze possono coprire **danni diretti, perdite economiche e responsabilità legale derivanti da incidenti informatici**.



## 1.22 Selezione di un partner assicurativo Agente o Broker

### Selezione di un partner assicurativo Agente o Broker

**Collaborazione con Esperti:** lavorare con un **intermediario assicurativo, consulente esperto in cybersecurity** per identificare le **migliori opzioni di polizza disponibili**, che aiuti a comprendere le **coperture necessarie** e a **negoziare le condizioni più favorevoli**.

**Analisi delle Offerte:** richiedere **preventivi da diverse compagnie assicurative** per **confrontare le coperture offerte, i massimali e i premi**.



## 1.23 Implementazione delle polizze assicurative

### Implementazione delle polizze assicurative

**Acquisto delle Polizze:** una volta **selezionate le polizze adeguate**, procedere all'**acquisto e alla formalizzazione dei contratti assicurativi**.

**Condizioni di Assicurabilità:** le compagnie richiedono alle aziende **requisiti minimi di sicurezza preventiva** prima di concedere coperture. **Solo le aziende con misure adeguate di sicurezza informatica possono ottenere polizze**, limitando l'accesso a quelle con posture di sicurezza insufficienti.

**Documentazione Necessaria:** assicurarsi che tutta la **documentazione necessaria sia in ordine** e che le **polizze siano chiaramente comprese da tutti i membri dell'organizzazione coinvolti nella gestione del rischio**.



## 1.24 Definizione delle esigenze di copertura

### Definizione delle esigenze di copertura

**Tipologia di Attività:** considerare il **settore in cui opera l'organizzazione** e le specifiche esigenze di copertura. Ad esempio, le aziende del settore sanitario potrebbero necessitare di coperture specifiche per la protezione dei dati sensibili.

**Tipi di Copertura Necessari:**

**Identificare quali tipi di copertura sono essenziali, come:**

- responsabilità civile per violazioni dei dati;
- costi per la gestione degli incidenti;
- danni da interruzione dell'attività;
- spese legali e di consulenza.



## 1.25 Definizione delle esigenze di copertura

### Definizione delle esigenze di copertura

Scegliere la **giusta polizza cyber** richiede un **approccio strategico** che integri la valutazione dei rischi, la definizione delle esigenze specifiche e un'attenta analisi delle opzioni disponibili.

Collaborare con **esperti del settore** e rimanere *proattivi nella gestione dei rischi* è **cruciale** per **garantire una protezione adeguata** contro le minacce informatiche in continua evoluzione.

Ciò comporta:

- ✓ **Revisione Periodica:** una volta scelta la polizza, **effettuare revisioni periodiche** per assicurarti che continui a soddisfare le esigenze dell'organizzazione man mano che evolvono i rischi informatici.
- ✓ **Aggiornamenti Normativi:** rimanere **aggiornati sulle normative** e le best practices nel settore della cybersicurezza, poiché potrebbero influenzare le esigenze assicurati.



## 1.26 Analisi delle condizioni delle polizze

### Analisi delle condizioni delle polizze

**Limiti e Franchigie:** esaminare **attentamente i limiti di copertura e le franchigie associate** a ciascuna polizza. Assicurarsi che siano adeguati rispetto ai rischi identificati.

**Esclusioni:** fare **attenzione alle esclusioni specifiche della polizza**, poiché potrebbero limitare la copertura in situazioni critiche.

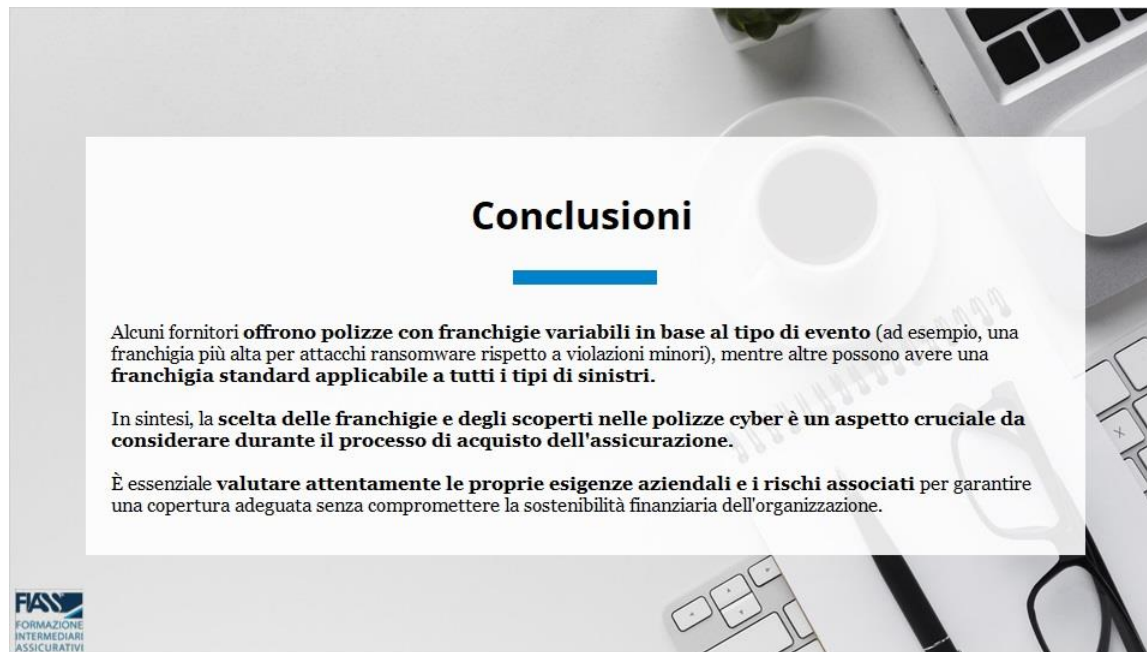
**Personalizzazione della Polizza:** le **franchigie e gli scoperti possono variare** notevolmente tra le diverse compagnie assicurative e le diverse polizze. È importante personalizzare questi elementi in base alle esigenze specifiche dell'organizzazione e alla sua tolleranza al rischio.

**Impatto sui Premi:** **Franchigie più elevate tendono a ridurre i premi assicurativi, ma aumentano il rischio finanziario** per l'assicurato in caso di sinistro. È fondamentale trovare un equilibrio tra costi e copertura adeguata.





## 1.27 Conclusioni



### Conclusioni

Alcuni fornitori **offrono polizze con franchigie variabili in base al tipo di evento** (ad esempio, una franchigia più alta per attacchi ransomware rispetto a violazioni minori), mentre altre possono avere una **franchigia standard applicabile a tutti i tipi di sinistri**.

In sintesi, la **scelta delle franchigie e degli scoperti nelle polizze cyber è un aspetto cruciale da considerare durante il processo di acquisto dell'assicurazione**.

È essenziale **valutare attentamente le proprie esigenze aziendali e i rischi associati** per garantire una copertura adeguata senza compromettere la sostenibilità finanziaria dell'organizzazione.

**FIASS**  
FORMAZIONE  
INTERMEDIARI  
ASSICURATIVI

## 1.28 Fine



**FIASS**  
FORMAZIONE  
INTERMEDIARI  
ASSICURATIVI

# Fine

*Terza e ultima 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"**

