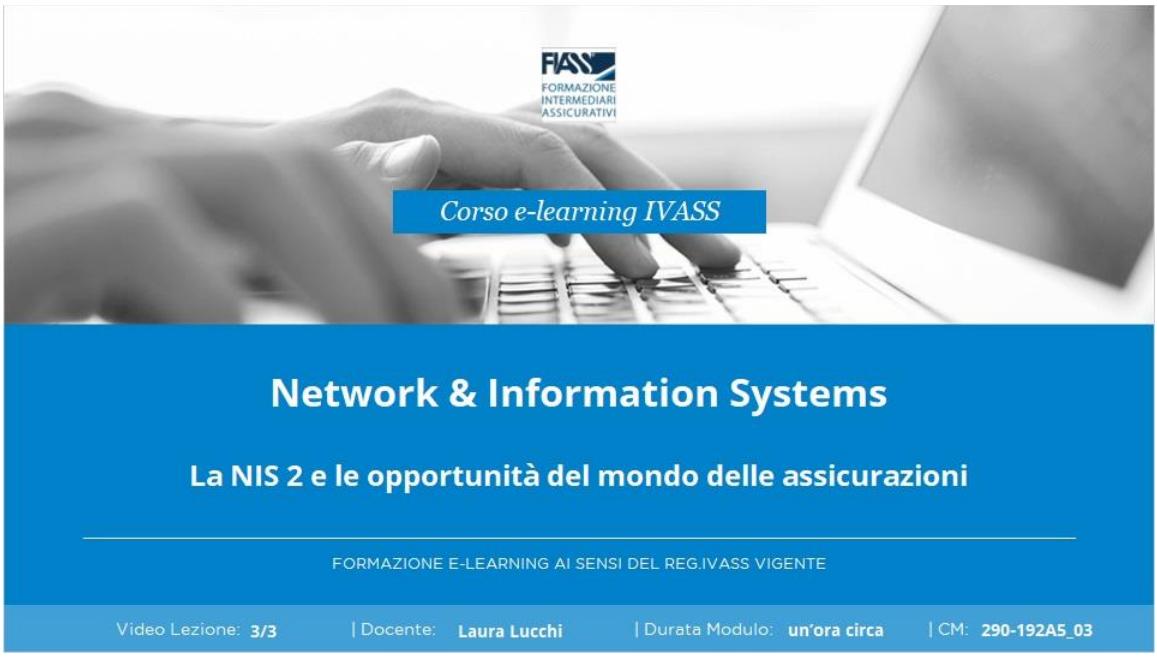
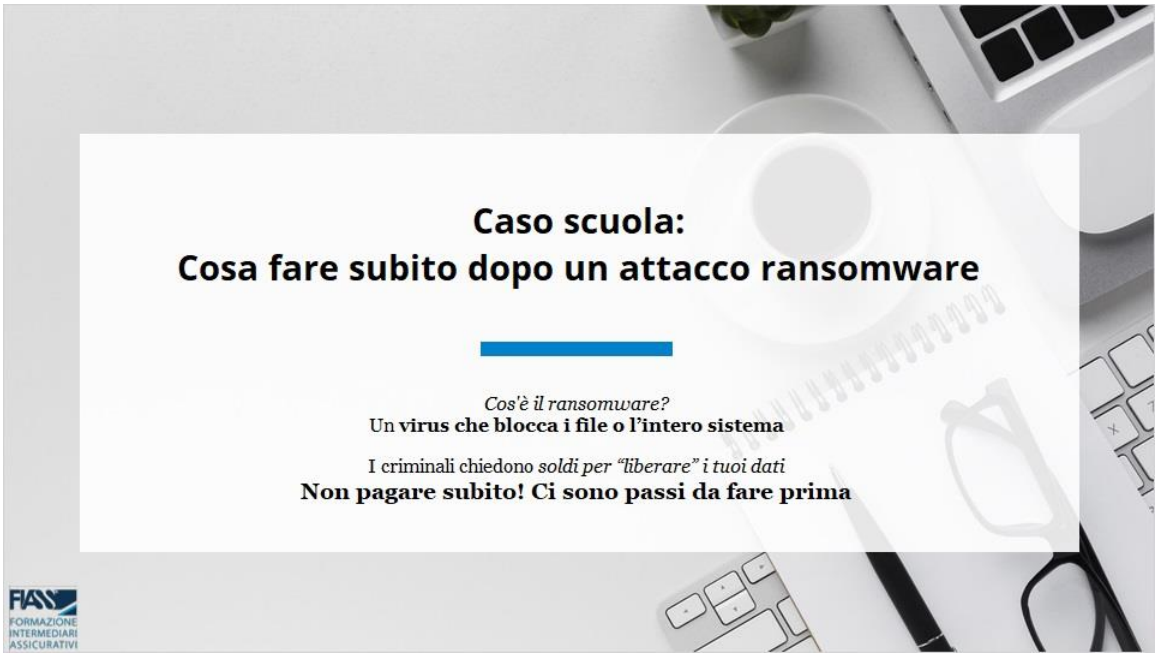
## 1. 290-192A5_03 - Network e information systems




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

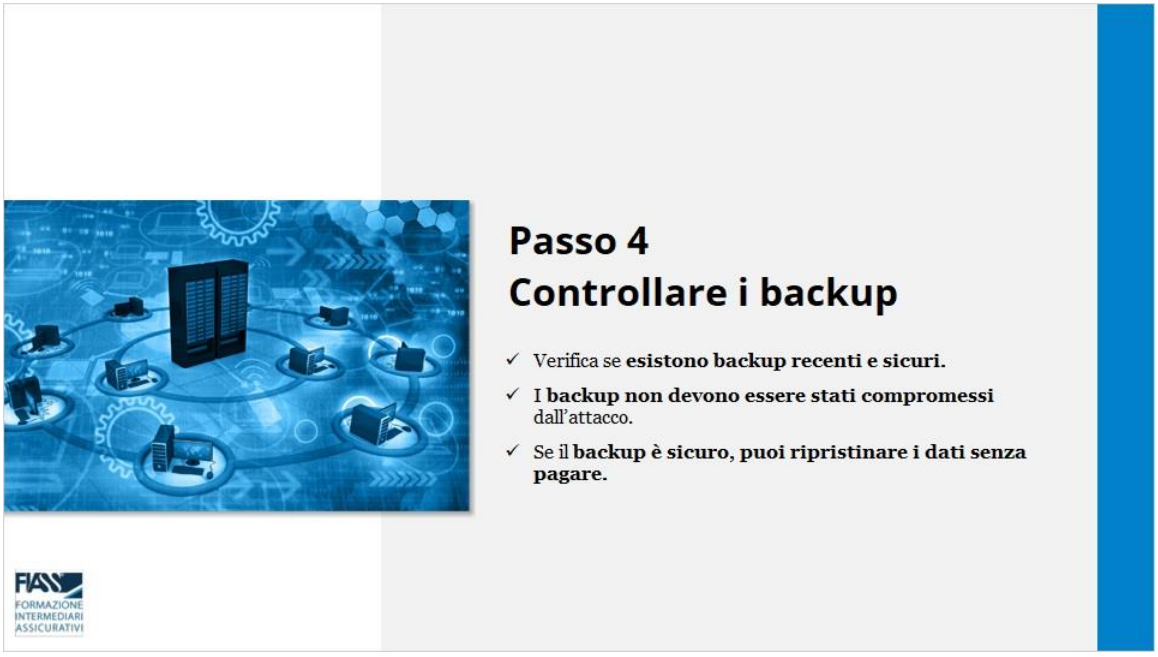


### *1.3 Passo 1 Spegnere i sistemi colpiti*

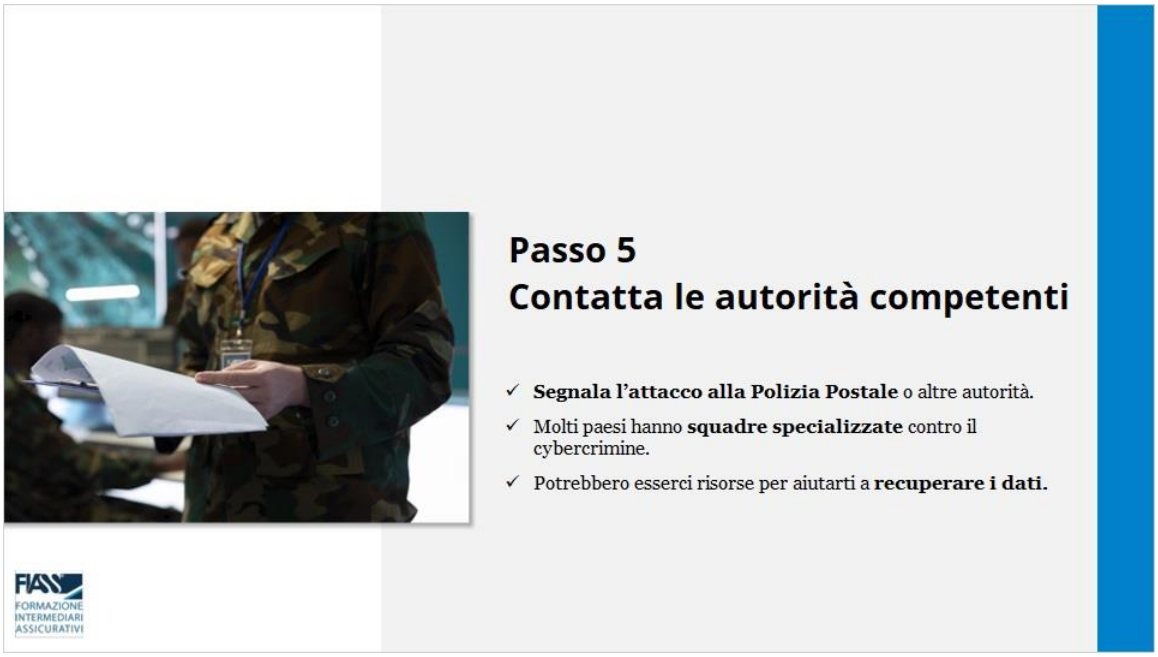

### *1.4 Passo 2 Informare il team IT e la sicurezza*

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


## *1.6 Passo 4 Controllare i backup*



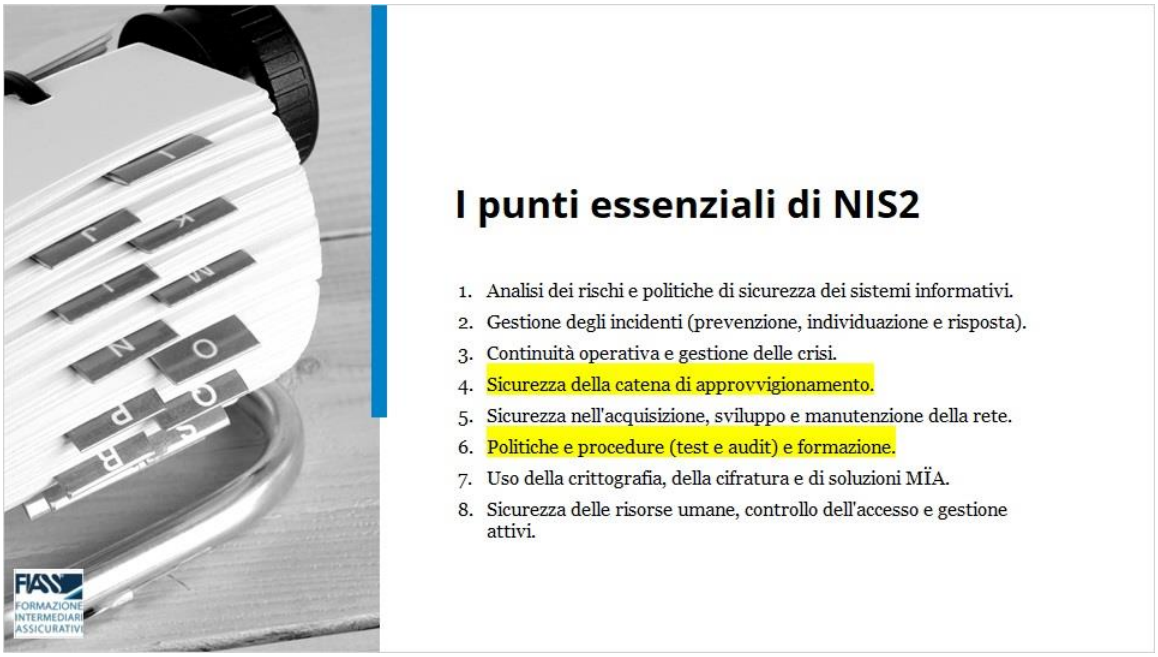
## *1.7 Passo 5 Contatta le autorità competenti*




## *1.8 Passo 6 Comunicazione*

## *1.9 Prevenire attacchi futuri*

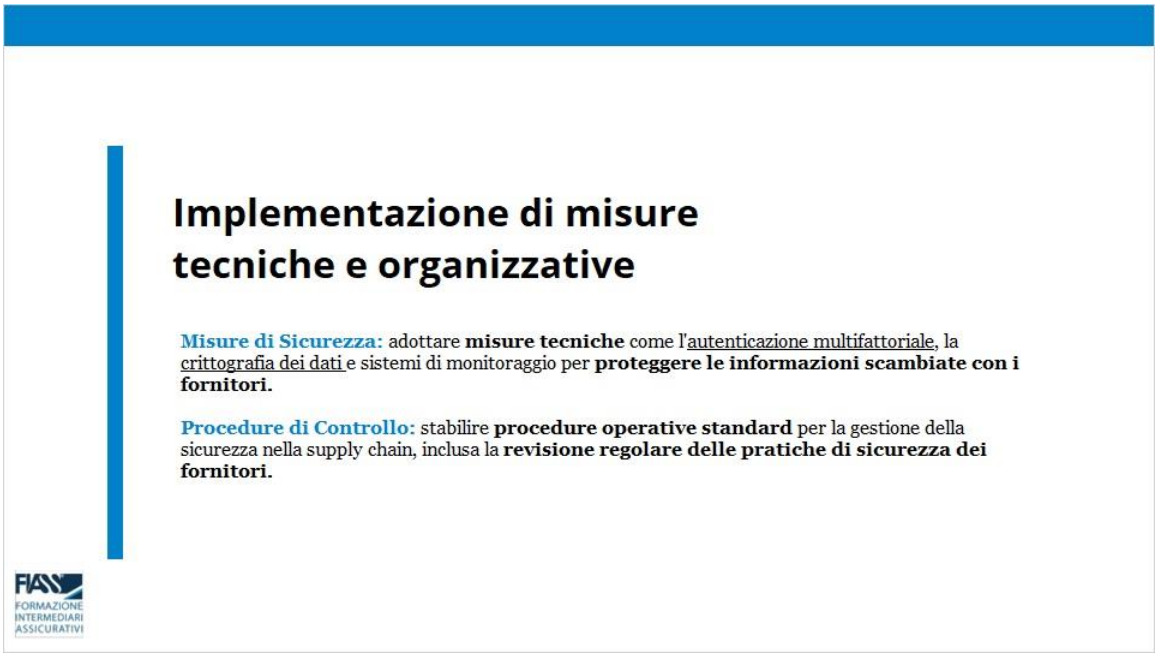

## *1.10 I punti essenziali di NIS2*



## *1.11 Gestione della Supply Chain*


## *1.12 Stabilire relazioni con i fornitori*

## *1.13 Implementazione di misure tecniche e organizzative*

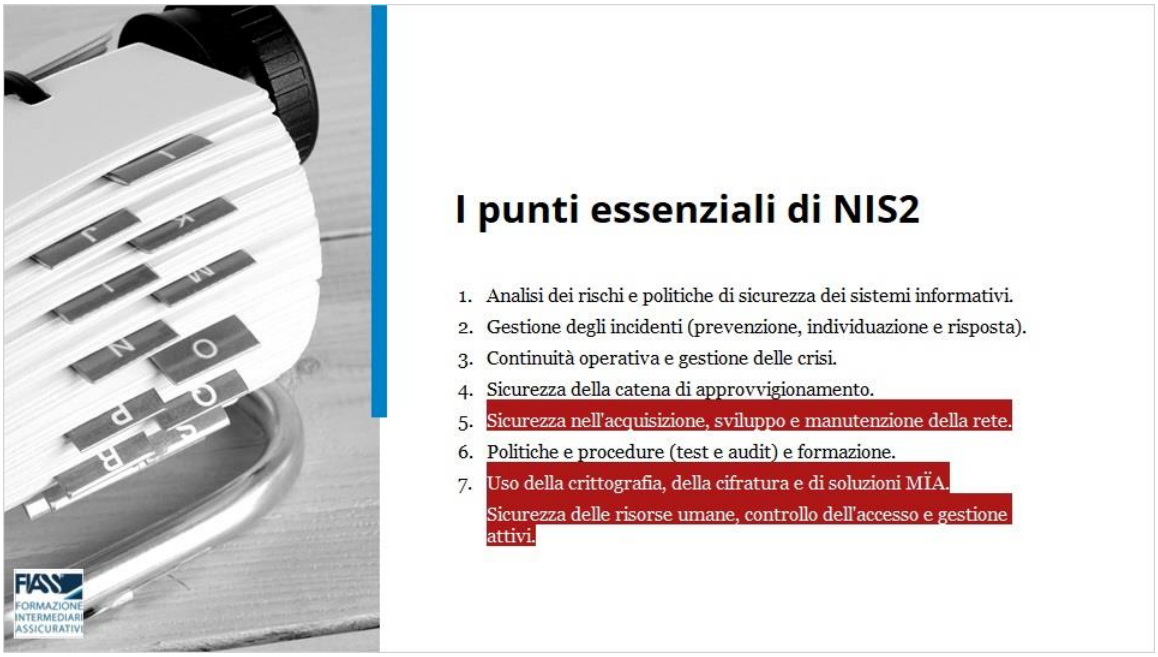



## *1.14 Monitoraggio continuo della catena di fornitura*

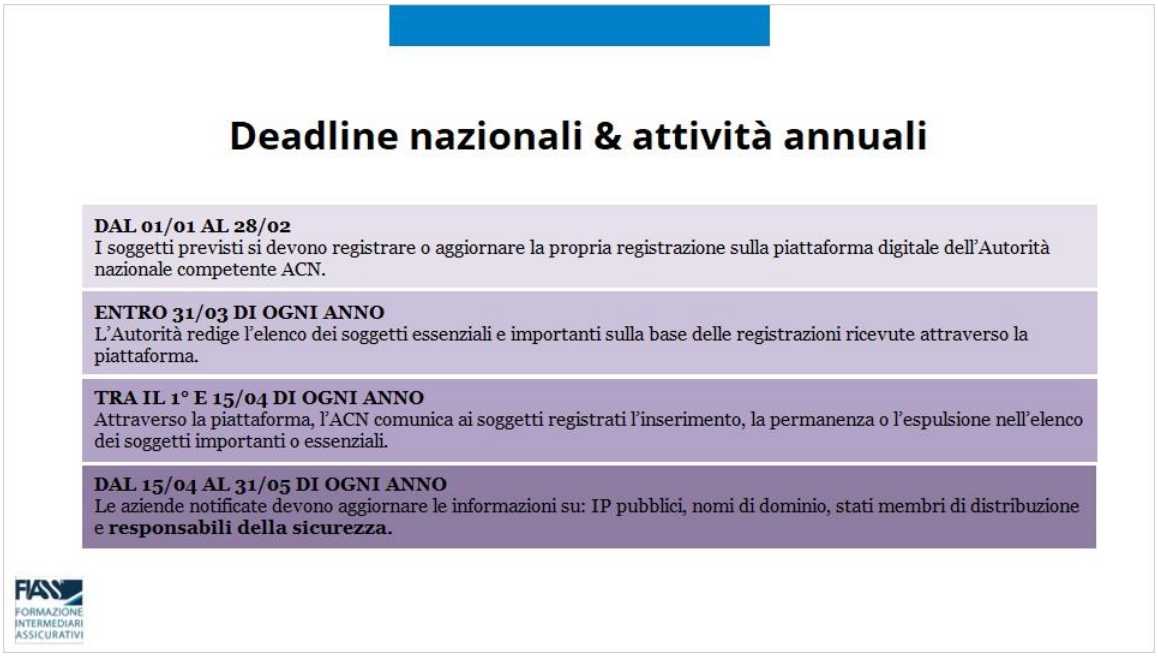
## *1.15 Pianificazione della continuità operativa*


## *1.16 Reporting e Comunicazione*

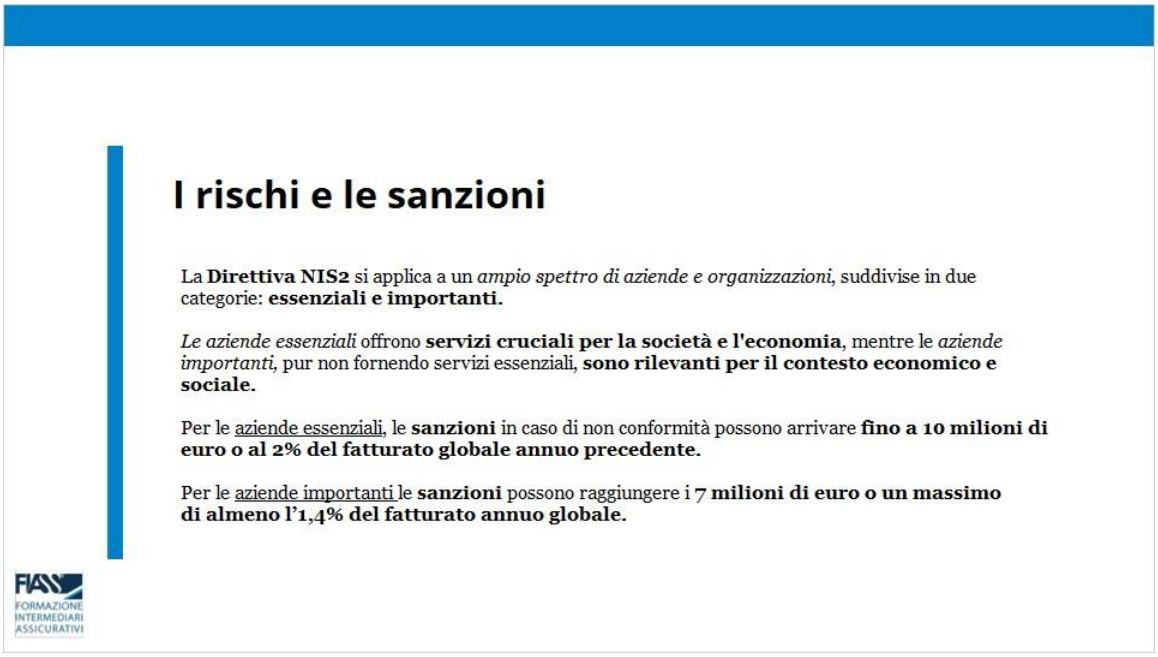
## *1.17 I punti essenziali di NIS2*



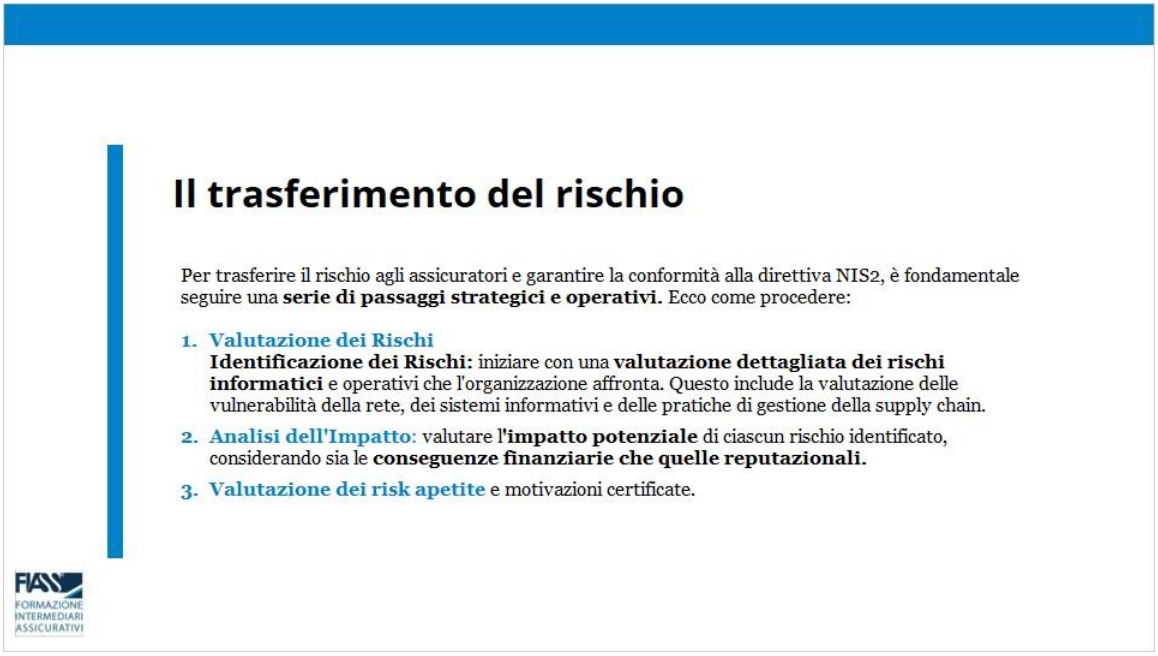

## *1.18 Deadline nazionali & attività annuali*



## *1.19 I rischi e le sanzioni*



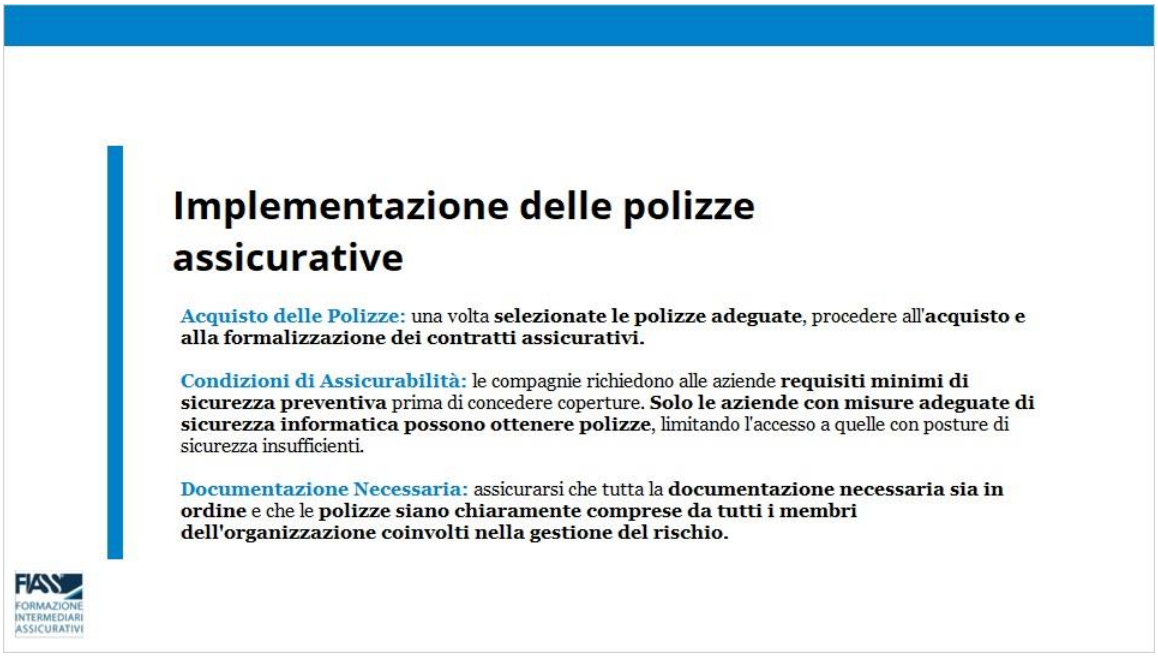

## *1.20 Il trasferimento del rischio*



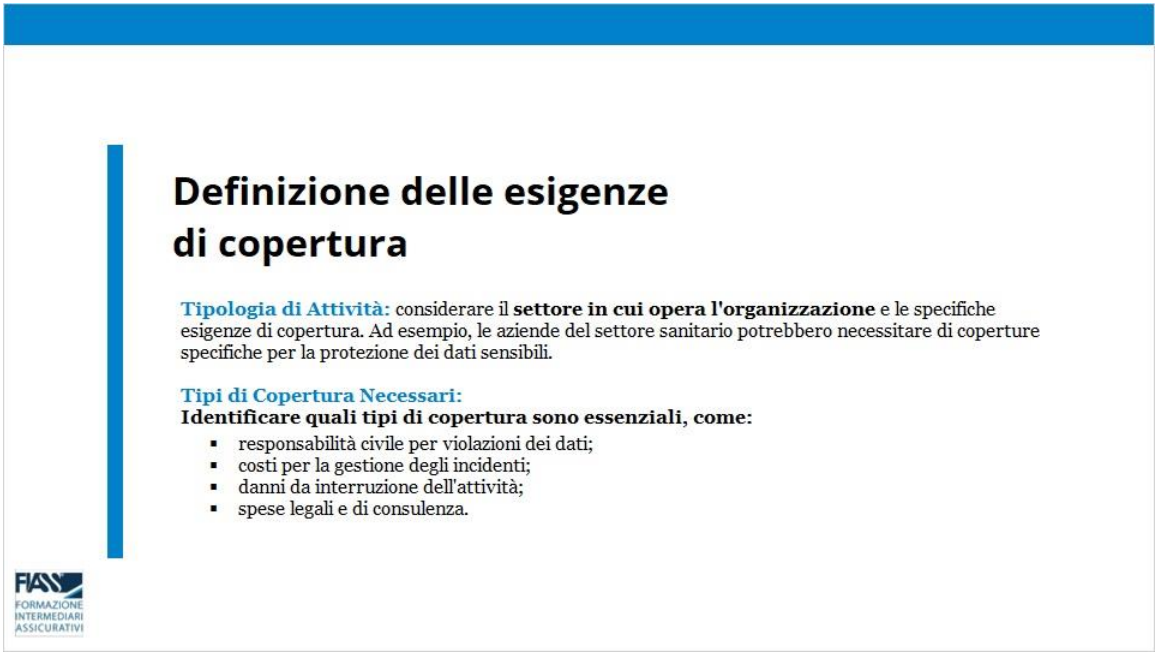
## *1.21 Sviluppo di una strategia di risk management*


## *1.22 Selezione di un partner assicurativo Agente o Broker*

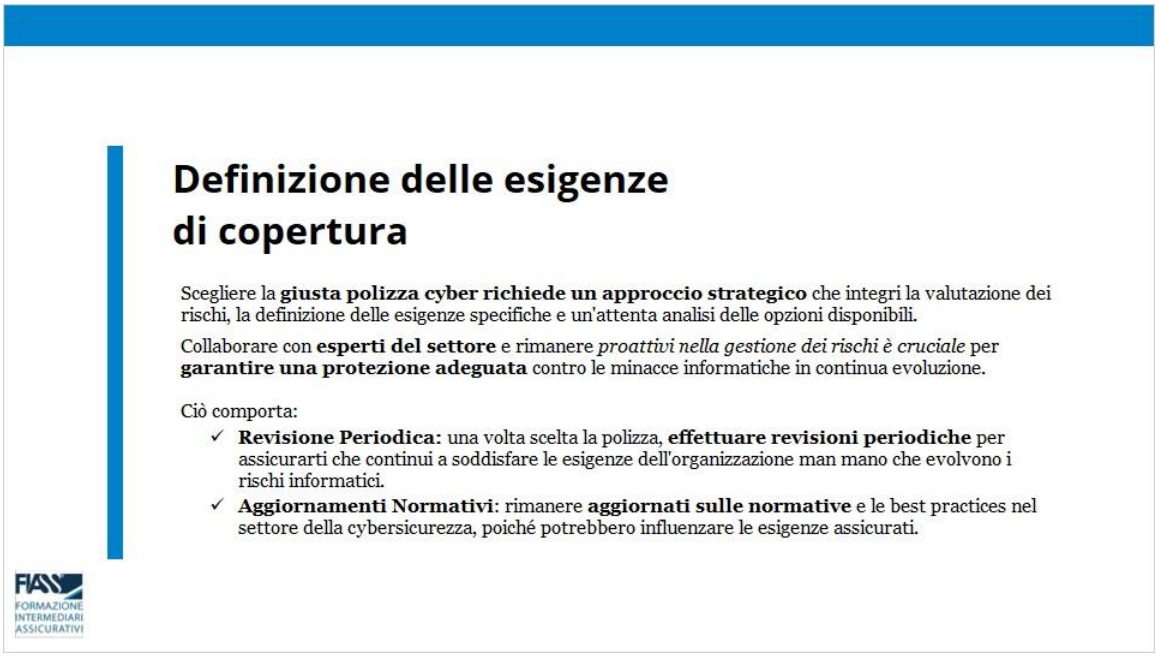
## *1.23 Implementazione delle polizze assicurative*



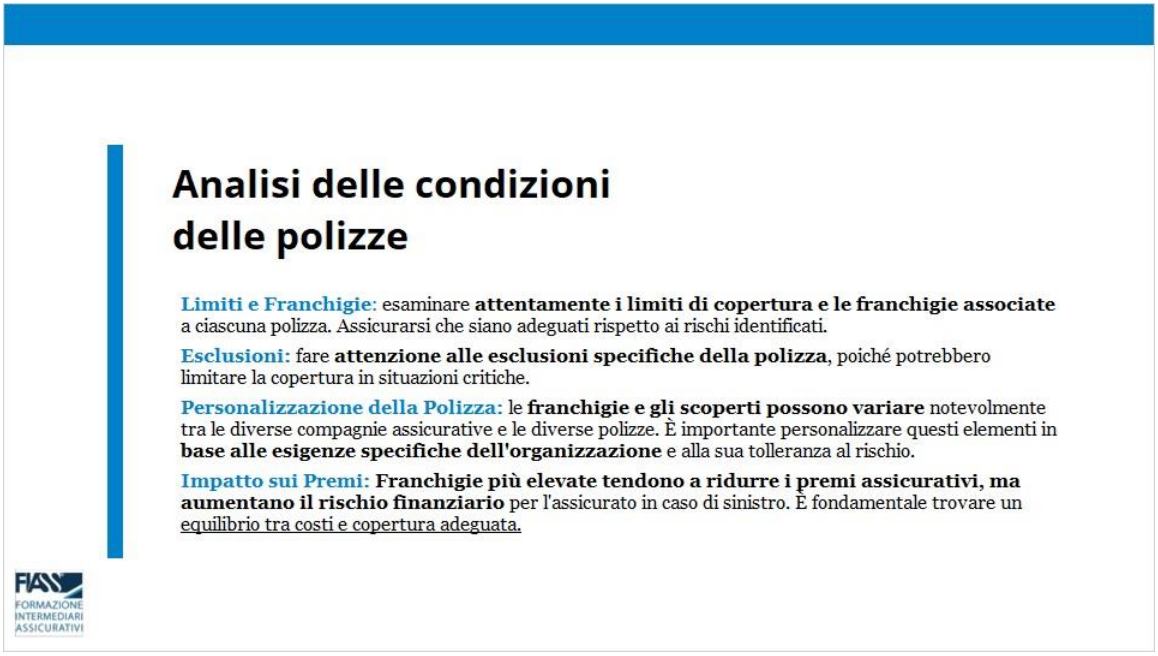

## *1.24 Definizione delle esigenze di copertura*



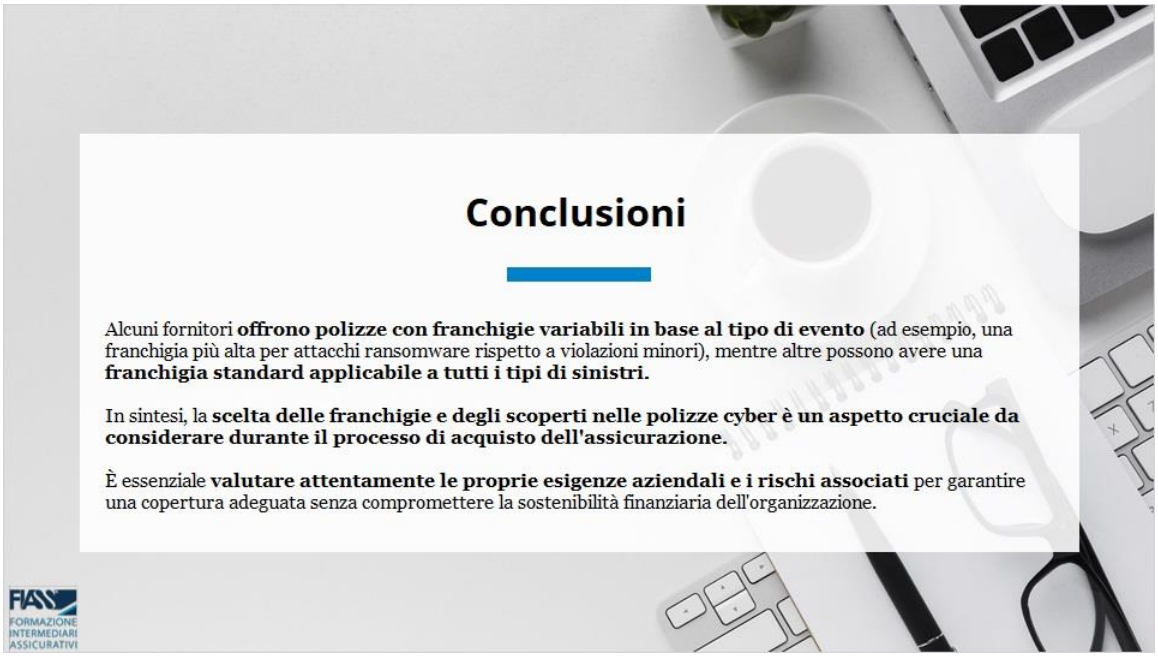
## *1.25 Definizione delle esigenze di copertura*




## *1.26 Analisi delle condizioni delle polizze*



## *1.27 Conclusioni*




## *1.28 Fine*