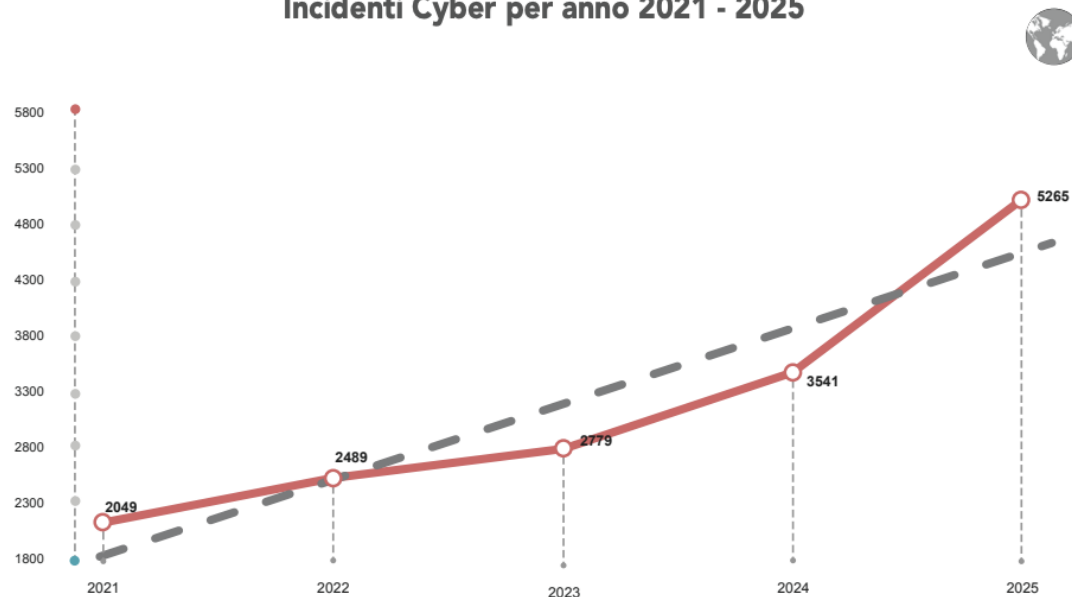


Cybersecurity per piccoli Comuni e le PMI:
sicurezza “a misura di ente”

Analisi del rischio e sicurezza dei fornitori

Alessandro Vallega Clusit CS e C4S, Università di Milano, Revo Insurance,
Rexilience

Incidenti Cyber per anno 2021 - 2025



© Clusit - Rapporto 2026 sulla Cybersecurity

Fig. 1 - Andamento degli incidenti cyber nel periodo 2021 - 2025

Consiste in un aumento di leggi e regolamenti orientati alla cybersecurity

- Legge 90/2024
- D.Lgs 138/2024 (NIS2)

Ma ci sono anche altre leggi, direttive, regolamenti orizzontali e settoriali per banche e assicurazioni, sanità, cloud provider, telecomunicazioni ecc.

- Crescente responsabilizzazione (dell'organizzazione e del vertice aziendale) e sanzioni significative
- Misure tecniche e organizzative via via più dettagliate e iniziative di armonizzazione con le migliori pratiche
- Obblighi di effettuazione di analisi del rischio
- Obblighi di gestire la sicurezza dei fornitori (sceglierli e vigilarli)

Analisi del rischio

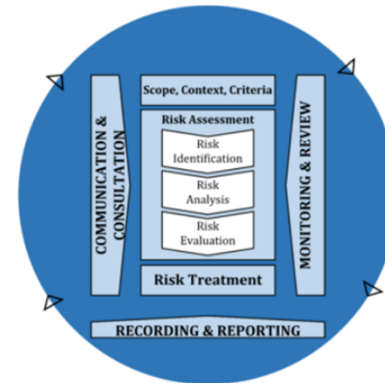
Per allocare le risorse aziendali nelle aree più indicate

- Le risorse sono per definizione scarse
- Il mondo è incerto
- Non si può fare tutto

Per ottemperare alla legge

Per dimostrare la propria responsabilizzazione

Risk Management Process (ISO 31000:2018)



Process (clause 6)

- Le funzioni di risk management organizzano e guidano il processo
- L'attività coinvolge molte persone a diversi livelli (stakeholder)
- Il risk owner è la persona o l'entità che è in grado di agire sul rischio (accountability and ownership)
- Per avere successo l'attività è supportata dalla direzione

Gestire la sicurezza dei fornitori

Per ridurre il rischio

- di subire un incidente a causa di un fornitore
- di interrompere il servizio perché il fornitore non è operativo

Per ottemperare alla legge

Per dimostrare la propria responsabilizzazione

- Appropriatamente e opportunisticamente nel ciclo di vita del fornitore e della fornitura (qualificazione, gara, assegnazione, monitoraggio, rinnovo, dismissione)
- Clausole contrattuali, questionari e verifiche automatiche o manuali e controlli (audit), processi di escalation
- Crescenti e differenziati in funzione del rischio e delle caratteristiche specifiche della fornitura

- La funzione acquisti rimane owner del processo
- La valutazione del fornitore include la sicurezza
- Ci sono fornitori monopolisti e che non si possono sottomettere alle nostre regole
- Bisogna essere pronti a negoziazioni e compromessi
- Il processo deve essere flessibile e prevedere misure compensative
- Il management può accettare il rischio residuo

Considerazioni finali

-
- L'evoluzione tecnologica non è mai stata così veloce
 - Le sfide globali creano un contesto imprevedibile
 - Le leggi sono un passo indietro e tutelano i terzi
 - Deve aumentare la consapevolezza dell'organizzazione (azienda / comune)
 - Risk management e esternalizzazioni sicure sono elementi chiave

alessandro.vallega@rexilience.eu

<https://clunit.it/blog/questionario-per-la-sicurezza-dei-fornitori-versione-2/>

<https://www.enisa.europa.eu/publications/risk-management-standards>

<https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks>

<https://myrisk.is/>

<https://myscore.is/it/>