UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

GESTIONE DEL RISCHIO NELLA SICUREZZA INFORMATICA E PROCESSO PENALE

Relatore: Massimo Bolognari

Laureanda Nicole Malaj
Matricola n. 2109566

Anno Accademico 2025/2026

Indice

Introduzione

La progressiva digitalizzazione delle attività economiche, amministrative e sociali ha determinato una crescente dipendenza delle organizzazioni dai sistemi informatici e dalle informazioni in essi trattate. Dati, infrastrutture digitali e servizi di rete costituiscono oggi risorse essenziali per il funzionamento delle imprese, delle pubbliche amministrazioni e, più in generale, della società. Questa trasformazione ha prodotto indubbi vantaggi in termini di rapidità, efficienza e accessibilità, ma ha anche ampliato l'esposizione a minacce informatiche sempre più frequenti, sofisticate e difficili da individuare. Gli incidenti informatici possono compromettere la riservatezza, l'integrità e la disponibilità delle informazioni, con conseguenze economiche, operative e reputazionali di rilievo. In alcuni casi, inoltre, essi assumono una specifica rilevanza giuridica e penale, poiché possono integrare fattispecie di reato, determinare l'attivazione di obblighi di notifica o far emergere responsabilità connesse all'inosservanza delle misure di sicurezza richieste dall'ordinamento. La cybersecurity non può quindi essere considerata esclusivamente una questione tecnica, affidata agli specialisti informatici, ma deve essere affrontata come un problema organizzativo, strategico e giuridico, che coinvolge direttamente la governance e i processi decisionali delle organizzazioni. In tale contesto, assume particolare importanza la gestione del rischio informatico. La sicurezza, infatti, non consiste nell'eliminazione assoluta di ogni possibile minaccia, obiettivo difficilmente raggiungibile in un ambiente tecnologico in continua evoluzione, ma nella capacità di identificare, valutare e trattare consapevolmente i rischi. Il presente elaborato si propone di analizzare il ruolo della gestione del rischio nell'ambito della sicurezza informatica, evidenziando come l'adozione di modelli organizzativi e standard internazionali costituisca uno strumento fondamentale per la prevenzione degli incidenti informatici e per il rispetto degli obblighi normativi introdotti dalla disciplina europea e nazionale. L'analisi prenderà in esame i principali standard della famiglia ISO/IEC 27000, con particolare riferimento alle norme ISO/IEC 27001 e ISO/IEC 27005, il NIST Cybersecurity Framework 2.0 e la direttiva NIS2, mettendone in luce caratteristiche, finalità e ambiti di applicazione.

1. LA SICUREZZA INFORMATICA E LA GESTIONE DEL RISCHIO

1. 1. La sicurezza delle informazioni nell'era digitale

Quando parliamo di sicurezza delle informazioni dobbiamo tener conto sia della dimensione privata sia di quella aziendale. È infatti necessario che le informazioni personali siano tutelate e accessibili a un numero limitato di soggetti, così come è fondamentale che un'impresa mantenga la riservatezza sui propri progetti innovativi e sull'elenco dei clienti.

È importante sottolineare che la sicurezza, non ha un significato assoluto e incontrovertibile, ma rappresenta piuttosto una condizione relativa.[1] In questo senso, essa deve essere proporzionata alla valutazione del rischio. Per chiarire con un esempio concreto, è evidente che sarà necessario usare password diverse per accedere all'home banking rispetto a quelle impiegate per un profilo su social network come TikTok. Questo perché gli attaccanti informatici tendono a riutilizzare le credenziali sottratte su più piattaforme (cosiddetto credential stuffing). Per tale motivo, è preferibile utilizzare password diverse per ciascun servizio, aumentando il livello di sicurezza in base alle conseguenze derivanti da una eventuale compromissione delle credenziali. Questa rappresenta, a tutti gli effetti, una valutazione del rischio.

È quindi indispensabile individuare il livello adeguato di sicurezza da raggiungere attraverso un'analisi del rischio accurata. Tale valutazione, tuttavia, non è statica, ma deve essere ripetuta nel tempo per verificare che le misure adottate siano ancora efficaci.[2] Come sottolineato, il rischio è una costruzione concettuale che deriva dall'incertezza e dalla possibilità che eventi futuri producano conseguenze negative sugli obiettivi di un sistema.[3] In questa prospettiva, si è evidenziato come la sicurezza non debba essere concepita come l'impossibile eliminazione completa del rischio, ma piuttosto come la sua gestione consapevole, sistematica e proporzionata.[4]

Nel corso degli anni, le esigenze di sicurezza non si sono ridotte; al contrario, si sono ampliate includendo sempre più l'ambito della tutela informatica. Nelle imprese, prima della diffusione delle tecnologie digitali, la sicurezza delle informazioni riguardava prevalentemente documenti cartacei e comunicazioni orali; oggi, invece, essa deve necessariamente comprendere anche la protezione dei sistemi informatici e dei dati digitali.

---

[1] C. Gallotti, *Sicurezza delle informazioni*, gennaio 2026, pp. 6.
[2] C. Gallotti, *Sicurezza delle informazioni*, gennaio 2026, pp. 7.
[3] A. Aven, *Risk Analysis*, Wiley, 2015, pp. 5–8.
[4] R. Anderson, *Security Engineering*, Wiley, 2020, pp. 32–34.

Per assicurare una corretta gestione della sicurezza informatica sono state approvate regole, standard e linee guida finalizzate alla tutela delle informazioni, sia in ambito aziendale sia per la protezione dei diritti dei cittadini nel contesto digitale. Tra queste, le più rilevanti sono il National Institute of Standards and Technology (NIST), agenzia governativa statunitense[5]; la Direttiva NIS, normativa europea in materia di sicurezza delle reti e dei sistemi informativi[6]; e lo standard ISO/IEC 27001, sviluppato a livello internazionale.[7]
Questi strumenti richiedono generalmente alle organizzazioni di valutare i rischi legati alla sicurezza delle informazioni e di adottare adeguate misure di protezione. Si può sinora anticipare che questo insieme di norme e linee guida ha generato un incremento complessivo del livello di sicurezza, pur accompagnandosi, in molti casi, ad un aumento degli oneri organizzativi e burocratici per le imprese.
Prima di analizzare il concetto di dati e informazioni, è necessario richiamare la definizione contenuta nelle versioni precedenti dello standard **ISO/IEC 27000**. Con l'espressione "informazione" (information) si intende la "*conoscenza o un insieme di dati che hanno valore per un individuo o un'organizzazione".*[8]

Le informazioni possono essere archiviate e trasmesse su diversi supporti, sia analogici, come la carta e le fotografie, sia digitali, come computer o dispositivi di memoria (ad esempio chiavette USB). Da ciò si deduce che, quando si parla di sicurezza delle informazioni, non ci si limita alla sola dimensione digitale, ma si fa riferimento a tutte le tipologie di informazione e ai sistemi utilizzati per raccoglierle, modificarle, conservarle, trasmetterle e distruggerle. In questo senso, il termine *informazione* assume una valenza più ampia ed è preferibile rispetto a *dato*, il quale invece, rappresenta un elemento grezzo che acquisisce significato solo a seguito di un processo di elaborazione.

Lo standard ISO/IEC 27000 definisce inoltre il concetto di "*Sicurezza delle informazioni" (information security)* che consiste nella *" preservazione della riservatezza, integrità e disponibilità delle informazioni";*[9]

E poi approfondisce le definizioni di questi termini in questo modo:

---

[5] NIST, *Cybersecurity Framework 2.0*, National Institute of Standards and Technology, 2024, pp. I-1;
[6] Unione Europea, Direttiva (UE) 2016/1148 (Direttiva NIS), considerando iniziale e artt. 14-16;
[7] ISO/IEC, *ISO/IEC 27001 — Information Security Management Systems*, ISO, 2022, clause 6, annex A.
[8] ISO/IEC, *ISO/IEC 27000 — Information security management systems — Overview and vocabulary*, ISO, 2024, clause 3, pp.13-15;
[9] ISO/IEC, *ISO/IEC 27000 — Information security management systems — Overview and vocabulary*, ISO, 2022.

- *Riservatezza (confidentiality): proprietà per cui un'informazione non è resa disponibile né divulgata a individui, entità o processi non autorizzati;*
- *Integrità (integrity): proprietà relativa all'accuratezza e completezza delle informazioni;*
- *Disponibilità (availability): proprietà per cui le informazioni sono accessibili e utilizzabili, nei tempi richiesti, da un'entità autorizzata.*[10]

Questi tre concetti sono considerati come il cuore della sicurezza delle informazioni. Essi esprimono principi fondamentali sul piano operativo: la *riservatezza* garantisce che le informazioni sensibili non vengano divulgate a soggetti non autorizzati; *l'integrità* assicura che i dati rimangano accurati e completi; la *disponibilità* permette che le informazioni siano accessibili quando necessario. Questi tre aspetti costituiscono la base per valutare il rischio e definire le misure di sicurezza più appropriate.

Quando si parla di sicurezza in una dimensione informatica, invece, si allude al trattamento delle informazioni contenute all'interno dei sistemi informatici. Tuttavia, esistono sistemi informatici che non gestiscono direttamente informazioni. Un esempio significativo si è verificato nel 2016, quando alcuni appartamenti in Finlandia rimasero senza acqua calda per circa una settimana a causa di un attacco informatico al sistema di riscaldamento. In questo caso non si è trattato propriamente di un attacco con impatto diretto sulle informazioni, bensì di un incidente che ha colpito il funzionamento di un sistema informatico. In tali situazioni è più corretto parlare di *cybersecurity*, che integra un concetto più ampio rispetto alla sicurezza delle informazioni. La cybersecurity riguarda infatti la protezione dei sistemi informatici nel loro complesso, indipendentemente dal fatto che trattino o meno informazioni.[11] Secondo alcuni, si è assistito a un'evoluzione concettuale che ha portato dalla *information security* alla *cybersecurity*, riflettendo l'ampliamento del perimetro delle minacce e la crescente interconnessione tra sistemi tecnologici e processi organizzativi.[12]

Cybersecurity: capacità di proteggere sistemi, reti e dispositivi da attacchi informatici.[13]

---

[10] ISO/IEC, *ISO/IEC 27000 — Information security management systems — Overview and vocabulary*, ISO, 2024.
[11] M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of Things Security and Forensics: Challenges and Opportunities, *Future Generation Computer Systems*, vol. 78, 2018, pp. 4-7.
[12] J. Von Solms, M. Van Niekerk, *From information security to cybersecurity*, Computers & Security, 2013, pp. 97–102.
[13] J. Von Solms, M. Van Niekerk, *op. cit.*, pp. 97–102.

In sintesi, la sicurezza delle informazioni non consiste nel raggiungere uno stato assoluto di protezione, ma nel preservare riservatezza, integrità e disponibilità dei dati in modo proporzionato alle esigenze dell'organizzazione o dell'individuo. Come illustrato dagli esempi precedenti, sia nel contesto fisico ma soprattutto in quello digitale, le minacce sono in continua evoluzione e le misure di sicurezza devono adattarsi di conseguenza. Per stabilire quali contromisure siano necessarie e in che misura, è indispensabile comprendere il concetto di rischio informatico.

1.2. Il concetto di rischio informatico

"Il rischio è insito nella natura delle cose e ci possono essere elementi che lo aumentano o lo diminuiscono". [14]

Tale affermazione evidenzia come ogni attività umana comporti un certo grado di rischio. Anche l'assenza di azione, contrariamente a quanto si potrebbe pensare, può esporre a conseguenze negative. Il rischio, dunque, può essere individuato sia in attività attive sia in situazioni apparentemente passive. L'analisi del rischio assume un ruolo fondamentale nella prevenzione dei danni, esaminando quali conseguenze possono derivare da un determinato evento e quali misure possono essere adottate per prevenirlo o, qualora ciò non sia possibile, per mitigarne gli effetti e ripristinare la situazione precedente. La valutazione del rischio riveste inoltre un'importanza centrale per le organizzazioni, che devono garantire la continuità operativa anche in presenza di eventi avversi. In questo contesto, la gestione del rischio è divenuta un elemento essenziale nei processi decisionali e nelle strategie aziendali, nonché un requisito previsto da numerosi standard e normative. Non a caso, la figura del risk manager è in continua evoluzione e assume un ruolo sempre più centrale all'interno delle organizzazioni.[15]

Negli ultimi anni, la digitalizzazione ha profondamente modificato la natura dei rischi, introducendo nuove minacce legate all'utilizzo delle tecnologie informatiche. In particolare, la pandemia da COVID-19 ha accelerato il processo di trasformazione digitale, favorendo la diffusione del lavoro da remoto e della didattica a distanza. Se, da un lato, ciò ha comportato

[14] CLUSIT (Associazione italiana per la sicurezza informatica), *Rischio digitale, innovazione e resilienza*, Clusit, 2022, p. 13.
[15] T. Aven, *Risk Analysis*, 2ª ed., Wiley, Chichester, 2015.

vantaggi in termini di efficienza e flessibilità, dall'altro ha esposto individui e organizzazioni a un aumento significativo delle minacce informatiche. Secondo i rapporti dell'ENISA, le minacce cyber sono in costante crescita, anche a causa di una diffusa sottovalutazione dei rischi connessi all'uso delle tecnologie digitali e di una conoscenza non sempre adeguata degli strumenti informatici. Tali minacce possono generare danni economici, reputazionali e, in alcuni casi, anche conseguenze legali.[16]

In questo contesto, si rileva il concetto di rischio digitale, che può essere definito come la possibilità che un evento connesso all'utilizzo delle tecnologie informatiche comprometta la sicurezza dei sistemi o dei servizi digitali, causando danni a individui o organizzazioni. Il rischio informatico rappresenta quindi una specifica declinazione del rischio nel contesto digitale e richiede un approccio sistematico basato sull'identificazione delle minacce, delle vulnerabilità e delle possibili conseguenze, al fine di adottare misure di prevenzione e mitigazione adeguate.[17]

Sebbene la digitalizzazione comporti numerosi benefici, essa introduce anche ulteriori profili di rischio connessi alla sostenibilità. Tali rischi non riguardano esclusivamente la dimensione ambientale, legata ad esempio al rapido ciclo di obsolescenza delle tecnologie, ma coinvolgono anche aspetti economici e sociali. In particolare, la trasformazione digitale può incidere sull'occupazione, modificare i modelli di distribuzione e accentuare le disuguaglianze tra aree geografiche e tra individui con differenti competenze digitali. Per questo motivo, accanto alla valutazione del rischio informatico, risulta sempre più rilevante adottare un approccio che consideri anche gli impatti complessivi della digitalizzazione in termini di sostenibilità.

1.3 Minacce, vulnerabilità e impatti sui sistemi informativi

L'identificazione del rischio rappresenta il processo attraverso il quale vengono individuati e descritti i rischi che possono incidere su un'organizzazione. Tale attività richiede una comprensione approfondita degli elementi che lo compongono, ovvero asset, minacce,

[16] ENISA, *Threat Landscape Report*, European Union Agency for Cybersecurity, 2023.
[17] P. Lagadec, A New Cosmology of Risks and Crises: Time for a radical shift in paradigm and practice, Review of policy research, vol.26, n. 4, 2009, pp. 27–34.

vulnerabilità e delle relazioni esistenti tra essi come previsto dagli standard internazionali di risk management.[18]

Gli asset possono essere definiti come qualsiasi elemento che possieda un valore per l'organizzazione e che contribuisca al raggiungimento dei suoi obiettivi. Essi includono non solo le informazioni, ma anche software, sistemi informatici, risorse fisiche e competenze del personale. Tuttavia, nell'ambito della sicurezza delle informazioni, assumono particolare rilevanza gli asset informativi e le modalità con cui questi vengono gestiti e protetti. Le informazioni costituiscono infatti il nucleo centrale della sicurezza informatica, in quanto vengono costantemente create, modificate, condivise e, in alcuni casi, distrutte.[19] La loro vulnerabilità aumenta nel momento in cui vengono trattate dalle persone, condizione inevitabile per il corretto funzionamento dell'organizzazione. In un contesto aziendale, ad esempio, le informazioni possono riguardare clienti, fornitori, personale o processi produttivi.

Dal canto loro, le minacce nel dominio cyber possono derivare sia da attori intenzionali, come cybercriminali o attori statali, sia da errori umani, configurazioni errate o malfunzionamenti tecnologici. [20] In questo senso, la dimensione tecnica del rischio si intreccia con quella organizzativa e comportamentale. Ai fini dell'analisi del rischio, non è necessario descrivere le minacce in maniera eccessivamente dettagliata; al contrario, risulta più efficace aggregarle in categorie omogenee, così da evitare una valutazione troppo complessa o dispersiva. Tale identificazione avviene generalmente coinvolgendo i responsabili dei processi, ai quali viene richiesto di indicare quali informazioni utilizzano, come vengono trattate e quali sarebbero le conseguenze di un loro uso improprio o non autorizzato. Una volta individuate le informazioni, è necessario identificare gli altri asset che ne consentono il trattamento e la conservazione, come i sistemi informatici, i software gestionali e gli archivi, sia digitali che cartacei.

Un ulteriore elemento fondamentale dell'analisi del rischio è rappresentato dalle minacce, definite dalla norma ISO/IEC 27000 come "cause potenziali di un incidente in grado di arrecare danni a un sistema o a un'organizzazione" . L'identificazione delle minacce deve essere condotta in maniera completa e sistematica, iniziando da una classificazione generale

[18] CLUSIT, *Rischio digitale, innovazione e resilienza*, Clusit, 2022, pp. 45–47
[19] ISO/IEC, *ISO/IEC 27000 — Information security management systems — Overview and vocabulary*, ISO, 2018.
[20]M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of Things Security and Forensics: Challenges and Opportunities, *Future Generation Computer Systems*, vol. 78, 2018, pp. 4-7.

per poi procedere con un livello di dettaglio crescente.[21] Esse possono essere ricondotte a diversi agenti, tra cui persone malintenzionate, soggetti non intenzionalmente dannosi, strumenti tecnici e fattori naturali. Nelle categorie delle persone malintenzionate sono compresi sia soggetti esterni, come clienti o fornitori, sia soggetti interni all'organizzazione. Le persone non malintenzionate, invece. rappresentano una fonte di rischio legata principalmente a errori o comportamenti inconsapevoli. Anche i sistemi tecnologici possono costituire una minaccia, a causa di malfunzionamenti o condizioni ambientali sfavorevoli, così come gli eventi naturali possono compromettere la disponibilità delle informazioni. Le minacce possono inoltre essere analizzate in funzione delle modalità attraverso cui si manifestano, come attacchi informatici, utilizzo eccessivo delle risorse o interruzioni operative. Un'analisi efficace richiede pertanto un approccio strutturato, aggiornato e in grado di considerare l'insieme delle possibili fonti di rischio. Nell'ambito della valutazione del rischio, risulta essenziale associare le minacce agli asset, al fine di determinarne la probabilità che le prime si verifichino e il loro potenziale impatto. Tale associazione viene generalmente effettuata a livello di categorie di asset, piuttosto che sui singoli elementi, considerando il contesto complessivo in cui l'organizzazione opera. La rilevanza di una minaccia dipende infatti principalmente da fattori quali l'ambiente interno ed esterno e le capacità degli agenti che la generano. Le minacce devono inoltre essere correlate alle possibili conseguenze sugli asset informativi, in particolare in termini di riservatezza, integrità e disponibilità, elementi fondamentali per la valutazione del livello di rischio. Le vulnerabilità costituiscono un ulteriore elemento chiave in questo processo e possono essere definite come debolezze di un asset o di un controllo di sicurezza che possono essere sfruttate da una minaccia. Esse sono spesso riconducibili all'assenza o l'inefficacia di adeguate misure di protezione e vengono generalmente analizzate in relazione a categorie di asset, al fine di semplificare il processo e individuare criticità comuni. Un aspetto centrale dell'analisi del rischio consiste nella correlazione tra minacce, vulnerabilità e controlli di sicurezza. Per ciascuna minaccia è infatti necessario individuare adeguati controlli, che possono presentarsi come soluzioni alternative, compensative, complementari o tra loro correlate. In particolare, i controlli alternativi rappresentano diverse modalità per affrontare uno stesso problema, mentre quelli compensativi vengono adottati quando non è possibile implementare le soluzioni ideali. [22] I controlli complementari, invece, operano congiuntamente per rafforzare il livello di sicurezza complessivo, secondo il principio della difesa in profondità, mentre quelli correlati risultano

[21] ISO/IEC, *ISO/IEC 27005 — Information security risk management*, ISO, 2022.
[22] ISO/IEC, *ISO/IEC 27001 — Annex A*, ISO, 2022.

efficaci solo se applicati in modo coordinato. Dal punto di vista funzionale, i controlli di sicurezza possono essere distinti in tre categorie principali: quelli di prevenzione, finalizzati a impedire il verificarsi di un attacco; quelli di recupero, volti a ripristinare la situazione precedente a un incidente; e quelli di rilevazione, che consentono di individuare e segnalare eventi o anomalie. Un sistema di sicurezza efficace deve necessariamente integrare tutte queste tipologie in modo equilibrato.[23]

In conclusione, l'identificazione e la correlazione tra asset, minacce, vulnerabilità e controlli rappresentano il fondamento dell'analisi del rischio. L'adozione di un approccio strutturato e sistematico consente di individuare le principali criticità e di valutare in modo accurato i rischi, supportando l'implementazione di adeguate misure di sicurezza a tutela dell'organizzazione. [24]

1.4 Il ruolo della gestione del rischio nelle organizzazioni

Nel contesto organizzativo contemporaneo, caratterizzato da elevati livelli di complessità, digitalizzazione e rapida evoluzione degli scenari competitivi, la gestione del rischio riveste un ruolo centrale per garantire la continuità operativa e la resilienza delle imprese. Le organizzazioni sono infatti esposte, come si è accennato, a una molteplicità di minacce – tecnologiche, operative, reputazionali e strategiche – che richiedono un approccio strutturato e integrato alla prevenzione, alla mitigazione e al monitoraggio del rischio. In quest'ottica, la gestione del rischio non rappresenta soltanto un insieme di strumenti tecnici, ma un vero e proprio pilastro della governance aziendale.

Secondo la ISO 31000, la gestione del rischio deve essere pienamente integrata nei processi di governance, nella strategia e nella cultura organizzativa, poiché essa permette di sviluppare una visione unificata del rischio, migliorare la consapevolezza delle incertezze e supportare decisioni informate.[25] Lo standard sottolinea in particolare l'importanza di creare e proteggere valore attraverso l'identificazione, la valutazione e il trattamento dei rischi, evidenziando come un approccio sistematico e proattivo contribuisca al miglioramento dell'efficacia decisionale e della fiducia degli stakeholder. [26] Inoltre, ISO 31000 offre un quadro

[23] NIST, *Guide for Conducting Risk Assessments* (SP 800-30), 2012.
[24] A. Boin, P. 't Hart, E. Stern, *The Politics of Crisis Management*, Cambridge University Press, 2016, pp. 1–10, 63–68.
[25] ISO, *ISO 31000:2018 – Risk Management: Principles and Guidelines*, ISO, 2018.
[26] ISO, *ISO 31000:2018 – Risk Management: Principles and Guidelines*, ISO, 2018.

metodologico che aiuta le organizzazioni a sviluppare una cultura del rischio, promuovendo continuità operativa, migliori controlli interni, allocazione ottimale delle risorse e maggiore trasparenza nei processi aziendali. L'efficacia della gestione del rischio si esprime anche nella capacità dell'organizzazione di coordinare informazioni, ruoli e responsabilità in modo coerente. La comunicazione interna, ad esempio, svolge una funzione strategica sia nelle attività ordinarie sia nelle situazioni di crisi: garantisce il flusso informativo tra unità operative e funzioni manageriali, facilita la coesione durante gli eventi critici e contribuisce alla riduzione dell'impatto negativo dell'incertezza. Una comunicazione tempestiva, multidirezionale e autorevole costituisce un elemento essenziale per preservare la fiducia degli stakeholder e proteggere il valore aziendale, soprattutto considerando che oltre il 70% del valore di un'organizzazione risiede oggi in asset immateriali quali reputazione, conoscenza, relazioni e identità digitale. [27]

Una delle caratteristiche distintive della norma ISO 31000 è la sua struttura basata su tre componenti interconnesse: i principi, il framework e il processo. Questi elementi non operano in modo isolato, ma si rafforzano reciprocamente, dando vita a un modello di gestione del rischio coerente, dinamico e adattabile alle specificità di ciascuna organizzazione. Tale architettura è evidenziata anche dalla letteratura tecnica sullo standard, che sottolinea come le tre componenti costituiscano la base concettuale, organizzativa e operativa dell'intero sistema di gestione del rischio. I principi ISO 31000 rappresentano l'intento, la visione e le caratteristiche che definiscono una gestione del rischio efficace. Essi includono: creazione di valore, integrazione nei processi aziendali, strutturazione e tempestività delle attività, intervento in base a informazioni affidabili, personalizzazione rispetto al contesto, considerazione dei fattori umani e culturali, inclusività, dinamicità e miglioramento continuo. Secondo ISO, questi principi costituiscono la "filosofia di fondo" che guida tutta l'attività di gestione del rischio e orientano la costruzione del framework organizzativo.[28]

Il framework definisce come la gestione del rischio viene integrata nella governance dell'organizzazione. Include attività di leadership, definizione delle responsabilità, allocazione delle risorse, sviluppo delle politiche aziendali, comunicazione e consultazione con gli stakeholder. Il framework ha lo scopo di rendere la gestione del rischio parte del DNA organizzativo, assicurando che essa non rimanga un processo isolato ma sia connessa alla strategia, ai processi decisionali e ai sistemi di reporting. La norma sottolinea l'importanza

[27] ISO, *ISO 31000:2018 – Risk Management: Principles and Guidelines* , ISO, 2018.
[28] ISO, *ISO 31000:2018 – Risk Management: Principles and Guidelines*, ISO, 2018.

dell'impegno del top management in termini di guida, coordinamento e verifica della coerenza delle attività di gestione del rischio rispetto agli obiettivi aziendali.

Il processo di gestione del rischio costituisce la componente operativa del modello e definisce le fasi necessarie per identificare, analizzare, valutare e trattare i rischi. Esso integra attività di comunicazione, consultazione, definizione del contesto, valutazione dei rischi (identificazione, analisi, valutazione), trattamento, monitoraggio e registrazione. Come evidenziato nelle risorse tecniche ISO, il processo rappresenta la "metodologia" quotidiana attraverso cui l'organizzazione gestisce l'incertezza in modo sistematico e coerente con gli orientamenti strategici definiti dal framework.

In parallelo, la gestione del rischio assume una dimensione particolarmente rilevante nella definizione di strutture organizzative dedicate, come le unità di crisi o i team di gestione dell'emergenza. Queste unità, composte da figure interne con ruoli chiave e supportate da esperti esterni, garantiscono reattività, coordinamento e leadership durante eventi avversi. Il loro operato consiste nell'individuare procedure, adottare strumenti idonei alla gestione dell'incertezza, monitorare le minacce emergenti e assicurare che il processo decisionale rimanga coerente con la strategia aziendale. L'esistenza di tali unità contribuisce inoltre a rafforzare la cultura del rischio e a trasformare gli eventi critici in opportunità di apprendimento e miglioramento organizzativo.

Un'altra dimensione fondamentale della gestione del rischio riguarda la comunicazione esterna, soprattutto nell'era digitale. Il consolidamento del web e dei social media ha radicalmente trasformato il modo in cui le organizzazioni comunicano durante le crisi: l'informazione circola con estrema rapidità, generando fenomeni di amplificazione, distorsione o polarizzazione. Per questo, le imprese devono dotarsi di piani di comunicazione strategici che includano politiche chiare per la gestione dei social media, linee guida per l'identificazione delle tipologie di crisi, procedure di approvazione dei messaggi pubblici e sistemi di monitoraggio continuo della reputazione online. Una comunicazione efficace contribuisce a tutelare sia la brand reputation sia la web reputation, oggi elementi imprescindibili per la resilienza delle organizzazioni e per la loro capacità di mantenere relazioni positive con il pubblico. A livello più ampio, la gestione del rischio nelle organizzazioni non riguarda esclusivamente aspetti tecnici, ma costituisce un fattore competitivo e strategico. Una governance basata sul rischio consente infatti di rafforzare la credibilità, di incrementare la trasparenza e di migliorare la capacità di anticipare scenari futuri. L'integrazione dei processi di gestione del rischio nei sistemi decisionali, operativi e comunicativi dell'organizzazione favorisce non solo una maggiore efficienza operativa, ma

anche un approccio orientato al miglioramento continuo, in linea con i principi internazionali di buona gestione e responsabilità sociale.

L'attacco informatico NotPetya del giugno 2017 costituisce uno dei casi più significativi nella storia della cybersecurity e rappresenta un esempio paradigmatico dell'importanza della gestione del rischio nelle organizzazioni complesse. A.P. Møller–Maersk, il principale operatore mondiale nel settore dello shipping e della logistica, fu infatti colpito da un malware che causò un blocco totale dei sistemi informativi aziendali, paralizzando porti, terminal e servizi di tracciamento merci in tutto il mondo.

Secondo la documentazione prodotta dalla Columbia University, Maersk si trovò coinvolta nel conflitto cibernetico derivante dalle tensioni geopolitiche tra Russia e Ucraina: il malware, circolante tramite un aggiornamento compromesso di un software contabile ucraino, si propagò rapidamente attraverso l'infrastruttura IT globale del gruppo, dimostrando come le interdipendenze digitali possano amplificare enormemente la vulnerabilità delle supply chain internazionali. L'infezione portò alla compromissione di circa 49.000 laptop e 7.000 server in tutta l'azienda, determinando l'interruzione delle operazioni in 76 porti e il fermo delle attività logistiche per diversi giorni. [29]

Dal punto di vista della gestione del rischio, l'evento mise in evidenza alcuni elementi cruciali. Innanzitutto, la struttura di rete non segmentata facilitò la diffusione del malware all'interno dell'organizzazione, confermando la necessità di adottare architetture IT orientate alla limitazione del cosiddetto "blast radius". In secondo luogo, l'attacco mostrò il valore della continuità operativa e della capacità di ripristino: Maersk riuscì a ricostruire la propria infrastruttura informatica grazie a un singolo server rimasto intatto in Ghana, sfuggito per caso al malware a causa di un blackout. Questa circostanza fortuita si rivelò essenziale per garantire la ripartenza delle attività e sottolinea l'importanza di backup distribuiti e di strategie robuste di disaster recovery.

Nonostante danni stimati in oltre 300 milioni di dollari, l'azienda fu in grado di reagire con rapidità attraverso l'attivazione di team di crisi globali, l'adozione di misure trasparenti di comunicazione interna ed esterna e un impegno significativo del top management, evitando gravi danni reputazionali e riportando l'operatività a livelli accettabili in poche settimane. Il caso dimostra dunque come un evento altamente distruttivo possa essere assorbito grazie a

[29] Columbia University – SIPA, *The NotPetya Cyber Attack*, 2022, https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf

principi robusti di gestione del rischio, tra cui la preparazione, la chiarezza delle responsabilità, la resilienza organizzativa e la comunicazione efficace con gli stakeholder.

L'esperienza di Maersk è oggi considerata un riferimento fondamentale per le organizzazioni che operano in contesti globali ad alta complessità digitale. Essa evidenzia non solo l'importanza dell'identificazione preventiva delle vulnerabilità e della creazione di un framework di gestione del rischio conforme a standard internazionali come ISO 31000, ma anche la necessità di sviluppare una cultura di rischio matura, capace di integrare sicurezza informatica, governance e continuità operativa in un unico ecosistema strategico[30]

In conclusione, il ruolo della gestione del rischio nelle organizzazioni è oggi più cruciale che mai: essa non solo protegge l'impresa dalle minacce, ma ne rafforza la competitività, ne sostiene la reputazione e costituisce una leva fondamentale per la creazione di valore duraturo. L'adozione di standard riconosciuti come ISO 31000 permette alle organizzazioni di sviluppare un approccio maturo e consapevole alla gestione dell'incertezza, ponendo le basi per una governance solida, resiliente e orientata al futuro.[31]

1.5 Approcci e modelli di cyber risk management

La gestione del rischio informatico rappresenta oggi una componente essenziale della governance delle organizzazioni, poiché l'evoluzione tecnologica, la crescente complessità delle infrastrutture digitali e la pervasività dei sistemi informativi espongono con continuità gli asset aziendali a minacce di natura tecnica, comportamentale e organizzativa.[32] Il cyber risk management può essere inteso come l'insieme degli approcci, dei modelli e delle misure orientati a identificare, valutare, mitigare e monitorare i rischi derivanti dall'uso delle tecnologie digitali, con la finalità di ridurre la probabilità di incidenti informatici e limitarne l'impatto sul business.[33] In questo contesto, la cybersecurity assume un ruolo specifico come sottodominio dell'information security, focalizzato sull'adozione di misure prevalentemente

[30] Yallo, *Operational meltdown from cyber attack: Maersk 2017*, https://yallo.co/?case-study=operational-meltdown-from-cyber-attack-maersk-2017
[31] ISO, *ISO 22301 — Business Continuity Management Systems*, ISO, 2019.
[32] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley, 2020, pp. 28–36
[33] T. Aven, *Risk Analysis*, Wiley, 2015, pp. 5–12

tecnologiche mirate a contenere gli effetti di un incidente, proteggendo l'organizzazione da intrusioni, interruzioni dei servizi e compromissioni dei dati. [34]

La protezione degli asset informativi si fonda sul riconosciuto paradigma della riservatezza, integrità e disponibilità (CIA o RID), secondo cui un sistema può considerarsi sicuro solo se i dati sono accessibili esclusivamente a soggetti autorizzati, non vengono alterati in modo improprio e restano fruibili nei tempi necessari. Secondo la norma internazionale ISO 31000, la sicurezza delle informazioni rappresenta un insieme di misure orientate a garantire la disponibilità, l'integrità e la riservatezza dei dati trattati, costituendo il presupposto fondamentale su cui si basano tutte le successive attività di gestione del rischio.[35] A tali proprietà si affiancano funzioni complementari, come il non ripudio, che consente di attribuire con certezza l'origine dei dati o dei documenti, e la tracciabilità, che permette di ricostruire quando e da chi una risorsa è stata consultata o modificata. [36]

La gestione del rischio informatico si articola attraverso molteplici tecniche e misure integrate, che operano su livelli diversi della cosiddetta difesa a strati. Le misure di prevenzione includono l'adozione di procedure di aggiornamento continuo dei sistemi, l'applicazione di politiche di accesso rigorose, la segmentazione delle reti, l'uso di antivirus e firewall configurati in modo corretto, l'implementazione di IDS e IPS per rilevare e bloccare traffico sospetto e il ricorso a crittografia simmetrica e asimmetrica per garantire la riservatezza dei dati. A ciò si aggiungono pratiche operative quali l'uso di backup locali e remoti, la riduzione dei privilegi tramite account non amministrativi per le attività quotidiane, e l'educazione degli utenti, che rimangono spesso uno degli anelli più deboli della catena di sicurezza.[37]

Un ruolo fondamentale è svolto dall'autenticazione degli utenti, che può basarsi su password robuste, tecniche biometriche, token fisici, certificati digitali e sistemi a più fattori (2FA). Nelle comunicazioni online, protocolli come TLS/SSL garantiscono l'autenticità delle controparti e la confidenzialità dei dati trasmessi, consentendo di stabilire connessioni sicure per transazioni commerciali e attività sensibili. Allo stesso modo, strumenti come MAC e HMAC permettono di verificare l'integrità dei messaggi, impedendo modifiche non

[34] ISO/IEC, *ISO/IEC 27000 — Information security management systems — Overview and vocabulary*, ISO, 2018, pp. 2–4
[35] ISO/IEC, *ISO/IEC 27000 — Overview and vocabulary*, ISO, 2018, pp. 6–8
[36] ISO, *ISO 31000:2018 – Risk Management: Principles and Guidelines*, ISO, 2018, pp. 5–7
[37] M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of Things Security and Forensics: Challenges and Opportunities, *Future Generation Computer Systems*, vol. 78, 2018, pp. 4-7.

autorizzate o falsificazioni. Parallelamente, la diffusione dei servizi cloud e delle architetture distribuite ha spostato l'attenzione verso un modello di sicurezza data-centrico, in cui la protezione è concentrata sull'informazione più che sul perimetro fisico delle infrastrutture.[38]

Dal punto di vista metodologico, l'applicazione di modelli strutturati consente alle organizzazioni di affrontare la gestione del rischio in modo sistematico e coerente. Tra i modelli maggiormente utilizzati a livello internazionale vi è l'ISO 31000, ma altrettanto rilevante è il Cybersecurity Framework (CSF), sviluppato dal National Institute of Standards and Technology (NIST), che identifica cinque funzioni fondamentali – Identify, Protect, Detect, Respond, Recover – considerate un riferimento globale per la gestione del rischio informatico. Il NIST CSF 2.0 amplia ulteriormente questa prospettiva, enfatizzando l'importanza della governance e della maturità dei processi di sicurezza, e fornendo un linguaggio comune per valutare, comunicare e migliorare la postura di sicurezza delle organizzazioni. [39]

Accanto ai modelli più diffusi, approcci come FAIR (Factor Analysis of Information Risk) consentono una quantificazione economica del rischio[40], mentre metodologie come OCTAVE Allegro focalizzano l'attenzione sugli aspetti organizzativi, sulle criticità degli asset e sugli impatti di natura operativa e reputazionale. Questi modelli – pur differenti nelle finalità e nel livello di dettaglio – condividono la necessità di integrare strumenti tecnici, processi operativi e comportamenti individuali, riconoscendo che la sicurezza è un processo continuo che richiede adattamento e revisione costante.[41]

La dimensione del rischio informatico si interseca anche con la tutela della privacy, soprattutto nell'era dei big data e dei servizi basati sulla localizzazione.[42] Non solo i dati rilasciati esplicitamente dagli utenti, ma anche le informazioni derivate possono costituire una minaccia per la loro riservatezza. Il Regolamento europeo 2016/679 (GDPR)[43] rappresenta oggi il principale riferimento normativo per la gestione e la protezione dei dati personali, imponendo vincoli di minimizzazione, trasparenza e controllo sui dati trattati, nonché la

[38] W. Stallings, *Cryptography and Network Security*, Pearson, 2021, pp. 89–102.
[39] NIST, *NIST Cybersecurity Framework 2.0*, National Institute of Standards and Technology, 2024.
[40] The FAIR Institute, Factor Analysis of Information Risk (FAIR) Standard v3.0, 2025.
[41] Caralli et al., *OCTAVE Allegro – Improving the Information Security Risk Assessment Process*, Software Engineering Institute, Carnegie Mellon University, 2007.
[42] N. Kshetri, *The emerging role of big data in key development issue*s: *Opportunities, challenges, and concerns, Big Data & Society*, 2014, pp. 4–8.
[43] The FAIR Institute, Factor Analysis of Information Risk (FAIR) Standard v3.0, 2025.

responsabilità delle organizzazioni nella definizione di misure adeguate per mitigarne il rischio di esposizione o abuso.[44]

In definitiva, gli approcci e i modelli di cyber risk management costituiscono un tessuto integrato di tecnologie, procedure, normative e responsabilità umane. La loro efficacia dipende dalla capacità di combinare strumenti tecnici – dalla crittografia ai firewall, dai sistemi di autenticazione alle architetture cloud sicure – con strategie organizzative basate su standard riconosciuti e una cultura aziendale orientata alla consapevolezza del rischio. Integrare queste dimensioni consente alle organizzazioni non solo di ridurre la vulnerabilità agli attacchi, ma anche di sviluppare resilienza, garantire continuità operativa e proteggere il valore informativo che rappresenta oggi uno degli asset più critici del contesto digitale. [45]

1.6 Il framework NIST per il cyber risk management

Il NIST Cybersecurity Framework rappresenta oggi uno dei modelli più adottati e riconosciuti per la gestione del rischio informatico. Introdotto per la prima volta nel 2014 dal National Institute of Standards and Technology con l'obiettivo di rafforzare la sicurezza delle infrastrutture critiche statunitensi, il framework ha rapidamente superato i confini settoriali e geografici, fino a diventare uno strumento di riferimento globale. Con la pubblicazione della versione CSF 2.0 nel febbraio 2024, la sua applicabilità è stata ampliata a qualsiasi tipo di organizzazione, indipendentemente dalle dimensioni, dal settore o dal livello di maturità digitale, confermandolo come una guida universale per affrontare in modo strutturato la crescente complessità delle minacce cyber.

La struttura del NIST CSF si fonda su tre componenti principali che ne definiscono l'operatività: il Core, i Profili organizzativi e i Tiers. Il Core raccoglie gli outcome di cybersecurity e li organizza in funzioni, categorie e sottocategorie, fornendo un modello chiaro e immediato di ciò che un'organizzazione dovrebbe ottenere per migliorare la propria resilienza.[46] La versione 2.0 introduce una novità significativa con la funzione Govern, che affianca e integra le cinque funzioni storiche del framework, ovvero Identify, Protect, Detect, Respond e Recover.[47] Tale espansione rispecchia l'evoluzione delle esigenze di governance

[44] N. Kshetri, *The emerging role of Big Data in key development issues: Opportunities, challenges, and concerns*, op. cit. , pp. 1–20.
[45] CLUSIT, Rischio digitale, innovazione e resilienza, Clusit, 2022, pp. 45–52.
[46] NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, 2024, pp. 11–15
[47] NIST, *Profiles and Tiers in the Cybersecurity Framework 2.0*, National Institute of Standards and Technology, 2024, pp. 3–7.

del rischio, portando attenzione ai processi decisionali e alla supervisione strategica, elementi considerati ormai fondamentali per una postura di sicurezza efficace e dinamica. I profili organizzativi consentono invece di rappresentare lo stato attuale e quello desiderato della sicurezza aziendale, facilitando l'analisi dei gap e la definizione delle priorità, mentre i tiers descrivono il livello di maturità della gestione del rischio cyber, da processi non strutturati a pratiche avanzate e adattive.

Le cinque funzioni originarie del framework continuano a costituire la base del modello operativo. "Identify" si concentra sulla comprensione degli asset, delle risorse critiche e delle vulnerabilità, ponendo le basi per una gestione consapevole delle priorità di sicurezza. "Protect" raccoglie l'insieme delle misure di prevenzione, dalla formazione del personale ai controlli di accesso, dalla crittografia alla protezione delle reti, con l'obiettivo di ridurre la probabilità di incidenti. "Detect" riguarda la capacità di individuare tempestivamente eventi anomali o possibili compromissioni, mentre "Respond" definisce le azioni necessarie per contenere e mitigare l'impatto degli incidenti una volta rilevati. "Recover", infine, si occupa del ripristino delle funzioni e dei servizi compromessi, garantendo continuità operativa e promuovendo un miglioramento costante attraverso l'analisi degli eventi passati. L'introduzione della funzione "Govern" nella versione più recente rafforza ulteriormente la visione integrata della cybersecurity come componente strutturale della governance aziendale. [48]

L'applicazione del NIST CSF nelle organizzazioni è caratterizzata da un approccio modulare e adattabile, che ne ha favorito la diffusione sia in contesti altamente regolamentati sia in realtà di dimensioni ridotte. Il framework permette di valutare la postura di sicurezza analizzando i risultati attesi espressi nelle diverse funzioni, individuare lacune e definire percorsi di miglioramento attraverso i profili organizzativi, oltre a favorire una comunicazione efficace tra team tecnici, management e stakeholder aziendali grazie al linguaggio comune che propone. La sua utilità si estende anche alla gestione del rischio nella supply chain e alla pianificazione delle competenze del personale, come dimostrato dalle nuove risorse e linee guida pubblicate nei Quick Start Guides del 2026, che integrano aspetti di workforce management e di allineamento strategico del rischio cyber all'interno dell'enterprise risk management.[49]

[48] NIST, *Profiles and Tiers in the Cybersecurity Framework 2.0*, National Institute of Standards and Technology, 2024, pp.4-9.
[49] NIST, *NIST Cybersecurity Framework 2.0*, National Institute of Standards and Technology, 2024, pp. 1-6.

Dal punto di vista del confronto con gli standard ISO, il NIST CSF si distingue per un approccio orientato ai risultati, volto a definire cosa un'organizzazione debba raggiungere piuttosto che come debba farlo. Al contrario, gli standard della serie ISO/IEC 27000 forniscono requisiti rigorosi e controlli specifici per la gestione strutturata della sicurezza delle informazioni. Mentre ISO/IEC 27001 è certificabile e permette di attestare formalmente la conformità a un sistema di gestione, il NIST CSF non è uno standard certificabile, ma un framework di riferimento.[50] Questa differenza non rappresenta tuttavia una contrapposizione, poiché i due modelli risultano fortemente complementari: molte organizzazioni adottano il NIST CSF come guida operativa e strategica, integrandolo con gli standard ISO per ottenere un sistema di gestione della sicurezza completo, verificabile e allineato alle best practice internazionali.[51]

[50] ISO/IEC, *ISO/IEC 27001 — Information Security Management Systems*, ISO, 2024, pp.1-4.
[51] NIST, *NIST Cybersecurity Framework 2.0*, National Institute of Standards and Technology, 2024 pp.25-27.

2. NORMATIVA EUROPEA SULLA SICUREZZA INFORMATICA

2.1 Origine e obiettivi della Direttiva NIS

La Direttiva NIS (Network and Information Security), adottata nel 2016 come Direttiva (UE) 2016/1148, rappresenta il primo quadro normativo europeo interamente dedicato alla sicurezza delle reti e dei sistemi informativi.[52] La sua introduzione si giustifica in ragione della crescente consapevolezza che la dipendenza dell'Unione Europea da infrastrutture digitali critiche espone gli Stati membri a rischi significativi, derivanti sia da minacce informatiche di origine criminale sia da attacchi di natura geopolitica.[53] Prima della NIS, infatti, la cybersecurity era trattata in modo disomogeneo, con approcci nazionali eterogenei e spesso privi di un coordinamento sovranazionale. [54]

Gli obiettivi principali della Direttiva NIS erano tre.
In primo luogo, assicurare un livello comune elevato di sicurezza delle reti e dei sistemi informativi all'interno dell'Unione Europea, promuovendo l'adozione di requisiti minimi e la standardizzazione delle procedure.
In secondo luogo, rafforzare la resilienza dei settori strategici, quali energia, trasporti, finanza, salute, approvvigionamento idrico e infrastrutture digitali, riconosciuti come essenziali per il funzionamento della società e dell'economia.
In terzo luogo, migliorare la cooperazione tra Stati membri, attraverso la creazione del *Cooperation Group* e del *CSIRT Network*, con l'obiettivo di condividere informazioni, allineare le policy e coordinare la gestione degli incidenti.[55]

La Direttiva NIS costituiva dunque un primo passo significativo verso una governance europea della sicurezza cibernetica più omogenea e strutturata. Tuttavia, l'evoluzione del contesto tecnologico e delle minacce informatiche ha presto evidenziato la necessità di un aggiornamento profondo.[56] [57]

---

[52] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, considerando (1)–(6).
[53] European Commission, *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, pp. 13–15
[54] R. Von Solms, J. Van Niekerk, "From information security to cybersecurity", *Computers & Security*, vol. 38, 2013, pp. 97–102
[55] Direttiva (UE) 2016/1148 (NIS), artt. 1–3
[56] European Commission, *Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises*, Official Journal of the European Union, 2017, pp. 36–58.
[57] A. Boin, P. 't Hart, E. Stern, *The Politics of Crisis Management: Public Leadership under Pressure*, Cambridge University Press, 2016, pp. 8–12

2.2 Evoluzione e contenuti della Direttiva NIS2

Per affrontare le sfide emergenti, il legislatore europeo ha approvato nel 2022 la Direttiva (UE) 2022/2555, nota come NIS2, che sostituisce integralmente la precedente. La revisione nasce dalla consapevolezza che, nonostante i progressi compiuti, la Direttiva NIS presentava limiti strutturali: una copertura insufficiente dei settori soggetti a obblighi, un livello di applicazione disomogeneo tra Stati membri e un quadro sanzionatorio debole rispetto alla gravità delle minacce cyber contemporanee.[58]

La NIS2 amplia significativamente il campo di applicazione, includendo non solo i settori già contemplati dalla NIS, ma anche nuove categorie considerate sempre più interconnesse e critiche. [59] Tra queste, il manifatturiero avanzato, la produzione di dispositivi critici, la gestione dei rifiuti, i servizi postali e di corriere, le infrastrutture spaziali e gran parte della pubblica amministrazione centrale. Viene introdotta, inoltre, una distinzione tra entità essenziali ed entità importanti, basata su criteri dimensionali, di settore e di impatto.

Tra le maggiori innovazioni si segnalano:

- Requisiti di sicurezza più stringenti e armonizzati, che definiscono misure minime obbligatorie per tutti i soggetti rientranti nella Direttiva.
- Un approccio risk-based, che richiede alle organizzazioni di proporzionare le misure di sicurezza al livello di rischio e alla criticità del servizio erogato.
- Il rafforzamento della supply chain security, riconoscendo l'importanza dei fornitori, soprattutto in un contesto di crescente interdipendenza tecnologica.
- La creazione dell'EU-CyCLONe, il network europeo di coordinamento per la gestione delle crisi cyber su larga scala.

La Direttiva NIS2 rappresenta quindi un salto di qualità nella strategia europea di cybersecurity, introducendo norme più coerenti e incisive e ponendo l'accento sulla prevenzione, sulla risposta coordinata e sulla responsabilizzazione del management.[60]

2.3 Obblighi di sicurezza e gestione del rischio

[58] Direttiva (UE) 2022/2555 (NIS2), considerando (5)–(8) e artt. 1–3.
[59] European Union Agency for Cybersecurity (ENISA), *Threat Landscape*, diverse edizioni, sez. Supply Chain Attacks, pp. 42–48
[60] R. Radu, *Negotiating Internet Governance*, Oxford University Press, 2019, pp. 71–78

La NIS2 stabilisce un set di misure tecniche, organizzative e procedurali obbligatorie, che tutte le entità essenziali e importanti devono implementare per garantire un livello elevato di sicurezza delle informazioni.[61] Le misure coprono l'intero ciclo di gestione del rischio e sono concepite per essere proporzionate alla dimensione dell'organizzazione e alla criticità dei servizi erogati. [62]

Sul piano organizzativo, le entità devono predisporre politiche formali di gestione del rischio, piani di gestione degli incidenti e protocolli di business continuity e disaster recovery. Deve inoltre essere prevista una formazione continua del personale in ambito cybersecurity, in modo da mitigare il fattore umano, spesso responsabile di una percentuale significativa degli incidenti informatici. La governance della sicurezza deve essere affidata a figure competenti e chiaramente identificate, con responsabilità dirette nei confronti del top management.

Sul piano tecnico, la Direttiva impone l'adozione di misure quali:

- sistemi di controllo degli accessi e gestione delle identità digitali;
- segmentazione e monitoraggio della rete;
- cifratura dei dati in transito e a riposo;
- gestione delle vulnerabilità, patching e scanning periodico;
- logging e tracciamento degli eventi;
- sicurezza della supply chain, con audit e controlli sui fornitori ICT.

Tali obblighi hanno la finalità di rafforzare la postura di sicurezza delle organizzazioni, ridurre la superficie di attacco e creare un sistema più resiliente e consapevole. [63]

2.4 Obblighi di notifica degli incidenti

Uno degli aspetti maggiormente innovativi della NIS2 riguarda il regime di notifica degli incidenti di sicurezza. [64]La Direttiva introduce tempistiche chiare e molto più stringenti, stabilendo una procedura che si articola in tre fasi principali.[65]

Entro 24 ore dall'individuazione dell'incidente, l'organizzazione deve inviare un'early warning, una comunicazione preliminare volta a segnalare l'evento e a indicare, se noti, gli

[61] Direttiva (UE) 2022/2555 (NIS2), art. 21
[62] T. Aven, *Risk Analysis*, Wiley, 2015, pp. 23–29
[63] B. Schneier, *Data and Goliath*, Norton, 2015, pp. 51–58
[64] Direttiva (UE) 2022/2555 (NIS2), art. 23
[65] ENISA, *CSIRTs in Europe*, 2023, pp. 6–10

elementi sospetti relativi a un'eventuale origine malevola. Questo passaggio ha un ruolo fondamentale nel facilitare l'intervento tempestivo dei CSIRT e nel prevenire potenziali effetti domino.[66]

Entro 72 ore, deve essere trasmessa una notifica dettagliata, contenente informazioni più precise sull'incidente: causa, dinamica, impatti accertati o probabili, e misure adottate per contenerlo. Questo step consente alle autorità competenti di valutare la gravità dell'incidente e di coordinare eventuali risposte a livello nazionale o europeo.

Entro un mese, l'organizzazione deve inoltrare una relazione finale, includendo l'analisi completa dell'accaduto, la valutazione degli impatti definitivi, le azioni correttive intraprese e le misure adottate per evitare il ripetersi dell'evento.[67]

La procedura così articolata mira a migliorare la capacità di risposta, garantire trasparenza e favorire la cooperazione tra soggetti pubblici e privati.

2.5 Responsabilità e regime sanzionatorio

La Direttiva NIS2 attribuisce grande rilevanza alla responsabilità della governance aziendale.[68] I membri del management sono direttamente responsabili dell'approvazione delle politiche di gestione del rischio e dell'adeguatezza delle misure adottate. Tale responsabilizzazione rappresenta un elemento di forte discontinuità rispetto alla Direttiva NIS, sottolineando l'importanza del coinvolgimento dei vertici nelle strategie di cybersecurity.

Il regime sanzionatorio diventa molto più severo. Per le entità essenziali, sono previste sanzioni amministrative fino a 10 milioni di euro o fino al 2% del fatturato globale annuo dell'organizzazione, se superiore. Per le entità importanti, le sanzioni possono arrivare fino a 7 milioni di euro o all'1,4% del fatturato. Inoltre, gli Stati membri possono introdurre misure aggiuntive, come ispezioni, audit obbligatori, ordini correttivi o la sospensione temporanea delle attività.[69]

---

[66] ENISA, *Coordinated Vulnerability Disclosure Policies*, 2022, pp. 11–14
[67] Direttiva (UE) 2022/2555 (NIS2), art. 23, par. 4, lett. d).
[68] Direttiva (UE) 2022/2555 (NIS2), art. 20
[69] N. Kshetri, The emerging role of big data in key development issues: Opportunities, challenges, and concerns, *op. cit.*, 2014, pp. 4–8

L’obiettivo del legislatore europeo è rendere la sicurezza informatica non solo un onere tecnico, ma un obbligo strategico per il vertice aziendale, promuovendo un cambio culturale che riconosca la cybersicurezza come elemento essenziale per il funzionamento e la reputazione delle organizzazioni moderne.[70]

[70] Taleb, N., *Antifragile: Things That Gain from Disorder*, Random House, 2012, pp. 38–44.

3. GLI STANDARD INTERNAZIONALI PER LA GESTIONE DEL RISCHIO INFORMATICO

3.1 La famiglia degli standard ISO/IEC 27001

La crescente dipendenza delle organizzazioni dai sistemi informativi e dai dati digitali ha reso la sicurezza delle informazioni un tema strategico, non più limitato alla sola dimensione tecnica ma esteso a quella organizzativa e gestionale. In questo contesto si inserisce la famiglia degli standard ISO/IEC 27000, sviluppata congiuntamente dall'International Organization for Standardization (ISO) e dall'International Electrotechnical Commission (IEC), con l'obiettivo di fornire un quadro di riferimento organico per la gestione della sicurezza delle informazioni attraverso un Information Security Management System (ISMS).[71]

La serie ISO/IEC 27000 comprende un insieme articolato di standard internazionali che condividono un approccio comune alla gestione dei rischi informativi, basato sui principi di confidenzialità, integrità e disponibilità delle informazioni.
Tali standard costituiscono un vero e proprio "linguaggio comune" per le organizzazioni, favorendo l'adozione di pratiche uniformi e riconoscibili a livello globale nella gestione della sicurezza informatica. [72]

La filosofia di fondo della famiglia ISO/IEC 27000 è analoga a quella di altri sistemi di gestione ISO, come ISO 9001 per la qualità o ISO 14001 per l'ambiente, prevedendo un ciclo di miglioramento continuo (Plan-Do-Check-Act) applicato alla sicurezza delle informazioni. Tale impostazione consente agli standard di adattarsi a organizzazioni di qualsiasi dimensione e settore, rendendoli flessibili rispetto al contesto operativo e al profilo di rischio specifico.

All'interno della famiglia, ISO/IEC 27001 rappresenta lo standard centrale e l'unico certificabile, definendo i requisiti formali per la progettazione, l'implementazione, il mantenimento e il miglioramento continuo di un ISMS.
La versione più recente, ISO/IEC 27001:2022, rafforza l'integrazione tra sicurezza delle informazioni, cybersecurity e protezione della privacy, evidenziando l'evoluzione del panorama delle minacce digitali. [73]

---

[71] ISO/IEC 27000, 27001 and 27002 for Information Security Management
[72] ISO/IEC 27000, 27001 and 27002 for Information Security Management
[73] ISO/IEC 27000, 27001 and 27002 for Information Security Management

Numerosi studi accademici sottolineano come l'adozione della ISO/IEC 27001 non rappresenti esclusivamente un adempimento normativo, ma un vero strumento di governance del rischio, capace di migliorare la resilienza organizzativa e la fiducia degli stakeholder. In particolare, si evidenzia come i benefici della certificazione includano non solo il rafforzamento delle misure di sicurezza, ma anche un impatto positivo sui processi decisionali e sulla cultura aziendale. [74]

Complementare alla ISO/IEC 27001 è lo standard ISO/IEC 27002, che fornisce una guida dettagliata all'implementazione dei controlli di sicurezza elencati nell'Annex A della 27001. L'edizione 2022 di ISO/IEC 27002 ha riorganizzato i controlli in quattro categorie (organizzativi, relativi alle persone, fisici e tecnologici), riducendone il numero complessivo e allineandoli alle moderne esigenze di cybersecurity e cloud security. [75]

L'Annex A non rappresenta una checklist rigida, ma un catalogo di controlli selezionabili in base all'analisi del rischio e formalizzati nello Statement of Applicability (SoA). Questo approccio consente di personalizzare l'ISMS, evitando l'applicazione indiscriminata di misure non proporzionate al contesto organizzativo. Oltre ai principali standard 27001 e 27002, la famiglia ISO/IEC 27000 include numerosi documenti di supporto, tra cui ISO/IEC 27000 (terminologia), ISO/IEC 27005 (gestione del rischio), ISO/IEC 27004 (misurazione dell'efficacia dell'ISMS) e standard verticali dedicati a settori specifici.
Questa articolazione consente di affrontare la sicurezza delle informazioni in modo sistemico, integrando aspetti tecnici, organizzativi e legali. [76]

La forza della famiglia ISO/IEC 27000 risiede proprio nella sua capacità di interoperare con altri framework di sicurezza, come NIST CSF o COBIT, offrendo una struttura formalizzata che facilita la comparabilità e l'audit delle misure adottate. [77]

In conclusione, la famiglia degli standard ISO/IEC 27001 rappresenta uno dei riferimenti più autorevoli e diffusi per la gestione della sicurezza delle informazioni a livello internazionale. La sua adozione consente alle organizzazioni di affrontare in modo strutturato le minacce informatiche, integrando la sicurezza nei processi decisionali e strategici.

---

[74] Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). *The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda*. The TQM Journal, 33(7), pp. 76–105.
[75]ISO/IEC, *ISO/IEC 27000: Information security management systems — Overview and vocabulary*, ISO, 2022/2024.
[76]G. Culot et al., *The ISO/IEC 27001 information security management standard*, op. cit., pp. 76–105.
[77] ISO/IEC 27000, 27001 and 27002 for Information Security Management

La letteratura scientifica concorda nel riconoscere alla serie ISO/IEC 27000 un ruolo chiave non solo nella mitigazione dei rischi, ma anche nel rafforzamento della fiducia, della conformità normativa e della maturità organizzativa in ambito cybersecurity.

3.2 Il sistema di gestione della sicurezza delle informazioni (ISMS)

Il Sistema di Gestione della Sicurezza delle Informazioni (Information Security Management System – ISMS) rappresenta l'insieme strutturato di politiche, procedure, processi e controlli adottati da un'organizzazione per proteggere le informazioni e i sistemi informativi da minacce interne ed esterne. L'ISMS ha come obiettivo principale la tutela della confidenzialità, integrità e disponibilità delle informazioni, principi cardine della sicurezza informatica. [78]

A differenza di un approccio puramente tecnico, l'ISMS si configura come un modello organizzativo e gestionale, che integra aspetti tecnologici, umani e procedurali. Esso non si limita all'implementazione di misure di sicurezza isolate, ma promuove una gestione sistematica e continuativa dei rischi informativi, in linea con gli obiettivi strategici dell'organizzazione. [79]

Un elemento centrale dell'ISMS è l'approccio risk-based, secondo il quale le misure di sicurezza vengono selezionate e implementate sulla base di un'analisi strutturata dei rischi. Tale analisi consente di identificare gli asset informativi, valutare le minacce e le vulnerabilità associate e stimare l'impatto potenziale di eventuali incidenti di sicurezza. In questo modo, le risorse vengono allocate in modo proporzionato, evitando sia carenze di protezione sia l'adozione di misure eccessive o non necessarie. [80]

L'analisi del rischio non rappresenta un'attività statica, ma un processo dinamico che deve essere aggiornato periodicamente, in funzione dell'evoluzione del contesto tecnologico, normativo e organizzativo. Questo consente all'ISMS di adattarsi ai cambiamenti e di mantenere un adeguato livello di sicurezza nel tempo.[81]

All'interno dell'ISMS rivestono un ruolo fondamentale le politiche di sicurezza, che definiscono le regole, i principi e le responsabilità per la gestione delle informazioni. Tali politiche devono essere formalizzate, comunicate a tutto il personale e supportate da

[78]G. Culot et al., *The ISO/IEC 27001 information security management standard*, op. cit., pp. 76–105.
[79] G. Culot et al., *The ISO/IEC 27001 information security management standard*, op. cit., pp. 76–105.
[80] ISO/IEC 27001:2022, Clause 6; Junaid, 2022, pp. 5–6
[81] G. Culot et al., *The ISO/IEC 27001 information security management standard*, op. cit., pp. 76–105.

procedure operative chiare. La consapevolezza e la formazione degli utenti costituiscono infatti un fattore critico, considerando che il fattore umano rappresenta una delle principali fonti di rischio per la sicurezza informatica. [82]

L'ISMS prevede inoltre l'adozione di processi di monitoraggio e controllo, finalizzati a verificare l'efficacia delle misure implementate e a individuare eventuali non conformità. In caso di incidenti di sicurezza, il sistema deve consentire una gestione strutturata degli eventi, includendo attività di risposta, ripristino e analisi delle cause. [83]

Un ulteriore aspetto importante dell'ISMS è il principio del miglioramento continuo, generalmente ispirato al ciclo Plan-Do-Check-Act (PDCA). Attraverso questo modello, l'organizzazione pianifica le misure di sicurezza, le implementa, ne verifica l'efficacia e adotta eventuali azioni correttive. Tale approccio permette di rafforzare progressivamente il livello di protezione delle informazioni e di accrescere la maturità della sicurezza informatica nel tempo. [84]

L'adozione di un ISMS non ha soltanto una valenza tecnica o di conformità normativa, ma rappresenta un vero e proprio strumento strategico per l'organizzazione. Un sistema di gestione efficace contribuisce a ridurre il rischio di incidenti informatici, a minimizzare l'impatto economico e reputazionale delle violazioni di sicurezza e a rafforzare la fiducia di clienti, partner e stakeholder. [85]

In conclusione, il sistema di gestione della sicurezza delle informazioni costituisce il fondamento di un approccio strutturato alla cybersecurity, in grado di integrare la sicurezza nei processi decisionali e operativi dell'organizzazione e di rispondere in modo coerente alle crescenti sfide del panorama digitale contemporaneo.

3.3 Il processo di gestione del rischio secondo ISO/IEC 27005

La gestione del rischio rappresenta uno degli elementi centrali del Sistema di Gestione della Sicurezza delle Informazioni (ISMS) e costituisce il fondamento metodologico su cui si basa l'intera famiglia degli standard ISO/IEC 27000. In particolare, lo standard ISO/IEC 27005

[82] G. Culot et al., *The ISO/IEC 27001 information security management standard*, op. cit., pp. 76–105.
[83] ISO/IEC 27001:2022, Clauses 9–10
[84] G. Culot et al., *The ISO/IEC 27001 information security management standard*, op. cit., pp. 88–90.
[85] G. Culot et al., *The ISO/IEC 27001 information security management standard*, op. cit., pp. 92–94.

fornisce una guida strutturata e sistematica alla gestione del rischio per la sicurezza delle informazioni, supportando l'implementazione dei requisiti definiti dalla ISO/IEC 27001.

Secondo la definizione fornita dalla norma, la gestione del rischio è un *processo coordinato volto a dirigere e controllare un'organizzazione in relazione ai rischi*.[86] Lo standard non introduce requisiti certificabili, ma propone un framework metodologico flessibile, adattabile a differenti contesti organizzativi, dimensioni e settori.

ISO/IEC 27005 si allinea ai principi generali della gestione del rischio definiti dalla ISO 31000, mantenendo però un focus specifico sulla sicurezza delle informazioni. Il rischio viene inteso come il risultato della combinazione tra probabilità di accadimento di un evento e impatto sulle informazioni e sui processi aziendali. [87]

Lo standard adotta un approccio pragmatico e orientato al business, in cui la sicurezza non è fine a sé stessa ma strumentale al raggiungimento degli obiettivi organizzativi. [88]

Tra i principi fondamentali del processo di gestione del rischio rientrano: l'integrazione con i processi decisionali aziendali, la documentazione e la tracciabilità delle decisioni, il miglioramento continuo il coinvolgimento degli stakeholder rilevanti.

ISO/IEC 27005 struttura il processo di gestione del rischio in una sequenza di fasi logicamente interconnesse, come illustrato nello schema normativo.[89]

La prima fase del processo riguarda la definizione del contesto interno ed esterno all'organizzazione, inclusi: obiettivi di business, requisiti normativi e contrattuali, ambito dell'ISMS, criteri di accettazione del rischio. Una definizione inaccurata del contesto è una delle principali cause di inefficacia delle analisi del rischio, poiché porta a valutazioni non coerenti con le reali priorità aziendali.[90]

Successivamente si procede con l'identificazione del rischio, fase nella quale vengono identificati: gli asset informativi (dati, sistemi, persone, processi), le minacce potenziali, le vulnerabilità associate, gli eventi indesiderati possibili. ISO/IEC 27005 sottolinea che l'identificazione deve essere sufficientemente dettagliata da consentire una valutazione

[86] ISO/IEC 27005:2018, ISO, Ginevra, p. 6
[87] ISO/IEC 27005:2018, ISO, p. 8
[88] Humphreys, *Information Security Management Standards: Compliance, Governance and Risk Management*, BSI Press, 2008, p. 114
[89] ISO/IEC 27005:2018, ISO, pp. 10–19
[90] Peltier, *Information Security Risk Analysis*, Auerbach Publications, 2016, p. 57

efficace, ma proporzionata al contesto organizzativo.[91] La letteratura evidenzia come un inventario incompleto degli asset rappresenti uno dei limiti più frequenti nei sistemi di gestione del rischio.

L'analisi del rischio, ovvero la terza fase del processo, consiste nella determinazione della probabilità di accadimento e dell'impatto delle minacce identificate, utilizzando approcci qualitativi, quantitativi o ibridi. La norma non prescrive una metodologia specifica, lasciando all'organizzazione la libertà di adottare modelli coerenti con il proprio livello di maturità.[92]

L'adozione di scale qualitative ben definite consente una maggiore comprensione del rischio da parte del management, facilitando il processo decisionale.[93]

I risultati dell'analisi vengono poi esaminati nella fase di valutazione del rischio. Questa fase ha lo scopo di confrontare i risultati dell'analisi con i criteri di rischio definiti in precedenza, al fine di stabilire quali rischi siano accettabili e quali richiedano un trattamento. Questa fase rappresenta un momento critico di sintesi e supporto alle decisioni strategiche. [94]

La valutazione del rischio consente di tradurre risultati tecnici in informazioni comprensibili per il top management, favorendo l'allineamento tra sicurezza e governance. [95]

Il processo continua con il trattamento del rischio può avvenire attraverso diverse opzioni: mitigazione tramite l'implementazione di controlli, accettazione del rischio, trasferimento (ad es. tramite assicurazioni), eliminazione del rischio. ISO/IEC 27005 collega direttamente questa fase alla selezione dei controlli dell'Annex A della ISO/IEC 27001, garantendo coerenza tra analisi del rischio e misure adottate.[96]

La norma evidenzia anche l'importanza della comunicazione continua del rischio tra le diverse parti interessate, al fine di garantire trasparenza, consapevolezza e responsabilità condivisa.

---

[91] ISO/IEC 27005:2018, ISO, p. 13
[92] ISO/IEC 27005:2018, ISO, p. 15.
[93] Stoneburner et al., *Risk Management Guide for Information Technology Systems*, NIST SP 800‑30, U.S. Government Printing Office, 2012, p. 21
[94] ISO/IEC 27005:2018, ISO, p. 17
[95] Dionne, *Risk Management: History, Current State, and Future Prospects*, Springer, 2013, p. 94
[96] ISO/IEC 27005:2018, ISO, p. 19

Il processo di gestione del rischio è di natura ciclica e richiede un monitoraggio costante per tener conto di cambiamenti tecnologici, organizzativi o normativi. Tale fase è strettamente connessa al principio del miglioramento continuo dell'ISMS. [97]

Nel contesto dell'ISMS, ISO/IEC 27005 svolge una funzione di supporto metodologico, assicurando che le decisioni relative alla sicurezza delle informazioni siano basate su una valutazione razionale e documentata dei rischi. La letteratura scientifica concorda nel riconoscere a questo standard un ruolo chiave nel rafforzare la coerenza, la ripetibilità e la trasparenza del processo decisionale in ambito cybersecurity. [98]

In conclusione, il modello proposto da ISO/IEC 27005 consente alle organizzazioni di integrare la gestione del rischio nel governo complessivo della sicurezza delle informazioni, trasformando la cybersecurity da funzione puramente tecnica a componente strategica della governance aziendale.

3.4 Controlli di sicurezza e best practice

I controlli di sicurezza rappresentano l'elemento operativo attraverso il quale le organizzazioni traducono i risultati del processo di gestione del rischio in misure concrete di protezione delle informazioni. Nell'ambito della famiglia ISO/IEC 27000, i controlli di sicurezza trovano il loro principale riferimento nello standard ISO/IEC 27002, che fornisce linee guida dettagliate per l'implementazione delle misure elencate nell'Annex A della ISO/IEC 27001. Tali controlli non devono essere interpretati come requisiti obbligatori da applicare indiscriminatamente, ma come un insieme di best practice selezionabili e adattabili in funzione del profilo di rischio dell'organizzazione.

La versione più recente dello standard, ISO/IEC 27002:2022, riflette l'evoluzione del panorama delle minacce informatiche e delle tecnologie digitali, ponendo maggiore enfasi su aspetti quali la sicurezza del cloud, la protezione delle informazioni lungo l'intero ciclo di vita e l'integrazione tra sicurezza delle informazioni, cybersecurity e privacy. Come indicato

[97] Humphreys, *Information Security Management Standards: Compliance, Governance and Risk Management*, op. cit. , pp. 121
[98] G. Culot et al., *The ISO/IEC 27001 information security management standard*, op. cit., pp. 76–105.

dalla norma, l'obiettivo dei controlli non è soltanto la prevenzione degli incidenti, ma anche la riduzione dell'impatto e il miglioramento della capacità di risposta dell'organizzazione. [99]

Un elemento qualificante dell'approccio proposto dagli standard ISO è la stretta relazione tra controlli di sicurezza e analisi del rischio. I controlli devono essere selezionati sulla base dei rischi identificati e valutati secondo ISO/IEC 27005, assicurando che le misure adottate siano proporzionate e coerenti con il contesto organizzativo. Tale relazione viene formalizzata attraverso lo Statement of Applicability (SoA), documento che esplicita quali controlli sono stati adottati, quali esclusi e per quali motivazioni. Secondo Humphreys, il SoA svolge una funzione essenziale di trasparenza e tracciabilità, rendendo evidente il legame tra decisioni strategiche, rischio e misure di sicurezza implementate. [100]

Dal punto di vista concettuale, i controlli di sicurezza coprono un ampio spettro di ambiti, includendo misure di natura organizzativa, procedurale, tecnica e fisica. Oltre agli aspetti tecnologici, la norma attribuisce particolare rilevanza alle politiche di sicurezza, alla definizione di ruoli e responsabilità e alla gestione delle risorse umane. La letteratura sottolinea come una parte significativa degli incidenti di sicurezza sia riconducibile a fattori organizzativi e comportamentali piuttosto che a vulnerabilità tecnologiche in senso stretto. In questo senso, l'adozione di controlli volti a promuovere la consapevolezza del personale e una cultura della sicurezza diffusa rappresenta una best practice fondamentale.[101]

Un ulteriore aspetto centrale riguarda i controlli relativi alla gestione degli accessi e alla protezione delle informazioni. ISO/IEC 27002 enfatizza la necessità di garantire che l'accesso alle informazioni sia consentito esclusivamente a soggetti autorizzati, in base al principio del minimo privilegio. Tali controlli contribuiscono in modo diretto alla tutela della confidenzialità e dell'integrità dei dati, riducendo il rischio di accessi non autorizzati o di abusi interni. [102]

I controlli tecnologici, pur mantenendo un ruolo cruciale, vengono inquadrati all'interno di una visione più ampia di governance della sicurezza. La norma evidenzia come strumenti quali la crittografia, il logging, il monitoraggio continuo e la gestione delle vulnerabilità debbano essere supportati da processi chiari e da responsabilità definite, al fine di garantirne

[99] ISO/IEC 27002:2022, ISO, pp. 1–3.
[100] Humphreys, *Information Security Management Standards*, BSI Press, op. cit., pp. 137
[101] M. Siponen, R. Willison, *Information Security Management Standards: Problem and Solutions,* in Systems Journal, Wiley, 2009, pp. 186
[102] ISO/IEC 27002:2022, ISO, pp. 32–35.

l'efficacia nel tempo. L'implementazione di strumenti avanzati senza un adeguato supporto organizzativo rischia di produrre una falsa percezione di sicurezza. [103]

Le best practice proposte dalla ISO/IEC 27002 includono inoltre la gestione strutturata degli incidenti di sicurezza, che deve prevedere attività di rilevazione, risposta, ripristino e analisi post-evento. La capacità di apprendere dagli incidenti e di aggiornare di conseguenza i controlli di sicurezza rappresenta un elemento chiave del miglioramento continuo dell'ISMS. Secondo la norma, la gestione degli incidenti non deve essere considerata un'attività straordinaria, ma parte integrante del sistema di gestione della sicurezza delle informazioni. [104]

In conclusione, i controlli di sicurezza e le best practice delineate dagli standard ISO/IEC 27001 e 27002 costituiscono il livello operativo attraverso cui l'organizzazione rende effettiva la propria strategia di gestione del rischio informatico. L'approccio risk-based e la flessibilità nella selezione dei controlli consentono di adattare l'ISMS a contesti organizzativi diversi, evitando soluzioni standardizzate e poco efficaci. La letteratura concorda nel riconoscere che l'efficacia dei controlli di sicurezza dipende non solo dalla loro corretta implementazione tecnica, ma soprattutto dalla loro integrazione nei processi decisionali, organizzativi e culturali dell'organizzazione.

3.5 Implementazione degli standard nelle organizzazioni

L'implementazione degli standard della famiglia ISO/IEC 27000 nelle organizzazioni rappresenta un processo complesso che va ben oltre la semplice adozione formale di procedure o la ricerca della certificazione. Essa richiede un cambiamento strutturato nel modo in cui l'organizzazione governa la sicurezza delle informazioni, integrandola nei processi decisionali, operativi e strategici. Numerosi studi evidenziano come il successo dell'implementazione dipenda principalmente dal grado di allineamento tra l'ISMS e gli obiettivi di business, piuttosto che dalla mera conformità ai requisiti normativi. [105]

Un fattore critico per una corretta implementazione riguarda il coinvolgimento del top management. ISO/IEC 27001 attribuisce alla leadership un ruolo centrale nel definire le

[103] P. W. Singer, A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, New York, 2014. , p. 74
[104] ISO/IEC 27002:2022, ISO, pp. 53–56.
[105] Humphreys, *Information Security Management Standards*, op. cit., pp. 148

politiche di sicurezza, allocare le risorse e promuovere una cultura organizzativa orientata alla gestione del rischio. Come sottolineato da Disterer, la sicurezza delle informazioni diventa efficace solo quando è riconosciuta come una responsabilità manageriale e non esclusivamente tecnica. In assenza di un chiaro supporto direzionale, l'ISMS rischia di rimanere un sistema formale, non realmente integrato nelle attività quotidiane.

L'implementazione pratica degli standard ISO/IEC 27001 e 27002 richiede inoltre un'attenta personalizzazione delle misure di sicurezza. Il principio risk‑based impone che i controlli non vengano applicati in modo uniforme, ma selezionati e adattati in funzione del contesto organizzativo, del settore di appartenenza e del profilo di rischio. Studi empirici dimostrano che le organizzazioni che adottano un approccio "one‑size‑fits‑all" tendono a ottenere benefici limitati dalla certificazione, mentre quelle che integrano l'ISMS nei propri processi mostrano un miglioramento significativo della resilienza operativa. [106]

Un altro aspetto rilevante riguarda l'impatto organizzativo e culturale dell'implementazione degli standard. La sicurezza delle informazioni incide direttamente sui comportamenti degli individui, richiedendo formazione continua, sensibilizzazione e definizione chiara delle responsabilità. La resistenza al cambiamento e la sottovalutazione del fattore umano rappresentano tra le principali criticità nell'adozione degli ISMS, soprattutto nelle organizzazioni di grandi dimensioni.[107] La diffusione di una cultura della sicurezza è quindi una condizione essenziale per rendere effettive le misure tecniche e procedurali.

Dal punto di vista operativo, l'implementazione degli standard comporta spesso la necessità di integrare l'ISMS con altri framework e normative, come il NIST Cybersecurity Framework, il GDPR o sistemi di gestione già esistenti (ISO 9001, ISO 14001). Questa integrazione consente di evitare duplicazioni, ridurre i costi e favorire una visione unitaria della governance del rischio. La compatibilità della ISO/IEC 27001 con altri modelli di governance costituisce uno dei principali fattori della sua diffusione a livello internazionale.

Le difficoltà di implementazione variano significativamente in base alle dimensioni e alla maturità organizzativa. Le piccole e medie imprese, pur riconoscendo i benefici della certificazione, incontrano spesso ostacoli legati alla limitata disponibilità di risorse economiche e competenze specialistiche. In questi contesti, la letteratura suggerisce un

[106] G. Culot et al., *The ISO/IEC 27001 information security management standard*, op. cit., pp. 76–105.
[107] M. T. Siponen, R. Willison, *Information Security Management Standards: Problems and Solutions*, op. cit., pp. 267–270.

approccio graduale, focalizzato sui rischi più critici e su un insieme essenziale di controlli, piuttosto che un'implementazione completa e immediata dello standard.[108]

Infine, l'implementazione degli standard ISO/IEC 27000 deve essere considerata un processo dinamico e continuo, piuttosto che un progetto a termine. Il mantenimento dell'ISMS richiede attività costanti di monitoraggio, audit interni e riesame della direzione, al fine di garantire che il sistema rimanga efficace rispetto all'evoluzione delle minacce e del contesto normativo. Come evidenziato dalla norma stessa, la certificazione non rappresenta un punto di arrivo, ma una tappa all'interno di un percorso di miglioramento continuo della sicurezza delle informazioni. [109]

In conclusione, l'implementazione degli standard internazionali per la sicurezza delle informazioni costituisce una leva strategica per rafforzare la governance del rischio informatico e la resilienza organizzativa. Quando correttamente integrati nei processi e nella cultura aziendale, gli standard ISO/IEC 27000 consentono alle organizzazioni di affrontare le minacce digitali in modo sistematico, migliorando al contempo la fiducia degli stakeholder e la capacità di conformarsi a un quadro normativo sempre più stringente.

[108] T.R. Peltier, *Information Security Risk Analysis*, Auerbach Publications, 2010, p. 213
[109] ISO/IEC 27001:2022, ISO, pp. 7–9

4. OBBLIGHI DI SICUREZZA E PROCESSO PENALE

4.1 Gli incidenti informatici tra sicurezza, normativa europea e diritto penale

Nel contesto della sicurezza informatica contemporanea, l'incidente cyber non può più essere ricondotto a una mera problematica tecnica o organizzativa. Esso assume una dimensione giuridica complessa, coinvolgendo il diritto amministrativo, il diritto civile e, con crescente intensità, il diritto penale. L'evoluzione tecnologica e la progressiva digitalizzazione delle attività economiche e sociali hanno infatti modificato profondamente le modalità di aggressione ai beni giuridici, imponendo una riflessione sull'adeguatezza delle categorie penalistiche tradizionali e sugli strumenti più efficaci per garantire una tutela effettiva nel cyberspazio.[110]

Le innovazioni tecnologiche, se da un lato rappresentano un fattore di sviluppo e di semplificazione delle attività umane, dall'altro ampliano le opportunità operative degli autori di reato, consentendo la realizzazione di condotte illecite sempre più sofisticate e difficilmente riconducibili agli schemi tradizionali di accertamento. In tale scenario, il diritto penale è chiamato a confrontarsi con fenomeni caratterizzati da elevata complessità tecnica, dimensione transnazionale e rapidità esecutiva, che rendono insufficiente una tutela esclusivamente fondata sulla repressione successiva alla consumazione del fatto. [111]

Lo sviluppo tecnologico ha progressivamente esteso l'area del penalmente rilevante, rendendo necessaria una rilettura delle categorie della responsabilità penale e dell'offesa al bene giuridico alla luce delle peculiarità dell'ambiente digitale. L'incidente informatico, in questa prospettiva, può assumere una duplice rilevanza: da un lato costituisce l'evento lesivo di una fattispecie incriminatrice; dall'altro rappresenta il presupposto per l'attivazione di obblighi di intervento da parte delle autorità competenti e dei meccanismi di prevenzione, gestione e repressione previsti dall'ordinamento. [112]

In questo contesto, assume particolare rilievo il progressivo spostamento del baricentro della tutela penale dalla sola repressione alla prevenzione del rischio. Il cyberspazio, per la sua natura decentralizzata, interconnessa e transnazionale, mette infatti in crisi i presupposti sui quali si è tradizionalmente fondato il paradigma penalistico. La sequenza classica che collega

---

[110] F. Delaini, *Verso un diritto penale della sicurezza digitale? La cyber-compliance del Regolamento DORA*, in *Rivista italiana di informatica e diritto*, anno VIII, n. 1, 2026, pp. 1-2, DOI: 10.32091/RIID0269.
[111] Delaini, *Verso un diritto penale della sicurezza digitale?*, cit., p. 3.
[112] F. Mantovani, *Diritto penale. Parte generale*, Cedam, Padova, 2025, XII ed. pp. 89-95 .

fatto, accertamento e sanzione risulta difficilmente applicabile ai cyber-attacchi, i quali si sviluppano nell'arco di pochi millisecondi, possono attraversare simultaneamente una pluralità di ordinamenti giuridici e produrre effetti lesivi prima ancora di essere individuati o attribuiti ai rispettivi autori. La velocità di propagazione delle minacce informatiche e la difficoltà di identificarne con certezza origine e responsabili riducono sensibilmente l'efficacia di un modello di intervento esclusivamente reattivo.[113]

Ne consegue che la funzione preventiva assume un ruolo sempre più centrale nella tutela dei beni giuridici digitali. La sicurezza informatica non rappresenta più soltanto un insieme di misure tecniche o organizzative, ma diviene uno strumento di prevenzione giuridicamente rilevante, capace di ridurre la probabilità che il rischio si trasformi in danno. In tale prospettiva, il diritto penale è chiamato a dialogare con modelli regolatori fondati sulla gestione del rischio, sulla resilienza organizzativa e sull'adozione di adeguati presidi di sicurezza, valorizzando una logica di anticipazione della tutela rispetto alla verificazione dell'evento lesivo.

Il legislatore italiano ha iniziato a intervenire in materia di cybersicurezza già a partire dai primi anni Duemila, nella consapevolezza della necessità di predisporre strumenti idonei a tutelare le infrastrutture strategiche e i cittadini dalle crescenti minacce informatiche. In questa fase iniziale, l'attenzione normativa si è concentrata prevalentemente sul settore pubblico e sulla protezione delle amministrazioni statali. Tale scelta si è rivelata particolarmente lungimirante alla luce dell'evoluzione dello scenario delle minacce: secondo la più recente relazione dell'Agenzia per la cybersicurezza nazionale, infatti, il settore pubblico è risultato tra quelli maggiormente colpiti dagli attacchi informatici registrati nel 2023. Nel 2025, invece, in Italia vi è stato un aumento significativo di aziende in cassa d’integrazione a causa di attacchi ransomware che hanno compromesso la continuità dell’azienda.[114]

Tale evoluzione si inserisce nel più ampio processo di giuridicizzazione del rischio informatico promosso anche dal legislatore europeo. Attraverso strumenti normativi quali la direttiva NIS 2 e il Regolamento DORA, l'attenzione si sposta progressivamente dalla mera repressione dell'illecito alla costruzione di sistemi organizzativi idonei a prevenire gli

[113] Delaini, *Verso un diritto penale della sicurezza digitale?*, cit., pp. 4
[114] F. Casarosa, *L'armonizzazione degli obblighi di notifica: il DDL Cybersicurezza verso la NIS 2*, in *Rivista italiana di informatica e diritto*, anno VI, n. 1, 2024, p. 1, DOI: 10.32091/RIID0146.

incidenti cyber e a garantirne una gestione tempestiva. In questo quadro, la cyber-compliance assume una funzione che trascende la dimensione amministrativa, incidendo anche sulla valutazione delle responsabilità e contribuendo alla definizione di un modello di tutela nel quale prevenzione e repressione operano in modo complementare.[115]

L'emersione di obblighi di governance, gestione del rischio, continuità operativa e notifica degli incidenti testimonia, infatti, una trasformazione della tecnica di tutela, orientata non soltanto alla punizione del fatto illecito, ma anche alla responsabilizzazione preventiva degli operatori. Si delinea così un modello che, pur senza sostituire il diritto penale tradizionale, ne integra la funzione mediante strumenti organizzativi e misure di sicurezza volti a rafforzare la resilienza digitale dei soggetti esposti alle minacce informatiche.

In questa prospettiva, appare sempre più evidente come la tutela dei beni giuridici nel cyberspazio non può più essere affidata esclusivamente alla sanzione successiva al verificarsi dell'offesa, ma richiede un sistema integrato nel quale sicurezza informatica, gestione del rischio e compliance normativa costituiscano elementi essenziali di una strategia complessiva di protezione. È in tale direzione che si colloca il dibattito sul possibile sviluppo di un diritto penale della sicurezza digitale, nel quale la funzione preventiva affianca quella repressiva, adattando gli strumenti penalistici alle caratteristiche del cyberspazio. [116]

4.2 Obblighi di notifica per la gestione del rischio e emersione della notizia di reato

Gli obblighi di gestione del rischio informatico introdotti dalla Direttiva NIS2, assumono un rilievo particolare nella fase di emersione della notitia criminis. La direttiva ha ampliato il proprio ambito di applicazione a 100.000 organizzazioni, tra cui enti pubblici, infrastrutture critiche e fornitori di servizi digitali. Tra tali obblighi rientrano l'adozione di sistemi di monitoraggio, la registrazione degli eventi attraverso strumenti di *logging* e la tempestiva comunicazione degli incidenti rilevanti alle autorità competenti. L'attuazione di tali misure comporta la raccolta e conservazione di informazioni tecniche strutturate, le quali possono assumere rilievo nell'accertamento di eventuali condotte penalmente rilevanti, sia sotto il profilo della responsabilità degli organi apicali, sia in relazione all'inosservanza degli obblighi previsti dalla normativa, comportando sanzioni fino a dieci milioni di euro, o al 2%

[115] P. G. Chiara, *DDL Cybersicurezza: tra l'inasprimento della risposta penale del legislatore nazionale e il modello preventivo-amministrativo della direttiva NIS2*. pp.33.
[116] P. G. Chiara, *DDL Cybersicurezza,*, op. cit., p. 34.

di fatturato globale. In questo scenario la conformità alla disciplina NIS 2 non costituisce solo un obbligo burocratico, ma una priorità assoluta per la protezione dell'organizzazione. [117] La direttiva introduce obblighi stringenti nei confronti di un'ampia platea di soggetti, imponendo l'adozione di adeguate misure di sicurezza informatica e la tempestiva notifica degli incidenti rilevanti. Tale disciplina mira a conseguire un livello più elevato di protezione delle informazioni, rafforzando la sicurezza digitale tanto nel settore privato quanto nell'ambito delle amministrazioni pubbliche. [118]

L'obbligo di notifica degli incidenti costituisce uno degli elementi centrali della Direttiva ed è disciplinato all'articolo 23. La direttiva prevede che i soggetti essenziali e rilevanti notifichino gli incidenti significativi al CSIRT o all'autorità competente con una procedura articolata in più fasi. [119] La notifica degli incidenti prevista dalla NIS2 si colloca dunque in una zona di confine tra prevenzione amministrativa e repressione penale. Pur non costituendo un atto processuale in senso stretto, essa produce effetti indiretti sull'attività investigativa, anticipando spesso l'intervento delle autorità rispetto ai modelli tradizionali di scoperta del reato. In questo contesto, la dimensione temporale assume un ruolo centrale: la rapidità della notifica può tradursi in un'attivazione più tempestiva degli strumenti investigativi, con conseguenze rilevanti anche sul piano della conservazione delle prove digitali. [120]

D'altra parte però questo sistema di notifica e in generale di comunicazione, sia esterna che interna all'organizzazione, rendono l'organizzazione un luogo privilegiato di individuazione del fatto penalmente rilevante. Ne deriva un cambiamento nella fisionomia della notitia criminis, che tende sempre meno a provenire da segnalazioni esterne e sempre più a originarsi all'interno dei sistemi di controllo dell'ente. [121] Ciò solleva questioni delicate sul confine tra attività di compliance, autodifesa organizzativa e collaborazione con l'autorità giudiziaria. In questa prospettiva, gli obblighi di sicurezza e di rilevazione degli incidenti contribuiscono a rendere più frequente l'emersione di fatti penalmente rilevanti. L'ente si trova in una posizione ambivalente: da un lato è tenuto a documentare accuratamente

---

[117] G. Comandè, C. Nasi, *Oltre la Conformità: dalle scelte strategiche ISO e NIST 2.0 alla gestione proattiva del rischio*, in *Rivista italiana di informatica e diritto*, anno VIII, n. 1, 2026, p. 26, DOI: 10.32091/RIID0268.
[118] G. Comandè, C. Nasi, *Oltre la Conformità: dalle scelte strategiche ISO e NIST 2.0 alla gestione proattiva del rischio*, op. cit., p.16.
[119] P. G. Chiara, *DDL Cybersicurezza: tra l'inasprimento della risposta penale del legislatore nazionale e il modello preventivo-amministrativo della direttiva NIS2*, in *Rivista italiana di informatica e diritto*, anno VI, n. 1, 2024, pp. 2-3, DOI: 10.32091/RIID0147.
[120] F. Delaini, *Verso un diritto penale della sicurezza digitale? La cyber-compliance del Regolamento DORA*, op.cit., pp. 18-21.
[121] F. Casarosa, *L'armonizzazione degli obblighi di notifica: il DDL Cybersicurezza verso la NIS 2*, cit., p. 15.

l'incidente per adempiere agli obblighi normativi; dall'altro, tale documentazione può costituire il presupposto per l'avvio di procedimenti penali nei suoi confronti o nei confronti dei soggetti apicali. [122]

4.3 La prova digitale e la sua acquisizione

Una volta avviate le indagini preliminari, l'incidente informatico diventa oggetto di accertamento penale attraverso l'acquisizione della prova digitale. Come evidenziato dalla dottrina processuale e dalla giurisprudenza di legittimità, la prova informatica presenta caratteristiche peculiari, legate in particolare alla sua volatilità, alla facile replicabilità e alla forte dipendenza dal contesto tecnico nel quale viene prodotta. L'ordinamento italiano ha iniziato a disciplinare il fenomeno della criminalità informatica e delle relative attività investigative attraverso la legge n. 547/1993, che ha introdotto le prime disposizioni in materia di reati informatici. Successivamente, il quadro normativo nazionale è stato integrato mediante la ratifica della Convenzione di Budapest del 2001, avvenuta con la legge n. 48/2008, che ha fornito principi comuni per il contrasto al cybercrime e per la gestione della prova digitale, ponendo particolare attenzione alla conservazione dell'integrità del dato e alla corretta documentazione delle operazioni investigative attraverso la catena di custodia. Nonostante l'assenza, nell'ordinamento italiano, di protocolli operativi completamente uniformi per lo svolgimento delle attività di informatica forense, la comunità scientifica e gli operatori del settore fanno riferimento a standard internazionali, tra cui la RFC 3227, al fine di garantire metodologie condivise per l'identificazione, acquisizione, conservazione e analisi delle evidenze digitali. L'analisi forense di strumenti digitali presenta numerose difficoltà, determinate dalla continua evoluzione tecnologica, dalla molteplicità dei sistemi operativi e delle architetture hardware, nonché dai meccanismi di protezione e cifratura dei dati. Parallelamente, lo sviluppo dell'intelligenza artificiale e delle tecniche di data analysis offre nuove possibilità nell'ambito dell'investigazione digitale, consentendo di elaborare grandi quantità di informazioni e individuare schemi complessi. Tuttavia, la crescente sofisticazione delle minacce informatiche e delle tecniche utilizzate dagli autori dei reati rende sempre più complesso il lavoro degli esperti forensi. Nel panorama attuale, le problematiche dell'informatica forense non riguardano esclusivamente gli aspetti tecnologici, ma

[122] F. Delaini, *Verso un diritto penale della sicurezza digitale? La cyber-compliance del Regolamento DORA*, op.cit., pp. 18-21.

coinvolgono anche profili giuridici legati alla trasparenza delle procedure, alla verificabilità delle metodologie utilizzate e alla corretta conservazione delle evidenze digitali. In particolare, il limitato coinvolgimento dello specialista forense in alcune fasi dell'attività investigativa può generare criticità rispetto al bilanciamento tra esigenze di accertamento penale e garanzie di affidabilità scientifica della prova.[123]

Come altre discipline forensi, quali la medicina legale o la balistica, essa nasce come strumento ausiliario dell'accertamento penale, assumendo tuttavia nel tempo un ruolo sempre più centrale, fino a divenire oggi una componente essenziale nella maggior parte delle indagini caratterizzate dalla presenza di elementi digitali.

La prova informatica può essere intesa come "la rappresentazione di dati e informazioni digitali riconducibili a un determinato fatto o evento, espressi attraverso un linguaggio tecnico che non risulta immediatamente percepibile o interpretabile dall'uomo"[124]. I sistemi informatici, infatti, elaborano e conservano le informazioni mediante un codice binario basato sulla combinazione di valori numerici (0 e 1), il cui contenuto può essere reso comprensibile soltanto attraverso specifici strumenti hardware e software. [125]

La raccolta delle evidenze digitali e l'identificazione del responsabile della condotta illecita possono risultare particolarmente complesse, poiché le tracce informatiche possono essere occultate, modificate o eliminate. Inoltre, gli autori degli attacchi possono adottare specifiche tecniche volte a nascondere la propria identità e a rendere più difficoltosa la loro individuazione da parte degli investigatori.[126] La polizia giudiziaria è chiamata a individuare e valutare le cosiddette "tracce elettroniche", identificando i dispositivi e i sistemi informatici potenzialmente collegati al reato. [127] L'attività investigativa deve quindi garantire il corretto recupero e la preservazione delle fonti digitali fino alla successiva fase di analisi tecnica, soprattutto nei casi in cui gli accertamenti non possano essere effettuati direttamente nel luogo dell'intervento.

---

[123] G. Verde, *Il percorso della prova digitale nelle attività di Digital Forensics, una review*, in *i-lex – Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, vol. 18, n. 1, 2025, DOI: 10.6092/issn.1825-1927/21507, pp. 49.
[124] L. Luparia, G. Ziccardi, Investigazione penale e tecnologia informatica, Giuffrè, Milano, 2007, pp. 128.
[125] G. Verde, *Il percorso della prova digitale nelle attività di Digital Forensics, una review*, cit., p. 50.
[126] G. Bragò, L'ispezione e la perquisizione di dati, informazioni e programmi informatici, in L. Luparia, Sistema e criminalità informatica, Giuffrè, Milano, 2009, pp.181-196.
[127] L. Cuomo, *La prova digitale*, in G. Canzio - L. Luparia (a cura di), *Prova scientifica e processo penale*, CEDAM, 2017, p.623.

Una peculiarità della prova digitale consiste nella possibilità di effettuare copie esatte dei dati attraverso procedure di duplicazione bit to bit, ottenendo una copia-clone perfettamente corrispondente all'originale sotto il profilo informatico. A differenza delle prove materiali tradizionali, infatti, il duplicato digitale non presenta differenze rilevabili rispetto al dato originario, purché siano rispettate adeguate procedure di acquisizione e verifica dell'integrità.[128]

Proprio per tale ragione, la fase di acquisizione della prova digitale rappresenta un momento particolarmente delicato, poiché un'operazione eseguita senza adeguate competenze tecniche e metodologiche può compromettere l'integrità del dato originario oppure produrre una copia non perfettamente corrispondente alla fonte acquisita. Tali alterazioni possono determinare la perdita dell'utilizzabilità processuale dell'informazione digitale, compromettendone il valore probatorio.[129]

Per questo motivo, la corretta gestione della catena di custodia assume un ruolo fondamentale sin dalle prime attività investigative, a partire dall'accesso alla scena del crimine e dall'individuazione dei dispositivi informatici potenzialmente coinvolti. Tale esigenza riguarda non solo i reati informatici in senso stretto, ma anche quei fenomeni criminosi nei quali gli strumenti digitali vengono utilizzati come mezzo di commissione del reato oppure costituiscono semplicemente una fonte di informazioni utili alla ricostruzione dei fatti. [130]

L'autenticità e la completezza dell'evidenza digitale possono essere garantite attraverso strumenti di verifica dell'integrità, come le funzioni crittografiche di hash, che consentono di accertare che il contenuto acquisito non abbia subito modifiche rispetto all'originale. In definitiva, la prova digitale può essere considerata attendibile solo quando sia possibile ricostruire in modo trasparente tutte le fasi della sua acquisizione, conservazione e analisi, escludendo qualsiasi possibilità di alterazione o manipolazione del dato e assicurando così la certezza della sua provenienza e del suo contenuto.[131]

In questa prospettiva, l'incidente informatico rappresenta una sfida significativa per il processo penale contemporaneo, poiché richiede un equilibrio tra competenze giuridiche e

[128] S. Golin, Questioni aperte sull'acquisizione probatoria di dati informatici (a cura di) R. Brighi, Nuove questioni di informatica forense, Aracne, Roma, 2022. pp.49.
[129] A. Ghirardini, G. Faggioli, Computer Forensics, Apogeo, Milano, 2009, pp.452.
[130] F. Cajani, S. Aterno, Aspetti giuridici comuni delle indagini informatiche, in S. Aterno, F. Cajani, G. Costaile, M. Attiucci, G. Mazzaraco, Computer forensics e indagini digitali, Experta, Milano, 2011, pg.15-20.
[131] G. Ziccardi, Informatica giuridica, Giuffrè, Milano, 2006, pp. 330-340.

conoscenze tecnico-scientifiche. L'autorità giudiziaria deve essere in grado di governare il sapere specialistico senza affidarsi in modo acritico agli esperti, ma evitando al contempo una semplificazione della complessità tecnologica. La prova digitale diventa così un banco di prova per l'effettiva capacità del sistema penale di confrontarsi con fenomeni caratterizzati da elevata rapidità evolutiva e da modalità di produzione della conoscenza profondamente diverse rispetto ai modelli tradizionali di accertamento. [132]

4.4 La documentazione dell'incidente, il logging e la prova nel processo penale

L'Agenzia per la Cybersicurezza Nazionale (ACN), istituita in Italia dal decreto-legge 14 giugno 2021, n. 82, rappresenta l'autorità nazionale competente in materia di cybersicurezza e coordina le attività di tutela dello spazio cibernetico. Al suo interno opera il CSIRT Italia, istituito dal d.lgs. 18 maggio 2018, n. 65 in attuazione della direttiva NIS, quale struttura responsabile della prevenzione, gestione e risposta agli incidenti informatici, nonché della raccolta delle segnalazioni e del supporto tecnico ai soggetti coinvolti. [133] Un profilo particolarmente significativo dell'attività svolta dall'ACN riguarda la capacità di classificare le entità in funzione del loro livello di criticità, attribuendo differenti priorità sulla base della rilevanza strategica dei servizi erogati e dell'impatto sistemico che un eventuale incidente informatico potrebbe determinare. Tale impostazione consente di orientare in modo più efficace le risorse disponibili, i controlli e le misure di sicurezza verso i soggetti maggiormente esposti, contribuendo al rafforzamento della resilienza dell'intero sistema nazionale. Le informazioni raccolte dall'Agenzia vengono inoltre condivise e integrate nel contesto europeo, favorendo la cooperazione tra gli Stati membri e con organismi sovranazionali quali ENISA. Questo sistema di collaborazione rafforza la capacità di prevenzione e risposta alle minacce cibernetiche, promuovendo la costruzione di un ecosistema di sicurezza digitale coordinato a livello europeo. [134]

La gestione delle notifiche degli incidenti si articola in quattro fasi: preparazione della notifica, trasmissione al CSIRT Italia, gestione dell'incidente mediante attività di analisi e

---

[132] G. Verde, *Il percorso della prova digitale nelle attività di Digital Forensics, una review*, cit., p. 65.
[133] Agenzia per la Cybersicurezza Nazionale (ACN), *Guida alla notifica degli incidenti al CSIRT Italia* (TLP:CLEAR), luglio 2024, pp. 2-3.
[134] G. Di Gennaro (a cura di), *Modelli di cybersecurity e prevenzione dei cyber crimes: aporie della legislazione vigente, problematiche applicative e prospettive de iure condendo*, Federico II University Press, Napoli, 2025, p. 99-101.

supporto tecnico e, infine, chiusura dell'incidente, con il completamento delle operazioni di ripristino e delle eventuali misure necessarie a prevenire il ripetersi di eventi analoghi.[135]

L'intero processo di gestione degli incidenti, oltre a garantire una risposta coordinata agli eventi di sicurezza, assume particolare rilievo anche sotto il profilo probatorio. La documentazione prodotta nel corso delle diverse fasi, unitamente ai log, ai report tecnici e alle informazioni raccolte durante l'incident handling, può infatti costituire una rilevante fonte di evidenza digitale nell'ambito di eventuali procedimenti giudiziari, purché acquisita e conservata nel rispetto delle garanzie di integrità, autenticità e tracciabilità richieste dall'ordinamento. [136]

La locuzione "file di log" fa riferimento a un file, in formato di testo, nel quale vengono indicate le operazioni compiute da un determinato utente durante una sessione di lavoro del proprio dispositivo elettronico, sia esso un personal computer, uno smartphone, un tablet, e così via. Possono essere considerati vere e proprie «impronte digitali» dell'attività informatica, poiché attraverso la loro analisi è possibile ricostruire elementi rilevanti quali gli orari e la durata delle connessioni alla rete, gli indirizzi IP utilizzati e numerose altre informazioni di interesse investigativo. La qualità e l'affidabilità di tali registrazioni assumono quindi un ruolo determinante: log incompleti, discontinui o privi di adeguate garanzie di integrità possono compromettere la ricostruzione degli eventi e ridurre l'attendibilità del materiale acquisito come possibile fonte di prova. Ne consegue che le misure tecniche e organizzative adottate dall'ente nella fase preventiva, in particolare con riferimento alla gestione e conservazione dei dati di registrazione, possono incidere direttamente sull'efficacia delle successive attività investigative e sull'utilizzabilità processuale delle informazioni raccolte. [137]

Come già osservato, la prova digitale richiede una valutazione tecnica e non può essere considerata automaticamente attendibile. In tale contesto, la documentazione prodotta durante la gestione dell'incidente assume un ruolo determinante, poiché consente di ricostruire le modalità di acquisizione, conservazione e trattamento dell'evidenza informatica. Ciò assume un rilievo decisivo per l'efficacia probatoria nella fase processuale.

---

[135] Agenzia per la Cybersicurezza Nazionale (ACN), *Guida alla notifica degli incidenti al CSIRT Italia* (TLP:CLEAR), op. cit.
[136] G. Verde, *Il percorso della prova digitale nelle attività di Digital Forensics, una review*, in *i-lex – Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, op cit., pp. 63-65.
[137]J. Della Torre, A. Malacarne, *L'utilizzo dei file di log per scopi di contrasto alla criminalità: nodi problematici e possibili soluzioni*, in Arch. Pen., 2022, pp. 3-9.

La dottrina ha inoltre richiamato l'attenzione sul rischio di una sovrapposizione tra esigenze di sicurezza informatica ed esigenze probatorie, evidenziando la necessità di evitare pratiche di logging invasive o sproporzionate. In particolare, occorre garantire il rispetto dei diritti fondamentali, come il diritto alla riservatezza e alla protezione dei dati personali, che possono essere incisi da forme di monitoraggio eccessivamente pervasive. [138]

Ne consegue che una corretta gestione dell'incidente informatico non risponde esclusivamente a esigenze di sicurezza delle informazioni, ma assume rilievo anche sotto il profilo processuale. L'adozione di procedure conformi agli standard internazionali, la corretta conservazione dei log e la completa documentazione delle attività di incident response costituiscono presupposti essenziali affinché le evidenze digitali possano essere efficacemente utilizzate nel procedimento penale, contribuendo all'accertamento dei fatti e all'individuazione delle eventuali responsabilità.

4.5 Cenni relativi alla responsabilità penale del management e alla luce della direttiva NIS2

Una valutazione del rischio efficace richiede il coinvolgimento di tutte le figure in grado di fornire una conoscenza adeguata delle attività, dei sistemi informativi e del contesto operativo dell'organizzazione. Per tale ragione, tutte le principali parti interessate dovrebbero partecipare al processo di valutazione del rischio, includendo il personale interno, i responsabili delle diverse funzioni aziendali, nonché soggetti esterni quali clienti, fornitori e partner. Il coinvolgimento dei diversi soggetti deve tuttavia essere gestito secondo il principio della necessaria conoscenza (*need to know*), fornendo a ciascun partecipante esclusivamente le informazioni indispensabili per contribuire alle attività di propria competenza. Tale approccio consente di garantire un adeguato equilibrio tra condivisione delle informazioni e tutela degli aspetti sensibili dell'organizzazione.[139]

Tra le figure previste dalla norma ISO/IEC 27001 assume particolare importanza il responsabile del rischio (*risk owner*), la cui definizione è contenuta nella norma ISO/IEC 27000: "Persona o entità con la responsabilità e con il potere per gestire un rischio". [140]

---

[138] P. Falletta, A. Marsano, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in Rivista italiana di informatica e diritto, n. 1/2024, DOI 10.32091/RIID0155, 2024, p. 120.
[139] Cesare Gallotti, *Sicurezza delle informazioni.* op. cit., pp. 35-36.
[140] ISO/IEC 27000:2018, op. cit., pp. 10.

Il responsabile del rischio ha il compito di assicurare che siano individuati, implementati e monitorati i controlli di sicurezza più adeguati rispetto ai rischi identificati. Nella pratica organizzativa, il ruolo di responsabile del rischio coincide frequentemente con la Direzione, in quanto tale funzione dispone generalmente del potere decisionale e delle risorse economiche necessarie per approvare l'adozione dei controlli di sicurezza. La Direzione può tuttavia delegare specifiche attività ad altre funzioni aziendali, incaricate di formulare proposte relative alla gestione del rischio, stimare le risorse necessarie e coordinare le attività operative. Nonostante tali deleghe, la responsabilità ultima della gestione del rischio rimane in capo alla Direzione. In ogni caso, i responsabili del rischio devono essere individuati tra soggetti dotati di adeguato livello gerarchico, autonomia decisionale e capacità di allocazione delle risorse economiche. [141]

Dal punto di vista penalistico, tale evoluzione rafforza l'attenzione sulla colpa organizzativa e sui criteri di prevedibilità ed evitabilità dell'evento. In questa prospettiva, l'incidente informatico diventa un indicatore della tenuta del sistema di governance, suscettibile di valutazione anche ex post da parte del giudice penale. La definizione precedentemente richiamata, secondo cui il responsabile del rischio è il soggetto dotato della responsabilità e del potere necessari per gestire un rischio all'interno dell'organizzazione, assume rilevanza anche sotto il profilo penalistico, andando oltre la mera dimensione organizzativa della gestione del rischio. In ambito cyber, la mancata adozione di misure minime di sicurezza o una gestione negligente degli incidenti da parte del responsabile, possono integrare profili di colpa, soprattutto in relazione a reati colposi o a fattispecie di evento aggravato dalla violazione di obblighi di protezione. [142]

La disciplina introdotta dalla NIS2 consente quindi di delineare una vera e propria figura di garante della sicurezza informatica in capo ai vertici dell'organizzazione. Questa posizione presenta evidenti analogie con quelle tradizionalmente analizzate dalla dottrina penalistica in materia di sicurezza sul lavoro o tutela dell'ambiente.

4.6 Caso di studio: analisi di un incidente di sicurezza informatica osservato durante il tirocinio.

[141] C. Gallotti, *Sicurezza delle informazioni*.- op. cit., pp. 35-37.
[142] C. Ogriseg, *Network and Information Security: la strategia europea nella Direttiva NIS II e le sfide che ci attendono,* in Ciberspazio e diritto: rivista internazionale di informatica giuridica*, 2024*, pp. 133-150.

Nel corso del tirocinio curriculare svolto presso Athesys S.r.l. si ha avuto modo di assistere ad un tentativo di Business Email Compromise (BEC), circostanza che ha consentito di osservare concretamente le modalità operative di un attacco di social engineering e le procedure interne di gestione dell'incidente. Il Business Email Compromise è una particolare forma di attacco informatico, nella quale un soggetto malevolo impersona un dirigente aziendale, un collega, un fornitore o un altro interlocutore ritenuto affidabile, utilizzando messaggi di posta elettronica apparentemente legittimi per indurre la vittima a effettuare pagamenti, acquistare beni, comunicare dati riservati o compiere altre operazioni fraudolente. A differenza delle tradizionali campagne di phishing, gli attacchi BEC sono generalmente altamente personalizzati e sfruttano informazioni pubblicamente disponibili sull'organizzazione e sui suoi dipendenti, rendendo il tentativo di frode particolarmente credibile.[143]

L'episodio si è verificato nell'ultimo giorno di tirocinio. Alla mia casella di posta elettronica aziendale, utilizzata esclusivamente per le comunicazioni interne e di lavoro, è pervenuto un messaggio che appariva provenire dall'amministratore delegato della società. La richiesta iniziale, formulata con toni del tutto plausibili, consisteva nel verificare la mia disponibilità a svolgere un'attività per suo conto. Tale circostanza non ha destato immediatamente sospetti, poiché nel corso del tirocinio le comunicazioni con il tutor aziendale avvenivano abitualmente tramite posta elettronica. Inoltre, il CEO non era presente in azienda quel giorno.

Dopo aver manifestato la mia disponibilità, il mittente ha richiesto di recarmi presso un supermercato per acquistare fiori, cioccolatini e gift card Apple. La natura inconsueta della richiesta mi ha indotto a effettuare un controllo più approfondito del messaggio. Esaminando l'indirizzo del mittente, ho constatato che l'e-mail non proveniva dall'effettivo indirizzo aziendale dell'amministratore delegato, bensì da un indirizzo fraudolento appositamente creato per impersonarne l'identità. Accertato il tentativo di frode, ho immediatamente informato i colleghi presenti in azienda e provveduto a inoltrare il messaggio al Chief Information Security Officer (CISO), consentendo l'attivazione delle verifiche e delle procedure di gestione dell'incidente previste dall'organizzazione, quali l'analisi dell'indirizzo del mittente, degli header dell'e-mail e degli eventuali indicatori di compromissione, nonché

143 https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise?

di valutare l'adozione di ulteriori misure di sicurezza per prevenire analoghi tentativi di frode. Successivamente è emerso che il tentativo di frode era stato verosimilmente agevolato da un'informazione resa pubblica sul mio profilo LinkedIn. Avevo infatti condiviso un post nel quale comunicavo l'inizio del tirocinio presso Athesys S.r.l. È plausibile che l'autore dell'attacco abbia individuato tale informazione, l'abbia utilizzata per identificarmi come potenziale destinataria e abbia successivamente tentato di impersonare l'amministratore delegato dell'azienda al fine di indurmi ad acquistare gift card e altri beni.

L'episodio ha evidenziato come gli attacchi di social engineering possano colpire anche attraverso strumenti di comunicazione aziendale apparentemente affidabili e che il fattore umano rappresenta uno dei principali elementi di vulnerabilità dei sistemi informativi. L'attaccante non ha tentato di sfruttare una debolezza tecnica dell'infrastruttura informatica, ma ha fatto leva su informazioni liberamente reperibili e su tecniche di ingegneria sociale finalizzate a instaurare un rapporto di fiducia con la vittima. Ciò pone in luce ancora una volta come una gestione efficace del rischio debba integrare strumenti tecnologici, procedure organizzative e attività di formazione continua del personale, in conformità ai principi espressi dagli standard internazionali di sicurezza delle informazioni.

Conclusione

L’analisi condotta nel presente elaborato ha evidenziato come la sicurezza informatica non possa più essere considerata una materia esclusivamente tecnica. La crescente dipendenza delle organizzazioni dai sistemi digitali, l’evoluzione delle minacce e la capacità degli incidenti cyber di produrre conseguenze economiche, operative, reputazionali e giuridiche impongono l’adozione di un approccio integrato, nel quale tecnologia, organizzazione, governance e diritto concorrano alla protezione delle informazioni e dei servizi essenziali.
Alla luce delle considerazioni svolte, è possibile concludere che una gestione efficace del rischio informatico assolve contemporaneamente una funzione preventiva, organizzativa e probatoria. Essa riduce la probabilità che le minacce si trasformino in eventi dannosi, consente di limitare gli effetti degli incidenti e crea le condizioni necessarie per la corretta ricostruzione dei fatti qualora intervenga l’autorità giudiziaria. La cybersecurity si configura pertanto come un processo continuo e condiviso, che richiede il coinvolgimento del management, delle funzioni tecniche, del personale e dei soggetti esterni con cui l’organizzazione interagisce. Nessun controllo tecnologico può essere pienamente efficace in assenza di una cultura della sicurezza, così come nessun adempimento normativo può essere realmente utile quando viene trattato come un mero obbligo formale.
La principale conclusione della ricerca è dunque che prevenzione e repressione non costituiscono modelli alternativi. Nel cyberspazio, la tutela dei beni giuridici richiede un sistema nel quale la gestione preventiva del rischio, la resilienza organizzativa, la conformità normativa e gli strumenti del processo penale operino in maniera complementare. La capacità di governare il rischio prima dell’incidente e di preservare correttamente le evidenze dopo il suo verificarsi rappresenta la condizione essenziale per costruire organizzazioni più sicure, responsabili e in grado di affrontare consapevolmente le sfide della trasformazione digitale.

BIBLIOGRAFIA

Monografie, contributi dottrinali e articoli scientifici

ACN – Agenzia per la Cybersicurezza Nazionale, *Guida alla notifica degli incidenti al CSIRT Italia (TLP:CLEAR)*, 2024.

Anderson, R., *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3ª ed., John Wiley & Sons Inc, 2021.

Aven, T., *Risk Analysis*, Wiley, Chichester, 2ª ed., 2015.

Bada, M., Sasse, A.,Nurse J.R., *Cybersecurity Awareness Campaigns: Why Do They Fail to change behaviour?*, arXiv preprint arXiv:1901.02672, 2019.

Boin, A., 't Hart, P., Stern, E., Sundelius, B., *The Politics of Crisis Management*, Cambridge University Press, 2016.

Bragò, G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatic*i, in L. Luparia (a cura di), Sistema e criminalità informatica, Giuffrè, Milano, 2009,

Cadoppi, A., Canestrari, S., Manna, A., Papa, M. (a cura di), *Cybercrime*,2ª ed.,Utet giuridica, Torino, 2023.

Cajani, F.; Aterno, S., *Aspetti giuridici comuni delle indagini informatiche,* in S. Aterno, F. Cajani, G. Costabile, M. Attiucci, G. Mazzaraco, *Computer forensics e indagini digitali*, Experta, Milano, 2011.

Caralli, R. A., Stevens, J. F., Young, L. R., Wilson, W. R., *OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 2007.

Casarosa F., *L'armonizzazione degli obblighi di notifica: il DDL Cybersicurezza verso la NIS 2,* Rivista italiana di informatica e diritto, anno VI, n. 1, 2024, DOI: 10.32091/RIID0146.

Chiara, P. G., *DDL Cybersicurezza: tra l'inasprimento della risposta penale del legislatore nazionale e il modello preventivo-amministrativo della direttiva NIS2*, Rivista italiana di informatica e diritto, anno VI, n. 1, 2024, DOI: 10.32091/RIID0147.

Comandè, G.; Nasi, C., *Oltre la conformità: dalle scelte strategiche ISO e NIST 2.0 alla gestione proattiva del rischio,* Rivista italiana di informatica e diritto, anno VIII, n. 1, 2026, DOI: 10.32091/RIID0268.

Conti M., Dehghantanha, A., Franke, K., Watson, S., *Internet of Things Security and Forensics: Challenges and Opportunities*, Future Generation Computer Systems, vol. 78, 2018.

CLUSIT (Associazione Italiana per la Sicurezza Informatica), *Rischio digitale, innovazione e resilienza*, Clusit, Milano, 2022.

Culot, G., Nassimbeni, G., Podrecca, M., Sartor, M., *The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory‑Based Research Agenda*, *The TQM Journal*, vol. 33, n.7, 76-105, 2021.

Cuomo, L., *La prova digitale*, in G. Canzio, L. Luparia (a cura di), *Prova scientifica e processo penale*, CEDAM, Padova, 2017.

Delaini, F., *Verso un diritto penale della sicurezza digitale? La cyber-compliance del Regolamento DORA,* Rivista italiana di informatica e diritto, anno VIII, n. 1, 2026, DOI: 10.32091/RIID0269.

Della Torre, J.; Malacarne, A., *L'utilizzo dei file di log per scopi di contrasto alla criminalità: nodi problematici e possibili soluzioni, in* Archivio Penale, n.3, 2023.

Di Gennaro, G. (a cura di), *Modelli di cybersecurity e prevenzione dei cyber crimes: aporie della legislazione vigente, problematiche applicative e prospettive de iure condendo*, Federico II University Press, Napoli, 2026.

Dionne, G., *Risk Management:History, Definition, and Critique, Risk Management and Insurance Review,* vol. 16, n. 2, 2013, pp. 147-166, DOI: 10.1111/rmir.12016.

Fiandaca, G., Musco, E., *Diritto penale. Parte generale*, X ed., Zanichelli, Bologna, 2026.

Gallotti, C., *Sicurezza delle informazioni*, *Gestione del rischio. I sistemi di gestione. La ISO/IEC 27001:2022. I controlli della ISO/IEC 27002:2022*, Youcanprint, 2022.

Ghirardini, A.; Faggioli, G., *Computer Forensics*, Apogeo, Milano, 2009.

Golin, S., *Questioni aperte sull'acquisizione probatoria di dati informatic*i, in R. Brighi (a cura di), Nuove questioni di informatica forense, Aracne, Roma, 2022.

Humphreys, E., *Information Security Management Standards: Compliance, governance and risk management*, BSI Press, 2008.

Kshetri, N., *The Emerging Role of Big Data in Key Development Issues: Opportunities, Challenges, and Concerns*, Big Data & Society, vol. 1, n. 2, 2014.

Lagadec, P., *A New Cosmology of Risks and Crises: Time for a radical shift in paradigm and practice,* Review of policy research, vol.26, n. 4, 2009.

Luparia, L., Ziccardi, G., *Investigazione penale e tecnologia informatica: l'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè, Milano, 2007.

Mantovani, F., Flora, G., *Diritto penale. Parte generale*, XIII ed., Cedam, 2025.

Marafioti, L., Paolozzi, G. (a cura di), *'Incontri ravvicinati' con la prova penale*, Giappichelli, Torino, 2014.

Ogriseg, C., *Network and Information Security: la strategia europea nella Direttiva NIS II e le sfide che ci attendono*, Ciberspazio e diritto: rivista internazionale di informatica giuridica, vol.25, n.76, fasc. 1, 2024.

Peltier, T., *Information Security Risk Analysis*, Auerbach Publications, Boca Raton, 3ª ed., 2010.

Radu, R., *Negotiating Internet Governance*, Oxford University Press, 2019.

Schneier, B., *Data and Goliath: The hidden battles to collect your data and control your world* ., W.W. Norton & Company, New York, 2015.

Singer, P. W., Friedman, A., *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oup Usa, 2014.

Siponen, M., Willison, R., *Information Security Management Standards: Problems and Solutions*, Information & Management, vol. 46, n. 5, 2009.

Stallings, W. *Cryptography and Network Security Principles and practices*, Pearson, 8ª ed., 2023.

Stoneburner, G., Goguen, A., Feringa, A. *Risk management guide for information technology systems. Nist special publication*, 800-30, 2002, DOI 10.6028/NIST.SP.800-30.

Taleb, N. N., *Antifragile: Things That Gain from Disorder*, Random House Publishing Group, 2014.

Ubertis, G., *Sistema di procedura penale. Volume I – Principi generali*, 6ª ed., Giuffrè, Milano, 2025.

Vaccari, G., *Cybersecurity nell'attività di impresa: profili penalistici*, Altalex, 2025.

Verde, G., *Il percorso della prova digitale nelle attività di Digital Forensics: una review*, i-lex – Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale, vol. 18, n. 1, 2025, DOI: 10.6092/issn.1825-1927/21507.

Von Solms, R., Van Niekerk, J., *From Information Security to Cybersecurity*, *Computers & Security*, 2013.

Ziccardi, G., *Informatica giuridica*, Giuffrè, Milano, 2008.

Fonti normative e standard tecnici

Direttiva (UE) 2016/1148 (NIS).

Direttiva (UE) 2022/2555 (NIS 2).

ENISA, *ENISA Threat Landscape*, varie edizioni.

ENISA, *CSIRTs and Cooperation Mechanisms*, 2023.

ENISA, *Coordinated Vulnerability Disclosure Policies*, Publications Office of the European Union, Luxembourg, 2022.

European Commission, *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, Brussels, 2015.

European Commission, *Raccomandazione (UE) 2017/1584 della Commissione del 13 settembre 2017 relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su larga scala*, *Gazzetta ufficiale dell'Unione europea*, L 239, 19 settembre 2017.

FAIR Institute, *Factor Analysis of Information Risk – Standard v. 3.0*, 2025.

ISO, *ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements*, International Organization for Standardization (ISO), Geneva, 2019.

ISO/IEC, *ISO/IEC 27000:2024 – Information Security, cybersecurity and privacy protection – Information security management systems – Overview and vocabulary, International Organization for Standardization (ISO), Geneva, 2024.*

ISO/IEC, ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements, International Organization for Standardization (ISO), Geneva, 2022.

ISO/IEC, ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls, International Organization for Standardization (ISO), Geneva, 2022.

ISO/IEC, *ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidance on managing information security risks*, International Organization for Standardization (ISO), Geneva, 2022.

ISO, *ISO 31000:2018 – Risk management – Guidelines*, International Organization for Standardization (ISO), Geneva, 2018.

NIST, *Cybersecurity Framework 2.0*, National Institute of Standards and Technology, 2024.

OCTAVE Allegro, *Improving the Information Security Risk Assessment Process*, Carnegie Mellon University, 2007.

Sitografia essenziale

- https://www.iso.org
- https://www.enisa.europa.eu

- https://www.nist.gov
- https://www.acn.gov.it
- https://eur-lex.europa.eu
- https://digital-strategy.ec.europa.eu

Case study:

- NotPetya Attack (Columbia SIPA): https://www.sipa.columbia.edu
- Yallo, *Operational meltdown from cyber attack: Maersk 2017*: https://yallo.co/?case-study=operational-meltdown-from-cyber-attack-maersk-2017
- Federal Bureau of Investigation (FBI), *Business Email Compromise*: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise?