Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

Fondazione
Nazionale dei
Commercialisti

RICERCA

DOCUMENTO

Cybersecurity e Modello 231: integrazione dei rischi informatici nella governance d'impresa

MAGGIO 2026

AREE DI DELEGA CNDCEC
Compliance e modelli organizzativi delle imprese

CONSIGLIERI DELEGATI
Fabrizio Escheri
Eliana Quintili

COMMISSIONE DI STUDIO CNDCEC
Compliance e modelli organizzativi d.lgs. 231

PRESIDENTE
Salvatore Sodano

Composizione del Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili

Presidente
Elbano de Nuccio

Vice Presidente
Antonio Repaci

Consigliere Segretario
Giovanna Greco

Consigliere Tesoriere
David Moro

Consiglieri
Gianluca Ancarani
Marina Andreatta
Cristina Bertinelli
Aldo Campo
Rosa D'Angiolella
Michele de Tavonatti
Fabrizio Escheri
Gian Luca Galletti
Cristina Marrone
Maurizio Masini
Pasquale Mazza
Eliana Quintili
Maria Lucetta Russotto
Pierpaolo Sanna
Liliana Smargiassi
Giuseppe Venneri
Gabriella Viggiano

Collegio dei revisori

Presidente
Rosanna Marotta

Componenti
Maura Rosano
Sergio Ceccotti

Composizione della Fondazione Nazionale di Ricerca dei Commercialisti

Consiglio di gestione

Presidente
Antonio Tuccillo

Vice Presidente
Giuseppe Tedesco

Consigliere Segretario
Andrea Manna

Consigliere Tesoriere
Massimo Da Re

Consiglieri
Francesca Biondelli
Antonia Coppola
Cosimo Damiano Latorre
Claudia Luigia Murgia
Antonio Soldani

Collegio dei revisori

Presidente
Rosario Giorgio Costa

Componenti
Ettore Lacopo
Antonio Mele

Commissione di studio "Compliance e modelli organizzativi d.lgs. 231"

Consiglieri CNDCEC delegati

Fabrizio Escheri
Eliana Quintili

Presidente

Salvatore Sodano

Segretario

Carlo De Luca

Componenti

Andrea Burlini
Paolo Caselli
Alessandro Cavalli
Aldo Giacomo Colantuono
Ernesto Devito
Sabrina Filiberto
Giuseppe Paternò
Attilio Pisani
Sandro Traversi
Paolo Vernero
Lucia Zazzetta

Staff tecnico

Annalisa De Vivo - *Ufficio Monitoraggio Legislativo CNDCEC*
Roberto De Luca - *Fondazione Nazionale Commercialisti - Ricerca*

Hanno collaborato alla redazione del documento i seguenti componenti della Commissione: Andrea Burlini, Paolo Caselli, Alessandro Cavalli, Carlo De Luca, Ernesto Devito, Giuseppe Paternò, Paolo Vernero, Lucia Zazzetta

Sommario

Introduzione

La crescente digitalizzazione dei processi aziendali e professionali sta modificando profondamente l'organizzazione delle imprese e, più in generale, il sistema dei controlli interni e della governance societaria. In tale contesto, i profili connessi alla sicurezza informatica assumono un rilievo sempre maggiore non soltanto sul piano tecnologico, ma anche sotto il profilo organizzativo, gestionale e della compliance.

L'evoluzione normativa nazionale ed europea, l'ampliamento dei reati informatici rilevanti ai sensi del d.lgs. 231/2001 e la crescente attenzione ai temi della resilienza digitale impongono oggi alle imprese un approccio sempre più strutturato alla gestione del rischio cyber. Parallelamente, anche il ruolo del professionista è destinato ad evolversi, poiché le problematiche connesse alla cybersecurity incidono ormai su molteplici ambiti dell'attività di consulenza e controllo: dagli assetti organizzativi ai sistemi di compliance, dall'attività degli Organismi di Vigilanza ai controlli societari, fino ai processi di *risk assessment* e gestione del rischio.

Il presente documento nasce dall'esigenza di offrire ai Commercialisti uno strumento di analisi e approfondimento su un tema destinato ad assumere un'importanza sempre più centrale nella vita delle imprese. L'obiettivo è quello di favorire una maggiore consapevolezza circa l'interazione tra *cybersecurity*, *governance* e Modello 231, evidenziando come il rischio informatico non possa più essere considerato un profilo esclusivamente tecnico, ma debba essere inserito all'interno dei sistemi di organizzazione, gestione e controllo dell'ente.

In tale prospettiva, il documento propone una lettura integrata dei principali profili normativi, organizzativi e operativi connessi alla gestione del rischio *cyber*, soffermandosi sui reati informatici rilevanti ai fini della responsabilità amministrativa degli enti, sull'analisi dei rischi e delle aree sensibili, sull'aggiornamento dei Modelli 231 e dei protocolli interni, nonché sul ruolo delle *best practices* e degli standard internazionali nella costruzione di adeguati presidi di sicurezza.

Particolare attenzione è dedicata anche all'impatto delle nuove tecnologie e dell'intelligenza artificiale sui sistemi di controllo e sull'attività degli Organismi di Vigilanza, in un contesto in cui la trasformazione digitale pone nuove opportunità, ma anche nuovi profili di rischio per le organizzazioni.

Fabrizio Escheri - Eliana Quintili

Consiglieri Delegati area compliance e modelli organizzativi delle imprese

1. Cybersecurity: una minaccia per le organizzazioni

Il tema della cybersicurezza assume una valenza sempre più centrale nei moderni sistemi di gestione e controllo del rischio d'impresa, anche alla luce dell'evoluzione normativa nazionale ed europea. Nel prosieguo, dopo aver delineato il concetto di c*ybersecurity* e le principali tipologie di rischio connesse agli strumenti informatici e digitali, verranno esaminati alcuni tra i più rilevanti fenomeni di attacco cyber e le relative conseguenze operative, economiche e organizzative per le imprese.

L'analisi evidenzia come la crescente esposizione ai rischi informatici imponga alle organizzazioni l'adozione di adeguati assetti organizzativi, tecnici e procedurali, nonché l'integrazione delle misure di cybersicurezza nei modelli di prevenzione e controllo dei rischi, anche ai fini della responsabilità amministrativa degli enti *ex* d.lgs. n. 231/2001[1].

1.1. Definizione di *cybersecurity* e principali rischi

Negli ultimi decenni l'informatica, la digitalizzazione e la rete internet, nelle loro varie forme e strumenti, hanno pervaso la vita lavorativa e la quotidianità degli individui, modificandone radicalmente il modo di operare e abbattendo i limiti rappresentati dalla distanza fisica.

Tali cambiamenti, così rilevanti e incisivi sulle attività umane, hanno inevitabilmente generato anche varie forme di comportamenti illeciti, abusi e veri e propri crimini, in grado di incidere profondamente e negativamente su persone, imprese e istituzioni, attraverso azioni generalmente definite come "*attacchi cyber",* posti in essere principalmente attraverso la rete.

Per lungo tempo, la diffusione del *cybercrime* è stata agevolata da un'impreparazione diffusa degli utenti, spesso incapaci di distinguere un pericolo di natura informatica e, verosimilmente, anche da un comprensibile ritardo nel porre in essere adeguate contromisure, nonché da uno scarso coordinamento tecnico e normativo da parte delle istituzioni nazionali e sovranazionali.

In questo contesto, è stato introdotto e sviluppato il concetto di "cybersecurity", inteso come l'insieme di pratiche finalizzate a proteggere persone, sistemi e dati dagli attacchi informatici utilizzando varie tecnologie, processi e regole.

In Italia, l'attenzione alla materia è suffragata dalla recente e corposa produzione normativa che mira a fornire un'organica disciplina a partire dal 2018, recependo anche le Direttive dell'UE, NIS[2] e NIS2[3]. Con il d.l. n. 82/2021[4], è stata istituita l'Agenzia per la Cybersicurezza Nazionale (ACN), che ha lo scopo di

[1] "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300".
[2] "Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione".
[3] "Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)".
[4] "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale".

prevenire e mitigare, quanto più possibile, gli attacchi informatici e di favorire il raggiungimento dell'autonomia tecnologica ai fini della tutela nazionale.

Più di recente, con l'intento di allinearsi agli standard europei della citata Direttiva NIS2, il Parlamento italiano ha approvato la l. 90/2024[5], nota come "Legge sulla Cybersecurity", integrata dal d.lgs. 138/2024[6], prevedendo nuovi obblighi a carico di aziende e Pubbliche Amministrazioni, orientati all'adozione di misure di gestione del rischio e all'implementazione di piani di risposta agli incidenti informatici.

La nuova disciplina sulla cybersicurezza incide inevitabilmente anche su aspetti di *risk management e risk assessment* sotto il profilo della responsabilità organizzativa delle imprese. Essa individua l'ambito soggettivo e disciplina obblighi e modalità di tempestiva segnalazione all'ACN degli attacchi o incidenti informatici rilevanti ai sensi del perimetro di sicurezza nazionale cibernetica, integrandosi ai principi già sanciti dal Regolamento Generale sulla Protezione dei Dati (GDPR)[7] in materia di violazioni dei dati personali. Inoltre, la norma istituisce, all'interno delle organizzazioni, la figura del *referente per la cybersicurezza*, il cui nominativo deve essere comunicato all'ACN stessa.

In sintesi, come meglio si vedrà nel prosieguo, i rischi nei quali possono incorrere le imprese attraverso l'utilizzo di strumenti informatici possono essere accorpati nelle seguenti macrocategorie di reati:

- delitti contro la fede pubblica, finalizzati ad esempio a produrre documenti ed atti falsi;
- delitti contro la persona, finalizzati a limitare la libertà individuale (impedendo il funzionamento di sistemi informatici) o a violare informazioni personali o segrete;
- delitti contro il patrimonio, finalizzati a frode o ad appropriazione indebita;
- violazione delle Direttive "NIS", relative a inadempienze degli obblighi previsti dall'impianto normativo in materia di mantenimento degli standard di sicurezza informatica e di comunicazione verso le istituzioni competenti.

Va inoltre osservato che la crescente integrazione tra sistemi informatici e di rete, infrastrutture, attrezzature, macchinari industriali e mezzi di trasporto, unitamente alla sempre più ampia diffusione di tecnologie "smart", comporta che le attività di *cybercrime* possano produrre effetti che travalicano il dominio digitale, incidendo concretamente sulla salute e sull'incolumità delle persone, nonché sull'ambiente e su altri ambiti di rilevanza collettiva.

Anche ai fini della cybersicurezza, la presenza di un assetto organizzativo adeguato, di buone prassi e codici di comportamento, ma soprattutto la redazione di un modello organizzativo che definisca specifiche misure preventive, risultano essenziali per tutelare l'impresa da misure sanzionatorie o

[5] "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici".
[6] "Recepimento della Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abroga la Direttiva (UE) 2016/1148".
[7] "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

interdittive, qualora dovesse verificarsi una condotta illecita che le arrechi un interesse e/o un vantaggio.

In affiancamento ad ovvi presidi di tipo tecnico/informatico, è opportuno, pertanto, che siano sviluppate anche misure di sicurezza di tipo fisico/logistico, per controllare l'accesso individuale ai sistemi e ai dispositivi elettronici.

1.2. Attacchi informatici rilevanti e conseguenze per le aziende

Il "Rapporto Clusit[8] sulla Cybersecurity 2026" evidenzia un incremento degli incidenti informatici nel 2025 pari al 48,7% rispetto all'anno precedente, che rappresenta il risultato più elevato mai registrato, con un totale di 5.265 eventi, dei quali per l'84% ad alto impatto.

Tra gli ambiti più colpiti figurano la P.A. e le istituzioni, il settore manifatturiero e i trasporti, ma in generale si riscontrano eventi in tutti i comparti di produzione, tra cui servizi professionali, sanitari e finanziari.

Tra le modalità di cyber attacco maggiormente diffuse, si segnala il *DDoS* (Distributed Denial-of-Service), che consiste nel saturare le capacità dei siti con un traffico proveniente contemporaneamente da fonti differenti, rendendo impossibile l'accesso per gli utenti. Un'altra tecnica è rappresentata dai cosiddetti *malware*, in grado di generare malfunzionamenti nei sistemi, al fine di rendere inutilizzabili o di rubare i dati sensibili presenti nelle banche dati.

Il citato documento conclude enfatizzando il valore aggiunto rappresentato dalle politiche aziendali di cybersecurity, trasformandole in fattori reputazionali verso la clientela, gli investitori e i finanziatori. Il Rapporto cita anche alcuni casi internazionali che vale la pena riportare:

- *Saint-Gobain (Francia, 27 giugno 2017 – NotPetya)*: il colosso francese dei materiali da costruzione, attivo in 220 stabilimenti in tutto il mondo con prodotti come vetro, cartongesso e sistemi di isolamento, viene colpito da NotPetya, un *malware* diffuso attraverso un aggiornamento del software fiscale ucraino M.E.Doc, utilizzato da un fornitore della *supply chain*. In poche ore, i server ERP vengono cifrati, i sistemi di produzione si bloccano e la logistica viene paralizzata. Fabbriche nel Nord Europa sono costrette a ricorrere a fogli Excel manuali per riavviare forni e linee produttive, mentre le forniture verso i cantieri si interrompono improvvisamente.
- *Bird Construction (Canada, 14 gennaio 2019 – ransomware)*: Bird, general contractor quotato alla Borsa di Toronto con circa 4.500 dipendenti, viene colpito da un attacco *ransomware* (sospettato di ricondursi alla famiglia Dharma/ Cryptolock) che cifra circa 60 GB di dati critici, tra progetti in corso, contratti e informazioni finanziarie. Il vettore probabile è un'e-mail di *phishing* rivolta a un impiegato o a un partner con accessi condivisi alle piattaforme cloud aziendali.

[8] L'Associazione Italiana per la Sicurezza Informatica Clusit, nata nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, rappresenta un autorevole riferimento nel campo della sicurezza informatica e pubblica periodicamente documenti informativi sulla Cybersicurezza in Italia e nel mondo.

- *Bouygues Construction (Francia, 13 gennaio 2020 – Maze)*: Bouygues Construction, multinazionale francese nota per la realizzazione di opere come l'aeroporto Charles de Gaulle e lo stadio di Wembley, viene colpita il 13 gennaio 2020 dall'attacco Maze. Prima del blocco crittografico, gli attaccanti riescono a esfiltrare circa 200 GB di dati sensibili, tra cui informazioni personali di 237 dipendenti (nomi, indirizzi, dati bancari), dettagli di progetti e offerte in Australia e risultati di test antidroga.

2. Il decreto legislativo 231/2001 e i reati presupposto rilevanti in ambito informatico

L'art. 24-*bis*[9] del d.lgs. 231/2001, introdotto dalla l. n. 48/2008[10], in attuazione della Convenzione di Budapest, ha incluso tra i reati presupposto della responsabilità amministrativa degli enti numerosi reati informatici. La normativa considera, in modo specifico, gli illeciti che richiedono necessariamente, per la loro consumazione, l'utilizzo di tecnologie dell'informazione e di sistemi informatici.

Tuttavia, l'art. 24-*bis* non esaurisce la propria portata ai soli reati informatici in senso stretto, ma abbraccia anche fattispecie che possono essere commesse o facilitate attraverso la rete o il web, quali i reati in materia di terrorismo (art. 25-*quater*), la pedopornografia virtuale (art. 25-*quinquies*) e il riciclaggio (art. 25-*octies*). Si tratta di reati che, pur non essendo strettamente legati all'informatica, trovano un terreno fertile di sviluppo nell'ambito digitale.

Per quanto concerne i reati informatici in senso stretto, è necessario sottolineare che essi sono volti a tutelare tre ambiti specifici:

- la riservatezza dei dati e delle comunicazioni informatiche;
- l'integrità dei dati e dei sistemi informatici;
- la fede pubblica.

Il primo profilo è protetto dall'art. 615-*ter* c.p., che punisce l'accesso abusivo a un sistema informatico o telematico. Questa fattispecie sanziona il comportamento di chi, senza autorizzazione, accede a un sistema informatico o telematico o vi si trattiene oltre i limiti consentiti. Nella stessa area di protezione della riservatezza si collocano anche i reati di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* c.p.), i quali rappresentano condotte prodromiche rispetto all'accesso abusivo, nonché le fattispecie di intercettazione abusiva di comunicazioni informatiche o telematiche (artt. 617-*quater* e *quinquies* c.p.).

Il secondo ambito di tutela, relativo all'integrità dei dati e dei sistemi informatici, è presidiato dalle fattispecie di danneggiamento introdotte con la l. n. 48/2008. Il legislatore ha articolato la risposta

[9] "Delitti informatici e trattamento illecito di dati".
[10] "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno".

sanzionatoria distinguendo tra il danneggiamento di dati, programmi o sistemi informatici privati e il danneggiamento di sistemi pubblici o di pubblica utilità. Le fattispecie più significative in questo ambito sono gli artt. 635-*bis* e 635-*ter* c.p., che tutelano rispettivamente i dati e i programmi informatici privati e pubblici, con una protezione anticipata per questi ultimi, e gli artt. 635-*quater* e 635-*quinquies* c.p., che puniscono le condotte di danneggiamento mediante l'utilizzo di virus o altri programmi dannosi. Una novità rilevante introdotta di recente è l'art. 635-*quater*.1 c.p.[11], il quale punisce la produzione, diffusione o semplice detenzione di programmi informatici progettati per danneggiare sistemi o dati, configurando una protezione avanzata per i sistemi di pubblica utilità.

Infine, tra i reati informatici, l'ultimo ambito di tutela riguarda la fede pubblica, con due fattispecie specifiche: l'art. 491-*bis* c.p., che estende la disciplina della falsità documentale anche al documento informatico, e l'art. 640-*quinquies* c.p., che punisce le frodi informatiche connesse all'alterazione di dati, specialmente se finalizzate a trarre un ingiusto profitto a discapito della pubblica amministrazione. Questi reati rappresentano una minaccia particolarmente rilevante nell'ambito dei rapporti con le pubbliche amministrazioni, ove l'utilizzo fraudolento di dati può compromettere la trasparenza e la correttezza delle transazioni pubbliche.

In tale contesto, l'approvazione delle l. n. 90/2024 mira ad aumentare la sicurezza informatica per difendersi dai cyber-attacchi, inasprendo le sanzioni previste per i c.d. "*computer crimes*". In particolare, introducendo modifiche sostanziali e procedurali riguardanti i reati informatici, la norma:

i. prevede un innalzamento delle pene;

ii. estende i confini del dolo specifico;

iii. introduce nuove circostanze aggravanti;

iv. vieta le attenuanti per diversi reati che siano stati commessi tramite l'utilizzo di apparecchiature informatiche al fine di ottenere indebiti vantaggi con danno altrui, o per accedere abusivamente a sistemi informatici e/o per intercettare o interrompere comunicazioni informatiche e telematiche.

La legge sulla cybersicurezza ha altresì notevoli impatti sull'art. 24-*bis* del Decreto 231. Innanzitutto, il primo comma dell'art. 24-*bis* è stato oggetto di un generale innalzamento delle sanzioni pecuniarie inflitte all'ente in relazione alla commissione di uno dei reati informatici ivi contemplati: infatti, in luogo della precedente cornice edittale da 100 a 200 quote, attualmente è previsto un intervallo compreso tra 500 e 700 quote. Al comma 2 dell'art. 24-*bis*, i riferimenti all'art. 615-*quinquies*[12], abrogato dalla l. n. 90/2024, sono stati sostituiti con l'art. 635-*quater*.1, i cui contenuti, seppur inaspriti dalla previsione di due nuove circostanze aggravanti, sono comunque sovrapponibili.

Infine, è stato introdotto il nuovo comma 1-*bis*, che punisce la nuova fattispecie di estorsione mediante reati informatici (art. 629, comma 3, c.p.) con la sanzione pecuniaria da 300 a 800 quote e con le

[11] Articolo introdotto dall'art. 16, comma 1, lett. q) della l. 90/2024.
[12] "Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico".

sanzioni interdittive previste dall'art. 9, comma 2, del d.lgs. n. 231/2001 per una durata non inferiore ai due anni.

La riforma amplia, quindi, la lista delle condotte che possono integrare un reato-presupposto 231, includendo reati informatici legati alla sicurezza cibernetica nazionale, nonché la già citata estorsione informatica. In questo modo, anche le aziende che non appartengono al settore tecnologico diventano più esposte a tali rischi, poiché qualunque uso improprio di un sistema informatico compiuto da dirigenti o dipendenti nell'interesse o a vantaggio dell'ente può potenzialmente integrare profili di responsabilità ai sensi del d.lgs. n. 231/2001.

Gli enti sono, quindi, chiamati a un lavoro di adeguamento dei propri Modelli di Organizzazione e Gestione, introducendo nuovi presìdi, rafforzando i controlli sugli accessi informatici, implementando misure tecniche di *cybersecurity* e prevedendo programmi di formazione dedicati. Inoltre, l'Organismo di Vigilanza sarà chiamato ad assumere un ruolo ancor più attivo nel monitoraggio dei rischi cibernetici, come meglio specificato di seguito.

2.1. La gestione del rischio informatico nel Modello 231

2.1.1. Reati informatici presupposto e "colpa di organizzazione": riferimenti normativi e giurisprudenziali

Il Modello di organizzazione, gestione e controllo previsto dal d.lgs. n. 231/2001 costituisce, nella sua più matura accezione, non solo un mero strumento di *compliance*, bensì un "sistema" organizzativo strutturato e dinamico, capace di individuare le aree "sensibili" e prevenire i rischi rilevanti per la vita dell'ente. In tale prospettiva, il rischio informatico – inteso come l'insieme delle minacce capaci di compromettere la riservatezza, l'integrità e la disponibilità delle informazioni e dei sistemi che le trattano – ha assunto una centralità crescente, tanto sul piano operativo quanto su quello giuridico-penale.

L'inserimento della *cybersecurity* nel "perimetro 231" non è il frutto di una scelta discrezionale dell'ente, ma è ormai una necessità sistematicamente imposta dall'evoluzione normativa e dalla casistica giudiziaria. Da un lato, il legislatore ha progressivamente ampliato il catalogo dei reati presupposto inclusi nel Decreto, ricomprendendovi anche le fattispecie relative ai delitti informatici in precedenza richiamate; dall'altro, normative settoriali di rango europeo – in primis il whistleblowing[13], il GDPR, la Direttiva NIS2 e il Regolamento DORA[14] – impongono all'impresa di dotarsi di misure organizzative e tecniche adeguate, creando un sistema di compliance integrata in cui il Modello 231

[13] Con il d.lgs. n. 24/2023 l'Italia ha recepito la Direttiva *whistleblowing* (Direttiva UE 2019/1937 del Parlamento Europeo e del Consiglio). Sul punto, si veda anche CNDCEC, "La disciplina *whistleblowing*. Aspetti procedurali e criticità", novembre 2024; CNDCEC-FNC, "Nuova disciplina del *whistleblowing* e impatto sul d.lgs. 231/2001", ottobre 2023.

[14] Digital Operational Resilience Act: "Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011". Trattasi della normativa europea, in vigore dal 17 gennaio 2025, che impone a banche, assicurazioni, intermediari finanziari, ecc., severi standard di sicurezza informatica e resilienza digitale al settore finanziario; essa mira ad armonizzare la gestione dei rischi ICT, la segnalazione degli incidenti e il controllo dei fornitori terzi.

svolge una funzione centrale. La gestione del rischio informatico nel Modello 231 muove da un principio cardine efficacemente sintetizzato nella formula «prevenzione mediante organizzazione»: la responsabilità dell'ente sorge per il fatto che un reato informatico è stato commesso nel suo interesse e/o a suo vantaggio, in quanto connessa alla dimostrazione di un deficit organizzativo, ossia alla mancata adozione o all'inefficace attuazione di un idoneo sistema di presidi preventivi. Questa impostazione è stata ripresa e approfondita dalla giurisprudenza di legittimità[15], che ha chiarito come il giudizio di adeguatezza del Modello debba essere condotto valutando la razionalità e la proporzionalità delle misure adottate rispetto ai rischi concretamente individuabili al momento della loro predisposizione[16]. Non è sufficiente l'adozione formale di un documento denominato «Modello»: ciò che conta è la sua effettiva integrazione nell'organizzazione aziendale e la sua concreta capacità di orientare i comportamenti e prevenire i rischi.

Oltre alle disposizioni normative inserite nel codice penale (e in gran parte richiamate nel d.lgs. n. 231/2001), la giurisprudenza penale[17] ha svolto un ruolo fondamentale per raccordare le condotte penalmente rilevanti, l'interpretazione e portata applicativa delle stesse ai casi concreti, facendo proprie diverse definizioni necessarie ad un corretto inquadramento delle fattispecie penali.

Interessanti sul punto, in via esemplificativa, le nozioni di:

- *sistema informatico*: un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate – per mezzo di un'attività di "codificazione" e "decodificazione" – dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati"[18];
- *dati informatici:* rappresentazioni elementari di un fatto, effettuate da simboli (*bit*), in combinazioni diverse e attraverso l'elaborazione automatica di tali dati, in modo da generare informazioni costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente.

Significativa è anche la chiave interpretativa che viene fornita per la nozione di "file", definiti come "*cose mobili ai sensi della legge penale*" in quanto "*il file, pur non potendo essere materialmente percepito dal punto di vista sensoriale, possiede una dimensione fisica costituita dalla grandezza dei dati che lo compongono, come dimostrano l'esistenza di unità di misurazione della capacità di un file di contenere dati e la differente grandezza dei supporti fisici in cui i files possono essere conservati e elaborati...*" [19]: dunque, i file sono elementi oggettivamente immateriali, ma misurabili.

D'altra parte, all'attività giudiziaria si devono anche alcune definizioni di *cyber* illeciti quali:

[15] Cfr. Cass. Pen., 18 febbraio 2010, n. 27735 e Cass. Pen. 30 gennaio 2014, n. 4677.
[16] Si veda tra le più recenti Cass. Pen. 15.6.2022 n. 23401, Cass. Pen. 11.1.2023 n. 570, Cass. Pen. 22.5.2023 n. 21704.
[17] Si vedano, tra le tante: Cass. Pen., Sez. V, 8 gennaio 2020, n. 4470.; Cass. Pen., Sez. II, 13 aprile 2020 (ud. 7 novembre 2019), n. 11959. Da notare che i giudici di legittimità prendono spunto nelle loro decisioni anche dalla Convenzione di Budapest del Consiglio d'Europa del 2001.
[18] L. 547/1993. Cfr., tra le altre, Cass. 28.6.2023 n. 27900.
[19] Cfr., fra le altre, Cass. Pen. 7 novembre 2019 (dep. 10 aprile 2020), n. 11959.

- *phishing*, cioè quella forma di frode telematica realizzata attraverso l'invio di messaggi di posta elettronica contraffatti, apparentemente riconducibili a istituti finanziari o a piattaforme di commercio elettronico affidabili, con l'obiettivo di indurre il destinatario a comunicare dati sensibili quali il numero della carta di credito, i codici di sicurezza e le informazioni personali;
- *skimming*, che consiste nell'acquisizione fraudolenta dei dati contenuti nelle bande magnetiche delle carte elettroniche mediante l'uso di dispositivi (gli *skimmer*), capaci di leggere e memorizzare tali informazioni, incluso il codice PIN nel caso di carte bancomat o di carte di credito multifunzione.

2.1.2. I rischi connessi all'intelligenza artificiale nella commissione dei reati presupposto 231

Come accennato, l'integrazione di sistemi di intelligenza artificiale (AI) nei processi aziendali determina un ampliamento qualitativo e quantitativo delle aree di rischio rilevanti ai fini della responsabilità *ex* d.lgs. n. 231/2001, imponendo una rilettura in chiave evolutiva del paradigma della "colpa di organizzazione". In tale prospettiva, l'AI non costituisce un autonomo elemento giuridico, ma un fattore tecnologico che può incidere sulla struttura organizzativa dell'ente, sul governo dei processi e, conseguentemente, sulla prevedibilità e sui profili di rischio delle condotte illecite.

Sotto il profilo normativo, il quadro di riferimento è oggi significativamente arricchito dal Regolamento (UE) 2024/1689[20], che introduce un sistema di regolazione basato sul rischio (*risk-based approach*)[21], distinguendo tra sistemi vietati, ad alto rischio e a rischio limitato o minimo. In particolare, gli artt. 9–15 del citato Regolamento prevedono, per i sistemi ad alto rischio, obblighi stringenti in materia di *risk management*, governance dei dati, documentazione tecnica, trasparenza, supervisione umana e robustezza, che si pongono in evidente continuità funzionale con i presidi richiesti dal Modello di organizzazione, gestione e controllo[22].

Il quadro regolatorio europeo risulta, inoltre, oggi integrato dalla recente legge 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", che rappresenta il primo intervento organico del legislatore italiano in materia di AI. La legge, in linea con l'impostazione antropocentrica dell'AI Act, valorizza i principi di trasparenza, sicurezza, supervisione umana, tracciabilità e protezione dei diritti fondamentali, introducendo altresì specifiche previsioni in materia di cybersicurezza, tutela dei dati personali e responsabilità derivante dall'utilizzo dei sistemi di intelligenza artificiale. Tali disposizioni rafforzano ulteriormente l'esigenza, per gli enti, di integrare i presidi di governance dell'AI all'interno dei Modelli di organizzazione, gestione e controllo *ex* d.lgs. n. 231/2001, al fine di prevenire i rischi derivanti dall'impiego di tecnologie algoritmiche nei processi aziendali.

[20] Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).
[21] European Commission, *Ethics Guidelines for Trustworthy AI*, 2019.
[22] Si veda, sul punto, anche ISO/IEC 42001:2023 ("*Information technology - Artificial intelligence - Management system*").

In tale contesto, i principali profili di rischio 231 connessi all'utilizzo dell'intelligenza artificiale possono essere ricondotti a tre direttrici fondamentali.

In primo luogo, rilevano i rischi di commissione di reati informatici. L'impiego di sistemi di AI, in particolare quelli dotati di capacità di automazione e apprendimento, può facilitare la realizzazione di condotte quali accesso abusivo a sistemi informatici (art. 615-*ter* c.p.), intercettazione illecita di comunicazioni (art. 617-*quater* c.p.) o danneggiamento di dati e sistemi (artt. 635-*bis* ss. c.p.), amplificando l'efficacia e la scalabilità dell'azione illecita. In tali ipotesi, l'elemento organizzativo assume rilievo decisivo, in quanto l'assenza di adeguati controlli sull'utilizzo degli strumenti AI può integrare un deficit organizzativo rilevante ai fini dell'imputazione della responsabilità all'ente.

In secondo luogo, emergono rischi connessi ai reati contro la pubblica amministrazione, societari e finanziari. L'utilizzo di sistemi algoritmici nei processi decisionali (ad esempio, nella gestione di procedure di gara, nella selezione dei fornitori o nella predisposizione di informazioni finanziarie) può determinare alterazioni della trasparenza, della correttezza e della tracciabilità delle decisioni. In particolare, fenomeni di *bias* algoritmico, errori nei modelli o manipolazioni dei dati di input possono incidere sulla veridicità delle informazioni rilevanti, configurando ipotesi di false comunicazioni sociali o di indebita influenza nei rapporti con la pubblica amministrazione.

In terzo luogo, assumono rilievo i rischi in materia di protezione dei dati personali, con possibili intersezioni con il reato di trattamento illecito di dati. I sistemi di AI, fondati su grandi volumi di dati, possono dar luogo a trattamenti non conformi ai principi del Regolamento (UE) 2016/679, in particolare in relazione alla liceità, minimizzazione, trasparenza e limitazione delle finalità. L'art. 22 del GDPR, relativo ai processi decisionali automatizzati, e gli artt. 13-14 dell'AI Act[23], in tema di trasparenza e supervisione umana, delineano un quadro normativo che impone all'ente di assicurare la comprensibilità e verificabilità delle decisioni assunte utilizzando strumenti algoritmici.

Un ulteriore profilo critico attiene alla opacità dei sistemi di AI (c.d. *black box*), che può compromettere la ricostruibilità *ex post* dei processi decisionali e, conseguentemente, la capacità dell'ente di dimostrare l'efficace attuazione del Modello 231, soprattutto in termini di effettiva tracciabilità e verificabilità dei processi decisionali.

Alla luce di quanto sopra, l'integrazione dei rischi AI nel Modello 231 richiede l'adozione di specifici presidi organizzativi e procedurali (*infra*), tra cui:

- la mappatura dei sistemi di intelligenza artificiale utilizzati nei processi aziendali, con classificazione secondo i livelli di rischio previsti dall'AI Act;
- l'implementazione di un sistema di gestione del rischio AI coerente con l'art. 9 dell'AI Act;

[23] "Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)".

- la definizione di policy interne sull'utilizzo dell'AI, con particolare riferimento alla qualità dei dati, alla validazione dei modelli e alla supervisione umana;
- l'introduzione di meccanismi di auditabilità e di *logging* delle decisioni automatizzate;
- l'integrazione dei flussi informativi verso l'Organismo di Vigilanza, ai fini del monitoraggio dei rischi emergenti.

In tale prospettiva, il Modello 231 si configura come il naturale contenitore sistemico entro cui ricondurre anche la governance dell'intelligenza artificiale, in un'ottica di compliance integrata che tenga conto, oltre che del d.lgs. n. 231/2001, del GDPR, dell'AI Act e delle *best practices* internazionali (tra cui, in particolare, lo standard ISO/IEC 42001:2023 sui sistemi di gestione dell'intelligenza artificiale).

3. Intersezione tra Modello 231 e *cybersecurity*

La progressiva digitalizzazione dell'economia e l'utilizzo dell'intelligenza artificiale[24] hanno reso la sicurezza informatica una variabile strategica della vita d'impresa non più confinabile al perimetro della gestione tecnica dei sistemi IT. Le minacce cyber colpiscono oggi con effetti dirompenti la continuità operativa, il patrimonio informativo, la reputazione e la solidità patrimoniale delle organizzazioni, indipendentemente dalla loro dimensione o dal settore di appartenenza.

In questo scenario, il d.lgs. n. 231/2001 – concepito come strumento di contrasto alla criminalità economica d'impresa – rivela, anche sotto il profilo delle *best practices* aziendali, una straordinaria attitudine a governare anche il rischio informatico[25], grazie alla sua architettura fondata sulla "prevenzione mediante organizzazione" e sulla logica del *risk assessment* strutturato. L'intersezione tra il Modello di organizzazione, gestione e controllo e la *cybersecurity* si sviluppa lungo tre direttrici fondamentali: la gestione del rischio informatico come componente organica del Modello 231 (§ 3.1); l'analisi dei rischi e la mappatura delle aree sensibili (§ 3.3); il ruolo del Codice Etico e dei protocolli specifici quale presidio comportamentale e procedurale (§ 3.4). Ciascuna di queste dimensioni contribuisce a delineare un sistema integrato di compliance in cui la sicurezza informatica non è un adempimento aggiuntivo, ma una componente strutturale della governance d'impresa.

3.1. Il *risk approach* strutturato: adeguati assetti OAC e Risk Appetite Framework

Sotto il profilo operativo, l'integrazione del rischio informatico nel Modello 231 richiede che l'ente adotti un *risk approach* strutturato, che viene pacificamente collocato[26] nel più ampio contesto degli

[24] Comunemente indicate anche come Digit-AI.
[25] Fermi restando, naturalmente, i rischi della responsabilità amministrativa di tipo "para-penale", cui è esposto l'Ente, ai sensi degli artt. 5, 6 e 7 del d.lgs. n. 231/2001, in particolare, in presenza di un vantaggio, o anche solo di un interesse, a favore dell'Ente medesimo.
[26] CNDCEC e FNC, Gruppo interdisciplinare ESG-231, "Modello 231 e fattori ESG: l'importanza di una virtuosa connessione", 2024.

adeguati assetti organizzativi, amministrativi e contabili (OAC) citati dagli artt. 2381, 2403 e 2086, secondo comma[27], del codice civile; tali riferimenti hanno visto – tempo per tempo – assurgere le *best practices* aziendali al rango di norme di legge (trend a cui è ormai indirizzato tutto il diritto d'impresa). La logica degli adeguati assetti e quella del sistema 231 condividono un medesimo fondamento – la prevenzione mediante organizzazione – di talché il Modello 231 è ormai sistematicamente ascritto nel novero dei fattori che qualificano l'adeguatezza degli assetti, fermo restando il principio di proporzionalità secondo la natura e la dimensione dell'impresa. Gli OAC costituiscono in concreto l'infrastruttura attraverso cui l'impresa individua, valuta e governa i rischi rilevanti, inclusi quelli penalmente, economicamente e reputazionalmente significativi.

Il *risk approach*, inteso come metodo ordinatore della gestione, trova nel principio di corretta amministrazione e nei relativi assetti OAC la propria concreta attuazione; in via meramente esemplificativa e non esaustiva, esso comprende: mappatura dei processi, identificazione delle aree sensibili, *gap analysis*, tracciabilità delle decisioni, flussi informativi strutturati e sistemi di controllo interno. In tale contesto, il *Risk Appetite Framework* (RAF) si presta a una lettura estesa quale strumento attraverso cui l'impresa definisce il livello e la tipologia di rischio che la stessa è disposta ad assumere in funzione dei propri obiettivi strategici. Nel contesto della *cybersecurity*, il RAF consente di determinare quali vulnerabilità siano accettabili, quali richiedano un intervento immediato e quali possano essere gestite mediante meccanismi di trasferimento del rischio, come polizze *cyber liability* o contratti di outsourcing con *Service Level Agreement* (SLA) adeguati. Il Modello deve essere aggiornato periodicamente in relazione all'evoluzione dell'attività e del contesto normativo[28], requisito che in ambito *cyber* si traduce nell'obbligo di riesaminare la mappa dei rischi informatici almeno annualmente.

3.2. La dimensione *forward looking* e la resilienza organizzativa

La dimensione *forward-looking* connaturata alla *compliance* 231 assume, nel contesto della cybersecurity, un significato ulteriore rispetto a quello che già le viene riconosciuto in materia di adeguati assetti. Atteso che il rischio informatico è per sua natura prospettico, la valutazione dei rischi e delle azioni da introdurre per mitigarne gli effetti deve avere una funzione predittiva. In un contesto in cui la cybercriminalità è in fortissima evoluzione, ancor più con l'avvento dell'intelligenza artificiale, le minacce del futuro (anche prossimo) sono spesso diverse da quelle passate; pertanto, un sistema di presidio calibrato esclusivamente sulla base di vulnerabilità già manifestatesi, quindi, in concreto, sull'analisi storica dei fattori che determinano il rischio (cioè: probabilità e impatto), è da considerarsi strutturalmente inadeguato. L'adeguatezza degli assetti OAC si misura, pertanto, nella loro valenza

[27] Introdotto con il d.lgs. n. 14/2019, Codice della crisi d'impresa e dell'insolvenza, in G.U. n. 38 del 14 febbraio 2019. L'art. 375 ha novellato l'art. 2086, secondo comma, c.c.

[28] CNDCEC, "Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza", 2019; Confindustria, "Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo *ex* d.lgs. 231/2001", ultimo aggiornamento 2021, p. 23 ss.; Ministero della Giustizia, "Criteri guida per la redazione dei codici di comportamento delle associazioni rappresentative", 2025; Assonime, "Sulla riforma della disciplina della responsabilità degli enti - Osservazioni e proposte", Position Paper 4/2025.

prognostica, ossia in relazione alla capacità di intercettare segnali anticipatori e di supportare l'organo amministrativo nella lettura di scenari evolutivi non lineari: la prevenzione non è più solo evitare il ripetersi di ciò che è già accaduto, ma prepararsi a ciò che è ragionevolmente prevedibile.

Ad ogni modo, resta fermo e impregiudicato il ruolo cardine attribuito all'OdV, chiamato a vigilare:

i. sulla efficace attuazione del Modello 231;

ii. sull'aggiornamento del Modello: la moderna concezione del Modello deve incorporare meccanismi di *intelligence* idonei a cogliere *warning* e *alert* per possibili violazioni dei protocolli e delle procedure ad essi sottesi;

iii. sulle minacce emergenti (*threat intelligence*);

iv. sulle anomalie ripetute, quali i *pattern* ricorrenti;

v. sulla simulazione di scenari avversi (*stress test* e *tabletop exercises*);

vi. sull'organizzazione dei *follow-up* sulle azioni di *remediation* riferite ai gap progressivamente riscontrati, nonché di aggiornamento periodico delle valutazioni del rischio secondo una logica di *continuous risk assessment* (CRA), che contribuisce ad attribuire al Modello 231 la corretta dinamicità e l'effettivo governo del rischio.

Il Modello deve quindi incorporare meccanismi di intelligence sulle minacce emergenti, di simulazione di scenari avversi e di aggiornamento periodico delle valutazioni del rischio, in linea con il ciclo *Identify-Protect-Detect-Respond-Recover* del *NIST Cybersecurity Framework*[29]. La gestione del rischio informatico non si esaurisce peraltro nella prevenzione degli incidenti, ma deve estendersi alla preparazione dell'ente a rispondere efficacemente agli eventi avversi (*incident response*) e a ripristinare la propria operatività nei tempi previsti dai piani di *business continuity* e *disaster recovery*. La capacità di resilienza – intesa come attitudine a resistere agli attacchi, ad assorbirne gli impatti e a ripristinare le funzioni critiche – è oggi uno degli indicatori più significativi dell'adeguatezza organizzativa di un ente ed è proprio su tale terreno che la *compliance* 231 si intreccia più profondamente con le prescrizioni delle già richiamate normative e con gli standard internazionali di sicurezza delle informazioni, primo tra tutti la norma ISO/IEC 27001:2022[30].

È proprio in questa confluenza tra prevenzione, reazione e resilienza che si misura la qualità del Modello 231 in chiave *cyber*: un Modello efficace non è quello che previene tutti gli incidenti – obiettivo per definizione irraggiungibile – ma quello che consente all'ente di dimostrare di aver adottato ogni ragionevole misura di prevenzione.

[29] NIST, Cybersecurity Framework 2.0, National Institute of Standards and Technology, Gaithersburg (MD), 2024, p. 7 ss.
[30] Information security, cybersecurity and privacy protection - Information security management systems - Requirements.

3.3. Analisi dei rischi e mappatura delle aree sensibili

3.3.1. Il fondamento metodologico: dalla norma alla prassi operativa

L'analisi dei rischi e la mappatura delle aree sensibili rappresentano il nucleo metodologico del Modello 231 e il fondamento operativo di qualsiasi sistema di *compliance* integrata che voglia includere efficacemente la dimensione della c*ybersecurity* nel *framework* di gestione dei rischi. Il Modello non può limitarsi a un elenco astratto di fattispecie di reato, ma la sua elaborazione deve scaturire da una ricognizione puntuale e documentata dei processi aziendali, delle attività sensibili e delle modalità concrete attraverso cui i reati presupposto potrebbero essere commessi nell'interesse o a vantaggio dell'ente. Questa esigenza, che nella prassi 231 si esprime nella cosiddetta «analisi *as-is*» dell'organizzazione, assume nella sua applicazione alla *cybersecurity* una complessità aggiuntiva dovuta alla rapidità con cui evolve il panorama delle minacce informatiche e delle modalità con cui le stesse si manifestano e, quindi, alla difficoltà di circoscrivere con precisione il perimetro dei sistemi e dei dati esposti.

Il concetto di "area sensibile", nella sua accezione originaria riferita ai reati presupposto del decreto 231, si arricchisce di contenuto quando applicato al rischio informatico. Un'area è sensibile sotto il profilo *cyber* non soltanto quando in essa si svolge un'attività che potrebbe dare luogo a un reato informatico presupposto (accesso abusivo, danneggiamento di sistemi, intercettazione illecita), ma anche quando essa tratta dati personali in misura tale da esporre l'ente a responsabilità ai sensi del GDPR, gestisce infrastrutture critiche rilevanti ai fini della normativa NIS2 o utilizza sistemi informatici la cui compromissione potrebbe determinare danni patrimoniali, operativi o reputazionali significativi.

Quanto sopra anche considerando attentamente che molti fra i reati informatici o, più in generale, le condotte di *cybercrime*, sono propedeutici alla commissione di altri illeciti di cui al c.d. "catalogo" dei reati 231 (si pensi ai reati di riciclaggio e autoriciclaggio, contro la PA, societari, fiscali, di *market abuse*, ecc.). In questa prospettiva ampliata, la mappatura delle aree sensibili in chiave *cyber* diventa uno strumento di lettura integrata dei rischi d'impresa.

3.3.2. L'inventario degli asset informatici e informativi

La mappatura prende avvio dall'inventario degli asset informatici e informativi dell'ente.

Tale attività deve quindi comprendere non solo i sistemi hardware e software in senso stretto, ma anche i dati (con grande cura della loro qualità intrinseca) nella loro dimensione strategica, quali esemplificativamente: dati di clienti/fornitori/terze parti, informazioni commerciali riservate, *know-how* tecnico, segreti industriali e quell'insieme di asset immateriali – i cosiddetti *intangibles* – quali reputazione, brand, capitale umano e relazionale, capacità di innovazione, posizionamento nella filiera, affidabilità ESG, ecc.

Nella maggior parte dei casi, tali asset non sono iscritti né valorizzati nel bilancio, determinando uno scollamento strutturale tra rappresentazione contabile e valore economico effettivo dell'impresa: ciò che non è misurato e monitorato tende a essere meno governato. In questa prospettiva, il Modello 231

– in chiave *cyber* – può assumere una funzione cruciale nel presidiare quei fattori immateriali che, pur non emergendo contabilmente, incidono in modo determinante sulla creazione di valore. La mappatura della situazione attuale [Current State Map (CSM) o analisi *As-Is*] degli asset in argomento trova nella digitalizzazione un alleato di fondamentale utilità[31] al fine di strutturarla, fra l'altro, secondo criteri di classificazione che tengano conto del livello di criticità per la continuità operativa, della sensibilità delle informazioni trattate ai fini della riservatezza, del valore economico e strategico delle informazioni in caso di sottrazione o di divulgazione non autorizzata e dei requisiti normativi applicabili alla loro conservazione e protezione. In merito, è utile considerare che la metodologia ISO/IEC 27005[32] fornisce un *framework* di riferimento consolidato.

3.3.3. La mappatura dei processi e le categorie di aree sensibili

Partendo dall'inventario degli *asset*, la mappatura procede attraverso l'identificazione dei processi aziendali che li trattano, con particolare attenzione ai flussi informativi interni ed esterni. In questa fase assume rilievo la nozione di «processo a rischio», inteso come qualsiasi attività organizzativa che, per la sua natura, per le sue modalità di esecuzione o per i soggetti che vi partecipano, presenta una concreta esposizione a minacce di natura informatica.

I processi di gestione delle identità digitali e dei privilegi di accesso rappresentano forse l'area di maggiore criticità: la capacità di controllare chi può accedere a quali sistemi e con quali permessi è il presupposto di qualsiasi architettura di sicurezza, e la sua compromissione – attraverso furto di credenziali, escalation di privilegi o uso improprio di account amministrativi – apre la strada alla quasi totalità delle tipologie di attacco. I processi di approvvigionamento e di gestione dei fornitori espongono l'ente al rischio della *supply chain*: un fornitore di servizi IT con accesso remoto ai sistemi o un software commerciale non aggiornato possono diventare vettori di attacco. I processi di gestione delle comunicazioni elettroniche – e-mail, messaggistica, videoconferenza – sono il canale privilegiato

[31] Fra i principali vantaggi della digitalizzazione nella mappatura As-Is degli asset in argomento:
- accuratezza e riduzione degli errori: l'uso di tecnologie digitali (come IoT, scanner 3D, LIDAR) per il rilievo degli asset elimina l'errore umano tipico delle mappature manuali, garantendo l'esatta ubicazione e conformità degli asset;
- visibilità in tempo reale e geolocalizzazione: la digitalizzazione consente di geolocalizzare gli asset e monitorarne lo stato in tempo reale. Questo permette di conoscere l'inventario dettagliato e la posizione esatta di ogni elemento;
- creazione di digital twin: la CSM digitalizzata costituisce la base per lo sviluppo di un Digital Twin (gemello digitale). Questo modello virtuale simula le condizioni reali dell'asset, permettendo di prevedere guasti, simulare scenari e ottimizzare le prestazioni;
- standardizzazione e centralizzazione dei dati: attraverso sistemi digitali, i dati sparsi (cartacei, fogli Excel) vengono centralizzati in un unico hub (Digital Asset Management - DAM), rendendo le informazioni accessibili, aggiornate e condivise tra i vari *stakeholder*;
- efficienza operativa e manutenzione predittiva: con una mappatura digitale è possibile analizzare i flussi di lavoro, identificare sprechi e inefficienze (Lean production) e pianificare interventi di manutenzione proattiva, riducendo i tempi di inattività;
- supporto alle decisioni (*decision making*): la visualizzazione chiara e interattiva degli *asset* (tramite mappe 2D/3D) facilita la comprensione del contesto e migliora le decisioni strategiche su investimenti, manutenzioni e gestione del ciclo di vita.

In sintesi, la digitalizzazione trasforma la *Current State Map* da documento statico a piattaforma dinamica di gestione, essenziale per la sostenibilità e la competitività industriale. Tratto con modifiche da "Digitalizzazione per la sostenibilità", Associazione Infrastrutture sostenibili, Position Paper n. 8, 2024.

[32] ISO/IEC 27005:2022, "Guidance on managing information security risks, International Organization for Standardization", 2022; Confindustria, "Linee guida", cit., p. 34 ss.

di attacchi di *phishing*, *spear phishing* e *Business E-mail Compromise* (BEC), che rappresentano oggi la causa più frequente di incidenti di sicurezza[33]. In particolare, processi che gestiscono transazioni finanziarie e autorizzazioni di pagamento sono altamente sensibili: in questi ambiti, la compromissione informatica si traduce direttamente in un danno patrimoniale e/o reputazionale, con tempi di reazione spesso insufficienti a impedire l'irreversibilità dell'operazione fraudolenta. I processi di gestione dei dispositivi mobili e del lavoro da remoto hanno acquisito una criticità del tutto nuova nel contesto post-pandemico: la dispersione del perimetro operativo ha amplificato significativamente la superficie di attacco disponibile. I processi di conservazione e backup dei dati assumono rilievo cruciale nella prospettiva della resilienza: un *ransomware* efficace mira sistematicamente a compromettere i *backup* prima di cifrare i dati produttivi, rendendo indispensabile l'adozione di architetture di *backup* immutabili e geograficamente distribuite.

3.3.4. Cenni sulla valutazione del rischio cyber-residuo

Ciascuna area sensibile deve essere oggetto di una valutazione del rischio che tenga conto di tre parametri fondamentali: *i)* la probabilità che una minaccia si materializzi (*likelihood*), *ii)* la gravità delle conseguenze (*impact*) e *iii)* l'efficacia dei controlli già esistenti (*control effectiveness*). La combinazione di questi tre fattori consente di costruire una mappa del rischio residuo, base informativa su cui fondare le decisioni di investimento in sicurezza e di adeguamento organizzativo.

La stima della probabilità deve tener conto sia della minaccia esterna che di quella interna, rappresentata dai comportamenti dolosi o colposi del personale. I dati statistici disponibili indicano che una quota significativa degli incidenti di sicurezza ha origine interna[34], sia per l'azione deliberata di soggetti che abusano dei propri privilegi di accesso (*insider threat*), sia per l'errore umano involontario. La valutazione dell'impatto deve essere condotta su più dimensioni: operativa, economica diretta, reputazionale, legale e regolatorio, nonché sugli *intangibles*. L'efficacia dei controlli esistenti deve essere valutata non solo in termini di presenza formale, ma di effettiva implementazione e funzionamento: in tal senso, un controllo previsto ma non effettivamente implementato non solo è inidoneo a prevenire il rischio ma può persino aggravare la posizione dell'ente in sede processuale[35].

3.3.5. Il rischio nella filiera (supply chain risk)

Un profilo di particolare complessità è rappresentato dalla catena di fornitura. Nelle organizzazioni moderne, i sistemi informatici sono profondamente interconnessi con quelli di fornitori, partner e subappaltatori, creando un perimetro di rischio che va ben oltre i confini fisici e giuridici dell'ente[36].

---

[33] European Union Agency for Cybersecurity (ENISA), "Threat Landscape 2024, European Union Agency for Cybersecurity", Atene, 2024, p. 28 ss.; CLUSIT, "Rapporto sulla sicurezza ICT in Italia 2025", p. 45 ss.

[34] Verizon, Data Breach Investigations Report 2024, Basking Ridge (NJ), 2024, p. 12: l'82% delle violazioni coinvolge il fattore umano (phishing, uso di credenziali rubate, errori).

[35] Si veda, ad esempio, Cass. pen., n. 30039/2025.

[36] Episodi come l'attacco alla supply chain di SolarWinds hanno reso drammaticamente evidente quanto questo vettore di rischio sia sottovalutato e difficile da prevenire. Da segnalare, inoltre, un ulteriore caso recentemente assurto alle cronache che ha coinvolto il celebre magazzino di lusso Harrods. In questo caso non è stato colpito direttamente Harrods, ma un suo fornitore di servizi e-commerce di terze parti. Dati esposti: sono stati compromessi i record di circa 430.000 clienti, inclusi nomi, contatti e dettagli dei programmi fedeltà. Questi episodi confermano che oggi gli *hacker* preferiscono colpire un singolo

Il Modello 231 deve pertanto estendere la sua analisi anche ai rischi indotti da soggetti terzi che hanno accesso – fisico o logico – ai sistemi o ai dati dell'ente. Tale estensione si traduce in requisiti contrattuali minimi di sicurezza informatica da imporre ai fornitori, in procedure di verifica periodica del loro rispetto (audit di sicurezza, questionari di autovalutazione, richiesta di certificazioni come ISO/IEC 27001) e in meccanismi di gestione degli incidenti che prevedano obblighi di notifica tempestiva. Non a caso, la normativa NIS2[37] impone agli operatori di servizi essenziali di adottare misure adeguate alla gestione dei rischi posti dalla catena di approvvigionamento, creando un raccordo diretto con la logica di presidio del Modello 231[38].

3.3.6. La dinamicità della mappatura e l'integrazione nel Modello 231

La mappatura delle aree sensibili non è un'attività episodica, ma un processo continuo che deve essere aggiornato ogniqualvolta intervengano modifiche significative nell'organizzazione, nei sistemi informatici, nel contesto normativo o nel panorama delle minacce e/o dei comportamenti *cybercrime*. Come già osservato, esiste una diversa velocità con cui evolvono diritto e mercato (nel caso di specie, il "mercato del crimine cibernetico"): il diritto procede per stratificazione e consolidamento, mentre il panorama delle minacce cyber è caratterizzato da accelerazioni improvvise e discontinuità tecnologiche. Questo divario determina il cosiddetto "*regulatory lag*": quando una norma entra in vigore, la tecnologia che intendeva regolare è spesso già superata. Per tentare di colmare questo gap, oggi si tende a passare da leggi rigide a *framework* dinamici (come il GDPR o l'AI Act) che non impongono regole tecniche fisse, ma stabiliscono obiettivi di sicurezza e gestione del rischio che le aziende devono aggiornare costantemente. In pratica, il diritto sta cercando di passare da una postura di tipo "fotografico" ad una fisionomia di "processo". D'altra parte, gli assetti organizzativi, se adeguati, consentono alle imprese di attenuare questo divario traducendo le regole giuridiche in capacità organizzativa; in tal senso, la mappatura cyber non è un mero "scatto fotografico", ma un "film in movimento", e la relativa compliance 231 deve dotarsi degli strumenti per seguirne l'evoluzione in tempo reale.

Va, infine, sottolineato il rapporto tra la mappatura delle aree sensibili e il più ampio sistema di compliance integrata che ha nel Modello 231 il proprio fulcro metodologico quale componente organica del processo di valutazione e presidio dei rischi che caratterizza una buona governance d'impresa. In particolare, la mappatura *cyber* non è un adempimento autonomo e settoriale, in quanto la sua peculiare caratteristica risiede proprio nella sua intrinseca trasversalità rispetto ai processi e alle aree aziendali sensibili ai rischi reato. La relativa integrazione nel Modello 231 consente di costruire un sistema unitario e razionale di gestione del rischio, evitando le duplicazioni tipiche degli approcci frammentati: una sola mappa dei processi, un solo sistema di valutazione del rischio, un solo sistema

fornitore di servizi o una libreria condivisa per ottenere l'accesso a migliaia di vittime contemporaneamente, piuttosto che tentare di violare ogni azienda singolarmente; NOVA News, marzo 2025 (www.agenzianova.com/news/attacco-hacker-a-harrods-rilevati-tentativi-di-accesso-non-autorizzato).

[37] Art. 21, par. 2, lett. d), Direttiva NIS2: gestione della sicurezza della catena di approvvigionamento.

[38] In particolare, l'art. 39 del decreto di recepimento NIS2 ha esplicitamente integrato l'art. 24-*bis* del d.lgs. n. 231/2001 inserendo nel catalogo dei reati presupposto l'omessa comunicazione o la comunicazione di dati falsi o incompleti all'Agenzia per la Cybersicurezza Nazionale (ACN).

di controllo capace di declinare i propri presidi in chiave 231, GDPR, NIS2, ESG, secondo una logica modulare e coerente.

Infine, in tema di evoluzione dell'adeguatezza degli assetti OAC e dei collegati organigrammi e funzionigrammi aziendali, anche il ruolo dell'Information Technology ha subito una metamorfosi: da tipica funzione aziendale di *staff*, ha assunto sempre più una funzione strategica che culmina negli attuali ruoli di IT, Digital Transformation e AI Manager. Questo cambiamento è guidato dall'integrazione pervasiva della tecnologia in ogni aspetto operativo, trasformando l'IT da centro di costo a soggetto decisionale e generatore di valore.

3.4. L'aggiornamento del Codice Etico e dei protocolli specifici della Parte Speciale "Reati informatici" del Modello

L'aggiornamento del Codice Etico e dei protocolli specifici della Parte Speciale "Reati informatici" risponde all'esigenza di rafforzare la cultura della legalità digitale, promuovere comportamenti corretti nell'utilizzo degli strumenti informatici e implementare misure organizzative, procedurali e tecnologiche idonee a prevenire il rischio di commissione dei reati presupposto.

Di seguito sono illustrati i principali interventi di revisione da effettuare, le motivazioni sottese all'aggiornamento e i presidi da introdurre al fine di garantire una più efficace gestione del rischio *cyber* e una maggiore integrazione tra compliance normativa, sicurezza informatica e governance aziendale.

3.4.1. Il Codice Etico come presidio comportamentale della sicurezza informatica

Il Codice Etico e i protocolli operativi specifici costituiscono la dimensione comportamentale e procedurale del Modello 231, quella attraverso cui i principi generali della compliance si traducono in regole concrete di condotta destinate a orientare l'agire quotidiano di tutti i soggetti che operano nell'ambito dell'ente. In materia di *cybersecurity*, questa dimensione assume un'importanza del tutto particolare, poiché una quota significativa degli incidenti di sicurezza informatica origina non da vulnerabilità tecniche irrisolvibili, bensì da comportamenti umani inadeguati: credenziali condivise o deboli, apertura di allegati malevoli, comunicazione di informazioni riservate attraverso canali non protetti, uso di dispositivi personali non autorizzati. Il "fattore umano" è, in ultima analisi, la principale superficie di attacco di qualsiasi organizzazione, indipendentemente dal livello di sofisticazione tecnologica dei sistemi di difesa adottati. Il Codice Etico, nella sua funzione di documento fondativo dei valori e dei principi di condotta – una sorta di "carta costituzionale" dell'ente – deve incorporare esplicitamente i principi della sicurezza delle informazioni. Sul piano sostanziale, il Codice deve affermare con chiarezza che la tutela delle informazioni aziendali, dei dati personali di clienti e dipendenti e dell'integrità dei sistemi informatici è un dovere di ogni membro dell'organizzazione, non una responsabilità esclusiva (nella prassi generalmente posta in capo alla funzione IT) e deve altresì sancire i principi di riservatezza, integrità e disponibilità delle informazioni (i cosiddetti principi CIA: *Confidentiality, Integrity, Availability*) come valori fondamentali.

Come evidenziato, la *compliance* 231, letta in chiave sostanziale, impone all'impresa di interrogarsi sulla razionalità dei processi decisionali, sulla chiarezza delle responsabilità e sull'effettività dei controlli. In tal senso, in materia di *cybersecurity*, il Codice Etico non è semplicemente un elenco di divieti, ma lo strumento attraverso cui l'organizzazione costruisce e trasmette una cultura della sicurezza informatica, rendendo ogni dipendente consapevole del proprio ruolo nel sistema di difesa collettiva. Un Codice Etico che non sia stato adeguatamente comunicato, formato e interiorizzato rimane un documento inerte, incapace di produrre gli effetti preventivi che il legislatore del 2001 aveva in mente.

Un discorso a parte merita la collocazione - nel Codice Etico e/o nel Modello 231 - delle policy sull'uso dei social media aziendali. Le stesse possono trovare sistemazione in entrambi i documenti, ma con finalità e livelli di dettaglio differenti. Spesso, la soluzione migliore è una integrazione tra i due. In particolare:

- nel Codice Etico andrebbero inseriti i principi generali di condotta, i valori aziendali, la riservatezza, il rispetto della reputazione aziendale e dei colleghi sui social. Il Codice Etico è il "luogo" ideale per definire come comportarsi in modo corretto e leale;
- nel Modello 231 andrebbero inseriti protocolli e i divieti sanzionabili, i controlli, i flussi informativi ad evento e periodici *ad hoc*, con richiamo alle procedure aziendali specifiche ad essi sottesi, specialmente se l'uso dei social è collegato ad aree a rischio reato (es. diffusione di notizie riservate, diffamazione, *cybercrime*, corruzione). La "Social Media Policy" in questo caso è a tutti gli effetti un protocollo preventivo.

In sintesi, l'integrazione tra Codice Etico e Modello consente di definire rispettivamente cosa è etico e *cosa* è sanzionabile e come prevenirlo.

3.4.2. I protocolli specifici: struttura e contenuti essenziali

Accanto al Codice Etico, in materia di reati informatici e *cybersecurity* il Modello 231 richiede l'adozione di un sistema articolato di protocolli operativi specifici, ciascuno destinato a disciplinare un'area di rischio o un processo aziendale determinato. Nella prassi, gli stessi trovano allocazione nella Parte Speciale del Modello dedicata ai reati informatici che: *i)* a fronte delle più volte richiamate evoluzioni organizzativo-tecnologiche e *ii)* dell'avvento della citata l. n. 132/2025 (e delle disposizioni che saranno definite dal Governo nell'esercizio della delega in essa contenuta) sarà sottoposta a un opportuno aggiornamento. La progettazione dell'aggiornamento del Modello in argomento deve rispondere a criteri di:

- proporzionalità rispetto alla dimensione e complessità dell'ente;
- coerenza con le previsioni del Codice Etico;
- allineamento all'*assessment*, relativa *gap analysis* e azioni di rimedio e miglioramento all'uopo individuate;
- verificabilità, attraverso indicatori misurabili di conformità ed efficacia, il tutto secondo la già richiamata valutazione del rischio e l'impostazione di *continuous risk assessment*.

Entrando nel merito della prassi e delle *best practices* riferite ai principali presidi del Modello atti a prevenire la violazione dello stesso e la commissione di illeciti e, in particolare, dei reati 231 commessi nell'interesse o vantaggio dell'ente, si segnalano i seguenti:

- il Protocollo di gestione delle identità e degli accessi, *c.d. Identity and Access Management* (IAM), si evidenzia fra i più "critici" e fa riferimento alle modalità di assegnazione, modifica e revoca dei privilegi di accesso ai sistemi informatici, in coerenza con il principio del minimo privilegio (*least privilege*) e con la segregazione dei compiti[39]. Tale policy si raccorda direttamente con il sistema di deleghe e poteri definiti dalla governance aziendale e, quindi, dal Modello 231; il principio di segregazione dei compiti – cardine della compliance 231 nella prevenzione delle frodi interne – trova nella IAM la sua applicazione più diretta in ambito digitale.
- Il Protocollo di gestione degli incidenti di sicurezza informatica definisce invece, attraverso una logica di conformità integrata, le procedure da attivare in caso di violazione (o sospetta violazione) della sicurezza dei sistemi o dei dati. Esso deve stabilire la catena di *escalation* interna, i tempi e le modalità di notifica alle autorità competenti (ad esempio: Garante per la protezione dei dati personali entro 72 ore e CSIRT nazionale entro 24 ore per gli operatori di servizi essenziali[40]), le misure di contenimento e di ripristino, nonché le procedure di conservazione delle evidenze forensi ai fini di eventuali procedimenti penali. Sul piano 231, la gestione documentale degli incidenti, oltre a soddisfare il fondamentale principio di evidenza/tracciabilità e la collegata funzione di mezzo di prova, dimostra l'efficace funzionamento del Modello attraverso la reattività dell'ente, oltreché la sua capacità di apprendimento dagli eventi avversi.
- Il Protocollo relativo ai dispositivi e al lavoro da remoto regola l'utilizzo dei dispositivi personali (BYOD), dei dispositivi aziendali fuori sede e delle connessioni da reti non protette (ad esempio, attraverso idonee prescrizioni sull'uso di reti VPN, sulla cifratura dei dispositivi e sulla gestione della perdita o del furto).
- Il Protocollo di gestione dei fornitori e dei soggetti terzi estende il perimetro dei presidi 231 alla catena di fornitura, imponendo requisiti minimi di sicurezza informatica ai fornitori che accedono ai sistemi o ai dati dell'ente e disciplinando le modalità di verifica periodica del loro rispetto.

Di cruciale importanza è il raccordo tra i protocolli cyber e il sistema dei flussi informativi – periodici e ad evento – verso l'Organismo di Vigilanza. Quest'ultimo deve infatti disporre di canali strutturati per ricevere segnalazioni di anomalie, incidenti e sospette violazioni in materia di *cybersecurity*, nonché di reporting periodici sulla impostazione di sicurezza dell'ente (*infra*). La normativa sul *whistleblowing*[41] rafforza ulteriormente questo sistema, imponendo la predisposizione di canali riservati per la segnalazione di violazioni che possono includere anche gli incidenti di sicurezza informatica. I protocolli cyber del Modello 231 dovrebbero infine raccordarsi con le prescrizioni dell'AI Act, contribuendo alla

[39] CIS Controls versione 8, Center for Internet Security, East Greenbush (NY), 2021, Control 6 (Access Control Management).
[40] Art. 33 GDPR (notifica al Garante entro 72 ore); art. 23 Direttiva NIS2 (notifica al CSIRT entro 24 ore per operatori di servizi essenziali).
[41] Sul punto si veda anche CNDCEC, "Linee guida per lo svolgimento delle funzioni dell'Organismo di vigilanza *ex* D.lgs. 8 giugno 2001, n. 231", a cura dell'Osservatorio nazionale D.lgs. 231/2001, novembre 2025.

costruzione di un sistema di compliance integrata che governi in modo unitario i rischi dell'innovazione digitale.

In conclusione, il Codice Etico e i protocolli specifici in materia di cybersecurity non costituiscono un apparato burocratico aggiuntivo, ma la naturale proiezione comportamentale e procedurale del Modello 231 nel dominio digitale. Essi traducono il *risk approach* e la mappa delle aree e dei processi sensibili in regole operative concrete, capaci di orientare i comportamenti quotidiani e di dimostrare, in caso di procedimento a carico dell'ente, che l'organizzazione aveva adottato ed efficacemente attuato un sistema idoneo a prevenire i reati informatici presupposto. In tale prospettiva, la *compliance cyber* non si sovrappone alla *compliance* 231, ma ne costituisce una componente organica e inscindibile, indispensabile in un contesto economico e normativo in cui il rischio informatico è ormai parte strutturale del rischio d'impresa.

3.5. Piani di formazione e sensibilizzazione per il personale

3.5.1. Premessa e finalità

Nell'ambito della prevenzione dei reati informatici e, più in generale, della gestione del rischio cyber, la formazione e la sensibilizzazione del personale assumono un ruolo centrale ai fini dell'efficace attuazione del Modello 231. L'esperienza applicativa maturata e le *best practices* in materia di responsabilità amministrativa degli enti ha, infatti, evidenziato come l'adozione di protocolli e procedure formalmente adeguati non sia, di per sé, sufficiente a garantire l'efficacia esimente del Modello, ove non sia accompagnata da un'attività formativa concreta, continuativa e adeguatamente documentata.

La crescente diffusione dei reati informatici, degli attacchi *cyber* e delle violazioni dei dati personali rende necessario che dipendenti, collaboratori e figure apicali siano adeguatamente formati non solo sotto il profilo tecnico, ma anche in relazione ai profili giuridici e organizzativi connessi all'utilizzo degli strumenti informatici. In tale prospettiva, la formazione rappresenta uno strumento essenziale per sviluppare consapevolezza circa i rischi derivanti da condotte imprudenti o non conformi alle procedure aziendali, favorendo altresì la tempestiva individuazione e segnalazione di anomalie, incidenti informatici o possibili violazioni.

Le attività formative dovrebbero pertanto essere orientate a diffondere una cultura aziendale della cybersicurezza coerente con i principi del Modello 231, con la disciplina in materia di protezione dei dati personali e con la normativa nazionale ed europea relativa alla sicurezza informatica, inclusa la Direttiva NIS2. Particolare attenzione dovrebbe essere riservata ai comportamenti quotidiani maggiormente esposti al rischio *cyber*, quali la gestione delle credenziali di accesso, l'utilizzo degli strumenti aziendali, il trattamento dei dati e il riconoscimento di tentativi di *phishing*, *malware* o altre forme di attacco informatico.

Sotto il profilo organizzativo, la predisposizione di programmi formativi periodici, differenziati in funzione dei ruoli e delle responsabilità ricoperte, contribuisce, inoltre, a rafforzare l'effettività del

sistema di controllo interno e consente all'ente di dimostrare l'adozione di misure preventive concretamente attuate e verificabili anche da parte dell'Organismo di Vigilanza.

3.5.2. Destinatari e livelli di formazione

Affinché le attività di formazione risultino effettivamente idonee a prevenire i rischi *cyber* e i reati informatici rilevanti ai sensi del d.lgs. n. 231/2001, i percorsi formativi dovrebbero essere strutturati secondo criteri di proporzionalità e differenziazione, tenendo conto delle funzioni svolte, del livello di responsabilità ricoperto e del grado di esposizione al rischio dei diversi destinatari.

Un primo livello di formazione dovrebbe riguardare l'intero personale aziendale, inclusi collaboratori esterni, lavoratori somministrati e, ove opportuno, soggetti terzi che abbiano accesso ai sistemi informativi dell'ente. In tale ambito, l'obiettivo principale consiste nel diffondere una conoscenza di base dei rischi informatici, delle principali tecniche di attacco e dei comportamenti corretti da adottare nella gestione quotidiana degli strumenti digitali e dei dati aziendali. La formazione di base assume particolare rilevanza in quanto numerosi incidenti informatici derivano da errori umani, utilizzo improprio delle credenziali di accesso o mancato riconoscimento di tentativi di *phishing* e altre attività fraudolente. Per tale ragione, essa dovrebbe essere erogata sin dall'inizio del rapporto lavorativo e aggiornata periodicamente attraverso contenuti pratici e aderenti alle concrete modalità operative dell'impresa.

Un secondo livello formativo interessa, invece, i soggetti che svolgono funzioni tecniche o di controllo in materia di sistemi informatici, sicurezza e compliance, quali responsabili IT, amministratori di sistema, referenti per la cybersicurezza, Data Protection Officer e personale delle funzioni di audit interno. Per tali figure si rende necessario un grado di approfondimento maggiore, finalizzato a garantire competenze adeguate nella prevenzione, individuazione e gestione degli incidenti informatici, nonché nella corretta applicazione delle misure di sicurezza richieste dalla normativa vigente. In questo ambito, assumono particolare importanza le attività di aggiornamento tecnico, le simulazioni operative e le esercitazioni relative alla gestione di possibili scenari di crisi *cyber*.

Un ulteriore livello di formazione dovrebbe, infine, coinvolgere gli organi di vertice dell'ente e l'Organismo di Vigilanza. La crescente rilevanza della cybersicurezza sotto il profilo della governance aziendale richiede infatti che amministratori, dirigenti apicali e componenti dell'OdV acquisiscano adeguata consapevolezza sia del quadro normativo di riferimento, sia delle implicazioni organizzative, economiche e sanzionatorie connesse ai rischi informatici. In particolare, anche alla luce della Direttiva NIS2 e della recente normativa nazionale in materia di cybersicurezza, tali soggetti sono chiamati a supervisionare le strategie di gestione del rischio cyber, valutare l'adeguatezza dei presìdi organizzativi adottati e verificare l'effettiva implementazione delle misure preventive previste dal Modello 231.

3.5.3. Argomenti e contenuti formativi

I principali argomenti da affrontare all'interno dei piani formativi possono essere sintetizzati come segue:

1) Modulo base — Sensibilizzazione generale

1.1 La responsabilità dell'ente per i reati informatici

- Il quadro del d.lgs. n. 231/2001: principi generali della responsabilità amministrativa degli enti dipendente da reato.
- L'art. 24-*bis* e il catalogo dei reati informatici presupposto, con evidenza delle novità introdotte dalla l. n. 90/2024.
- Il concetto di "interesse o vantaggio" dell'ente nella commissione di reati informatici.
- Le sanzioni applicabili: sanzioni pecuniarie, sanzioni interdittive, confisca.
- Casi pratici: esempi di condotte che possono integrare reati presupposto nell'operatività quotidiana (es. accesso non autorizzato a sistemi, utilizzo improprio di credenziali, manomissione di dati).

1.2 Il perimetro di sicurezza e il ruolo del singolo

- Ogni dipendente come "anello" della catena di sicurezza: il fattore umano come principale vettore di attacco.
- Panoramica delle minacce più diffuse: *phishing* (e-mail fraudolente), *spear phishing*, *smishing* (SMS), *vishing* (chiamate telefoniche), *social engineering*, Business E-mail Compromise (BEC).
- Riconoscimento dei segnali di allarme: URL sospetti, richieste urgenti e inusuali, allegati non attesi, mittenti contraffatti.
- Simulazioni pratiche di phishing: analisi di e-mail campione, riconoscimento di pagine web contraffatte.

1.3 Igiene digitale e uso sicuro degli strumenti

- Gestione sicura delle password: complessità, unicità, non condivisione, utilizzo di *password manager*.
- Autenticazione a più fattori (MFA): principi di funzionamento, attivazione e utilizzo.
- Uso accettabile degli asset aziendali: dispositivi, e-mail, servizi cloud, reti Wi-Fi, supporti rimovibili.
- Navigazione sicura: riconoscimento di siti fraudolenti, download solo da fonti verificate, attenzione ai certificati digitali.
- Sicurezza dei dispositivi mobili: aggiornamenti, blocco schermo, separazione dati aziendali/personali.
- Lavoro da remoto e *smart working*: utilizzo della VPN, sicurezza della rete domestica, *clean desk policy*, gestione di stampe e documenti.
- Politiche di restituzione e dismissione degli asset.

1.4 Protezione dei dati e privacy

- Principi fondamentali del GDPR e loro applicazione pratica quotidiana.

- Classificazione dei dati: personali, particolari, aziendali riservati.
- Trattamento illecito di dati come reato-presupposto 231 (art. 167 d.lgs. n. 196/2003).
- Misure minime per la protezione dei dati nell'operatività di ciascun ruolo.

1.5 Segnalazione degli incidenti e whistleblowing

- Cosa si intende per "incidente di sicurezza": definizione ampia, comprensiva di sospetti e quasi-incidenti.
- Procedure interne di segnalazione: a chi segnalare, come segnalare, entro quali tempi.
- Il canale di segnalazione *whistleblowing*: modalità di accesso, tutela della riservatezza del segnalante, protezione contro le ritorsioni, in conformità alle Linee Guida ANAC n. 1/2025.
- L'importanza della tempestività: obbligo di segnalazione entro 24 ore dal rilevamento (pre-notifica) e 72 ore (notifica completa) ai sensi della NIS2.
- Conseguenze della mancata segnalazione nel sistema disciplinare previsto dal Modello 231.

2) Modulo intermedio — Sicurezza operativa

2.1 Architettura di sicurezza e gestione delle vulnerabilità

- Inventario e governance degli asset IT: dispositivi, software, licenze, configurazioni.
- Principi di *hardening* dei sistemi: disabilitazione di servizi non necessari, configurazione sicura, principio del privilegio minimo.
- *Vulnerability assessment* e *penetration testing*: finalità, periodicità, gestione dei risultati.
- *Patch management*: processi per l'applicazione tempestiva degli aggiornamenti di sicurezza.
- Protezione perimetrale: *firewall*, sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS), segmentazione della rete.

2.2 Incident response

- Piano di risposta agli incidenti: struttura, ruoli e responsabilità.
- Playbook operativi per le principali tipologie di incidente (ransomware, *data breach*, compromissione account, DDoS).
- Fasi della gestione dell'incidente: identificazione, contenimento, eradicazione, ripristino, *lessons learned*.
- Obblighi di notifica agli enti competenti: CSIRT Italia (ACN), Garante Privacy, Autorità giudiziaria.
- Coordinamento con CISO, DPO e OdV durante e dopo l'incidente.
- Documentazione e conservazione delle evidenze digitali (*digital forensics*).

2.3 Log management e monitoraggio

- Raccolta, conservazione e analisi dei log di sistema e di sicurezza.

- Monitoraggio continuo: strumenti SIEM (Security Information and Event Management).
- Rilevamento di anomalie: accessi fuori orario, escalation di privilegi, trasferimenti massivi di dati.
- Revisione periodica dei log come misura di prevenzione e di audit.

2.4 Crittografia e protezione dei dati

- Crittografia dei dati *at rest* e *in transit*.
- Gestione delle chiavi crittografiche.
- Firma digitale e certificati.
- Protocolli sicuri per le comunicazioni.

2.5 Sicurezza della supply chain digitale

- Valutazione del rischio *cyber* dei fornitori e dei partner.
- Requisiti di sicurezza contrattuali.
- Gestione degli accessi di terze parti ai sistemi aziendali.
- Monitoraggio continuativo della postura di sicurezza della catena di fornitura.

3) Modulo apicale — Governance della cybersicurezza

3.1 Il quadro normativo integrato

- Visione d'insieme del sistema normativo.
- Disamina delle principali Linee Guida e delle *best practices.*
- Registrazione obbligatoria sulla piattaforma dell'Agenzia per la Cybersicurezza Nazionale (ACN).

3.2 Responsabilità personali degli organi di vertice

- Art. 20 della Direttiva NIS2: obbligo formativo diretto per gli organi di amministrazione e direzione.
- Responsabilità personale dei dirigenti per la supervisione delle misure di cybersicurezza.
- Implicazioni sanzionatorie: sanzioni amministrative, interdittive e penali.
- Assicurazione D&O e rischio *cyber*.

3.3 Governance della cybersicurezza

- Nomina e ruolo del Responsabile della sicurezza informatica (CISO) e del Responsabile degli adempimenti per la conformità NIS.
- Approvazione e supervisione del piano di gestione del rischio cyber.
- Definizione delle policy di sicurezza: politica di sicurezza delle informazioni, politica di uso accettabile, politica di gestione degli incidenti, *business continuity* e *disaster recovery*.
- Integrazione tra Modello 231, modello privacy, procedure IT e governance ESG.

- Il ruolo dell'OdV nella vigilanza sulla cybersicurezza: verifiche, flussi informativi, evidenze e *follow up*.

3.4 Obblighi di notifica e gestione delle crisi

- Il sistema di notifica degli incidenti: tempistiche (segnalazione preliminare entro 24 ore, notifica completa entro 72 ore), modalità, destinatari.
- Gestione della comunicazione in caso di crisi *cyber*: comunicazione interna, comunicazione esterna, rapporti con le autorità, comunicazione ai media.
- Rischio reputazionale e impatto economico degli incidenti *cyber*.

3.5 Intelligenza artificiale e nuovi rischi

- L'impiego dell'AI nei processi aziendali: opportunità e rischi.
- Trasparenza e tracciabilità delle decisioni automatizzate.
- Principi di intervento e sorveglianza umana.
- Sicurezza degli algoritmi: prevenzione di manipolazioni, attacchi avversariali, utilizzi non autorizzati.
- Aggiornamento del Modello 231 con specifico focus sull'AI.

4) Metodologie di erogazione

L'efficacia della formazione dipende in misura significativa dalla scelta delle metodologie di erogazione, che devono essere diversificate, coinvolgenti e adeguate al profilo dei destinatari.

4.1 Formazione in modalità e-learning

La formazione base è erogata prevalentemente attraverso piattaforme di e-learning, con moduli brevi (15-30 minuti), interattivi e basati su scenari realistici. L'approccio "scenario-based" consente ai partecipanti di calarsi in situazioni concrete - come la ricezione di un'e-mail di *phishing* o una richiesta sospetta di condivisione credenziali - e di esercitare il processo decisionale in un ambiente sicuro.

I moduli e-learning devono essere fruibili da qualsiasi dispositivo aziendale e completati entro scadenze definite. Al termine di ciascun modulo è previsto un test di apprendimento, il cui superamento è condizione per il completamento della formazione.

4.2 Simulazioni di phishing e social engineering

Le simulazioni di *phishing* costituiscono uno strumento essenziale per misurare il livello di consapevolezza del personale e per rinforzare i comportamenti appesi in fase formativa. Le simulazioni sono condotte con cadenza almeno trimestrale, variando progressivamente le tipologie di attacco per evitare fenomeni di assuefazione (*training fatigue*):

- primo trimestre: simulazione di *credential phishing* (e-mail con link a pagine di login contraffatte);

- secondo trimestre: simulazione di BEC (Business E-mail Compromise), con richieste fraudolente attribuite a figure apicali;
- terzo trimestre: simulazione di *vishing* o *smishing*;
- quarto trimestre: simulazione basata su tecniche avanzate (es. deepfake audio/video, QR code malevoli).

I risultati delle simulazioni sono tracciati individualmente e per funzione aziendale. I soggetti che non superano la simulazione sono sottoposti a un percorso formativo integrativo.

4.3 Formazione in aula e workshop

La formazione di livello intermedio e apicale è erogata prevalentemente in forma seminariale - in presenza o in aula virtuale - con il coinvolgimento di docenti specializzati (esperti di cybersicurezza, legali, consulenti 231). I workshop prevedono una componente interattiva significativa, con discussione di casi reali, analisi di incidenti, esercitazioni di gruppo.

4.4 Esercitazioni su scenario

Con cadenza almeno annuale, l'ente organizza esercitazioni su scenario ("*tabletop exercise*") che simulano un incidente di sicurezza significativo (es. attacco *ransomware*, esfiltrazione di dati, compromissione della *supply chain*). L'esercitazione coinvolge tutti i livelli organizzativi rilevanti - management, IT/CISO, DPO, OdV, comunicazione, legale - e ha l'obiettivo di:

- testare l'efficacia del piano di risposta agli incidenti;
- verificare la conoscenza dei ruoli e delle responsabilità;
- identificare *gap* operativi e organizzativi;
- migliorare il coordinamento tra le funzioni.

Al termine di ciascuna esercitazione, è redatto un report con le evidenze emerse e le azioni correttive da intraprendere.

4.5 Micro-learning e campagne di sensibilizzazione

A integrazione della formazione strutturata, l'ente promuove iniziative di sensibilizzazione continua attraverso:

- "pillole formative": brevi comunicazioni periodiche (newsletter, intranet, bacheca digitale) su temi di sicurezza informatica di attualità;
- "infografiche e poster": materiali visivi per il rinforzo delle buone pratiche, esposti nei luoghi di lavoro e diffusi via canali digitali;
- "alert e *advisory*": comunicazioni tempestive in occasione di nuove minacce, campagne di *phishing* in corso, vulnerabilità note;
- "*gamification*": quiz interattivi, *challenge* tra *team*, badge di completamento;

- "*peer-to-peer* learning": condivisione di esperienze e buone pratiche tra colleghi, con il coinvolgimento dei "*security champions*" di ciascuna funzione.

4.6 Formazione all'ingresso e per nuovi collaboratori

Ogni neoassunto, collaboratore esterno o fornitore, che acceda ai sistemi informativi dell'ente è tenuto a completare il modulo formativo di base prima dell'inizio dell'operatività (o comunque entro i primi quindici giorni). Il completamento della formazione è condizione per l'attivazione delle credenziali di accesso ai sistemi. L'assolvimento dell'obbligo formativo è documentato e conservato a cura della funzione Risorse Umane.

5) Periodicità e aggiornamento

5.1 Calendario formativo

Attività	Destinatari	Frequenza
Formazione base (e-learning)	Tutto il personale	Annuale (rinnovabile)
Formazione all'ingresso	Neoassunti e nuovi collaboratori	All'inizio del rapporto
Simulazioni di phishing	Tutto il personale	Trimestrale
Formazione intermedia	Referenti IT e sicurezza	Semestrale
Formazione apicale	CdA, dirigenti, OdV	Annuale
Tabletop exercise	Team cross-funzionale	Annuale
Micro-learning e campagne	Tutto il personale	Continuativa

5.2 Aggiornamento dei contenuti

I contenuti formativi sono aggiornati:

a) con cadenza almeno annuale, nel contesto della revisione del piano formativo;

b) in occasione di modifiche normative rilevanti (introduzione di nuovi reati presupposto, recepimento di direttive europee, emanazione di linee guida da parte delle autorità competenti);

c) a seguito di incidenti di sicurezza occorsi all'ente o rilevanti nel settore di riferimento, secondo l'approccio delle "*lessons learned*";

d) in funzione dell'evoluzione del panorama delle minacce, sulla base delle indicazioni fornite dal CISO/responsabile della sicurezza informatica, dal DPO e dalle raccomandazioni delle agenzie (ACN, ENISA, CERT nazionali);

e) in occasione di cambiamenti organizzativi, tecnologici o di processo che modifichino il profilo di rischio dell'ente.

6) Indicatori di efficacia (KPI)

L'ente definisce e monitora un set di indicatori chiave per misurare l'efficacia del programma formativo e per consentire all'Organismo di Vigilanza di esprimere un giudizio sull'effettività delle misure adottate.

6.1 Indicatori quantitativi (schema esemplificativo)

KPI	Target	Frequenza di rilevazione
Tasso di completamento dei corsi obbligatori	100% del personale destinatario	Trimestrale
Tasso di superamento dei test di apprendimento	≥ 85% al primo tentativo	A ogni sessione formativa
Click-rate nelle simulazioni di phishing	Riduzione progressiva; target < 5%	Trimestrale
Tempo medio di segnalazione di e-mail sospette	Riduzione progressiva	Trimestrale
Numero di segnalazioni di incidenti o quasi-incidenti	Tendenzialmente crescente (indice di maggiore consapevolezza)	Mensile
Ore di formazione erogate per dipendente/anno	Conforme al piano formativo	Annuale

6.2 Indicatori qualitativi

- Esiti degli audit dell'OdV sull'effettività delle misure formative.
- Qualità e pertinenza delle segnalazioni di incidenti.
- Risultati delle esercitazioni su scenario: grado di coordinamento, tempestività di risposta, aderenza ai protocolli.
- Feedback dei partecipanti sulla qualità e utilità della formazione.
- Grado di aggiornamento dei contenuti rispetto al panorama delle minacce.

6.3 Reporting

I risultati degli indicatori sono consolidati in un report periodico (almeno semestrale) a cura della funzione incaricata della gestione del piano formativo (Risorse Umane, in coordinamento con il CISO e la funzione Compliance), e trasmessi all'Organismo di Vigilanza nell'ambito dei flussi informativi di cui alla sezione successiva.

7) Flussi informativi verso l'Organismo di Vigilanza

In coerenza con le citate Linee Guida CNDCEC del novembre 2025, l'Organismo di Vigilanza deve ricevere informazioni adeguate, tempestive e strutturate che gli consentano di esercitare la propria funzione di vigilanza sull'effettività del Modello 231 anche con riferimento ai presidi di cybersicurezza.

7.1 Flussi informativi periodici

L'OdV riceve con cadenza periodica:

a) il "piano formativo annuale" in materia di cybersicurezza, con indicazione dei contenuti, dei destinatari, delle modalità di erogazione e del calendario;

b) il "report di partecipazione e completamento", con evidenza dei tassi di adesione, dei test superati/non superati, delle eventuali criticità;

c) i "risultati delle simulazioni di phishing", disaggregati per funzione aziendale e con indicazione delle azioni correttive intraprese;

d) le "raccomandazioni del CISO e del DPO" in materia di formazione, con evidenza del relativo follow-up;

e) le "variazioni al piano formativo", con la motivazione delle modifiche apportate.

7.2 Flussi informativi ad evento

L'OdV è tempestivamente informato in caso di:

a) "incidenti di sicurezza informatica" di qualsiasi natura, comprensivi delle misure di contenimento adottate e delle notifiche effettuate alle autorità competenti;

b) "data breach" ai sensi del GDPR, con indicazione dell'impatto e delle comunicazioni effettuate al Garante Privacy e agli interessati;

c) "esiti negativi delle simulazioni di phishing" che evidenzino criticità significative in specifiche aree o funzioni;

d) "segnalazioni *whistleblowing*" riconducibili a condotte in ambito informatico;

e) "modifiche normative" o "provvedimenti delle autorità competenti" (ACN, Garante Privacy, ANAC) che incidano sugli obblighi formativi dell'ente.

7.3 Verifiche dell'OdV sulle attività formative

L'OdV inserisce nel proprio piano di vigilanza verifiche specifiche in materia di formazione sulla cybersicurezza, volte ad accertare:

- l'effettiva erogazione della formazione secondo il piano approvato;
- la completezza e l'aggiornamento dei contenuti formativi;
- il rispetto delle periodicità previste;
- la coerenza tra i risultati della formazione e la politica di gestione del rischio cyber dell'ente;
- l'adozione di misure correttive a fronte di criticità emerse dalle simulazioni, dagli incidenti o dagli audit;
- l'adeguatezza dei flussi informativi ricevuti.

8) Sistema disciplinare

Il mancato rispetto degli obblighi formativi in materia di cybersicurezza è sanzionato nell'ambito del sistema disciplinare previsto dal Modello 231. In particolare, costituiscono condotte sanzionabili:

a) la mancata partecipazione ai corsi di formazione obbligatori, senza giustificato motivo;

b) il mancato superamento dei test di apprendimento, qualora non seguito dal completamento del percorso formativo integrativo;

c) la violazione delle policy di sicurezza informatica oggetto della formazione;

d) la mancata o ritardata segnalazione di incidenti di sicurezza, anomalie o sospetti;

e) l'ostruzione o l'interferenza con le attività di simulazione e verifica.

Le sanzioni sono graduate in funzione della gravità della condotta, della posizione del soggetto nell'organizzazione e della reiterazione, nel rispetto delle previsioni del contratto collettivo applicabile e della normativa lavoristica vigente. Per i soggetti apicali, le sanzioni sono definite dall'organo competente secondo le previsioni del sistema disciplinare del Modello 231.

9) Ruoli e responsabilità

Funzione / Organo	Responsabilità
Consiglio di Amministrazione	Approva il piano formativo annuale; assicura adeguate risorse; adempie in prima persona all'obbligo formativo *ex* NIS2
Amministratore Delegato / Direzione Generale	Garantisce l'attuazione del piano formativo; promuove la cultura della sicurezza
CISO / Responsabile Sicurezza Informatica	Definisce i contenuti tecnici della formazione; conduce le simulazioni; fornisce aggiornamenti sul panorama delle minacce; predispone il report periodico
DPO	Collabora alla definizione dei contenuti in materia di protezione dei dati; segnala esigenze formative connesse a trattamenti specifici
Risorse Umane	Pianifica e gestisce la logistica della formazione; registra la partecipazione; gestisce i flussi verso il sistema disciplinare
Funzione Compliance / Legal	Assicura la coerenza normativa dei contenuti; collabora all'aggiornamento in caso di novità legislative
Organismo di Vigilanza	Vigila sull'effettività della formazione; verifica i KPI; riceve i flussi informativi; formula raccomandazioni
Responsabili di funzione	Favoriscono la partecipazione del personale; segnalano esigenze formative specifiche
Tutti i dipendenti e collaboratori	Partecipano alla formazione obbligatoria; applicano le conoscenze acquisite; segnalano tempestivamente incidenti e anomalie

10) Documentazione e conservazione

L'ente conserva, per un periodo verosimilmente non inferiore a dieci anni, la seguente documentazione relativa al programma formativo:

a) piano formativo annuale approvato e le eventuali revisioni;

b) materiali didattici utilizzati per ciascuna sessione formativa;

c) registri di partecipazione, con evidenza di data, durata, modalità di erogazione, nominativi dei partecipanti e dei docenti;

d) risultati dei test di apprendimento;

e) risultati delle simulazioni di *phishing* e delle esercitazioni su scenario;

f) report periodici trasmessi all'OdV;

g) attestazioni individuali di completamento della formazione;

h) eventuali comunicazioni relative a mancata partecipazione e conseguenti provvedimenti.

La documentazione è conservata in formato digitale, in ambiente protetto, con garanzia di integrità, disponibilità e riservatezza.

4. *Best practices* per la *cybersecurity*

L'efficacia del Modello 231 rispetto ai reati informatici di cui all'art. 24-bis dipende dalla capacità dell'ente di adottare presidi organizzativi e tecnici adeguati, aggiornati e concretamente attuati. In un contesto caratterizzato da minacce informatiche in continua evoluzione, la cybersecurity deve essere considerata non come un insieme di misure isolate, ma come un processo continuo di gestione del rischio.

In tale prospettiva, assumono rilievo non soltanto le attività di monitoraggio e controllo, ma anche l'adozione di policy interne, procedure di verifica periodica, programmi di formazione del personale e standard organizzativi riconosciuti a livello internazionale. Tra questi, particolare importanza rivestono gli standard della famiglia ISO/IEC 27000 – e in particolare la già citata ISO/IEC 27001 – che rappresentano un utile parametro di riferimento nella costruzione di sistemi di gestione della sicurezza delle informazioni strutturati e verificabili.

Le considerazioni che seguono esaminano alcune delle principali best practice rilevanti ai fini della prevenzione del rischio cyber e della verifica dell'idoneità del Modello 231.

4.1. Monitoraggio continuo e audit periodici

L'adeguatezza del Modello 231 rispetto ai reati informatici di cui all'art. 24-*bis* si misura anche in relazione alla sua capacità di adattarsi al mutare delle minacce a cui l'ente è esposto. Un sistema di presidi cristallizzato al momento dell'adozione del Modello 231 tende, infatti, a rivelarsi progressivamente inidoneo rispetto a rischi che evolvono con rapidità e continuità. Il monitoraggio del rischio informatico richiede quindi un approccio dinamico, articolato lungo due direttrici complementari: da un lato, la sorveglianza continuativa dell'infrastruttura; dall'altro, lo svolgimento di verifiche periodiche programmate.

Prima di esaminare gli strumenti di monitoraggio, va precisato che il Modello 231 non è diretto a proteggere l'ente dagli attacchi informatici in quanto tali, ma a prevenire la commissione dei reati informatici richiamati dall'art. 24-*bis* del d.lgs. n. 231/2001 da parte di soggetti apicali o sottoposti, nell'interesse o a vantaggio dell'ente. In questa prospettiva, il sistema di controllo deve essere calibrato non solo sulla difesa dell'infrastruttura tecnologica, ma anche sui processi aziendali nei quali le risorse informatiche possono essere utilizzate in modo illecito: accessi non autorizzati a sistemi di terzi, alterazione o soppressione di dati, utilizzo improprio di credenziali e strumenti di intrusione, falsificazione di documenti informatici, omissione di adempimenti di sicurezza normativamente imposti. Il monitoraggio continuo e gli audit periodici assumono dunque rilievo non soltanto come

misure di sicurezza tecnica, ma come strumenti di verifica dell'idoneità del Modello 231 a prevenire condotte penalmente rilevanti.

Questa impostazione è coerente con l'evoluzione del quadro normativo europeo. Il Regolamento (UE) 2022/2554, ad esempio, impone ai soggetti del settore finanziario sistemi di sorveglianza permanente delle risorse ICT. La Direttiva (UE) 2022/2555 estende obblighi analoghi di monitoraggio e notifica degli incidenti a un perimetro molto più ampio, che comprende anche imprese medie e grandi operanti in numerosi comparti dell'economia reale. Per molte imprese assistite dai Commercialisti la NIS2 rappresenta il primo vero obbligo cogente in materia di *cybersecurity*. Anche per gli enti non direttamente soggetti a tali discipline, i principi da esse espressi costituiscono comunque un utile parametro di riferimento nella calibrazione delle misure di controllo.

Il primo livello di presidio è rappresentato dal monitoraggio continuo, che ha la funzione di intercettare tempestivamente le anomalie, riducendo la finestra di esposizione dell'ente. In tale ambito, assumono rilievo le piattaforme SIEM (*Security Information and Event Management*), che raccolgono e correlano i log generati da sistemi, applicazioni e dispositivi di rete, consentendo di individuare in tempo reale *pattern* riconducibili a tentativi di intrusione o a comportamenti anomali. L'attività di analisi può essere presidiata da un SOC (*Security Operations Center*) interno oppure, soluzione spesso più accessibile per le PMI, esternalizzata tramite servizi SOC-as-a-Service o piattaforme SIEM in *cloud*, capaci di garantire continuità operativa senza richiedere una struttura dedicata.

Analoga rilevanza assumono le soluzioni EDR/XDR, che consentono di monitorare il comportamento degli *endpoint* aziendali - postazioni di lavoro, server e dispositivi mobili - rilevando attività sospette e attivando, nei casi più evoluti, misure automatiche o semiautomatiche di contenimento. Per le PMI, i servizi di *detection and response* rappresentano una soluzione sostenibile, in grado di innalzare sensibilmente il livello di protezione rispetto ai tradizionali *antivirus*. A ciò si aggiunge il monitoraggio degli accessi e delle identità digitali, che costituisce un presidio essenziale in ogni contesto organizzativo: rientrano in tale ambito il controllo dei privilegi amministrativi, la revisione delle utenze attive - con particolare attenzione a quelle non più riconducibili a personale in servizio - e la sorveglianza degli accessi a dati sensibili e a risorse critiche.

Accanto alla sorveglianza continuativa, le organizzazioni devono programmare verifiche periodiche finalizzate a misurare la reale tenuta del perimetro informatico. Le prassi operative si concentrano, in particolare, su due strumenti. Il primo è il *vulnerability assessment*, consistente in scansioni automatizzate e ricorrenti, volte a individuare vulnerabilità note nei sistemi, nei *software* e nelle configurazioni di rete. Il secondo è il *penetration test*, ossia la simulazione controllata di attacchi informatici da parte di specialisti, finalizzata a verificare non solo l'esistenza di una vulnerabilità, ma anche la sua concreta sfruttabilità. Tali test possono essere condotti con diversi livelli di conoscenza iniziale del sistema (*black box*, *grey box*, *white box*) e dovrebbero riguardare, oltre alla componente tecnica, anche il fattore umano, ad esempio mediante campagne di *social engineering*. In termini di buona prassi, il *penetration test* dovrebbe essere eseguito con cadenza almeno annuale o, comunque, in occasione di modifiche rilevanti dell'infrastruttura IT.

Sul piano procedurale, un presidio centrale è costituito dal *log management*. Il tracciamento degli accessi ai sistemi e delle operazioni compiute, soprattutto da parte degli amministratori di sistema, risponde infatti a una duplice esigenza: consente, da un lato, di ricostruire gli eventi in caso di incidente e, dall'altro, rafforza la capacità dell'ente di prevenire e rilevare abusi interni. In proposito, il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, come successivamente integrato, impone la registrazione degli *access log* degli amministratori di sistema secondo requisiti di completezza, inalterabilità e verificabilità dell'integrità, con conservazione per un periodo non inferiore a sei mesi. La violazione di tali prescrizioni, oltre ai profili sanzionatori propri della disciplina *privacy*, può rilevare anche nella valutazione dell'idoneità del Modello 231, poiché l'assenza di tracciabilità compromette la ricostruzione degli eventi e indebolisce il sistema di prevenzione.

Il monitoraggio si completa con l'audit periodico, che ha la funzione di verificare la concreta attuazione delle misure di controllo e non la loro mera esistenza formale. Per ragioni di indipendenza, la predisposizione e l'esecuzione delle attività di audit non dovrebbero essere rimesse in via esclusiva al reparto IT, ma affidate alla funzione di *Internal Audit*, ove presente, oppure a un IT Auditor esterno indipendente, secondo metodologie coerenti con i *framework* internazionali di riferimento. Il reparto IT resta naturalmente un interlocutore necessario nella mappatura del perimetro tecnologico e nel supporto tecnico, ma gli esiti delle verifiche devono confluire in flussi informativi strutturati verso l'Organismo di Vigilanza, che li valuta nell'ambito della propria attività di verifica sull'effettiva attuazione del Modello.

Nelle PMI, in applicazione del principio di proporzionalità, l'assenza di una funzione interna di audit non impedisce comunque l'attivazione di controlli adeguati. In tali contesti, l'OdV può acquisire evidenze documentali oggettive dai fornitori IT esterni - ad esempio *log* di *firewall*, *report* sugli aggiornamenti di sicurezza, attestazioni relative ai servizi *cloud* - così da mantenere un adeguato grado di terzietà nella verifica. Ciò che rileva, in definitiva, è che il controllo sia effettivo, documentato e periodico.

Nel corso dell'audit occorre verificare, in concreto, se:

- le credenziali di accesso vengano revocate tempestivamente alla cessazione del rapporto di lavoro o di collaborazione;
- i *backup* siano sottoposti non soltanto a verifica di esecuzione, ma anche a test di ripristino completi;
- le *policy* in materia di *password* siano effettivamente rispettate;
- l'autenticazione multifattore sia attiva almeno per gli accessi amministrativi e da remoto;
- le *patch* di sicurezza, specie quelle riferite a vulnerabilità critiche, siano applicate con tempestività.

Gli esiti di tali verifiche possono, inoltre, costituire occasione per alimentare flussi informativi costanti verso il Collegio Sindacale o il Sindaco Unico. Una lacuna significativa nei presidi di sicurezza informatica, rilevata dall'OdV in ottica 231, può infatti assumere rilievo anche quale possibile indice di inadeguatezza degli assetti organizzativi ai sensi dell'art. 2086 c.c., nonché quale elemento di interesse

ai fini dell'attività di vigilanza demandata al Collegio Sindacale ai sensi dell'art. 2403 c.c. In tal senso, il Sindaco può offrire un contributo particolarmente utile, in quanto la sua formazione consente di cogliere congiuntamente il profilo organizzativo, quello patrimoniale e quello di compliance del rischio informatico.

Quando, negli enti di minori dimensioni, il Collegio Sindacale assume anche le funzioni di Organismo di Vigilanza *ex* d.lgs. n. 231/2001 ai sensi dell'art. 6, comma 4-*bis*, del d.lgs. n. 231/2001, tale integrazione risulta ancora più evidente.

5. Il supporto all'attività dell'Organismo di Vigilanza: digitalizzazione e intelligenza artificiale

5.1. Il doppio impatto dell'AI sull'Organismo di Vigilanza

Il contesto sin qui delineato, che presenta una estesa diffusione di strumenti di intelligenza artificiale e trasformazione digitale dei processi aziendali, ridefinisce l'ecosistema in cui operano le imprese, con effetti diretti e profondi anche sull'attività dell'Organismo di Vigilanza. La sfida che l'OdV è chiamato ad affrontare è duplice e strutturale:

- da un lato, valutare e presidiare i nuovi rischi che derivano dall'utilizzo di sistemi di AI all'interno dell'organizzazione;
- dall'altro, trarre vantaggio dagli stessi strumenti per elevare la qualità, la tempestività e l'efficacia della propria vigilanza.

Si è già detto che in materia di adeguati assetti organizzativi la digitalizzazione e l'AI non rappresentano soltanto strumenti di efficientamento operativo, ma incidono strutturalmente sui processi decisionali, sui flussi informativi, sulle modalità di gestione dei rischi e sulle responsabilità organizzative, imponendo un'evoluzione del Modello Organizzativo in chiave (ancor più) dinamica e prospettica. Ne consegue che la compliance 231 – e con essa l'attività dell'OdV – non può essere valutata prescindendo dal contesto digitale in cui l'impresa opera.

5.2. La vigilanza sui rischi derivanti dall'utilizzo dell'AI in azienda

L'introduzione di sistemi di digitalizzazione e AI nell'operatività aziendale genera un'area di rischio inedita che l'OdV è chiamato a ricondurre nel perimetro del Modello, distinguendo tra rischi diretti e rischi indiretti. In particolare:

- i rischi diretti attengono alle ipotesi in cui l'AI costituisce lo strumento attraverso cui un reato presupposto potrebbe essere commesso a vantaggio o nell'interesse dell'ente: manipolazione di informazioni contabili o di bilancio mediante sistemi generativi, produzione di documentazione contrattuale o fiscale falsificata, esfiltrazione di dati riservati attraverso modelli addestrati su dati

illecitamente acquisiti; a ciò si aggiunga quanto evidenziato in precedenza in merito alla l. n. 132/2025;

- i rischi indiretti riguardano invece l'amplificazione di condotte illecite già note, quali, esemplificativamente: la sofisticazione degli attacchi di *phishing* e *social engineering*, la velocità di replicazione automatizzata di condotte fraudolente e la difficoltà di attribuire responsabilità in presenza di decisioni algoritmiche che richiedono una revisione critica delle aree sensibili già mappate nel Modello.

L'OdV deve quindi curare che l'aggiornamento periodico del Modello 231 includa sistematicamente una valutazione dei sistemi Digit-AI adottati dall'ente, classificandoli per tipologia e per livello di rischio e verificando il loro impatto sui processi e le aree sensibili. In concreto, l'OdV dovrà accertare che l'ente abbia: (*i*) istituito un sistema di gestione del rischio Digit-AI coerente con il Modello 231[42]; (*ii*) definito protocolli per l'approvazione e il monitoraggio dei sistemi algoritmici nei processi sensibili; (*iii*) previsto adeguati meccanismi di supervisione umana[43] per le decisioni assunte con supporto AI in aree potenzialmente rilevanti ai fini penali; (*iv*) garantito la tracciabilità delle decisioni algoritmiche nel rispetto dei requisiti probatori del decreto[44]. La qualità del dato (*c.d. data quality*) su cui i sistemi di AI operano[45] è condizione preliminare di affidabilità dell'intero sistema: un modello addestrato su dati incompleti o distorti produce output inaffidabili, con rischi per l'OdV più gravi dell'assenza dello strumento stesso.

5.3. L'AI a supporto dell'OdV: dall'approccio tradizionale all'«osservazione aumentata»[46]

5.3.1. *Classificazione documentale,* knowledge base *e* anomaly detection

L'attività dell'OdV si esplica, molto spesso, attraverso strumenti tradizionali – verbali redatti manualmente, fogli di calcolo, applicativi di base di *Governance Risk* e *Compliance* (GRC) – che presentano limiti oggettivi di fronte ai volumi di dati e documenti prodotti dalle organizzazioni contemporanee. I sistemi di AI basati su *machine learning* e *Natural Language Processing* (NLP) / *Large Language Model* (LLM) offrono la possibilità di superare questi limiti attraverso quella che può essere definita "osservazione aumentata".

Si tratta della capacità di processare in modo automatizzato big data e grandi volumi di informazioni non strutturate – verbali, report di audit, e-mail, segnalazioni, flussi informativi periodici – classificandoli per provenienza, area di rischio 231, processo/area sensibile coinvolti, tipologia e grado di sensibilità dell'informazione, *track record* degli eventi. Su archivi di tipo pluriennale, un sistema

[42] ISO/IEC 42001: 2023, Artificial intelligence — Management system, International Organization for Standardization, Ginevra, 2023; NIST, AI Risk Management Framework (AI RMF 1.0), Gaithersburg (MD), 2023.
[43] Art. 9, par. 1, Regolamento UE AI Act: obbligo di sistema di gestione del rischio per i sistemi di AI ad alto rischio. Art. 14: requisiti di supervisione umana.
[44] Sul principio di tracciabilità quale requisito funzionale del Modello 231 v. Confindustria, "Linee guida", cit., pp. 30-31.
[45] Garante per la protezione dei dati personali, "Linee guida sull'intelligenza artificiale nel trattamento dei dati personali", Roma, 2024; Regolamento (UE) 2016/679 (GDPR), artt. 5, 25 e 35; art. 10, Regolamento UE AI Act (qualità dei dati).
[46] Sull'argomento CNDCEC, "Linee Guida per lo svolgimento delle funzioni dell'Organismo di vigilanza *ex* d.lgs. 231/2001", cit.

adeguato di Digit-AI può rendere i contenuti ricercabili semanticamente, consentendo quindi all'Organismo di ricostruire l'intera storia documentale di un'area di rischio, di estrarre tutte le occorrenze in cui un determinato tema, fornitore o soggetto apicale è stato trattato nel corso degli anni, di identificare *pattern* ricorrenti nei flussi informativi periodici/ad evento e molto altro ancora. Ribadito che il rispetto del principio di evidenza – attraverso la tracciabilità dei dati e delle attività svolte – è requisito essenziale per l'attività dell'OdV, la tassonomia adottata dal sistema di AI deve essere formalizzata, approvata dall'Organismo e periodicamente revisionata.

Sul piano della prevenzione, sistemi di AI applicati ai dati operativi dell'ente possono svolgere una funzione di *anomaly detection* di grande valore, anche al fine di:

- orientare al meglio la definizione del Piano di audit verso le cosiddette aree "*red flag*" (ad esempio, in funzione del rilevamento di anomalie su transazioni economico-finanziarie, *log* di accesso IT, dati di magazzino e tempi di lavorazione);
- intercettare *pattern* tipici di comportamenti a rischio come il frazionamento sistematico degli ordini, gli accessi fuori orario da determinate utenze o gli scostamenti anomali tra preventivi e consuntivi;
- evidenziare correlazioni tra non conformità e specifiche condizioni organizzative, distinguendo tra errore episodico e debolezza strutturale del presidio.

Questa capacità predittiva risponde direttamente al più volte richiamato principio di "prevenzione mediante organizzazione", quale chiave di volta dell'efficace funzionamento del Modello; l'OdV arricchisce così la sua capacità di vigilanza sul Modello 231 con ulteriori strumenti per individuare gli *alert* e i segnali di debolezza, prima che si traducano in violazioni del Modello o accadimento di reati.

5.3.2. Le tre linee di intervento: prioritizzazione, monitoraggio e valutazione dell'efficacia

Il contributo della Digit-AI all'attività dell'OdV si può articolare secondo tre principali linee di intervento tra loro complementari e in particolare:

(a) supporto alla prioritizzazione: combinando dati, esemplificativamente, su gravità, frequenza, area di rischio 231, soggetti coinvolti e impatti economici, il sistema produce un *risk scoring* dinamico delle non conformità, evidenziando all'OdV quali situazioni meritino un *follow-up* ravvicinato e quali possano restare in monitoraggio periodico. Questa funzione consente un'allocazione delle risorse proporzionata all'effettivo profilo di rischio, riducendo il rischio che situazioni critiche ricevano la stessa attenzione di quelle marginali;

(b) monitoraggio automatizzato degli impegni: l'integrazione dell'AI con sistemi di workflow/GRC consente di: (*i*) tracciare ogni azione correttiva come *"ticket"* con scadenza, *process-owner* e documenti relativi; (*ii*) monitorare ritardi e implementazioni parziali e *backlog*; (*iii*) produrre *tableau de bord* analitici per l'Organismo e report sullo stato delle azioni correttive ad alta criticità 231, riducendo così il rischio che i *follow-up* svaniscano nella routine operativa;

(c) valutazione dell'efficacia*:* su orizzonti temporali più lunghi, i modelli predittivi possono confrontare periodi pre e *post*-intervento, stimare se le misure adottate hanno effettivamente ridotto il rischio e contribuire a codificare idonei mezzi di prova sull'attività di vigilanza dell'OdV, quale parte integrante del giudizio sull'efficace attuazione del Modello 231. Questa circostanza è dirimente in occasione di indagini preliminari o di procedimenti circa la responsabilità amministrativa dell'ente. In questa prospettiva, il tracciamento non è più soltanto una "conservazione di documenti", ma capacità di "leggere la storia complessiva del rischio in ambito compliance".

L'utilizzo da parte dell'Organismo della Digit-AI deve restare nell'ambito della sua essenziale "funzione strumentale", onde evitare possibili rischi e limiti nel loro utilizzo, tra cui, a titolo esemplificativo:

- rischio di deresponsabilizzazione: come per gli Organi Sociali, l'OdV non deve (e non può) "nascondersi dietro l'algoritmo": la valutazione finale su gravità, priorità e adeguatezza delle misure resta di sua assoluta competenza. In ottica 231, un Modello che si affida in modo "acritico" all'AI potrebbe essere facilmente giudicato inidoneo e, quindi, la vigilanza dell'Organismo potrebbe essere ritenuta non efficace;
- qualità e *bias* dei dati: si è già avuto modo di rilevare che se i dati di partenza sono incompleti, distorti o mal classificati, l'AI rischia di amplificare l'errore, inducendo a possibili "distorsioni", ad esempio, nella classificazione delle segnalazioni, nella prioritizzazione delle non conformità, nella programmazione dei follow-up, ecc.;
- opacità dei modelli ("*black box*"): Modelli troppo complessi o non adeguatamente comprensibili e/o trasparenti rischiano di essere difficili da difendere in sede giudiziaria.

5.4. Gli *audit* critici per l'OdV nel 2026: NIS2, DORA e AI Act

Il 2026 presenta una densità normativa straordinaria per gli Organismi di Vigilanza. L'entrata in vigore operativa di NIS2 e DORA per gli enti del settore finanziario, nonché la progressiva applicazione dell'AI Act, definiscono un quadro di *compliance* integrata in cui l'OdV è chiamato a svolgere un ruolo di presidio trasversale, verificando che le misure adottate dall'ente in risposta a ciascuno di questi regimi siano coerenti tra loro e con il Modello in materia di *compliance* 231.

In particolare, circa la NIS2, l'OdV dovrà verificare l'adozione di misure di gestione dei rischi di sicurezza informatica adeguate, procedure di notifica degli incidenti significativi nei tempi previsti e misure di sicurezza della catena di approvvigionamento coerenti con i presidi già previsti nel Modello per la gestione dei fornitori terzi. La sovrapposizione tra requisiti NIS2 e presidi *cyber* del Modello è ampia e richiede una mappatura integrata che eviti duplicazioni e garantisca un unico sistema di controllo interno. In relazione a DORA, applicabile agli enti del settore finanziario, l'OdV dovrà verificare la coerenza tra i requisiti di resilienza operativa Digit-AI e i presidi *cyber* del Modello, con particolare attenzione alla gestione del rischio ICT di terze parti e ai test di resilienza operativa digitale. In relazione

all'AI Act, l'OdV dovrà verificare che i sistemi di AI classificati ad alto rischio[47] soddisfino i requisiti di governance, qualità dei dati, trasparenza e supervisione umana previsti dal Regolamento e che la loro integrazione nei processi aziendali non generi nuove aree di rischio non adeguatamente presidiate dal Modello.

6. Proposte per il rafforzamento della sinergia tra Modello 231 e *cybersecurity*

In base alle considerazioni fin qui svolte, appare opportuno sintetizzare i principali concetti espressi ed elaborare alcune proposte tese a rafforzare la sinergia tra gli aspetti di *cybersecurity* e la gestione dei rischi in ottica 231.

La separazione operativa tra funzione IT e area *compliance* rappresenta, nella prassi, un fattore di debolezza del sistema di controllo interno. La *cybersecurity* viene spesso trattata come questione esclusivamente tecnica, mentre il Modello 231 resta confinato nell'ambito degli adempimenti legali e organizzativi. In realtà, i due piani sono strettamente interconnessi: la vulnerabilità dell'infrastruttura tecnologica può creare le condizioni per la commissione di reati presupposto e, al contempo, incidere sull'adeguatezza complessiva degli assetti organizzativi dell'impresa. Per superare tale separazione, è opportuno intervenire lungo tre direttrici operative, tra loro coordinate.

La prima riguarda il riconoscimento del rischio *cyber* quale tema di *governance* e di adeguatezza degli assetti. Un'infrastruttura IT non adeguatamente protetta non costituisce soltanto una criticità tecnica, ma può tradursi in una carenza dell'assetto organizzativo, amministrativo e contabile ai sensi dell'art. 2086 c.c. In termini concreti, un attacco *ransomware* che renda indisponibili i sistemi gestionali può bloccare la fatturazione, compromettere la visibilità sui flussi finanziari e ostacolare l'adempimento degli obblighi fiscali, incidendo sulla continuità aziendale. Occorre, tuttavia, evitare una lettura riduttiva: il Modello 231 non presidia soltanto la resilienza dell'ente rispetto ad attacchi subiti, ma è chiamato a prevenire la commissione, nell'interesse o a vantaggio dell'ente, dei reati informatici richiamati dall'art. 24-*bis* del d.lgs. n. 231/2001. Il vertice aziendale deve quindi assumere un ruolo diretto non solo nell'approvazione delle misure difensive, ma anche nella definizione di regole di condotta idonee a prevenire l'uso illecito delle risorse informatiche aziendali. In tale prospettiva, la presenza di investimenti coerenti e documentabili in materia di sicurezza informatica costituisce un indice di effettiva attuazione del Modello; al contrario, un evidente squilibrio tra livello del rischio e mezzi destinati a fronteggiarlo può essere valutato come sintomo di carenze organizzative.

La seconda direttrice concerne l'integrazione tra *risk assessment* informatico e mappatura dei rischi 231. Nella pratica, le imprese tendono a mantenere separate le due analisi: da un lato, la valutazione tecnica delle vulnerabilità; dall'altro, la mappatura delle attività sensibili ai fini del d.lgs. n. 231/2001. Questa duplicazione riduce l'efficacia del controllo, perché non consente di cogliere come una

[47] Art. 16, Regolamento UE AI Act: sistemi di intelligenza artificiale ad alto rischio impiegati in infrastrutture critiche, processi decisionali rilevanti o applicazione della legge, soggetti a requisiti rafforzati di trasparenza, registrazione e supervisione umana.

vulnerabilità tecnica possa tradursi in rischio-reato. È quindi necessario adottare un processo unitario, nel quale gli esiti delle attività di sicurezza (*vulnerability assessment*, *penetration test*, gestione degli incidenti e *remediation*) confluiscano nell'aggiornamento della mappa dei rischi 231 e dei relativi protocolli.

In tale prospettiva, assumono rilievo adeguati flussi informativi verso l'Organismo di Vigilanza, in relazione agli esiti delle verifiche di sicurezza e ad eventuali incidenti informatici. Tali eventi possono infatti assumere rilievo sia ai sensi della disciplina GDPR e NIS2, sia nell'ambito dei presidi adottati ai fini del d.lgs. n. 231/2001, evidenziando l'esigenza di una gestione integrata del rischio informatico.

Nel medesimo quadro si colloca il sistema di *whistleblowing*. Le procedure adottate ai sensi del d.lgs. n. 24/2023 dovrebbero prevedere espressamente la possibilità di segnalare condotte od omissioni in materia di sicurezza informatica che possano esporre l'ente a rischi di commissione di reati o a violazioni rilevanti del Modello. Non ogni inosservanza tecnica assume rilievo in questa prospettiva; devono tuttavia poter emergere, attraverso canali protetti, situazioni quali l'elusione sistematica dei protocolli di accesso, l'occultamento di vulnerabilità critiche o la mancata attuazione di misure di sicurezza già deliberate. L'assenza di una previsione di questo tipo può costituire una lacuna del sistema di controllo.

La terza direttrice riguarda l'estensione del presidio 231 alla *supply chain* tecnologica. Nella prassi degli attacchi informatici il fornitore rappresenta spesso un punto di ingresso verso il bersaglio principale. Ne deriva che il Modello non può limitarsi ai soli processi interni, ma deve includere criteri di selezione, valutazione e controllo dei fornitori IT e *cloud*, calibrati in funzione della criticità del servizio affidato e dei dati trattati.

In tale prospettiva, i contratti con i fornitori critici dovrebbero contenere clausole specifiche in materia di sicurezza: obbligo di notifica tempestiva degli incidenti, definizione di standard minimi, diritto di audit e rimedi contrattuali in caso di inadempimento. Si tratta di una scelta coerente non solo con la logica del Modello 231, ma anche con l'impostazione della Direttiva NIS2, che include la sicurezza della catena di approvvigionamento tra le misure di gestione del rischio. Per gli enti soggetti a tale disciplina, il tema assume rilievo normativo diretto; per gli altri, rappresenta comunque un indicatore significativo dell'adeguatezza del sistema di controllo.

I tre interventi richiamati - coinvolgimento del vertice, integrazione del *risk assessment* e presidio della *supply chain* - non rappresentano misure autonome, ma componenti di un'unica struttura di prevenzione. Senza un adeguato impegno del vertice, mancano risorse e indirizzo; senza flussi informativi integrati, le vulnerabilità restano invisibili agli organi di controllo; senza attenzione alla catena dei fornitori, il sistema rimane esposto nei punti di maggiore fragilità. La sinergia tra Modello 231 e *cybersecurity* si realizza, quindi, quando la sicurezza informatica non è più trattata come funzione tecnica separata, ma come parte integrante della *governance* e del sistema dei controlli dell'ente.

7. Appendici

7.1. Questionario Cyber Risk

Elemento di rischio	Livello Rischio	Riscontro al quesito/note
Adeguatezza del dipartimento IT • Come è strutturato l'Ufficio IT dell'Ente e quali sono le competenze e le esperienze maturate dai singoli componenti del *team*? • L'Ente si avvale anche di consulenti esterni in materia IT? • L'Ente ha adottato procedure in materia di sicurezza informatica? (con elencazione delle *policies* in caso affermativo)		
Utilizzo postazioni informatiche e sistemi informatici • Quanti dipendenti utilizzano una postazione informatica nell'ambito dello svolgimento delle proprie mansioni? • I locali in cui si trovano i dispositivi e le apparecchiature sono sottoposti a controlli al fine di prevenire accessi di terzi non autorizzati e danni? • I dispositivi e le postazioni informatiche possono essere utilizzati per scopi ulteriori rispetto a quelli rientranti nell'ambito delle proprie mansioni? • Quali azioni devono essere intraprese in caso di furto o smarrimento di dispositivi/apparecchiature dell'Ente? (es. obblighi informativi, denuncia all'Autorità ecc.) • Quali sistemi informatici sono utilizzati all'interno dell'Ente? • L'accesso ai sistemi informatici, alla rete e alle applicazioni avviene mediante credenziali? Gli accessi sono monitorati e tracciati?		
Accessi esterni non autorizzati • Quali strumenti sono utilizzati per impedire la connessione di dispositivi non autorizzati alla rete dell'Ente? • Per accedere alla rete dell'Ente sono richieste credenziali? Ogni quanto tempo vengono rinnovate? • Con quali strumenti viene monitorata la sicurezza dei computer (*firewall*, *antivirus*, aggiornamenti)?		
Perdita di dati • È attivo un sistema di backup periodico del sistema operativo aziendale? Con quale frequenza viene effettuato? • Dove sono custodite le copie di *backup*?		
Attacchi da virus • Sono presenti antivirus? Quanti livelli? Vengono aggiornati automaticamente e con quale frequenza?		

Elemento di rischio	Livello Rischio	Riscontro al quesito/note
• Con quale frequenza vengono condotti i test per verificare la sicurezza dei servizi verso internet e la presenza di vulnerabilità o *backdoor*? • I test vengono effettuati internamente o esternamente? • Viene tenuta traccia dei test condotti? • Come vengono monitorate eventuali anomalie del sistema? • Come viene gestita la posta elettronica? Sono presenti sistemi di filtraggio? • Come sono gestiti gli accessi a internet? • Come sono gestite le altre piattaforme aziendali (es. CRM)?		
Cancellazione non autorizzata o manomissione di dati: Remediation Plan • Esiste un Remediation Plan in caso di attacco del sistema dell'Ente finalizzato al furto, all'alterazione o alla distruzione dei dati e/o del sistema informatico? • Si sono verificati negli ultimi anni incidenti sulla sicurezza informatica? Se sì, come sono stati gestiti e quali danni hanno comportato?		
Accesso a sistemi informatici di terzi • A quali sistemi informatici di terzi viene effettuato l'accesso nell'ambito dello svolgimento delle attività dell'Ente? • L'accesso a tali sistemi avviene mediante credenziali? • Gli accessi sono monitorati e tracciati?		
Cyber Security risk assessment • Con quale frequenza e da chi (internamente /tramite consulenti esterni) viene effettuato/aggiornato il *Cyber Security risk assessment*?		
Formazione • Ai dipendenti è fornita formazione in ambito di sicurezza informatica e protezione dei dati (sessioni in aula, corsi o aggiornamenti sui comportamenti da adottare o meno, sulle minacce possibili etc.)?		
Copertura assicurativa Cyber Risk • La Società ha sottoscritto una polizza assicurativa a tutela dei dati e della produttività dal rischio di un attacco informatico? • Se sì, con quale Compagnia, rischi coperti, massimali e premi.		

7.2. Check list - Adempimento obblighi derivanti dall'applicazione della Direttiva NIS2 in materia di cybersicurezza

PUNTO DI VERIFICA	SI	NO	RISPOSTA AL QUESITO/NOTE
La Società opera in un settore ad alta criticità (All. 1 Direttiva NIS2)?			
La Società opera in un altro settore critico (All. 2 Direttiva NIS2)?			
TEMI REGOLAMENTARI			
Adozione di una procedura			
• Valutazione del rischio			
• Sono stati evidenziati dei gap da colmare?			
• Adozione di una procedura			
Individuazione del Referente per la cybersicurezza			
Formazione			
• Su procedura			
• Su adempimenti *cybersicurezza*			
• Soggetti coinvolti			
• Dipendenti			
ADOZIONE MISURE TECNICHE			
• Politiche di analisi dei rischi e di sicurezza dei sistemi informatici • Gestione degli incidenti e processo di notifica • Continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi • Sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi • Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità • Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di *cybersicurezza* • Pratiche di igiene informatica di base e formazione in materia di *cybersicurezza* • Politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura • Sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi • Uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso			

ISCRIZIONE PIATTAFORMA ACN (Agenzia per la c*ybersicurezza* nazionale)			
• **La Società si è registrata sul Portale ACN?**			
• **Se sì, quando?**			
• **La Società ha comunicato all'ACN il Referente per la *Cybersicurezza* individuato?**			
INCIDENTI SIGNIFICATIVI			
La Società ha adottato misure tecniche organizzative per la gestione degli incidenti?			
La procedura contiene i seguenti elementi?			
• Classificazione degli incidenti			
• Processo di notifica al CSIRT Italia (*Computer Security Incident Response Team* dell'ACN)			
• Regolamentazione delle ipotesi delle notifiche volontarie			

Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili
Piazza della Repubblica, 59 00185 Roma