Vantaggi per lo studio

Dal CNDCEC un *vademecum* per accompagnare le imprese nella gestione del rischio *cyber* e nell'adeguamento dei modelli organizzativi ai più recenti sviluppi normativi e tecnologici. Le minacce informatiche rappresentano, infatti, un fattore di rischio per le imprese e impongono un approccio sempre più integrato tra sistemi di controllo interno, *governance* e *compliance*.

Cybersecurity e modello 231: rischio informatico nella governance d'impresa

L'ordine dei dottori commercialisti e degli esperti contabili, congiuntamente alla fondazione nazionale di ricerca dei commercialisti, ha sviluppato un'analisi dedicata agli effetti della digitalizzazione sui processi aziendali e professionali, fenomeno che sta incidendo in modo significativo sull'organizzazione delle imprese e sui sistemi di controllo interno e di *governance* societaria. L'evoluzione della normativa nazionale ed europea, insieme all'ampliamento dei reati informatici rilevanti ai sensi del D.Lgs. 231/2001, impone alle organizzazioni l'adozione di modelli strutturati di gestione del rischio *cyber*.
In tale contesto, anche il ruolo del commercialista è destinato ad evolversi, poiché le problematiche connesse alla *cybersecurity* coinvolgono ormai numerosi ambiti dell'attività di consulenza e controllo, tra cui gli assetti organizzativi, i sistemi di *compliance*, l'attività degli organismi di vigilanza, i controlli societari e i processi di *risk assessment*.
Alla luce di tali trasformazioni, assume particolare rilevanza la formazione dei professionisti sulle tematiche della sicurezza informatica e della *governance* digitale, al fine di fornire competenze adeguate alla nuova gestione delle imprese; in particolare, è essenziale promuovere una maggiore consapevolezza del rapporto tra *cyber-security*, *governance* societaria e modello 231, riconoscendo che il rischio informatico non può più essere considerato un profilo esclusivamente tecnico, ma deve essere pienamente integrato nei sistemi di organizzazione, gestione e controllo dell'ente.

RISCHI PER LE IMPRESE DERIVANTI DALL'UTILIZZO DI STRUMENTI INFORMATICI	⇨	• Delitti contro la persona. • Delitti contro la fede pubblica. • Delitti contro il patrimonio. • Violazione delle direttive europee "*NIS*".
PRINCIPALI AMBITI DI TUTELA NEI REATI INFORMATICI	⇨	• Riservatezza dei dati e delle comunicazioni informatiche. • Integrità dei dati e dei sistemi informatici. • Fede pubblica.
COME SI STRUTTURA L'INTEGRAZIONE DEL RISCHIO INFORMATICO NEL MODELLO 231	⇨	L'impresa deve adottare un *risk approach* strutturato da collocare nel più ampio contesto degli adeguati assetti organizzativi, amministrativi e contabili (OAC).
	⇨	La valutazione dei rischi e delle misure da introdurre per mitigarne gli effetti deve essere continuativa e periodicamente aggiornata.
	⇨	La mappatura dei rischi informatici deve comprendere i sistemi *hardware* e *software*, i dati strategici, i flussi informativi interni ed esterni e i rischi indotti da soggetti terzi che hanno accesso ai sistemi o ai dati dell'impresa.
	⇨	È necessario l'aggiornamento del codice etico e dei protocolli specifici per promuovere comportamenti corretti nell'utilizzo degli strumenti informatici, oltre che piani di formazione e sensibilizzazione per il personale.
	⇨	L'organismo di vigilanza deve vigilare sulla efficace attuazione e sull'aggiornamento del modello 231, sulle minacce emergenti, sulle anomalie ripetute, sulla simulazione di scenari avversi.

EVOLUZIONE DEL CYBERCRIME

La progressiva digitalizzazione dell'economia ha reso la sicurezza informatica una variabile strategica della vita d'impresa: 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. Ciò ha generato inevitabilmente 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 definite come "*attacchi cyber*". L'**Associazione Italiana per la Sicurezza Informatica Clusit** rappresenta un punto di riferimento autorevole nel settore della sicurezza informatica. L'associazione pubblica periodicamente rapporti e analisi sull'evoluzione della *cyber*sicurezza in Italia e a livello globale. Nel "*Rapporto Clusit sulla Cybersecurity 2026*" viene evidenziato un incremento significativo degli incidenti informatici registrati nel 2025, pari al 48,7% rispetto all'anno precedente, corrispondente al valore più elevato mai rilevato, per un totale di 5.265 eventi. I settori maggiormente colpiti risultano essere la pubblica amministrazione e le istituzioni, il comparto manifatturiero e quello dei trasporti, sebbene fenomeni analoghi si riscontrino trasversalmente in diversi ambiti produttivi, inclusi i servizi professionali, sanitari e finanziari.

Tra le principali tipologie di attacco informatico si segnalano:

- **attacchi DDoS** (*Distributed Denial of Service*), finalizzati a sovraccaricare i sistemi informatici mediante un volume di traffico generato simultaneamente da molteplici fonti, con conseguente indisponibilità dei servizi per gli utenti;
- ***malware***, ossia *software* malevoli in grado di compromettere il funzionamento dei sistemi informatici, con finalità di danneggiamento, interruzione operativa o sottrazione di dati sensibili presenti nelle banche dati.

Per lungo tempo, il fenomeno del *cybercrime* è stato favorito da una diffusa impreparazione degli utenti, nonché da un insufficiente coordinamento tecnico e normativo da parte delle istituzioni nazionali e sovranazionali. In risposta alla crescente esposizione ai rischi digitali, si è affermato il concetto di "*cybersecurity*", inteso come l'insieme delle misure, delle tecnologie, dei processi e delle regole finalizzati alla protezione di persone, sistemi informatici e dati dagli attacchi e dagli incidenti di natura *cyber*.

A partire dal 2018, il legislatore italiano ha progressivamente sviluppato un articolato quadro normativo in materia di *cybersecurity*, anche attraverso il recepimento delle direttive europee in materia di sicurezza delle reti e dei sistemi informativi, tra cui la **Direttiva NIS** e la successiva **Direttiva NIS2**. In tale percorso si inserisce anche l'istituzione dell'**Agenzia per la Cybersicurezza Nazionale (ACN)**. Più recentemente, il quadro normativo nazionale è stato ulteriormente rafforzato con l'approvazione della L. 90/2024, comunemente definita "***Legge sulla Cybersecurity***", e con il successivo D.Lgs. 138/2024, introducendo nuovi obblighi a carico delle imprese e delle pubbliche amministrazioni, attraverso l'adozione di misure strutturate di gestione del rischio informatico e l'implementazione di procedure e piani di risposta agli incidenti *cyber*.

La disciplina in materia di *cyber*sicurezza incide in modo significativo anche sui profili di ***risk management e risk assessment*** connessi alla responsabilità organizzativa delle imprese. La normativa individua l'ambito soggettivo di applicazione e definisce specifici obblighi di segnalazione tempestiva all'Agenzia per la Cybersicurezza Nazionale (ACN) in relazione agli attacchi e agli incidenti informatici rilevanti ai fini del perimetro di sicurezza nazionale cibernetica, in coordinamento con i principi già previsti dal GDPR in materia di *data breach* e tutela dei dati personali. Nell'ambito degli assetti organizzativi interni, la normativa prevede l'individuazione di un **referente per la *cyber*sicurezza**, il cui nominativo deve essere comunicato all'ACN, rafforzando così i meccanismi di coordinamento e presidio del rischio informatico all'interno delle organizzazioni.

REATI RILEVANTI IN AMBITO INFORMATICO

L'**art. 24-*bis* D.Lgs. 231/2001** include tra i reati presupposto della responsabilità amministrativa degli enti un ampio insieme di fattispecie di natura informatica. La disposizione normativa contempla, in particolare, gli illeciti che richiedono, ai fini della loro consumazione, l'impiego di tecnologie dell'informazione e di sistemi informatici o telematici; tra questi si registrano diverse categorie di illeciti, tra cui:

- **i delitti contro la fede pubblica**, finalizzati, ad esempio, alla formazione o all'utilizzo di documenti e atti falsi;
- **i delitti contro la persona**, volti a compromettere la libertà individuale mediante l'interruzione o l'alterazione del funzionamento dei sistemi informatici, ovvero attraverso la violazione di informazioni personali o riservate;
- **i delitti contro il patrimonio**, riconducibili a condotte fraudolente o di appropriazione indebita realizzate mediante strumenti digitali;
- **le violazioni della disciplina derivante dalle Direttive NIS e NIS2**, connesse all'inadempimento degli obblighi previsti in materia di sicurezza delle reti e dei sistemi informativi, nonché degli obblighi di comunicazione verso le autorità competenti.

In considerazione degli illeciti sopra delineati, è possibile individuare 3 principali ambiti di tutela:

- il primo riguarda la **riservatezza dei dati e delle comunicazioni informatiche**, affinché si eviti l'accesso abusivo a un sistema informatico o telematico, sanzionando chi vi accede o vi si mantiene senza autorizzazione o oltre i limiti consentiti. In tale area rientrano anche le fattispecie relative alla detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, condotte spesso prodromiche rispetto all'accesso illecito, nonché i reati di intercettazione abusiva di comunicazioni informatiche o telematiche;
- il secondo profilo di tutela riguarda **l'integrità dei dati e**

dei sistemi informatici, presidiata da fattispecie di danneggiamento introdotte con la normativa di riferimento in materia di criminalità informatica. In tale ambito, il legislatore distingue tra il danneggiamento di dati, programmi o sistemi informatici di natura privata e quello relativo a sistemi pubblici o di pubblica utilità;

- il terzo profilo di tutela concerne la **fede pubblica** che rappresenta un ulteriore ambito di rilevanza dei reati informatici. In particolare, la tutela è estesa anche ai documenti in formato digitale, equiparandoli, sotto il profilo della tutela penale, ai documenti tradizionali; tra le ipotesi di reato vengono considerate la falsificazione documentale realizzata attraverso strumenti informatici, nonché le condotte di frode informatica caratterizzate dall'alterazione o manipolazione di dati digitali al fine di conseguire un ingiusto profitto, spesso in danno della pubblica amministrazione.

Alla luce dei principali profili dei reati informatici, la normativa in materia di *cyber*sicurezza persegue l'obiettivo di rafforzare la protezione dei sistemi informativi e di contrastare in modo più efficace i *cyber*-attacchi, attraverso un generale inasprimento del trattamento sanzionatorio relativo ai c.d. ***computer crimes***. In tale prospettiva, sono state introdotte modifiche sia di natura sostanziale sia procedurale, che incidono sulla disciplina dei reati informatici mediante l'innalzamento delle pene edittali, l'ampliamento del dolo specifico, l'introduzione di nuove circostanze aggravanti e la limitazione dell'applicabilità di attenuanti in relazione a diverse condotte realizzate tramite strumenti informatici. La normativa in materia di *cyber*sicurezza ha prodotto rilevanti effetti sull'impianto del D.Lgs. 231/2001, con particolare riferimento alla disciplina dei reati informatici. In primo luogo, sono state valorizzate le fattispecie connesse all'utilizzo dei sistemi informatici per il conseguimento di indebiti vantaggi in danno di terzi, nonché le condotte di accesso abusivo ai sistemi, di intercettazione e di interruzione delle comunicazioni informatiche e telematiche. In secondo luogo, la riforma ha inciso in modo significativo sulla responsabilità amministrativa degli enti, soprattutto in relazione ai reati informatici; si registra infatti un incremento delle sanzioni pecuniarie applicabili all'ente in caso di commissione dei reati presupposto, unitamente all'introduzione di ulteriori misure sanzionatorie, comprese quelle interdittive, per nuove fattispecie riconducibili alla criminalità informatica e alla sicurezza cibernetica nazionale, tra cui le ipotesi di estorsione realizzata mediante strumenti digitali.

L'ampliamento del catalogo dei reati presupposto determina un aumento dell'esposizione al rischio anche per le imprese non operanti nel settore tecnologico, poiché qualsiasi utilizzo improprio dei sistemi informativi da parte di soggetti apicali o subordinati, se realizzato nell'interesse o a vantaggio dell'ente, può integrare profili di responsabilità ai sensi della disciplina vigente.

Ne consegue la necessità per gli enti di adeguare i modelli di organizzazione e gestione attraverso l'introduzione di nuovi presidi di controllo, il potenziamento delle misure di sicurezza relative agli accessi ai sistemi informatici, l'implementazione di strumenti di *cyber*security e la predisposizione di specifici programmi formativi.

GESTIONE DEL RISCHIO INFORMATICO NEL MODELLO 231

Dal momento che il rischio informatico ha assunto una crescente centralità sia sotto il profilo operativo sia sotto quello giuridico-penale, il modello di organizzazione, gestione e controllo previsto dal D.Lgs. 231/2001 rappresenta, in questo contesto, un sistema organizzativo strutturato e dinamico, finalizzato all'individuazione delle aree sensibili e alla prevenzione dei rischi rilevanti per l'ente. L'inclusione della *cyber*security nell'ambito del perimetro 231 non costituisce una scelta discrezionale dell'ente, ma si configura come un'**esigenza sistemica** derivante dall'evoluzione normativa. Da un lato, il legislatore ha progressivamente ampliato il catalogo dei reati presupposto, includendovi anche le principali fattispecie di criminalità informatica; dall'altro, la normativa di settore, anche di derivazione europea, impone l'adozione di misure organizzative e tecniche adeguate, contribuendo alla formazione di un sistema di *compliance* integrata nel quale il modello 231 assume una funzione centrale. La gestione del rischio informatico all'interno del modello 231 si fonda sul principio della "***prevenzione mediante organizzazione***": la responsabilità dell'ente può infatti derivare dalla commissione di un reato informatico nell'interesse o a vantaggio dell'organizzazione, laddove tale evento sia riconducibile a un *deficit* organizzativo, ossia alla mancata adozione o all'inefficace attuazione di adeguati presidi preventivi. Il giudizio di idoneità del modello deve essere svolto verificando la razionalità e la proporzionalità delle misure adottate rispetto ai rischi concretamente individuabili al momento della loro predisposizione. Non è sufficiente, pertanto, la mera adozione formale del modello: ciò che rileva è la sua effettiva integrazione nei processi aziendali e la sua concreta capacità di orientare i comportamenti organizzativi e prevenire il verificarsi dei rischi.

È logico anche che l'integrazione di sistemi di **intelligenza artificiale** nei processi aziendali comporti un ampliamento delle aree di rischio rilevanti ai fini della responsabilità prevista dal D.Lgs. 231/2001, richiedendo una rilettura evolutiva del paradigma della "***colpa di organizzazione***". In quest'ottica l'AI costituisce un fattore tecnologico in grado di incidere sull'assetto organizzativo, sul governo dei processi e sulla prevedibilità delle condotte illecite. Il quadro normativo di riferimento è oggi arricchito dal regolamento europeo sull'intelligenza artificiale, che adotta un approccio basato sul rischio e distingue tra sistemi vietati, ad alto rischio e a rischio limitato o minimo. Per i sistemi ad alto rischio sono previsti obblighi specifici in materia di gestione del rischio, *governance* dei dati, documentazione tecnica, trasparenza, supervisione umana e robustezza, in evidente continuità con i presidi richiesti dai modelli organizzativi *ex* D.Lgs. 231.

A livello nazionale, la recente legge in materia di intelligenza artificiale rafforza ulteriormente tali principi, valorizzando tra-

sparenza, sicurezza, tracciabilità, supervisione umana e tutela dei diritti fondamentali, e introducendo specifiche disposizioni in tema di *cyber*sicurezza, protezione dei dati e responsabilità connessa all'utilizzo dei sistemi di AI.

INTEGRAZIONE TRA MODELLO 231 E CYBERSECURITY

Il D.Lgs. 231/2001 rappresenta una significativa capacità di **gestione del rischio informatico**, grazie a un impianto fondato sulla prevenzione mediante organizzazione e su un approccio strutturato al *risk assessment*. L'integrazione tra modello 231 e *cyber*security si articola principalmente lungo 3 direttrici: la gestione del rischio informatico come componente essenziale del modello 231; l'analisi dei rischi con la conseguente **mappatura delle aree sensibili**; il ruolo del **codice etico e dei protocolli interni** come strumenti di presidio sia comportamentale sia procedurale.

Sotto il profilo operativo, l'integrazione del rischio informatico nel modello 231 richiede l'adozione di un **approccio strutturato al rischio**, coerente con il sistema degli adeguati assetti organizzativi, amministrativi e contabili. In tale prospettiva, la logica della prevenzione mediante organizzazione è comune sia al sistema 231 sia agli assetti organizzativi, rendendo il modello un elemento rilevante ai fini della loro adeguatezza, secondo criteri di proporzionalità rispetto a natura e dimensioni dell'impresa. Gli assetti organizzativi costituiscono l'infrastruttura attraverso cui l'impresa identifica, valuta e governa i rischi rilevanti, inclusi quelli di natura penale, economica e reputazionale. Il ***risk approach*** si traduce operativamente in attività quali mappatura dei processi, individuazione delle aree sensibili, *gap analysis*, tracciabilità delle decisioni e strutturazione dei flussi informativi. In tale contesto, il ***risk appetite framework*** consente di definire il livello di rischio accettabile e di individuare le modalità di gestione, riduzione o trasferimento del rischio, anche tramite strumenti assicurativi o contrattuali.

Il modello 231 deve essere aggiornato in modo continuo, in coerenza con l'evoluzione normativa e organizzativa; in ambito *cyber* ciò implica una revisione **periodica della mappa dei rischi informatici** e un approccio necessariamente ***forward looking***. Poiché il rischio informatico è intrinsecamente evolutivo, la sua gestione non può basarsi esclusivamente su dati storici, ma deve includere capacità predittive e di anticipazione delle minacce emergenti. Il monitoraggio del rischio informatico, quindi, richiede un approccio dinamico basato su sorveglianza continua e verifiche periodiche. In questo quadro assume rilievo il ruolo dell'**organismo di vigilanza**, chiamato a monitorare l'efficace attuazione e l'aggiornamento del modello, nonché a presidiare sulle minacce emergenti, sulle anomalie ricorrenti, sulla simulazione di scenari avversi, secondo una logica di *continuous risk assessment*. Il modello deve, inoltre, integrare logiche di *incident response*, *business continuity* e *disaster recovery*, in linea con i principali *framework* internazionali.

In merito all'analisi dei rischi e la mappatura delle aree sensibili, il modello 231 non può limitarsi a un'elencazione astratta di fattispecie di reato, ma deve fondarsi su una **ricognizione puntuale dei processi aziendali** e delle modalità concrete di possibile commissione degli illeciti. In questa prospettiva, il concetto di "*area sensibile*" si amplia in ambito *cyber*, includendo non solo i processi potenzialmente rilevanti ai fini dei reati informatici, ma anche quelli che trattano dati personali, gestiscono infrastrutture critiche o utilizzano sistemi la cui compromissione può generare impatti patrimoniali, operativi o reputazionali significativi, anche in connessione con la normativa *privacy* e la disciplina sulla sicurezza delle reti e dei sistemi informativi. Su tale base si procede all'identificazione dei processi aziendali e dei relativi flussi informativi, con particolare attenzione ai sistemi di gestione delle identità e degli accessi, ai processi di approvvigionamento e *supply chain*, alle comunicazioni elettroniche, alla gestione dei dispositivi mobili e del lavoro da remoto, nonché ai sistemi di conservazione e *backup* dei dati, fondamentali in ottica di resilienza. La valutazione del rischio *cyber* si articola, quindi, secondo 3 parametri: la **probabilità di accadimento**; l'**impatto**; l'**efficacia dei controlli esistenti**. La dimensione della *supply chain* amplifica ulteriormente l'esposizione al rischio, estendendo il perimetro di vulnerabilità oltre i confini dell'ente e rendendo essenziale una gestione coordinata dei rischi lungo **tutta la catena di fornitura**. Inoltre, poiché l'efficacia del modello 231 rispetto ai reati informatici dipende dall'adozione di presidi organizzativi e tecnici adeguati, aggiornati e concretamente attuati, un ruolo centrale è svolto anche dal ***log management***, che garantisce tracciabilità e ricostruzione degli eventi, e dagli *audit* periodici, volti a verificare l'effettiva attuazione delle misure e non la sola loro esistenza formale.

Infine, di rilievo è anche l'aggiornamento del **codice etico** e dei **protocolli interni** dedicati ai reati informatici che rispondono all'esigenza di rafforzare l'integrazione tra *cybersecurity*, *compliance* 231 e *governance* aziendale. Nello specifico, il codice etico assume un ruolo centrale nella diffusione di una cultura della sicurezza informatica, promuovendo comportamenti corretti nell'utilizzo degli strumenti digitali e richiamando i principi di riservatezza, integrità e disponibilità delle informazioni. Oltre a ciò, il modello 231 richiede l'adozione di protocolli operativi specifici finalizzati a disciplinare le principali aree di rischio *cyber*, con particolare riferimento alla gestione degli accessi ai sistemi informatici, agli incidenti di sicurezza, all'utilizzo dei dispositivi aziendali e ai rapporti con fornitori e soggetti terzi. Un ruolo essenziale è, inoltre, svolto dalla **formazione del personale**, quale strumento indispensabile per assicurare l'effettiva attuazione del modello e sviluppare una diffusa consapevolezza dei rischi informatici e delle corrette misure di prevenzione.