CONTROLLO

Modello 231: strumento aziendale in costante evoluzione e al passo con la tecnologia – Cyber Risk

di **Andrea Onori**

Il **Modello 231 è uno strumento aziendale strategico** in continua evoluzione e non può che essere così.

Un modello di gestione e organizzazione aziendale deve essere al **passo con i tempi** e, non di meno, al passo con **l'evoluzione tecnologica**.

I modelli di organizzazione e gestione, in ambito di responsabilità amministrativa di impresa, devono tener conto di quelli che sono i **maggiori rischi che le aziende si trovano ad affrontare**.

L'"***Allianz Risk Barometer***", pubblicato a gennaio 2025, ha identificato i **principali rischi aziendali per il 2025**.

La **criminalità informatica**, le **interruzioni della rete e dei servizi IT**, i *malware/ransomware* e le violazioni dei dati sono i **maggiori rischi** ai quali le aziende sono esposte.

Anche la circolare Assonime n. 1/2025 evidenzia come "*nell'attuale contesto socio-economico, caratterizzato da un'intensa digitalizzazione, il rischio cyber costituisce una minaccia crescente per le imprese di ogni dimensione, natura e settore. L'incremento della connettività insieme alla progressiva diffusione del cloud, dell'IOT e, da ultimo, dell'intelligenza artificiale, se da una parte, ha apportato benefici in termini di efficienza e innovazione, dall'altra, espone sempre di più le imprese a nuove vulnerabilità e rischi, come la perdita di dati sensibili, furti di proprietà intellettuale, svariate tipologie di frodi e interruzioni dell'attività, che possono avere impatti disastrosi non solo sul piano economico e legale, ma anche in termini reputazionali*".

Nella **seconda metà del 2024**, dapprima con la L. 90/2024 e successivamente con il D.Lgs. 138/2024, sono stati introdotti provvedimenti che hanno aumentato gli **obblighi di attenzione da parte delle imprese in ambito di *Cyber Security*.**

Con la prima sono state introdotte disposizioni rilevanti in materia di cybersicurezza e di reati informatici:

- è stato introdotto il nuovo reato di "***estorsione informatica***" (**articolo 629, comma 3, c.p.**

), con il conseguente ampliamento dei reati presupposto di cui al D.Lgs. 231/2001;
- è stato introdotto nel **codice penale l'articolo 635-1** rubricato "***Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico***".

Come seguito di tali modifiche, nello specifico, l'**articolo 20, L. 90/2024**, ha apportato modifiche all'**articolo 24-*bis*, D.Lgs. 231/2001**, inserendo all'interno dello stesso:

1. il **reato di estorsione informatica**; e
2. il nuovo reato di cui all'**articolo 635-*quater*.1, c.p.**;

facendoli, pertanto, entrare tra quelli rilevanti ai fini della **prevenzione della responsabilità amministrativa d'impresa.**

Lo stesso **articolo 20, L. 90/2024**, interviene anche nell'ambito delle **sanzioni pecuniarie**.

Viene previsto un considerevole **incremento delle quote** (sanzioni):

1. *da duecento a settecento quote*, per la commissione dei delitti informatici presupposto di cui all'**articolo 24-*bis*, comma 1, D.Lgs. 231/2001**;
2. *fino a quattrocento quote*, per i delitti di "*Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici*" e "*Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*";
3. *da trecento a ottocento quote*, per il nuovo reato di estorsione informatica in cui gli altri delitti informatici (o la minaccia di compierli) fungono da strumento per mettere in atto la tipica fattispecie estorsiva.

Con il D.Lgs. 138/2024 è stata **recepita la Direttiva UE 2022/2555** (NIS 2) che incrementa ulteriormente gli obblighi in ambito di *Cyber Security* sia per le **aziende del settore privato che pubblico** in ambiti considerati critici e ad alta criticità.

L'introduzione degli obblighi previsti dalla NIS 2, assieme alla **conseguente implementazione dei Modelli di gestione della cybersecurity**, portano al conseguente aggiornamento e adeguamento del Modello di Organizzazione e Gestione alla luce delle modifiche apportate in tema di reati informatici a cura della L. 90/2024 di cui si è parlato sopra.

Il Modello 231 deve prevedere, **in ambito di sicurezza informatica**:

1. **procedure, politiche e controlli**: l'ente deve implementare politiche, procedure e controlli tecnici adeguati a mitigare i rischi informatici. L'Organismo di vigilanza (OdV) deve eseguire controlli periodici sulle misure di cybersecurity aziendali adottate;
2. **procedure per gestione degli incidenti**: la Direttiva NIS 2 prevede protocolli specifici per la notifica degli incidenti relativi alla **sicurezza informatica** nel modo più rapido e

tempestivo possibile. L'azienda deve adottare un **approccio strutturato per l'identificazione, l'analisi e la gestione dei rischi** L'OdV deve assicurarsi che l'azienda abbia adottato tali procedure e protocolli interni, nonché dovrà monitorarne il loro rispetto;

3. **documentazione e controllo**: l'azienda deve predisporre la documentazione richiesta dalla NIS 2 e l'OdV deve verificare che tutta la **documentazione richiesta sia presente, aggiornata e conforme** ai requisiti normativi;
4. **aggiornamento continuo, formazione e sensibilizzazione**: gli organi di amministrazione e gli organi direttivi sono tenuti a seguire una formazione in materia di sicurezza informatica, nonché promuovono una formazione periodica ai loro dipendenti al fine di individuare i rischi e valutare le pratiche di gestione degli stessi. L'Odv dovrà **aggiornare periodicamente il Modello 231 per mantenere adeguata la protezione dell'azienda** contro i *Cyber Risks*, nonché dovrà vigilare affinché il personale sia adeguatamente formato sui temi della sicurezza informatica e sui protocolli da seguire in caso di incidenti.

Anche l'attività dell'Organismo di Vigilanza è condizionata dalle **modifiche introdotte dai provvedimenti relativi alla *Cyber Security***, dovendo ampliare le proprie funzioni al fine di includere il **monitoraggio alla conformità della Direttiva NIS 2.**

Dovrà anche verificare:

- l'avvenuta **registrazione obbligatoria sulla piattaforma** dell'Agenzia per la cybersicurezza nazionale (ACN);
- la **nomina del Responsabile della sicurezza informatica** e del **Responsabile degli adempimenti** per la conformità alla NIS;
- che il **MOG 231 includa la sicurezza informatica**, nonché la **prevenzione del *Cyber Risk*** come parte integrante della prevenzione di reati informatici;
- la **corretta e costante collaborazione con i responsabili della sicurezza informatica**;
- la **predisposizione di idonei flussi informativi** per la tempestiva notifica di incidenti per una corretta e adeguata gestione degli incidenti informatici;
- che i **responsabili aziendali coinvolti siano formati e rispettino le tempistiche previste**.