

IL D.LGS. 231/2001 - EVOLUZIONE CONTINUA. FONDAMENTI NORMATIVI, RISCHI EMERGENTI E GIURISPRUDENZA RECENTE

CYBER E INTELLIGENZA ARTIFICIALE - SANZIONI INTERNAZIONALI - LE MISURE DI SELF CLEANING -
ORIENTAMENTI GIURISPRUDENZIALI RECENTI

Cyber, IA e Modello 231:
rischi emergenti e ruolo dell'OdV

Avv. Donato ANCONA

21 luglio 2026

AGENDA

1. Perché la cybersecurity è ormai un tema 231, non solo IT
2. Com'è cambiata la normativa negli ultimi anni
3. Modello 231: come aggiornarlo
4. OdV: come comportarsi
5. Consigli operativi

PUNTO DI PARTENZA

La cybersecurity non è (più) solo un problema dell'IT

- **Rischio strutturale d'impresa.** Tocca continuità operativa, patrimonio informativo e reputazione.
- **Rilievo 231.** Un reato informatico commesso nell'interesse o a vantaggio dell'ente attiva la responsabilità dell'ente (artt. 5-7 e 24-bis d.lgs. 231/2001).
- **Anche le imprese "non tech".** Qualunque uso improprio di un sistema da parte di apicali o sottoposti può integrare un reato-presupposto.
- **Il ruolo del Modello.** Non difendere l'ente dall'attacco subito, ma prevenire il reato commesso nel suo interesse o vantaggio.

ATTENZIONE — ERRORE RICORRENTE

Trattare la cyber come questione tecnica separata dal Modello. È invece una componente organica del sistema di controllo.

COSA È CAMBIATO

2024–2026: un triennio di svolta normativa

- **2024 - L. 90/2024:** “Legge cybersicurezza”: inasprisce i reati informatici e le sanzioni 231 dell’art. 24-bis.
- **2024 - d.lgs. 138/2024:** Recepisce la NIS2 che impone a enti e aziende di settori critici di adottare misure organizzative e tecniche per gestire il rischio informatico e notificare gli incidenti cyber significativi.
- **2025 – DORA:** (Reg. UE 2022/2554) pienamente operativo per il settore finanziario dal 17.1.2025.
- **2024/26 - AI Act:** (Reg. UE 2024/1689) in applicazione progressiva.
- **2025 - L. 132/2025:** Prima legge organica italiana sull’IA, con delega al Governo.

OPERATIVAMENTE

Per molte PMI, la NIS2 è il primo vero obbligo cogente in materia di cybersecurity.

IL PERIMETRO PENALE

Art. 24-*bis* d.lgs 231/01: i reati informatici presupposto, oggi

- **Tre beni tutelati:** (i) Riservatezza (615-*ter/quater*, 617-*quater/quinquies*); (ii) integrità di dati e sistemi (635-*bis* ... 635-*quater.1*); (iii) fede pubblica (491-*bis*, 640-*quinquies*).
- **L. 90/2024:** Pene più alte, nuove aggravanti, divieto di attenuanti per alcuni *computer crimes*.
- **Impatto sulla 231:** Sanzione del comma 1 elevata da 100/500 a 200/700 quote; il 615-*quinquies* c.p. abrogato e sostituito dal 635-*quater.1* c.p.
- **Nuovo comma 1-*bis* dell'art. 24-*bis*:** Estorsione mediante reati informatici (art. 629 co. 3 c.p.): 300/800 quote e interdittive non inferiori a 2 anni.

ATTENZIONE

Il baricentro resta la “**colpa di organizzazione**”: la responsabilità nasce dal deficit organizzativo, non dal solo fatto tecnico.

PERCHÉ RIGUARDA IL PROFESSIONISTA

Rischio cyber = adeguatezza degli assetti (art. 2086 c.c.)

- **Stesso fondamento:** Modello 231 e adeguati assetti OAC condividono la logica della “prevenzione mediante organizzazione” (artt. 2086, 2381, 2403 c.c.).
- **Non solo tecnica:** Un’infrastruttura IT non protetta può tradursi in inadeguatezza degli assetti *ex art.* 2086 c.c.
- **Esempio:** Un *ransomware* (dati sequestrati) che blocca i gestionali blocca la fatturazione, oscura i flussi finanziari, ostacola gli adempimenti fiscali → colpisce la continuità aziendale.
- **Per il professionista:** Il tema entra negli assetti, nella continuità, nell’attività del collegio sindacale/sindaco e dell’OdV.

COSA CHIEDERE AL CLIENTE

Esiste una mappa aggiornata dei rischi informatici? Chi la aggiorna e ogni quanto? (*Best practice*: riesame almeno annuale)

IL MODELLO 231

Quattro cantieri di aggiornamento del Modello

1. **Mappatura:** Estendere l'analisi *as-is* alle aree sensibili cyber: identità/accessi, comunicazioni, pagamenti, backup, fornitori.
2. **Parte Speciale / protocolli:** Aggiornare i protocolli "reati informatici", anche in vista della delega L. 132/2025.
3. **Codice Etico:** Sancire i principi CIA (*Confidentiality, Integrity, Availability*) - riservatezza, integrità, disponibilità - come doveri di tutti, non solo dell'IT.
4. **Formazione:** Piani differenziati (base/intermedio/apicale), simulazioni di *phishing, tabletop*; documentata e verificabile.

OPERATIVAMENTE

Far coincidere l'aggiornamento cyber con il riesame periodico del Modello 231.

I PRESIDI OPERATIVI

I protocolli cyber che non possono mancare

- **Identità – Accessi:** Assegnazione, modifica e revoca degli accessi, minimo privilegio, segregazione dei compiti: il presidio più critico.
- **Gestione incidenti.** *Escalation* e notifiche (Garante 72h; CSIRT/ACN 24h per i soggetti obbligati) + conservazione delle evidenze forensi.
- **Dispositivi e lavoro remoto:** VPN, cifratura, gestione di furto e smarrimento.
- **Fornitori e terzi:** Requisiti minimi di sicurezza e verifiche periodiche.

COSA DOCUMENTARE NELL'ATTIVITÀ DI VIGILANZA

Prova della revoca tempestiva delle credenziali a fine rapporto, dei test di ripristino dei backup, autenticazione a 2 fattori sugli accessi critici (MFA).

IL PUNTO DEBOLE

Il rischio della catena di fornitura (*supply chain*)

- **Perimetro esteso:** I sistemi dell'ente sono interconnessi con quelli di fornitori e partner: il rischio supera i confini aziendali.
- **Casi:** SolarWinds - 2020 (società statunitense che sviluppa software per la gestione e il monitoraggio delle infrastrutture IT) e Harrods – 2025 (grandi magazzini di lusso).
- **Obbligo NIS2:** Gestire la sicurezza della catena di approvvigionamento (art. 21, par. 2, lett. d).
- **Contratto fornitori:** Clausole di sicurezza, notifica tempestiva, standard minimi, diritto di audit, rimedi per l'inadempimento.

CAMPANELLO D'ALLARME

Un fornitore IT con accesso remoto ai sistemi, o un software non aggiornato, può diventare il vettore d'attacco principale.

L'ORGANISMO DI VIGILANZA

L'OdV alla prova del cyber: flussi e verifiche

- **Flussi informativi:** Periodici e ad evento: incidenti, *data breach*, esiti delle simulazioni di *phishing*, segnalazioni *whistleblowing* informatiche.
- **Audit:** Revoca credenziali a fine rapporto, test di ripristino backup, *policy password*, MFA (Multi-Factor Authentication - autenticazione a più fattori) sugli accessi critici, tempestività delle patch (aggiornamento correttivo di vulnerabilità di sicurezza, errori (bug) o malfunzionamenti).
- **Indipendenza:** Non lasciare l'audit al solo IT; nelle PMI l'OdV acquisisce evidenze oggettive dai fornitori (*log firewall*, report *patch*, attestazioni *cloud*). (➡ Eventualmente conferendo audit esterno con budget OdV!)
- **Raccordo:** Con collegio sindacale/sindaco e con gli assetti *ex art. 2086 c.c.*

OPERATIVAMENTE

Inserire nel piano di vigilanza dell'OdV verifiche cyber specifiche e pretendere flussi strutturati (Linee guida CNDCEC, nov. 2025).

GLI APPUNTAMENTI OdV DEL 2026

NIS2, DORA, AI Act: cosa verificare

- **NIS2 (imprese in perimetro).** Misure di gestione del rischio, notifica incidenti nei tempi, sicurezza della *supply chain* coerenti col Modello.
- **DORA (settore finanziario).** Resilienza operativa digitale, rischio ICT di terze parti, test di resilienza.
- **AI Act (sistemi ad alto rischio).** Governance, qualità dei dati, trasparenza, supervisione umana; nessuna area di rischio non presidiata.

REGOLA D'ORO

Mappatura integrata e un unico sistema di controllo interno: evitare le duplicazioni.

INTELLIGENZA ARTIFICIALE

L'IA per l'OdV: rischio da presidiare e strumento da usare

- **Rischi diretti.** L'IA come strumento del reato: manipolazione di dati o bilancio, documenti falsi, esfiltrazione.
- **Rischi indiretti.** *Phishing* e *social engineering* più sofisticati; opacità "*black box*"; tracciabilità delle decisioni.
- **Strumento ("osservazione aumentata").** Classificazione documentale, knowledge base ricercabile, *anomaly detection*, *risk scoring*, monitoraggio dei *follow-up*.

ATTENZIONE

L'OdV non si nasconde dietro l'algoritmo: la valutazione finale resta sua. Occhio a qualità/bias dei dati e opacità dei modelli.

DA PORTARE A CASA

Consigli operativi per il professionista

1. In sede di incarico OdV: chiedere la mappa dei rischi cyber e la data dell'ultimo aggiornamento ($\geq$ annuale).
2. Verificare la Parte Speciale "reati informatici" aggiornata post L. 90/2024.
3. Pretendere flussi informativi cyber verso l'OdV (incidenti, *data breach*, *phishing*, *whistleblowing*).
4. Controllare 5 presidi minimi: IAM, MFA, backup con test di ripristino, *patch*, revoca credenziali a fine rapporto.
5. Estendere i controlli ai fornitori IT/*cloud* (clausole + verifiche).
6. Leggere il rischio cyber come tema di adeguati assetti (art. 2086 c.c.) e di continuità aziendale.
7. Governare l'IA nel Modello: mappatura dei sistemi, supervisione umana, tracciabilità.

CHECKLIST

Autodiagnosi rapida: 10 domande

- ☐ Parte Speciale “reati informatici” aggiornata (post L. 90/2024)?
- ☐ Mappa dei rischi cyber riesaminata almeno una volta l’anno?
- ☐ Protocollo IAM (accessi, minimo privilegio, segregazione dei compiti)?
- ☐ MFA attiva sugli accessi amministrativi e da remoto?
- ☐ Backup testati con prove di ripristino (non solo eseguiti)?
- ☐ Protocollo di gestione incidenti con tempi di notifica (24h/72h)?
- ☐ Fornitori IT/cloud con clausole di sicurezza e verifiche?
- ☐ Formazione cyber differenziata, documentata, con simulazioni di *phishing*?
- ☐ OdV con flussi informativi cyber periodici e ad evento?
- ☐ Uso dell’IA in azienda mappato e supervisionato (tracciabilità)?

Grazie per l'attenzione...

Avv. Donato ANCONA

Responsabile Dipartimento Penale d'Impresa e 231 di Studio Rock

ancona@studiorock.net

STUDIO  ROCK