Pirola
Pennuto
Zei

AI E CYBER RISK: EVOLUZIONE DELLA GOVERNANCE E PROFILI DI RESPONSABILITÀ DEGLI ORGANI SOCIALI

CYBERSICUREZZA E RESPONSABILITÀ DEGLI ORGANI SOCIALI:

IL QUADRO NORMATIVO EUROPEO TRA DIRETTIVA NIS II, COMPLIANCE E ACCOUNTABILITY

Mattia Salerno
Pirola Pennuto Zei & Associati

Pirola Pennuto Zei

QUADRO NORMATIVO ITALIANO E EUROPEOSULLA CYBERSECURITY

DIRETTIVA (UE) N. 2022/2555 (DIRETTIVA NIS2)

- **Aggiorna le regole sulla cybersicurezza dell'unione europea,** modernizzando e armonizzando il quadro giuridico esistente
- **Fa parte di un ampio pacchetto di strumenti e iniziative legali a livello dell'unione** volte ad aumentare la resilienza di enti pubblici e privati alle minacce informatiche
- **mira a garantire un aumento del livello comune di cybersecurity** armonizzando le regole applicabili ai diversi operatori in diversi stati membri e rafforzando i livelli standard di sicurezza rispetto a quelli previsti dalla legislazione attuale

La Direttiva NIS2 è stata trasposta nell'ordinamento italiano con il **Decreto Legislativo n. 138/2024 (Decreto NIS2).**

Il Decreto NIS2 richiede l'adozione di misure di sicurezza proporzionate basate su un approccio multi-rischio. Rafforza inoltre i meccanismi di notifica degli incidenti e i poteri di ispezione e sanzione delle autorità competenti. I soggetti che rientrano nell'ambito del Decreto NIS2 (Soggetti NIS), distinti tra essenziali e importanti, devono soddisfare **i seguenti requisiti cumulativi (salvo eccezioni):**

Requisito settoriale: entità pubbliche e private dei tipi menzionati negli Allegati I (settori altamente critici), II (settori critici), III (amministrazioni pubbliche) e IV (altri tipi).

Requisito territoriale: organizzazioni che sono soggette alla giurisdizione nazionale.

Requisito di dimensione: entità dei tipi elencati negli Allegati I e II che superano i limiti per le piccole imprese – una «piccola impresa» significa un'impresa che impiega meno di 50 dipendenti e raggiunge un fatturato o un bilancio annuo totale non superiore a 10 milioni di euro.

Pirola Pennuto Zei

ORGANI AMMINISTRATIVI E DI GESTIONE

ORGANI DI AMMINISTRAZIONE E DIRETTIVI

Con la locuzione “organi di amministrazione” e “organi direttivi” ci si riferisce a quegli organi che detengono il potere di direzione dell’Organizzazione, incluso, ove presente, il Consiglio di amministrazione dell’organizzazione (cfr. articolo 1, comma 1, lettera e) della Determinazione ACN 379887/2025).

Le persone fisiche che devono essere elencate ai sensi dell’articolo 7(4)(c) del Decreto NIS2 sono le persone fisiche responsabili ai sensi dell’articolo 38(5) del Decreto NIS2. In altre parole, **si tratta delle persone fisiche che fanno parte degli organi amministrativi e degli organi di governo dei Soggetti essenziali e importanti del NIS a cui si fa riferimento all’Articolo 23 del Decreto NIS2.**

https://www.acn.gov.it/portale/faq/nis/ruoli-e-procedure

Pirola Pennuto Zei

PRINCIPALI RESPONSABILITA'

"GLI ORGANI AMMINISTRATIVI E DI GESTIONE DEGLI ENTI ESSENZIALI E IMPORTANTI SONO RESPONSABILI DELLE VIOLAZIONI DI CUI AL PRESENTE DECRETO." (ART. 23, DECRETO NIS2)

APPROVAZIONE DELLE MISURE DI GESTIONE DEL RISCHIO

Il CdA approva i metodi per l'implementazione delle misure di gestione del rischio di cybersecurity

SUPERVISIONE ALL'ATTUAZIONE DELLE MISURE

Il CdA supervisiona all'attuazione delle misure applicate per la gestione del rischio

FORMAZIONE OBBLIGATORIA

Gli organi di gestione seguono una formazione specifica in materia di cybersicurezza e promuovono formazione regolare per i dipendenti

Responsabilità personale

Il Decreto, insieme alla responsabilità della Società, prevede la responsabilità personale da parte dei membri degli organi amministrativi e di gestione

Gli organi amministrativi e di gestione sono responsabili delle violazioni menzionate nel Decreto NIS2.

Pirola Pennuto Zei

PRINCIPALI RESPONSABILITA'

DECRETO NIS2

ARTICOLO 23, PARAGRAFO 1, DECRETO NIS:

"Gli organi amministrativi e di gestione degli enti essenziali e importanti sono responsabili delle violazioni di cui al presente decreto."

ARTICOLO 38, PARAGRAFO 5, DECRETO NIS:

"Qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale con l'autorità di rappresentarlo, di prendere decisioni per suo conto o di esercitare un controllo sul soggetto stesso, assicura il rispetto delle disposizioni di cui al presente decreto. **Tali persone fisiche possono essere ritenute responsabili dell'inadempimento** in caso di violazione del presente decreto da parte del soggetto di cui hanno rappresentanza."

*Il Decreto NIS, insieme alla responsabilità della Società, prevede la **responsabilità personale** da parte dei membri degli organi amministrativi e di gestione.*

IL DECRETO NIS (ART. 38, PARAGRAFO 6) PREVEDE L'IMPOSIZIONE DI SANZIONI AMMINISTRATIVE.

"Qualora il soggetto non adempia nei termini stabiliti dalla diffida di cui all'articolo 37, commi 6 e 7, l'Autorità nazionale competente NIS può disporre nei confronti delle persone fisiche di cui al comma 5 del presente articolo, ivi inclusi gli organi di amministrazione e gli organi direttivi di cui all'articolo 23 dei soggetti essenziali e dei soggetti importanti, nonché di quelle che svolgono funzioni dirigenziali a livello di amministratore delegato o rappresentante legale di un soggetto essenziale o importante, l'applicazione della sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali all'interno del medesimo soggetto. Tale sospensione temporanea è applicata finchè il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle diffide di cui all'articolo 37, commi 6 e 7".

Pirola Pennuto Zei

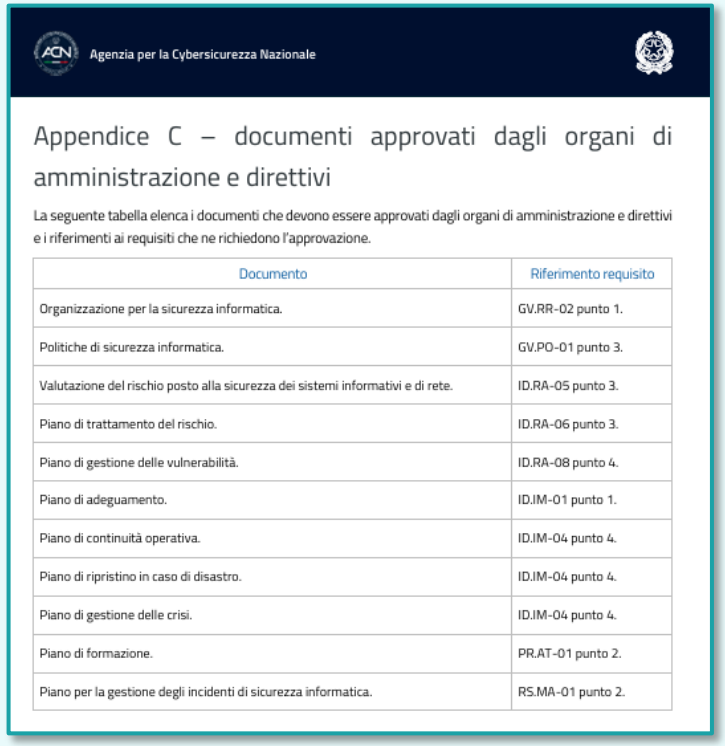
DALLA COMPLIANCE ALL'ACCOUNTABILITY

LA PERSONA FISICA È RESPONSABILE PER CONDOTTE NEGLIGENTI O OMISSIVE IN VIOLAZIONE DEI DOVERI DI DILIGENZA, SUPERVISIONE E GESTIONE AZIENDALE E DELL'ARTICOLO 23 DEL DECRETO NIS2.

È necessario dimostrare che si ha agito, o non agito, senza colpa, con la diligenza richiesta dal ruolo. Per andare esente da responsabilità, spetta all'amministratore **provare** di aver esercitato la diligenza richiesta dal ruolo

È necessario dimostrare che si ha agito, o non agito, senza colpa, con la diligenza richiesta dal ruolo. Per andare esente da responsabilità, spetta all'amministratore **provare** di aver esercitato la diligenza richiesta dal ruolo

Nessuna delega di autorità può esentare gli organi amministrativi e di gestione dalla responsabilità ai sensi dell'Articolo 23 del Decreto NIS2



Agenzia per la Cybersicurezza Nazionale

Appendice C – documenti approvati dagli organi di amministrazione e direttivi

La seguente tabella elenca i documenti che devono essere approvati dagli organi di amministrazione e direttivi e i riferimenti ai requisiti che ne richiedono l'approvazione.

Documento	Riferimento requisito
Organizzazione per la sicurezza informatica.	GV.RR-02 punto 1.
Politiche di sicurezza informatica.	GV.PO-01 punto 3.
Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete.	ID.RA-05 punto 3.
Piano di trattamento del rischio.	ID.RA-06 punto 3.
Piano di gestione delle vulnerabilità.	ID.RA-08 punto 4.
Piano di adeguamento.	ID.IM-01 punto 1.
Piano di continuità operativa.	ID.IM-04 punto 4.
Piano di ripristino in caso di disastro.	ID.IM-04 punto 4.
Piano di gestione delle crisi.	ID.IM-04 punto 4.
Piano di formazione.	PR.AT-01 punto 2.
Piano per la gestione degli incidenti di sicurezza informatica.	RS.MA-01 punto 2.

Il board deve essere in grado di dimostrare di aver valutato, approvato e monitorato nel tempo ciascuno di questi documenti

https://www.acn.gov.it/portale/documents/d/guest/guida-alla-lettura-specifiche-di-base

Pirola Pennuto Zei

OBBLIGHI E BEST PRACTICE: OVERVIEW

OBBLIGO	IMPLICAZIONI OPERATIVE	BEST PRACTICE
APPROVARE I METODI PER L'IMPLEMENTAZIONE DELLE MISURE DI GESTIONE DEL RISCHIO IT COME PREVISTO DALL'ARTICOLO 24	❑ Selezione e adeguatezza delle misure amministrative e tecniche ❑ Piani di implementazione e risorse allocate ❑ Coerenza con il profilo di rischio e le misure previste dall'Articolo 24	❑ Verbali o risoluzione formale del Consiglio di Amministrazione ❑ Supporto con la valutazione del rischio e i piani di mitigazione ❑ Rapporti di funzionamento IT ❑ Integrazione nel sistema di controllo interno (Gestione del Rischio; Modello 231, ecc.)
SUPERVISIONARE L'ATTUAZIONE DEGLI OBBLIGHI E L'AGGIORNAMENTO DELLE INFORMAZIONI AI SENSI DELL'ARTICOLO 7, PARAGRAFI 4, 5 E 7 DEL PRESENTE DECRETO	❑ Integrazione della supervisione nei modelli di controllo e governance ❑ Definire ruoli e responsabilità ❑ Approvare le procedure di gestione degli incidenti e notifica ❑ Ricevere rapporti periodici	❑ Sistemi di log sicuri, completi e accessibili ❑ Eventi di sicurezza tracciati in tempo reale ❑ Supporto per indagini e audit forensi ❑ Notifica dell'incidente: entro i termini previsti dalla legge
SEGUIRE UNA FORMAZIONE SPECIFICA SULL'ARGOMENTO E OFFRIRLA PERIODICAMENTE AI DIPENDENTI	❑ Piano di formazione aziendale aggiornato ❑ Riferire al Consiglio di Amministrazione sulle attività di formazione	❑ Tracciabilità dell'addestramento ❑ Piani di formazione personalizzati per il Consiglio di Amministrazione e i dipendenti
ESSERE INFORMATI PERIODICAMENTE O, DOVE OPPORTUNO, TEMPESTIVAMENTE DI INCIDENTI E NOTIFICHE.	Il Consiglio di Amministrazione deve essere formalmente aggiornato su: ❑ Incidenti significativi (ad esempio violazioni, ransomware, DDoS) ❑ Notifiche inviate a CSIRT, ACN o altri enti regolatori ❑ Misure adottate in risposta e stato delle indagini	❑ Rapporti periodici (trimestrali o semestrali a seconda della criticità) ❑ Comunicazioni tempestive (24 ore su 24) ❑ Tracciabilità delle comunicazioni (ad esempio tramite verbali, email interne, dashboard) ❑ Canale ufficiale strutturato tra il Consiglio di Amministrazione e le funzioni IT

Pirola Pennuto Zei

MODELLO 231 & CYBERSECURITY

PROPOSTE OPERATIVE

I tre interventi sono complementari e inseparabili:

1) Senza impegno del vertice - mancano risorse e indirizzo
2) Senza flussi informativi integrati - le vulnerabilità restano invisibili agli organi di controllo
3) Senza presidio della supply chain - il sistema rimane esposto nei punti di maggiore fragilità

01	02	03
GOVERNANCE & ADEGUATEZZA DEGLI ASSETTI	**RISK ASSESSMENT INTEGRATO**	**PRESIDIO DELLA SUPPLY CHAIN**
❑ Il rischio cyber è tema di governance (art. 2086 c.c.): infrastruttura IT non protetta integra carenza degli assetti OAC ❑ Il vertice approva misure difensive e regole di condotta per prevenire uso illecito dei sistemi ❑ Investimenti documentabili in cybersecurity = indice di effettiva attuazione del Modello 231 ❑ Il Modello 231 non presidia solo la resilienza, ma previene la commissione di reati informatici nell'interesse dell'ente	❑ Unico processo: esiti di vulnerability assessment e penetration test confluiscono nella mappa dei rischi 231 ❑ Area sensibile cyber: reati ex art. 24-bis D.Lgs. 231/2001, GDPR, NIS2 e danni patrimoniali/reputazionali ❑ I reati informatici sono spesso propedeutici ad altri reati 231 (riciclaggio, PA, societari, market abuse) ❑ Flussi informativi OdV su incidenti, verifiche sicurezza e whistleblowing su omissioni informatiche	❑ Il fornitore IT è spesso il principale vettore d'attacco ❑ Clausole contrattuali minime: notifica incidenti, standard di sicurezza, diritto di audit ❑ NIS2 art. 24: sicurezza della catena di approvvigionamento tra le misure obbligatorie ❑ Criteri di selezione e controllo fornitori IT calibrati sulla criticità del servizio e dei dati trattati

Fonte: CNDCEC – Fondazione Nazionale dei Commercialisti, *«Cybersecurity e Modello 231», maggio 2026*

Pirola Pennuto Zei

MODELLO 231 & AI

QUADRO NORMATIVO DI RIFERIMENTO

AI Act (Reg. UE 2024/1689) – risk-based approach; artt. 6 e seguenti: obblighi per sistemi ad alto rischio in continuità con i presidi del Modello 231.

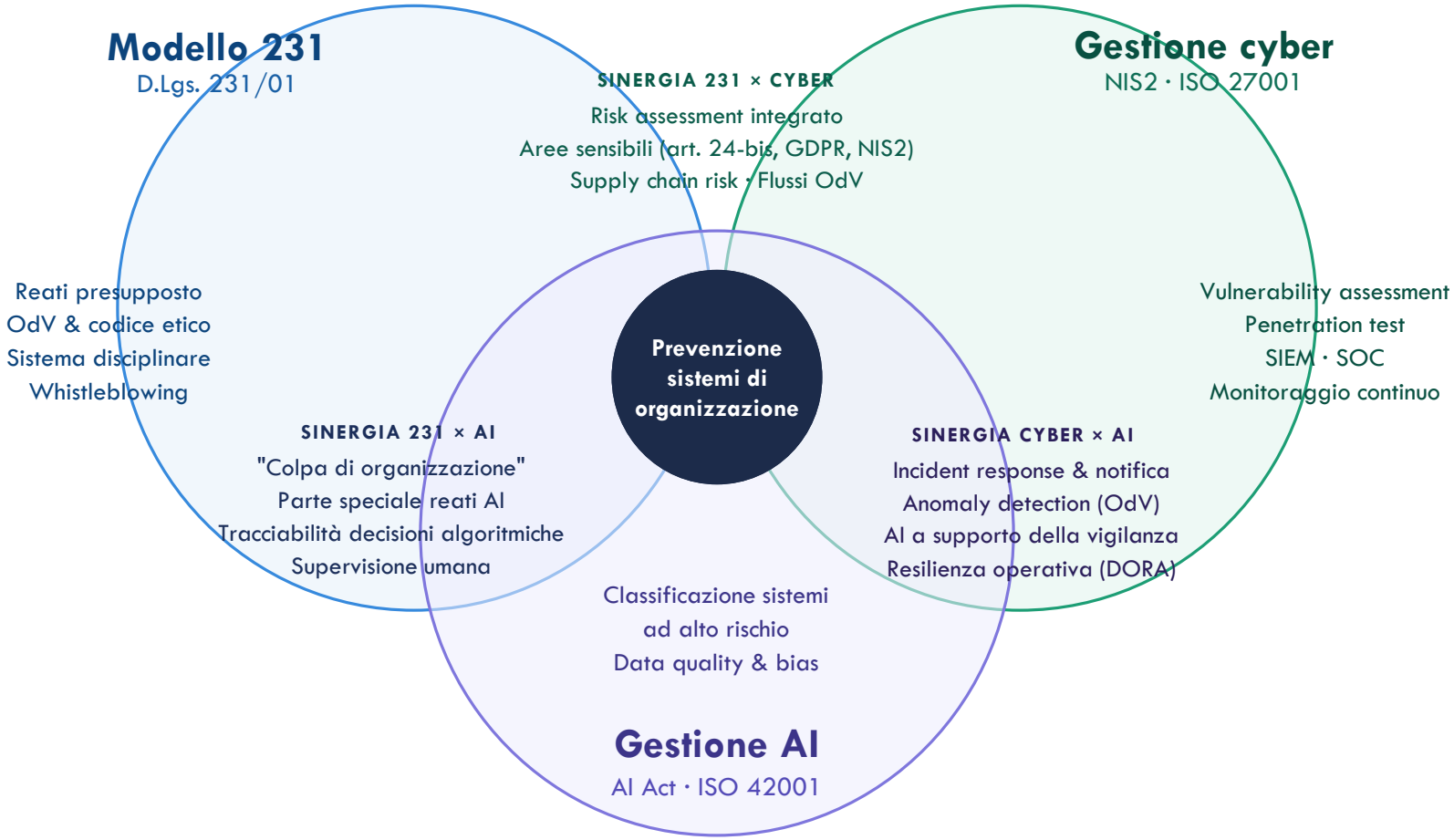
L.132/2025 (Legge italiana AI) – Trasparenza, supervisione umana, tracciabilità e cybersicurezza: rafforzano l'esigenza di integrare i presidi AI nel Modello 231.

TRE PROFILI DI RISCHIO 231		
01	**02**	**03**
REATI INFORMATICI	**REATI VS. PA, SOCIETARI E FINANZIARI**	**DATI PERSONALI & BLACK BOX**
Sistemi AI con capacità di automazione possono facilitare accesso abusivo (art. 615-ter c.p.), intercettazione illecita (art. 617-quater c.p.) o danneggiamento di dati (artt. 635-bis ss. c.p.). L'assenza di controlli sull'uso degli strumenti AI integra un deficit organizzativo rilevante ex 231.	Algoritmi decisionali nei processi di gara, selezione fornitori o reporting possono alterare trasparenza e tracciabilità. Fenomeni di bias algoritmico possono configurare false comunicazioni sociali o indebita influenza su PA.	Sistemi AI su grandi volumi di dati rischiano trattamenti non conformi al GDPR (liceità, minimizzazione, finalità). L'opacità dei modelli (black box) compromette la ricostruibilità delle decisioni e la prova dell'efficace attuazione del Modello 231.

Fonte: CNDCEC – Fondazione Nazionale dei Commercialisti, *«Cybersecurity e Modello 231», maggio 2026*

Pirola Pennuto Zei

LE SINERGIE: MODELLO 231, CYBERSECURITY & AI



Fonte: CNDCEC – Fondazione Nazionale dei Commercialisti, *«Cybersecurity e Modello 231», maggio 2026*

GRAZIE PER L'ATTENZIONE

Mattia Salerno
mattia.salerno@studiopirola.com