

Il CISO sotto processo: responsabilità personale, D.Lgs. 231 e la nuova esposizione legale



NIS2 e DORA hanno spostato la responsabilità dagli uffici IT ai vertici aziendali. Analisi giuridica delle implicazioni per CISO e board: quando scatta la responsabilità personale, cosa prevede il 231 e come tutelarsi contrattualmente.

Il cambio di paradigma: dalla responsabilità tecnica a quella personale

Per anni il Chief Information Security Officer ha operato in una zona grigia del diritto: figura tecnicamente essenziale, giuridicamente indefinita. Nessuna norma primaria ne disciplinava i poteri, nessuna sanzione ne colpiva esplicitamente le omissioni. La sicurezza informatica era percepita come un dominio tecnico, non come una funzione di governance con riflessi penali e civili.

Quel paradigma è finito.

L'entrata in vigore della Direttiva NIS2, recepita in Italia con il D.Lgs. 4 settembre 2024, n. 138 (pubblicato in Gazzetta Ufficiale n. 230 del 1° ottobre 2024 e in vigore dal 16 ottobre 2024), e del Regolamento DORA (UE) 2022/2554, applicabile dal 17 gennaio 2025, ha operato una trasformazione strutturale: la responsabilità per la sicurezza informatica non è più una questione che si risolve tra il reparto IT e il fornitore esterno. È una responsabilità degli organi di

vertice, nominativamente identificata, sanzionabile in via diretta.

Il CISO si trova oggi al centro di un sistema di obblighi che intersecano il diritto penale dell'impresa, la responsabilità amministrativa degli enti ex D.Lgs. 231/2001, il diritto civile contrattuale e le sanzioni amministrative proprie delle normative di settore. Comprendere questa architettura è diventato un prerequisito professionale imprescindibile.

Per un quadro aggiornato sul ruolo del CISO nel panorama normativo attuale, si vedano *Il CISO e la conformità normativa: gestire le leggi sulla cybersecurity e Cybersecurity 2026: dalla difesa del perimetro alla resilienza come disciplina* su ICT Security Magazine.

NIS2: gli obblighi del management e le sanzioni personali

Il D.Lgs. 138/2024, attuando la Direttiva (UE) 2022/2555, introduce un impianto di responsabilità che colpisce specificamente gli organi di amministrazione e direzione dei soggetti essenziali e importanti. Secondo le stime dell'Agenzia per la Cybersicurezza Nazionale (ACN), circa 50.000 organizzazioni italiane rientrano nel perimetro di applicazione.

L'art. 23 del D.Lgs. 138/2024, che recepisce l'art. 20 della Direttiva NIS2, costituisce la disposizione cardine in materia di governance della cybersecurity. Il comma 1 stabilisce che gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e importanti approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica, ne sorvegliano l'attuazione e seguono una formazione in materia di sicurezza informatica.

Il **comma 2** dello stesso articolo prevede esplicitamente che le

persone fisiche che svolgono funzioni dirigenziali (a livello di amministratore delegato, rappresentante legale o componente degli organi direttivi) possano essere ritenute personalmente responsabili dell'inadempimento in caso di violazione del decreto. Per un'analisi approfondita si vedano *NIS2 e oltre: la cybersicurezza diventa governance aziendale* e *NIS2: ruoli, responsabilità e autorità nella cybersecurity* su ICT Security Magazine.

Tre profili meritano attenzione specifica.

1. **La responsabilità per omessa sorveglianza.** Non è necessario che il membro del board abbia personalmente disposto la misura di sicurezza carente: è sufficiente che non abbia adeguatamente sorvegliato la sua implementazione. Il dovere di supervisione diventa, dunque, fonte autonoma di responsabilità.
2. **La sanzione accessoria dell'incapacità dirigenziale.** Gli artt. 23 e 39 del D.Lgs. 138/2024 prevedono che, nei confronti degli organi di amministrazione e degli organi direttivi responsabili delle violazioni, l'ACN possa applicare la sanzione amministrativa accessoria dell'**incapacità a svolgere funzioni dirigenziali all'interno del medesimo soggetto**. Si tratta di un istituto di rilevante impatto sul piano professionale, che colpisce direttamente la persona fisica con una misura restrittiva della capacità manageriale.
3. **Le sanzioni pecuniarie agli enti.** Ai sensi dell'art. 38 del D.Lgs. 138/2024, per la violazione degli obblighi in materia di gestione del rischio e notifica degli incidenti (artt. 23, 24 e 25): fino a **10 milioni di euro o il 2% del fatturato mondiale** annuo per i soggetti essenziali (escluse le PA); fino a **7 milioni di euro o l'1,4% del fatturato mondiale** per i soggetti importanti (escluse le PA). Il volume sanzionatorio crea una pressione sistemica che risale inevitabilmente lungo la catena del comando.

Si ricorda che gli obblighi in materia di organi di amministrazione (art. 23) e misure di sicurezza (art. 24) decorrono 18 mesi dalla comunicazione da parte di ACN ai soggetti qualificati come essenziali o importanti. Per le scadenze operative si consulti *Adempimenti NIS2: cosa bisogna fare entro ottobre 2026* su ICT Security Magazine.

Il CISO, in questo contesto, è la figura tecnica di riferimento su cui il board fa affidamento per assolvere i propri obblighi di sorveglianza. Se le informazioni che il CISO fornisce al board sono incomplete, erranee o ritardate, il corto circuito di responsabilità diventa immediato: sia verso l'ente, che non può affermare di aver vigilato adeguatamente; sia verso lo stesso CISO, che ha omesso di abilitare la governance a fare il proprio lavoro.

DORA: la responsabilità operativa nel settore finanziario

Il Regolamento DORA (UE) 2022/2554 disegna un regime ancora più puntuale per le entità finanziarie: banche, assicurazioni, gestori di fondi, infrastrutture di mercato, fornitori di crypto-attività. Applicabile dal 17 gennaio 2025, come chiarito dalla Banca d'Italia nella sua comunicazione del 30 dicembre 2024, il framework di ICT risk management previsto dagli artt. 5-16 DORA attribuisce all'organo di gestione la responsabilità diretta e non delegabile della strategia di resilienza operativa digitale.

L'**art. 5, par. 2, DORA** stabilisce che l'organo di gestione dell'entità finanziaria definisce e approva l'attuazione di tutte le disposizioni concernenti il quadro per la gestione dei rischi informatici, vigila su tale attuazione e ne è responsabile. Tale responsabilità include, tra l'altro, l'approvazione della strategia di rischio ICT, le politiche di continuità operativa e i piani di risposta agli incidenti. La norma introduce inoltre un obbligo di formazione continua: i

membri del board devono possedere e mantenere attivamente aggiornate le conoscenze e le competenze necessarie per comprendere e valutare i rischi informatici. Per un'analisi dell'implementazione pratica si veda *DORA compliance operativa* su ICT Security Magazine.

L'implicazione pratica è rilevante: in un procedimento sanzionatorio condotto da Banca d'Italia o Consob, le autorità potrebbero verificare non solo se la policy esisteva, ma se il CISO l'aveva effettivamente sottoposta all'organo di gestione, se questi l'aveva approvata con adeguata comprensione tecnica e se era stata effettivamente implementata. La catena di documentazione diventa essa stessa un elemento di prova.

Il D.Lgs. 231/2001: quando la cybersecurity entra nel perimetro penale dell'ente

Il Decreto Legislativo 8 giugno 2001, n. 231, sulla responsabilità amministrativa degli enti, è lo strumento attraverso cui i reati informatici commessi nell'interesse o a vantaggio dell'azienda possono generare una responsabilità diretta dell'ente stesso. Il catalogo dei reati presupposto rilevanti per la sicurezza informatica include oggi i **reati informatici e il trattamento illecito di dati** (art. 24-bis D.Lgs. 231/2001), tra cui l'accesso abusivo a sistemi informatici (art. 615-ter c.p.), il danneggiamento di sistemi informatici (artt. 635-bis e 635-ter c.p.) e l'intercettazione fraudolenta di comunicazioni (art. 617-quater c.p.).

Va segnalato che la L. 90/2024 ha ulteriormente rafforzato l'impianto sanzionatorio, raddoppiando le quote per i delitti informatici di cui all'art. 24-bis, co. 1, D.Lgs. 231/2001 e introducendo il nuovo reato di estorsione informatica (art. 629, co. 3 c.p.), con relative ricadute sul catalogo 231. Per l'intersezione tra NIS2 e modelli 231 si veda *I nuovi*

adempimenti della normativa NIS 2: scadenze e sanzioni su ICT Security Magazine.

Il modello organizzativo 231 come strumento di tutela

La legge prevede che l'ente sia esonerato da responsabilità se ha adottato ed efficacemente attuato un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire i reati della specie verificatasi. In materia informatica, ciò significa che il Modello 231 deve contenere una sezione specifica dedicata ai rischi cyber: politiche di accesso, gestione degli incidenti, hardening dei sistemi, gestione dei fornitori ICT, procedure di patch management. Le misure di sicurezza previste dall'art. 24 del D.Lgs. 138/2024 possono costituire linee guida di riferimento anche per la redazione del componente cyber del Modello 231.

Qui il CISO entra in gioco in modo duplice. Da un lato, è tipicamente il soggetto che alimenta tecnicamente la costruzione del Modello 231 nella componente cyber. Dall'altro, in un procedimento giudiziario, il pubblico ministero potrebbe contestare che il Modello era inadeguato o che non veniva effettivamente attuato, e il CISO è la persona fisica che sarà chiamata a rispondere di quelle scelte.

Il rischio del concorso nel reato

Se un dipendente commette un reato informatico (ad esempio accede abusivamente ai sistemi di un concorrente, o partecipa a un attacco su istruzione aziendale), il CISO che era a conoscenza della condotta o che avrebbe dovuto rilevarne i segnali tramite i sistemi di monitoraggio potrebbe essere indagato a titolo di concorso per omessa impedimento dell'evento, ai sensi dell'art. 40, co. 2, c.p., qualora abbia una posizione di garanzia.

La posizione di garanzia: quando il CISO risponde penalmente in proprio

La posizione di garanzia rappresenta il meccanismo giuridico più insidioso per il CISO. Nell'ordinamento italiano, chi si trova in posizione di garanzia ha l'obbligo giuridico di impedire eventi dannosi. Se l'evento si verifica e il garante poteva impedirlo, risponde dell'evento come se lo avesse causato (art. 40, co. 2, c.p.). Questo meccanismo, originariamente sviluppato per i reati colposi in materia di sicurezza sul lavoro, è stato progressivamente richiamato dalla giurisprudenza anche in contesti di sicurezza informatica.

Perché il CISO abbia una posizione di garanzia occorre che: disponga di poteri effettivi di intervento sui sistemi (non meramente consultivi); abbia conoscenza dei rischi specifici che si sono materializzati; disponesse degli strumenti tecnici per rilevare e prevenire l'evento. La combinazione di questi tre elementi, ampiamente ricorrente nella prassi, crea un profilo di rischio penale concreto.

Un esempio emblematico: una violazione di dati causata da una vulnerabilità nota, già segnalata dal team di sicurezza ma non corretta per mancanza di budget approvato dal board. In questo scenario, il CISO potrebbe trovarsi in una posizione difensiva difficile. Ha segnalato il rischio, ma ha documentato formalmente l'escalation? Ha messo a verbale il rifiuto del board?

Come tutelarsi: le leve contrattuali e organizzative

La consapevolezza del rischio deve tradursi in precauzioni concrete. Per una panoramica della convergenza normativa e delle sue implicazioni si veda *NIS2*, *DORA* e *CER*: *navigare la*

convergenza normativa europea sulla cybersecurity su ICT Security Magazine.

Il contratto come scudo

Il contratto di lavoro o di incarico del CISO deve contenere clausole esplicite su cinque punti fondamentali.

Il **perimetro di responsabilità**: una definizione precisa delle aree di competenza del CISO e di quelle che rimangono in capo ad altri soggetti (IT operations, HR per la sicurezza degli endpoint, procurement per i fornitori ICT).

I **poteri di spesa autonomi**: senza un budget sotto il controllo diretto del CISO, qualsiasi responsabilità per misure non implementate per carenza di risorse è trasferibile al board. Il contratto deve rispecchiare questa architettura di potere.

I **meccanismi di escalation documentata**: la previsione contrattuale del diritto-dovere del CISO di mettere a verbale i rischi segnalati e non gestiti dal vertice.

L'**indennizzo e la manleva**: una clausola con cui l'ente si impegna a tenere indenne il CISO dalle conseguenze di decisioni assunte dal board su materie di competenza del board stesso, purché il CISO abbia correttamente e documentalmente informato.

La **copertura assicurativa D&O**: la polizza Directors & Officers deve essere estesa esplicitamente al CISO, anche quando non sia formalmente membro del consiglio di amministrazione.

Il verbale di escalation come documento probatorio

Ogni qual volta il CISO segnala un rischio che non viene gestito per decisione del management, quella segnalazione deve essere formalizzata per iscritto: una comunicazione formale al CEO, un'annotazione nel registro dei rischi, un verbale del

comitato di sicurezza. Questo documento ha una funzione probatoria diretta: dimostra che il CISO ha adempiuto al proprio obbligo di informazione e che la decisione di non agire è stata presa da altri soggetti.

Il modello organizzativo interno

Il CISO dovrebbe promuovere la redazione tecnica della sezione cyber del Modello 231, facendosi formalmente intestare il contributo. Questo crea una documentazione del processo di analisi del rischio e delle misure adottate che può essere prodotta in giudizio. Un Modello 231 cyber aggiornato, approvato dal board, dimostra che l'organizzazione aveva consapevolezza dei rischi e li aveva presidiati nella misura possibile. L'ACN ha pubblicato linee guida che possono costituire un riferimento tecnico utile in sede di costruzione del Modello.

Il nodo irrisolto: il CISO senza potere decisionale

L'architettura normativa di NIS2 e DORA presuppone che chi ha responsabilità abbia anche poteri. Come evidenziato nel dibattito emerso al 23° Forum ICT Security, nella realtà organizzativa italiana il CISO è spesso una figura con responsabilità tecniche ma senza potere di spesa autonomo, senza accesso diretto al consiglio di amministrazione, inserita in strutture di riporto che attraversano tre o quattro livelli gerarchici prima di arrivare al vertice.

Questa discrasia tra responsabilità e potere è il principale fattore di rischio personale per il CISO italiano. NIS2 e DORA spingono verso un modello in cui il CISO riferisce direttamente al board o a un comitato di audit. Le prassi aziendali consolidate collocano spesso il CISO sotto il CIO o, in casi ancora più problematici, sotto il CFO.

Finché questa tensione non verrà risolta con una revisione organizzativa sostanziale, il CISO si troverà nella condizione paradossale di essere la prima figura a cui si guarda in caso di incidente, pur essendo stata l'ultima a cui è stato concesso il potere di prevenirlo. Come sottolineato nell'analisi su *Implementazione NIS2, un anno dopo* su ICT Security Magazine, il cambiamento più notevole di NIS2 è precisamente lo shift di liability da corporate a personal, un deterrente significativo che impone una revisione profonda delle strutture di governance.

Conclusioni

Il CISO del 2026 non è più soltanto un professionista della sicurezza informatica: è un soggetto giuridicamente esposto, con obblighi normativi diretti, una potenziale posizione di garanzia penale e una responsabilità che si proietta tanto verso il basso (verso i sistemi e i team che supervisiona) quanto verso l'alto (verso il board che deve mettere in condizione di governare il rischio cyber).

NIS2, DORA e il D.Lgs. 231/2001 hanno costruito, senza coordinamento esplicito, un sistema in cui la cybersecurity mal gestita può avere conseguenze penali, amministrative e civili per le persone fisiche e non solo per gli enti.

La risposta non può essere solo tecnica. Richiede una ridefinizione dei contratti, una revisione degli organigrammi, una cultura della documentazione e, soprattutto, una conversazione onesta all'interno di ogni organizzazione su chi ha davvero il potere di decidere in materia di sicurezza e chi, di conseguenza, deve assumersene la responsabilità.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/ciso-d-lgs-231/>