Sispi
Persone, Idee, Innovazione

Il MOGC 231
aziendale in 10 punti

Breve Guida del MOGC Sispi

Estratto ragionato della Parte Generale del Modello di Organizzazione, Gestione e Controllo vigente in azienda, formulato ai sensi del D.Lgs. 231/2001

Organizzazione · chi fa che cosa
Controllo · regole e verifiche
Responsabilità · il contributo di ciascuno

Riferimento: *MOGC – Parte Generale, Revisione n. 05 approvata dal Consiglio di Amministrazione il 30.04.2026.*
Questa guida ha finalità divulgative e ***non sostituisce*** *il Modello né i suoi allegati, che restano gli unici testi di riferimento. Il Modello integrale è consultabile nell'area «MOGC D.lgs. 231/01» della intranet aziendale Intr@com.*

Indice

N.	Argomento	Rif. Parte Generale	Pag.
P	Come usare questa guida	—	3
1	SISPI: chi siamo e come siamo organizzati	§ 1	3
	› Le tappe principali		3
	› La governance		4
	› L'organizzazione per Centri di Competenza		4
2	Il quadro normativo	§§ 2.1–2.3	5
	› Il TUSP in tre punti		5
	› Il D.Lgs. 231/2001: la responsabilità dell'ente		5
	› Le sanzioni per la Società		6
	› Novità normative 2024–2026 recepite		6
	› Le linee guida di riferimento		6
3	Pubblica Amministrazione e Cybersicurezza	§§ 2.4–2.5	7
	› Chi è «pubblico» per il diritto penale		7
	› Cybersicurezza, NIS2 e ISO/IEC 27001		7
4	Come è costruito il Modello	§ 3 e § 9	8
	› L'architettura		8
	› I contenuti obbligatori (art. 6 D.Lgs. 231/2001)		8
	› Le cinque fasi della metodologia		8
	› L'aggiornamento del Modello		9
5	L'Organismo di Vigilanza	§ 4	9
	› Requisiti		9
	› Poteri		10
	› A chi riferisce		10
6	Flussi informativi verso l'OdV	§ 5	10
7	Formazione e divulgazione	§ 6	11
8	Sistema disciplinare	§ 7	11
	› Principi		12
	› Come si misura la sanzione (art. 2106 c.c.)		12
9	Il sistema integrato 231 – Anticorruzione e Trasparenza	§ 8.1	12
10	Whistleblowing: come segnalare	§ 8.2	13
	› I tempi della gestione		13
	› Le tutele		13
A	I reati-presupposto in sintesi	App. A	14
B	Cosa devo fare se… / Contatti utili	—	15

Premessa Come usare questa guida

Il Presente documento contiene una sintesi della Parte Generale del Modello di Organizzazione, Gestione e Controllo (MOGC) che Sispi ha adottato ai sensi e per gli effetti del D.Lgs 231/01 ed ogni paragrafo in premessa evidenzia il capitolo del MOGC di riferimento.

Il documento si propone di assistere coloro che sono tenuti al rispetto del Modello evidenziando la ratio della norma, l'architettura adottata e le principali previsioni.

L'intento è di mettere a disposizione un documento di facile ed immediata consultazione in grado di rispondere alle domande principali che possono sorgere per l'applicazione della norma e del Modello adottato anche quale esimente

Nel testo che segue alcune parole chiave sono **evidenziate per segnalare il rimando contenuto nella colonna laterale**, dove trovi la spiegazione o il riferimento normativo.

Così funziona un richiamo
Il contenuto della colonna laterale approfondisce il testo evidenziato

1 SISPI: chi siamo e come siamo organizzati

Storia, natura giuridica, governance e organizzazione (Cap. 1 della Parte Generale).

SISPI – Sistema Palermo Innovazione S.p.A. è una società a **totale capitale pubblico**[1] che opera in regime di **in house providing**[2]: fornisce servizi informatici strumentali al Comune di Palermo, socio unico, che esercita sulla Società il **controllo analogo**[3].

È il partner tecnologico del Comune per la progettazione, lo sviluppo e la conduzione del Sistema Informatico e Telematico Comunale (**SITEC**) e, dal 2020, per le soluzioni di transizione digitale della città.

1 Socio unico
Dal 2009 il capitale è interamente del Comune di Palermo (Delib. C.C. n. 26/2009). Dal 2014 SISPI è nell'elenco ISTAT degli enti inclusi nel conto economico consolidato della PA.

2 In house
Affidamento diretto, senza gara, da parte dell'ente che controlla la Società (art. 16 TUSP; art. 7, c. 2, D.Lgs. 36/2023). → vedi § 2

3 Controllo analogo
Controllo simile a quello che il Comune esercita sui propri uffici: societario, economico-finanziario, ispettivo e informativo (Regolamento Unico dei controlli, Delib. C.C. n. 4/2017, Capo VI).

Le tappe principali

1988	1990	2009	2017	2020	2024
Costituzione Sistema Palermo Informatica (Comune + Finsiel)	**Operatività** Partner tecnologico del Comune	**Socio unico** Capitale 100% Comune di Palermo	**ISO 9001:2015** Avvio del Sistema di Gestione Integrato	**Innovazione** Nuova denominazione	**Convenzione** SITEC 2024–2033 (Delib. C.C. 17/2024)

La governance

Assemblea dei Soci	Nomina gli organi su designazione sindacale (art. 2449 c.c.)
Organo amministrativo	Amministratore Unico o CdA: poteri di gestione ordinaria e straordinaria (art. 25 Statuto)
Direttore Generale	Poteri assegnati dall'organo amministrativo
Collegio Sindacale	Controllo di legalità e sull'assetto organizzativo
Revisore legale	Nominato dall'Assemblea su proposta motivata del Collegio (art. 13 D.Lgs. 39/2010)
Organismo di Vigilanza	Vigila sul Modello 231 (art. 34 Statuto) → § 5

Alla Società si applicano il Codice civile e il **TUSP** [4]. Il **sistema di deleghe e procure** [5] attribuisce poteri coerenti con le responsabilità.

[4] TUSP
D.Lgs. 175/2016, Testo unico in materia di società a partecipazione pubblica.

[5] Deleghe
Il CdA può delegare la gestione a un solo amministratore, salvo le deleghe al Presidente autorizzate dall'Assemblea. Ogni modifica va comunicata all'OdV (→ § 6).

L'organizzazione per Centri di Competenza

Dal 2025 (OdS n. 1/2025) la struttura è articolata in sette **Centri di Competenza (CdC)**: non sono livelli gerarchici, ma raggruppano per omogeneità funzioni e servizi collegati alla Direzione generale.

Centro di Competenza	Principali funzioni
Servizi alla Direzione	Segreteria di Presidenza e Protocollo; Affari Legali e Contrattuali; Affari Societari; Relazioni esterne e Comunicazione
Pianificazione, Amministrazione e Controllo	Risorse Umane, Formazione e SSL; Amministrazione, Controllo di Gestione e Magazzino; Acquisti; Staff DG
Tecnologie	Sistemi e Sicurezza ICT; Sviluppo Soluzioni
Customer Care	Processi interni, Certificazioni, Sede; CRM e Contact Center; Sistemi periferici e Logistica
Smart City	Servizi di livello urbano
e-Government	Gestione Entrate; Servizi alle Persone; Urbanistica e Data Analisi; Dematerializzazione, Polizia Municipale e Cultura
Macchina Comunale	Personale, CoGe e Bilancio; LL.PP. e Uffici tecnici

2 Il quadro normativo

Le regole per le società pubbliche (TUSP) e la responsabilità degli enti da reato (D.Lgs. 231/2001).

Il TUSP in tre punti

Art. 4	Art. 16	Art. 19
Perché esiste SISPI	**Regole dell'in house**	**Personale**
Autoproduzione di servizi strumentali all'ente socio (lett. d)	No capitali privati; ≥ 80% del fatturato verso il socio; acquisti con il Codice dei contratti	Rapporto di lavoro privatistico (CCNL Metalmeccanici); reclutamento con principi pubblicistici

Il mancato rispetto del limite dell'80% è una **grave irregolarità**, sanabile entro tre mesi. Il reclutamento segue il Regolamento aziendale e l'Atto di indirizzo del Sindaco: dando priorità alla mobilità tra società partecipate e progressioni di carriera ed assunzioni solo per i profili previsti nel Piano di fabbisogno del personale.

Il D.Lgs. 231/2001: la responsabilità dell'ente

Il Decreto prevede una responsabilità **amministrativa** della Società, accertata nel processo penale e autonoma da quella della persona fisica. Scatta quando un **reato-presupposto** (1) è commesso **nell'interesse o a vantaggio** (2) della Società da:

- **soggetti apicali** – amministratori, direttori, chi gestisce o controlla anche di fatto;
- **soggetti sottoposti** – dipendenti e collaboratori diretti o vigilati dagli apicali.

La Società non risponde se dimostra di aver adottato ed efficacemente attuato un **Modello idoneo** (3).

(1) Reato-presupposto
Solo i reati espressamente richiamati dal Decreto o da altre leggi (es. L. 146/2006, reati transnazionali). → Appendice A

(2) Interesse o vantaggio
Se l'autore ha agito nell'esclusivo interesse proprio o di terzi, la Società non risponde.

(3) Idoneità del Modello quale esimente
Conta l'attuazione concreta, non la sola adozione formale: conoscenza del Modello, adozione dei protocolli, monitoraggio continuo e aggiornamento tempestivo.

	Reato commesso da un APICALE	Reato commesso da un SOTTOPOSTO
Onere della prova	Colpa di organizzazione presunta: è la Società a dover provare la propria estraneità	Spetta all'accusa provare la violazione degli obblighi di direzione e vigilanza
Come si difende la Società	Modello idoneo ed efficace + elusione fraudolenta del Modello da parte dell'autore + vigilanza adeguata dell'OdV	Modello idoneo ed efficacemente attuato prima del fatto

Le sanzioni per la Società

Sanzione	In sintesi
Pecuniaria	Sistema «per quote»: il giudice fissa il numero di quote (in base a gravità, responsabilità, condotte riparatorie) e il valore della singola quota (da € 258,23 a € 1.549,37). Riducibile fino a 2/3 (es. danno lieve o risarcito, Modello adottato dopo il fatto).

Sanzione	In sintesi
Interdittive	Interdizione dall'attività; sospensione/revoca di autorizzazioni; **divieto di contrattare con la PA**; esclusione da finanziamenti e contributi; divieto di pubblicizzare beni e servizi. Applicabili anche in via cautelare (art. 13 e ss.).
Confisca	Del prezzo o del profitto del reato, anche per equivalente; possibile sequestro preventivo.

Perché conta per un servizio pubblico come SISPI

Nel caso in cui l'interruzione dell'attività provocasse danni alla collettività, il giudice, al posto della sanzione interdittiva, potrebbe procedere con la nomina di un **commissario giudiziale**. Le misure interdittive non si applicano se, prima del processo, la Società ha provveduto a risarcire il danno, ha adottato un Modello idoneo e messo a disposizione il profitto.

Novità normative 2024–2026 recepite

Provvedimento	Effetto sul catalogo 231
L. 90/2024	Rafforza i **delitti informatici** (art. 24-bis): particolarmente rilevante per una società ICT
D.L. 92/2024 conv.	Modifica l'art. 25 (reati contro la PA) dopo l'abrogazione dell'abuso d'ufficio
D.Lgs. 141/2024	Riforma dei reati di contrabbando (art. 25-sexiesdecies)
D.Lgs. 138/2024 (NIS2)	Non crea nuovi reati, ma rafforza governance e gestione del rischio cyber → § 3
Novità 2025	Nuovo art. 25-undevicies (delitti contro gli animali)
D.Lgs. 81/2026	Tutela penale dell'ambiente: rimodula l'art. 25-undecies
L. 75/2026	Tutela dei prodotti alimentari italiani: modifica l'art. 25-bis.1

Fonte: Parte Generale, § 2.2. Ogni novità è sottoposta a valutazione d'impatto su processi, protocolli, flussi, sistema disciplinare e formazione.

Le linee guida di riferimento

Il Modello è stato redatto tenendo conto delle **Linee Guida Confindustria** (aggiornamento giugno 2021) e dei documenti del **CNDCEC** (tra cui i Principi consolidati del 2019 e le Linee Guida sulle funzioni dell'OdV del 2025).

Le componenti essenziali del sistema di controllo sono: Codice Etico, organizzazione, procedure, deleghe e procure, controllo delle risorse finanziarie, sistema disciplinare, formazione e un OdV autonomo; i principi trasversali sono **tracciabilità, segregazione delle funzioni, coerenza tra poteri e responsabilità**.

3 Pubblica Amministrazione e Cybersicurezza

Definizioni utili per i reati contro la PA e presidi sulla sicurezza informatica (§§ 2.4–2.5).

Chi è «pubblico» per il diritto penale

Molti reati contro la PA sono **reati propri** [1]. Per riconoscere i rischi nei rapporti quotidiani occorre distinguere:

Pubblica Amministrazione	Soggetti, pubblici o privati, italiani o europei, che svolgono una funzione pubblica o un pubblico servizio
Pubblico ufficiale (art. 357 c.p.)	Esercita una funzione legislativa, giudiziaria o amministrativa con **poteri autoritativi, deliberativi o certificativi** [2]
Incaricato di pubblico servizio (art. 358 c.p.)	Svolge un'attività disciplinata come la funzione pubblica ma senza i relativi poteri (escluse mansioni d'ordine o meramente materiali)

[1] Reati propri
Reati che possono essere commessi solo da chi ha una particolare qualifica (es. pubblico ufficiale). La Società può risponderne anche in concorso.

[2] I tre poteri
Autoritativo: imporre comandi (es. accertamenti, autorizzazioni).
Deliberativo: formare la volontà della PA.
Certificativo: attestare come certa una situazione.

Cybersicurezza, NIS2 e ISO/IEC 27001

SISPI è destinataria di una specifica comunicazione dell'**ACN** [3] ai fini della disciplina **NIS2** [4]: la sicurezza di reti e sistemi ha quindi rilievo strategico e trasversale.

La Società ha adottato un sistema di gestione della sicurezza delle informazioni conforme alla **ISO/IEC 27001**, con valutazione periodica del rischio cyber. Questo processo è anche un presidio 231 contro:

- i **delitti informatici** (art. 24-bis);
- i reati societari e contro la PA commessi alterando o rendendo indisponibili dati e sistemi;
- i reati agevolati da carenze negli accessi e nelle autorizzazioni.

L'organo di gestione supervisiona il sistema di sicurezza; policy dedicate disciplinano accessi, protezione dati, vulnerabilità, continuità operativa, incident response e supply chain ICT.

[3] ACN
Agenzia per la cybersicurezza nazionale.

[4] NIS2
Dir. (UE) 2022/2555, recepita con D.Lgs. 138/2024. Gli obblighi di notifica NIS2 restano distinti dai flussi verso l'OdV.

Flussi cyber PERIODICI verso l'OdV	Flussi cyber AD EVENTO verso l'OdV
• Esiti di audit interni ed esterni • Risultanze del risk assessment cyber e vulnerabilità rilevanti • Stato di azioni correttive e piani di rimedio	• Incidenti significativi e notifiche alle autorità • Vulnerabilità che richiedono interventi urgenti • Violazioni delle policy di sicurezza • Modifiche a ruoli, deleghe e responsabilità ICT • Eventi rilevanti della supply chain ICT

4 Come è costruito il Modello

Architettura documentale e metodologia risk based (Premessa e Cap. 3).

L'architettura

Parte Generale	Parte Speciale	Allegati 1–5
Contesto, norme, OdV, flussi, formazione, sanzioni	**Attività sensibili e protocolli per funzione**	**Documenti separati collegati**

All.	Documento
1	Codice Etico e di Comportamento
2	Sistema Disciplinare
3	Regolamento istitutivo dell'OdV
4	Regolamento Whistleblowing
5	Schema dei flussi informativi verso l'OdV

I contenuti obbligatori (art. 6 D.Lgs. 231/2001)

Attività a rischio	Protocolli	Risorse finanziarie	Flussi all'OdV	Sistema disciplinare	Segnalazioni
individuare dove si possono commettere reati	regole per formare e attuare le decisioni	modalità di gestione che impediscano reati	obblighi di informazione	sanzioni per chi viola il Modello	canali interni whistleblowing e divieto di ritorsione (c. 2-bis)

Le cinque fasi della metodologia

1	2	3	4	5
Raccolta documentale	**Responsabili di processo**	**Gap Analysis**	**Protocolli**	**Approvazione e attuazione**
organigramma, deleghe, procedure, audit	interviste e questionari sul controllo interno	controlli esistenti vs controlli adeguati	regole operative e controlli verificabili	delibera, comunicazione, formazione, monitoraggio

Gli scostamenti rilevati confluiscono in un **piano di adeguamento** con azioni, responsabili e tempi. I protocolli si integrano con le procedure esistenti, con il Sistema di Gestione Integrato, con l'anticorruzione, la cybersecurity e la protezione dei dati, evitando duplicazioni. Esiti dei controlli, segnalazioni, incidenti e novità normative alimentano il ciclo successivo.

L'aggiornamento del Modello

Un processo continuo (Cap. 9).

Modifiche descrittive	Modifiche sostanziali
Variazioni formali o anagrafiche che non toccano rischi, protocolli, responsabilità, flussi o sanzioni. → Recepite **senza nuova delibera**, previa informativa all'OdV e successiva presa d'atto dell'organo di gestione.	Dovute a: novità normative, organizzative o di processo; nuove attività o tecnologie; esiti di risk assessment e audit; violazioni, segnalazioni o incidenti rilevanti. → **Delibera dell'organo di gestione**, anche su proposta dell'OdV.

> Il riesame organico va svolto **almeno ogni tre anni**, ma l'aggiornamento è dovuto tempestivamente ogni volta che cambiano norme, organizzazione, tecnologie o profilo di rischio.

5 L'Organismo di Vigilanza

Composizione, requisiti, poteri e reporting (Cap. 4).

L'OdV vigila su funzionamento, osservanza e aggiornamento del Modello. È previsto dall'**art. 34 dello Statuto** [1] ed è disciplinato dal **Regolamento istitutivo** [2].

È un organo **collegiale di tre componenti**:

[1] Statuto
Clausola introdotta dal Socio unico con l'adeguamento degli statuti al TUSP.

[2] Allegato 3
Approvato dal Socio; disciplina nomina, requisiti, cause di ineleggibilità e decadenza.

2	1	3
Componenti esterni	**Componente interno**	**Anni di mandato**
uno con funzioni di Presidente, scelti con avviso pubblico tra esperti 231 e di controllo	responsabile di una funzione non coinvolta nei processi a rischio, nominato dall'organo di gestione	con prorogatio fino alla nuova nomina; revoca solo per giusta causa

Requisiti

Autonomia e indipendenza	Assenza di conflitti di interessi, poteri autonomi di iniziativa e controllo, nessun compito operativo, riporto diretto all'organo di gestione
Professionalità	Competenze specialistiche, anche con il supporto di consulenti esterni; astensione sulle materie di diretta competenza aziendale
Continuità d'azione	Mandato indipendente da quello degli altri organi; controlli periodici
Onorabilità	Dichiarazione di assenza di cause di ineleggibilità, decadenza e incompatibilità all'atto della nomina
Risorse	Budget annuo assegnato dall'organo di gestione

Poteri

- Verifiche periodiche e **controlli a sorpresa** su tutte le funzioni.
- **Libero accesso** a uffici, informazioni, documenti e dati, senza consenso preventivo.
- Collaborazione di tutte le funzioni aziendali e di consulenti esterni.

A chi riferisce

Quando	Destinatari e strumenti
Periodicamente	**Relazione semestrale** all'organo di gestione e al Collegio Sindacale
Fatti gravi / situazioni straordinarie	Nota tempestiva a DG, organo di gestione o Collegio Sindacale
Violazioni da parte di amministratori	Informativa al Collegio Sindacale

Gli incontri sono verbalizzati; organo di gestione e Collegio possono convocare l'OdV in qualsiasi momento.

6 Flussi informativi verso l'OdV

Cosa comunicare, come e a chi (Cap. 5).

Le strutture aziendali trasmettono all'OdV flussi **periodici** e **ad evento** secondo lo **Schema dei flussi**[1], che indica responsabile, contenuto, documenti e tempi.

Oltre ai flussi cyber (→ § 3), vanno comunicati, ad esempio:

- informazioni su contratti, attività produttive e impiego dei fattori produttivi;
- adempimenti di settore (sicurezza, privacy, qualità, ambiente);
- **atti di autorità**[2] da cui risultino indagini per reati 231 che possano coinvolgere SISPI;
- richieste di assistenza legale di dipendenti indagati per reati 231;
- rapporti di controllo delle funzioni aziendali con profili critici;
- il sistema di **deleghe e procure** e ogni sua modifica;
- ogni altra informazione utile alla vigilanza.

Tutta la documentazione ricevuta è **archiviata dall'OdV**[3].

[1] Allegato 5
Ogni funzione, organo, dipendente, consulente e collaboratore deve consultarlo e individuare i flussi di propria competenza.

[2] Autorità
Polizia giudiziaria o altra autorità, anche per indagini contro ignoti, salvo divieto dell'autorità giudiziaria.

[3] Conservazione
Informazioni, segnalazioni e relazioni sono archiviate dall'OdV per almeno 10 anni.

Indirizzo dell'OdV

odv@sispi.it – per i flussi informativi e le comunicazioni ordinarie.

Le segnalazioni whistleblowing **non** vanno inviate qui, ma tramite i canali dedicati (→ § 10), per godere delle tutele di legge.

7 Formazione e divulgazione

Come il Modello viene fatto conoscere a dipendenti, organi e terzi (Cap. 6).

SISPI vuole che chiunque operi per suo conto sappia che una violazione del Modello comporta **sanzioni o la risoluzione del rapporto**, e che non tollera comportamenti illeciti **neppure se apparentemente vantaggiosi** per la Società.

La formazione è concordata con l'OdV e con la Funzione Risorse Umane (e, per i temi anticorruzione, con il RPC) ed è differenziata per destinatari, in aula o **a distanza**[1].

[1] Modalità
Staff meeting, aula, videoconferenza, e-learning. Al termine si compila un questionario che attesta la partecipazione.

Destinatari	Cosa ricevono / cosa sottoscrivono
Dipendenti e nuovi assunti	Copia del Codice Etico e di Comportamento; accesso al Modello su Intr@com («MOGC D.lgs. 231/01»); dichiarazione di conoscenza e osservanza
Collaboratori esterni stabili	Come sopra; se privi di accesso alla rete, documenti tramite bacheche, sito istituzionale o e-mail

Destinatari	Cosa ricevono / cosa sottoscrivono
Organi sociali e rappresentanti	Copia del MOGC all'accettazione della carica; dichiarazione di osservanza; aggiornamenti periodici
Consulenti, fornitori, partner	Clausole contrattuali di rispetto del Modello e del Codice Etico

In pratica: cosa devi fare

- Conoscere i principi del Modello e del Codice Etico e le regole operative della tua attività.
- Firmare la dichiarazione di conoscenza e osservanza.
- Partecipare alla formazione e prendere visione degli aggiornamenti inviati via e-mail.
- Contribuire all'attuazione del Modello **segnalando carenze** che riscontri.

8 Sistema disciplinare

Presupposto essenziale perché il Modello sia efficace (Cap. 7 e Allegato 2).

Il **Codice disciplinare**[1] individua infrazioni, sanzioni e procedure per le violazioni del Modello e del Codice Etico e di Comportamento, che integra anche le regole anticorruzione ispirate al **DPR 62/2013**[2].

Si applica a **dipendenti, dirigenti, amministratori, collaboratori** e a chi ha rapporti contrattuali con SISPI. Le sanzioni sono applicate **indipendentemente dall'esito** di eventuali procedimenti penali, civili o amministrativi.

[1] **Pubblicità**
Affisso in luogo accessibile, diffuso con il sistema informatico interno e pubblicato sul sito istituzionale (art. 7 L. 300/1970).

[2] **Codice di Comportamento**
Come integrato dal DPR 81/2023.

Principi

Complementarità si aggiunge al CCNL Metalmeccanici, non lo sostituisce	**Pubblicità** regole conoscibili in anticipo	**Contraddittorio** contestazione scritta, specifica e immediata	**Gradualità** sanzione proporzionata alla gravità	**Tempestività** procedimento in tempi ragionevoli e certi

Come si misura la sanzione (art. 2106 c.c.)

Elementi di valutazione	Circostanze aggravanti
• Gravità oggettiva e intenzionalità • Modalità della condotta • Gravità dell'evento • Tipo di violazione e contesto • Per i lavoratori: mansioni, posizione, precedenti, grado di colpa	• Più violazioni nella stessa condotta • Concorso di più persone • Livello di rischio a cui è esposta la Società • Recidiva • Altre circostanze particolari

Restano salvi il diritto della Società al risarcimento dei danni e i diritti di difesa e opposizione dei lavoratori.

9 Il sistema integrato 231 – Anticorruzione e Trasparenza

Due discipline distinte, coordinate in un unico documento (§ 8.1).

	Sistema 231	Anticorruzione e Trasparenza
Finalità	Prevenire i reati-presupposto commessi nell'interesse o a vantaggio della Società	Prevenire corruzione in senso ampio e **cattiva amministrazione**, anche a danno della Società; garantire trasparenza e accesso civico
Norme	D.Lgs. 231/2001	L. 190/2012; D.Lgs. 33/2013; Linee Guida ANAC (del. 1134/2017); PNA 2026–2028 (del. ANAC 19/2026)
Presidi	MOGC, protocolli, sistema disciplinare, formazione, flussi all'OdV	Misure di prevenzione, mappatura processi, conflitti di interessi, obblighi di pubblicazione, monitoraggio
Chi controlla	Organismo di Vigilanza	RPC e RT (in SISPI funzioni separate), sotto la responsabilità dell'organo di gestione

Le misure anticorruzione e trasparenza sono coordinate con il MOGC in un **documento unitario**, con sezioni e responsabilità distinguibili. Negli ambiti comuni (mappatura dei rischi, controlli, formazione, flussi, azioni correttive) OdV, RPC e RT si scambiano le informazioni pertinenti **senza sovrapposizioni**: le funzioni del RPC e del RT non sono assorbite dall'OdV.

10 Whistleblowing: come segnalare

Principi del canale di segnalazione interno (§ 8.2 e Allegato 4).

Chi, nel contesto lavorativo, viene a conoscenza di **violazioni** [1] – compresi illeciti 231 e violazioni del Modello – può segnalarle tramite il canale interno, gestito dal **RPC** [2].

Le segnalazioni possono essere:

- **scritte**, tramite la piattaforma informatica aziendale (canale prioritario);
- **orali**, tramite messaggistica vocale o, su richiesta, con **incontro diretto**.

Modalità e recapiti sono pubblicati sul sito istituzionale e nel Regolamento Whistleblowing. Per i fatti rilevanti ai fini 231 è previsto il **raccordo con l'OdV** [3].

[1] Cosa non rientra
Rivendicazioni esclusivamente personali legate al proprio rapporto di lavoro.

[2] Gestore
Art. 4, c. 5, D.Lgs. 24/2023. In caso di conflitto di interessi o impedimento opera un gestore sostitutivo.

[3] Raccordo con l'OdV
Per fatti rilevanti ai fini 231 il RPC trasmette all'OdV solo le informazioni pertinenti, nel rispetto della riservatezza.

I tempi della gestione

①	7 gg	→	3 mesi	5 anni
Segnalazione scritta o orale sul canale interno	**Avviso di ricevimento** al segnalante	**Istruttoria** imparziale, riservata, con dati minimi necessari	**Riscontro** esito o stato della gestione	**Conservazione** massimo, dall'esito finale

Una segnalazione ricevuta da un soggetto diverso dal gestore va trasmessa a quest'ultimo **entro 7 giorni**, informandone il segnalante.

Le tutele

Riservatezza	Identità del segnalante, delle persone coinvolte e contenuto protetti; trattamento dati conforme a GDPR e D.Lgs. 196/2003
Divieto di ritorsione	Vietata ogni ritorsione, anche solo tentata o minacciata; tutela estesa a facilitatori e persone collegate
Condizione	Fondati motivi, al momento della segnalazione, per ritenere vere le informazioni
Limite	Le tutele cessano se è accertata la responsabilità per diffamazione o calunnia (art. 16 D.Lgs. 24/2023)

N.B. Ostacolare una segnalazione, violare la riservatezza o compiere ritorsioni è **sanzionato** dal sistema disciplinare.

Alle condizioni dell'art. 6 D.Lgs. 24/2023 (es. canale interno inefficace, rischio di ritorsione, pericolo per il pubblico interesse) è possibile rivolgersi al **canale esterno ANAC**; restano ferme divulgazione pubblica e denuncia all'autorità giudiziaria o contabile.

A I reati-presupposto in sintesi

Macro-categorie del catalogo 231 (Appendice A della Parte Generale).

Norma	Categoria	Norma	Categoria
Artt. 24, 25	Reati contro la PA e il patrimonio	Art. 24-bis	Delitti informatici e trattamento illecito di dati
Art. 24-ter	Criminalità organizzata	Art. 25-bis	Falsità in monete, valori e segni di riconoscimento
Art. 25-bis.1	Delitti contro l'industria e il commercio	Art. 25-ter	Reati societari
Art. 25-quater	Terrorismo ed eversione	Art. 25-quater.1	Mutilazioni genitali femminili
Art. 25-quinquies	Delitti contro la personalità individuale	Art. 25-sexies	Abusi di mercato
Art. 25-septies	Omicidio e lesioni colpose (salute e sicurezza sul lavoro)	Art. 25-octies	Ricettazione, riciclaggio, autoriciclaggio
Art. 25-octies.1	Strumenti di pagamento diversi dai contanti	Art. 25-octies.2	Violazione di misure restrittive UE
Art. 25-novies	Diritto d'autore	Art. 25-decies	Induzione a dichiarazioni mendaci all'A.G.
Art. 25-undecies	Reati ambientali	Art. 25-duodecies	Impiego di cittadini di Paesi terzi irregolari
Art. 25-terdecies	Razzismo e xenofobia	Art. 25-quaterdecies	Frode sportiva e giochi vietati
Art. 25-quinquiesdecies	Reati tributari	Art. 25-sexiesdecies	Contrabbando
Art. 25-septiesdecies	Delitti contro il patrimonio culturale	Art. 25-duodevicies	Riciclaggio e devastazione di beni culturali
Art. 25-undevicies	Delitti contro gli animali	L. 9/2013, art. 12	Filiera degli oli vergini di oliva
L. 146/2006	Reati transnazionali		

In evidenza nella Parte Speciale le aree di maggiore pertinenza per SISPI (es. PA, informatici, societari, SSL, tributari). Il catalogo è soggetto a verifica periodica.

B Cosa devo fare se… / Contatti utili

Orientamento rapido per i casi più frequenti.

Se…	Cosa fare
Devo trasmettere un flusso informativo periodico o ad evento	Consulta l'Allegato 5 e invia a **odv@sispi.it**
Vengo a conoscenza di un possibile illecito o di una violazione del Modello	Usa il **canale whistleblowing** (piattaforma o canale orale) secondo il Regolamento – non la e-mail ordinaria
Ricevo un atto di polizia giudiziaria o di altra autorità su reati 231	Informa senza ritardo la tua funzione e l'OdV
Ho un dubbio su come applicare una regola del Modello o del Codice Etico	Rivolgiti al tuo responsabile o all'OdV
Si verifica un incidente informatico significativo	Segui le procedure di incident response; la funzione competente informa l'OdV
Cambiano deleghe, procure o ruoli di responsabilità	La funzione competente comunica la modifica all'OdV
Mi offrono o chiedono denaro o utilità in rapporti con la PA	Rifiuta e segnala tramite il canale whistleblowing

Riferimento	Dove trovarlo
Organismo di Vigilanza	odv@sispi.it
Canale whistleblowing	Piattaforma e recapiti pubblicati sul sito istituzionale (Regolamento Whistleblowing – All. 4)
Modello 231 e allegati	Intranet Intr@com – area «MOGC D.lgs. 231/01»
Codice disciplinare e regolamenti	Sito istituzionale, sezione regolamenti
Certificazioni	www.sispi.it/certificazioni