Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 e Codice Etico Integrato per OverApp Srl

Capitolo 1: Il Codice Etico Integrato di OverApp Srl

L'adozione del presente Codice Etico da parte di OverApp Srl non costituisce unicamente l'adempimento di un onere formale previsto dal Decreto Legislativo 8 giugno 2001, n. 231, ma rappresenta la formalizzazione di una cultura aziendale preesistente, orientata all'eccellenza e alla responsabilità sociale.[1] In un mercato tecnologico caratterizzato da una rapida evoluzione e da una crescente complessità normativa, OverApp Srl riconosce che l'integrità etica è una componente inscindibile del proprio valore industriale. Il Codice Etico funge da "Costituzione" aziendale, definendo i confini invalicabili entro i quali deve svilupparsi ogni iniziativa di business, garantendo che il perseguimento degli obiettivi economici non entri mai in conflitto con i valori fondamentali dell'ordinamento giuridico e della convivenza civile.[3]

1.1 Vision, Mission e i Pilastri dell'Etica Aziendale

La visione di OverApp Srl è quella di porsi come leader nello sviluppo di soluzioni software innovative che non solo risolvano problemi tecnici complessi, ma che siano progettate secondo principi di "Ethics by Design".[5] La missione aziendale consiste nel fornire infrastrutture digitali sicure, inclusive e trasparenti, capaci di supportare la trasformazione digitale della Pubblica Amministrazione e delle grandi imprese private. Per raggiungere tali traguardi, OverApp Srl si ispira a tre pilastri fondamentali: Legalità, Trasparenza e Integrità.[7]

Il principio di Legalità impone a tutti i destinatari del Codice — siano essi amministratori, dipendenti o partner esterni — l'osservanza rigorosa delle leggi nazionali e comunitarie, nonché delle procedure interne.[4] Nessun interesse aziendale può giustificare la violazione di una norma di legge, né la società trarrà alcun vantaggio da condotte illecite. La Trasparenza, intesa come accessibilità e veridicità delle informazioni, permea ogni processo decisionale e contabile, assicurando che ogni operazione sia documentata, autorizzata e verificabile.[7] L'Integrità si manifesta nella coerenza tra i valori dichiarati e le condotte praticate, ripudiando ogni forma di favoritismo, nepotismo o corruzione, sia essa pubblica o tra privati.[1]

1.2 La Cybersecurity come Valore Etico e Conformità ISO 27001

Nel contesto delle società tecnologiche, la sicurezza delle informazioni non è un mero requisito tecnico, ma un dovere etico verso i clienti e la collettività.[10] OverApp Srl, in linea con la certificazione ISO 27001, assume la responsabilità di garantire la Riservatezza, l'Integrità e la Disponibilità (R.I.D.) dei dati trattati.[11] La cybersecurity viene elevata a principio comportamentale: ogni collaboratore è tenuto a gestire le risorse informatiche con la massima diligenza, consapevole che una vulnerabilità tecnica può tradursi in un danno sociale o in una fattispecie di reato informatico rilevante ai sensi dell'art. 24-bis del D.Lgs. 231/01.[6]

L'impegno verso la protezione dei dati si estende alla piena conformità al Regolamento UE 2016/679 (GDPR). OverApp Srl ripudia ogni forma di sfruttamento illecito dei dati personali e si impegna a implementare misure tecniche e organizzative che eccedano i requisiti minimi di legge, promuovendo una cultura della privacy come espressione di rispetto per la libertà individuale.[5] La società riconosce che la fiducia degli utenti è l'asset più prezioso e che tale fiducia riposa sulla capacità di dimostrare una gestione dei dati inattaccabile sotto il profilo etico e legale.

Componente ISO 27001	**Declinazione Etica in OverApp Srl**	**Rilevanza 231 (Esempi)**
Gestione degli Accessi	Uso responsabile delle identità digitali	Prevenzione Accesso Abusivo (Art. 615-ter) [12]
Integrità del Software	Qualità e veridicità degli output digitali	Prevenzione Frode Informatica (Art. 640-ter) [12]
Continuità Operativa	Resilienza dei servizi critici per la PA	Prevenzione Interruzione Pubblico Servizio [7]

1.3 Parità di Genere, Inclusione e Politiche Anti-molestie (UNI/PdR 125:2022)

OverApp Srl riconosce che il talento non ha genere e che la diversità è un driver fondamentale per l'innovazione software. In conformità con la prassi UNI/PdR 125:2022, la società integra nel proprio Codice Etico l'impegno per la parità di genere a tutti i livelli dell'organizzazione.[14] L'obiettivo non è solo formale, ma sostanziale: creare un ambiente di lavoro dove uomini e donne abbiano le medesime opportunità di accesso, crescita professionale e remunerazione.[16]

Le politiche anti-molestie di OverApp Srl sono improntate alla "tolleranza zero".[18] Viene definita molestia ogni atto o comportamento, anche verbale, che risulti indesiderato e abbia lo scopo o l'effetto di violare la dignità di una persona o di creare un clima intimidatorio, ostile, degradante o umiliante.[3] La società si impegna a proteggere chiunque segnali tali comportamenti da ritorsioni o vittimizzazione, utilizzando i medesimi canali riservati previsti per il whistleblowing.[19] La tutela della genitorialità e l'equilibrio tra vita professionale e privata (Work-Life Balance) sono considerati pilastri per garantire che la carriera delle lavoratrici non subisca rallentamenti ingiustificati in corrispondenza di eventi familiari.[16]

1.4 Norme di Comportamento verso Clienti, Fornitori e Terzi

L'eccellenza di OverApp Srl si misura anche attraverso la qualità dei suoi rapporti esterni. Verso i Clienti, l'azienda garantisce correttezza informativa e rispetto dei tempi di consegna, evitando clausole vessatorie o pratiche commerciali ingannevoli.[1] Nei confronti dei Fornitori, la società adotta processi di selezione imparziali e trasparenti, basati su criteri di qualità, prezzo e conformità etica.[23] OverApp Srl richiede a tutti i fornitori critici la sottoscrizione di "Clausole 231", attraverso le quali essi si impegnano a non commettere reati nell'interesse della società e a segnalare eventuali condotte sospette all'Organismo di Vigilanza.[25]

I rapporti con terzi partner, consulenti e intermediari devono essere improntati alla massima prudenza. È fatto divieto di utilizzare consulenze fittizie o sovra-remunerate per la creazione di fondi neri o per influenzare indebitamente decisioni di controparti pubbliche o private.[24] Ogni contratto deve specificare chiaramente l'oggetto della prestazione e le modalità di rendicontazione, garantendo la piena tracciabilità di ogni compenso erogato.[26]

Capitolo 2: Modello 231 - Parte Generale e Governance

La Parte Generale del Modello 231 definisce l'impalcatura organizzativa su cui poggia l'intero sistema di controllo di OverApp Srl. Essa ha lo scopo di dimostrare, in sede giudiziale, che l'ente ha adottato ed efficacemente attuato un modello di organizzazione idoneo a prevenire reati della specie di quello verificatosi.[8]

2.1 Governance Aziendale: Sistema di Procure e Deleghe

La struttura di governance di OverApp Srl è ispirata al principio di "segregazione delle funzioni", per cui nessun individuo può gestire autonomamente e senza controllo un intero processo sensibile.[7] Il sistema di deleghe e procure costituisce lo strumento principale per la distribuzione dei poteri e la definizione delle responsabilità.[8]

Le deleghe sono strutturate secondo i seguenti requisiti di validità:

1. **Formabilità e Pubblicità**: Ogni delega deve risultare da un atto scritto avente data certa e deve essere comunicata ai livelli gerarchici interessati.[8] Le procure che comportano poteri di rappresentanza verso l'esterno devono essere depositate presso la Camera di Commercio.[29]
2. **Specificità e Limiti**: La delega deve individuare puntualmente i poteri attribuiti e i limiti di spesa. Per le operazioni che eccedono le soglie ordinarie, è previsto l'obbligo di firma congiunta tra due o più soggetti apicali.[23]
3. **Capacità di Controllo**: Il delegante non è esonerato dall'obbligo di vigilanza sull'operato del delegato. Il sistema deve prevedere flussi di reporting periodici dal basso verso l'alto.[8]

Livello Gerarchico	Potere Attribuito	Meccanismo di Controllo
Amministratore Delegato	Firma contratti strategici e procure generali	Reporting trimestrale al CdA e OdV [1]
Direttore Tecnico (CTO)	Gestione infrastruttura e rilascio software	Audit log e controlli di sicurezza ISO 27001 [6]
Responsabile HR	Gestione personale e parità di genere	Monitoraggio KPI UNI/PdR 125:2022 [15]

2.2 L'Organismo di Vigilanza (OdV)

L'Organismo di Vigilanza è l'organo incaricato di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento.[1] Per OverApp Srl, data la complessità tecnica dei processi informatici, si è optato per un OdV a composizione collegiale, garantendo la multidisciplinarietà necessaria.[32]

2.2.1 Requisiti di Efficacia

L'OdV di OverApp Srl deve possedere tre requisiti fondamentali:

- **Autonomia e Indipendenza**: L'Organismo non deve avere compiti operativi e deve riferire direttamente al Consiglio di Amministrazione.[32] I componenti esterni non devono avere rapporti di consulenza continuativa che ne minino la terzietà.[1]
- **Professionalità**: I membri devono possedere competenze specialistiche in ambito penale, di audit societario e di sicurezza informatica.[32] Tale ultimo requisito è essenziale per comprendere i rischi legati ai reati cyber.[6]
- **Continuità di Azione**: L'OdV deve operare in modo costante, programmando verifiche periodiche (audit) e garantendo un presidio informativo continuo per i dipendenti.[32]

2.2.2 Compiti, Poteri e Flussi Informativi

All'OdV sono conferiti poteri di iniziativa e controllo illimitati su ogni settore aziendale. Esso può procedere ad ispezioni senza preavviso, audizioni dei dipendenti e accesso a database aziendali.[1] È istituito un sistema di flussi informativi obbligatori: le direzioni aziendali devono segnalare all'OdV ogni anomalia, l'avvio di indagini penali, i rapporti ispettivi di enti pubblici o la pendenza di controversie civili rilevanti.[1]

2.3 Il Sistema Disciplinare e Sanzionatorio

Il Modello 231 è efficace solo se supportato da un sistema sanzionatorio idoneo a punire le violazioni delle misure di prevenzione, indipendentemente dall'esito di un eventuale procedimento penale.[35]

Per i Dipendenti (quadri, impiegati, operai), le sanzioni sono mutuate dal CCNL Metalmeccanico e dal CCNL Commercio applicabili.[25] Esse comprendono:

- **Rimprovero verbale/scritto**: per lievi inosservanze delle procedure.[25]
- **Multa (fino a 4 ore)**: per violazioni colpose dei protocolli di controllo.[25]
- **Sospensione (fino a 10 giorni)**: per gravi inosservanze o recidiva.[25]
- **Licenziamento per giusta causa**: per violazioni dolose dei protocolli o commissione di reati che comportano la responsabilità dell'ente, tali da rompere il vincolo fiduciario.[25]

Per i Dirigenti e i Partner Esterni, le sanzioni prevedono la sospensione cautelare, la revoca dell'incarico per giusta causa o la risoluzione immediata del contratto con richiesta di risarcimento danni.[26]

2.4 Whistleblowing: La Nuova Procedura D.Lgs. 24/2023

OverApp Srl ha implementato una procedura di Whistleblowing all'avanguardia, conforme alla Direttiva UE 2019/1937 e al decreto di recepimento nazionale.[20] Il sistema consente di segnalare violazioni del Codice Etico, del Modello 231, delle normative europee e nazionali, nonché episodi di molestie o discriminazioni.[20]

Il canale di segnalazione è una piattaforma informatica crittografata (SaaS) che garantisce l'anonimato del segnalante e la protezione dei dati attraverso tecniche di cifratura conformi alla ISO 27001.[20] L'identità del segnalante non può essere rivelata senza il suo consenso espresso a persone diverse da quelle competenti a gestire la segnalazione.[41] La società ripudia ogni forma di ritorsione; qualsiasi atto ritorsivo (licenziamento, demansionamento, mutamento sede) è nullo di diritto e comporta sanzioni per l'autore.[20]

Capitolo 3: Parte Speciale A - Reati contro la Pubblica Amministrazione

I reati contro la Pubblica Amministrazione (Artt. 24 e 25) rappresentano una delle aree a più alto rischio per OverApp Srl, specialmente nell'ambito della fornitura di servizi software critici e della gestione di fondi pubblici (PNRR).[43]

3.1 Mappatura delle Attività Sensibili e Analisi dei Rischi

L'analisi dei processi aziendali ha evidenziato le seguenti "attività sensibili":

1. **Gare d'Appalto e Contrattualistica PA**: Rischio di turbata libertà degli incanti o corruzione per ottenere l'aggiudicazione di licenze o servizi di manutenzione.[7]

2. **Gestione di Finanziamenti e Contributi**: Rischio di indebita percezione di erogazioni pubbliche attraverso l'esposizione di dati falsi o rendicontazioni mendaci.[44]
3. **Rapporti Ispettivi**: Rischio di corruzione o induzione indebita verso funzionari di INPS, INAIL, Agenzia delle Entrate o Garante Privacy durante le verifiche.[24]
4. **Gestione Fondi PNRR**: Focus specifico sulla corretta esecuzione delle milestone tecnologiche per evitare la revoca dei finanziamenti.[14]

3.2 Protocolli di Controllo Operativi

Per ridurre il rischio residuo, sono stati definiti protocolli rigorosi applicabili a ogni interazione con la PA.[7]

3.2.1 Segregazione delle Funzioni (SoD) e Tracciabilità

Il processo di partecipazione a una gara deve prevedere la separazione tra chi individua l'opportunità, chi redige l'offerta tecnica e chi autorizza l'offerta economica.[9] Ogni fase del procedimento amministrativo deve essere tracciata tramite un sistema di "fascicolo digitale" inalterabile.[7]

3.2.2 Tracciabilità dei Flussi Finanziari

Tutti i pagamenti in uscita devono essere effettuati con strumenti che garantiscano la piena tracciabilità (bonifici bancari) e devono essere preceduti da una verifica di conformità della fattura rispetto all'ordine e alla prestazione effettiva.[7] È fatto assoluto divieto di operare con soggetti che rifiutano di indicare il destinatario reale del pagamento o che richiedono versamenti su conti in paradisi fiscali.[27]

3.2.3 Archiviazione a Norma e Gestione dei Rapporti con Terzi

La documentazione prodotta nei rapporti con la PA deve essere archiviata secondo le linee guida AgID per la conservazione sostitutiva, garantendo che i documenti originali (es. autodichiarazioni, bilanci) non possano essere modificati per celare irregolarità.[48] Nei rapporti con consulenti che agiscono per conto di OverApp Srl presso enti pubblici, è obbligatorio svolgere una *due diligence* preventiva per verificare l'onorabilità del soggetto e la congruità del compenso pattuito.[24]

Capitolo 4: Parte Speciale B - Reati Informatici e Societari

In quanto software house, OverApp Srl deve presidiare con particolare attenzione l'Art. 24-bis del D.Lgs. 231/01, relativo ai delitti informatici e al trattamento illecito dei dati.[5]

4.1 Accesso Abusivo e Alterazione di Dati PA

Il rischio specifico riguarda il personale tecnico che, per facilitare lo sviluppo o la manutenzione, potrebbe eccedere i propri privilegi di accesso ai sistemi dei clienti pubblici o alterare dati per nascondere inadempienze contrattuali.[12]

Protocolli Tecnici (Integrazione ISO 27001):

- **Gestione Privilegi (PAM)**: Gli accessi ai database della PA devono essere nominali, autorizzati a tempo e costantemente loggati.[6]
- **Vulnerability Assessment**: OverApp Srl esegue periodicamente test di sicurezza sulle proprie applicazioni prima del rilascio in produzione per prevenire falle sfruttabili da terzi.[6]
- **Integrità del Codice (DevOps Security)**: Il processo di rilascio del software deve essere automatizzato e protetto, garantendo che il codice distribuito non contenga *malware* o funzioni nascoste volte al danneggiamento di sistemi informatici (Art. 635-bis c.p.).[6]

4.2 Prevenzione dell'Estorsione Informatica (Legge 90/2024)

Recependo le recenti novità legislative del 2024, OverApp Srl ha introdotto misure specifiche contro l'estorsione informatica.[7] È fatto divieto a chiunque agisca per conto della società di utilizzare tool informatici per minacciare terzi o concorrenti al fine di ottenere vantaggi patrimoniali.[50] Allo stesso modo, la società adotta protocolli di *Business Continuity* per non soccombere a tentativi di estorsione esterna (Ransomware), evitando pagamenti illeciti che potrebbero configurare altre fattispecie di reato.[10]

Fattispecie di Reato (24-bis)	**Presidio Tecnico di Controllo**	**Standard ISO/UNI correlato**
Accesso abusivo (615-ter)	MFA (Multi-Factor Authentication)	ISO 27001 - Access Control [6]
Falsità in doc. informatici	Firma Digitale e Marca Temporale	AgID Conservazione [51]
Frode informatica PA	Segregazione dev/prod environments	ISO 27001 - Operations [11]

Capitolo 5: Implementazione, Formazione e Monitoraggio

L'efficacia del Modello 231 risiede nella sua natura dinamica. OverApp Srl si impegna a diffondere la cultura della compliance attraverso piani formativi annuali obbligatori per tutti i livelli aziendali.[11] La formazione deve

includere casi pratici su come riconoscere un conflitto di interessi, come utilizzare la piattaforma di whistleblowing e quali siano le responsabilità penali legate al codice software prodotto.[11]

L'Organismo di Vigilanza redige semestralmente una relazione sull'attività svolta, indicando lo stato dei controlli, le criticità emerse e le proposte di aggiornamento del Modello in base all'evoluzione normativa (es. nuove fattispecie di reato) o organizzativa della società.[1] Tale processo di miglioramento continuo assicura che OverApp Srl rimanga un ente eticamente integro e legalmente protetto, capace di trasformare la conformità normativa in un vantaggio competitivo duraturo.[16]

Sassari 03/03/2026

Il Presidente

OverApp Srl
Via Duca degli Abruzzi 12/C - 07100 Sassari (SS) - Italy
VAT IT02661870903 - REA SS-194371
www.overapp.com - info@overapp.it

Bibliografia

1. Modello 231, accesso eseguito il giorno marzo 4, 2026, https://www.basilicasanpietro.va/it/modello-231
2. Modello organizzativo 231: come funziona? - Avvocato Marco Ticozzi, accesso eseguito il giorno marzo 4, 2026, https://www.avvocatoticozzi.it/it/blog/388/modello-231-guida-completa-al-modello-organizzativo-ex-dlgs-23101
3. UNI/PdR 125:2022 - Parità di Genere - Auroradomus, accesso eseguito il giorno marzo 4, 2026, https://www.auroradomus.it/le-certificazioni/certificati/uni-pdr-125-2022.html
4. MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO AI SENSI DEL D.LGS. 231/01 - Pa Digitale S.p.A., accesso eseguito il giorno marzo 4, 2026, https://www.padigitale.it/wp-content/uploads/2025/10/Modello-PA-Digitale_Parte-Generale.pdf
5. L'esperienza del penalista dentro e fuori dall'OdV - AODV 231, accesso eseguito il giorno marzo 4, 2026, https://www.aodv231.it/images/img-editor/files/Montani%2017%2001%202024.pdf
6. Diapositiva 1 - AODV 231, accesso eseguito il giorno marzo 4, 2026, https://www.aodv231.it/images/img-editor/files/De%20Masi%2017%2001%202024.pdf
7. Modello 231 - EHT, accesso eseguito il giorno marzo 4, 2026, https://www.eht.eu/modello-231/
8. Modello di Organizzazione, Gestione e Controllo ai ... - Leonardo, accesso eseguito il giorno marzo 4, 2026, https://www.leonardo.com/documents/15646808/16737537/MOG+231_Parte+Generale_2025_ITA_05112025.pdf?t=1762762264707
9. NetSuite Segregation of Duties: Miglioramento dei controlli e della conformità - Netwrix, accesso eseguito il giorno marzo 4, 2026, https://netwrix.com/it/resources/blog/netsuite-segregation-of-duties/
10. UNI PdR 125:2022 - Kyndryl, accesso eseguito il giorno marzo 4, 2026, https://www.kyndryl.com/content/dam/kyndrylprogram/certifications/uni/kyndryl_italy_s.p.a._uni_pdr_125_2022_ita_05_sep_2027.pdf
11. Modello di Organizzazione Gestione e Controllo ex D.Lgs ... - ENG, accesso eseguito il giorno marzo 4, 2026, https://www.eng.it/content/dam/eng-portal/resources/documents/corporate-governance/EII_Modello_di_Organizzazione_e_Gestione_231.pdf
12. CATALOGO 231: delitti informatici e trattamento illeciti di dati (art. 24 bis d.lgs. 231/2001), accesso eseguito il giorno marzo 4, 2026, https://www.solo231.it/catalogo-231-delitti-informatici/
13. Responsabilità penale degli amministratori per data breach: quando la violazione dei dati diventa reato - ICT Security Magazine, accesso eseguito il giorno marzo 4, 2026, https://www.ictsecuritymagazine.com/articoli/responsabilita-penale-degli-amministratori-per-data-breach/
14. La linea guida per la parità di genere UNI/PdR 125:2022 - DNV, accesso eseguito il giorno marzo 4, 2026, https://www.dnv.it/services/la-linea-guida-per-la-parita-di-genere-uni-pdr-125-2022-227043/
15. Certificazione UNI/PdR 125:2022 - Parità di genere in azienda - Amtivo, accesso eseguito il giorno marzo 4, 2026, https://amtivo.com/it/altri-servizi-di-certificazione/certificazione-uni-pdr-125-2022-parita-di-genere/
16. UNI/PdR 125:2022 | Certificazione per la Parità di Genere - Intertek, accesso eseguito il giorno marzo 4, 2026, https://www.intertek.it/certificazioni/sistema/UNIPdR125/
17. PRASSI DI RIFERIMENTO UNI/PdR 125:2022 - Consigliera di Parità regionale, accesso eseguito il giorno marzo 4, 2026, https://www.consiglieradiparita.regione.lombardia.it/wps/wcm/connect/6decf39c-f5a2-4c3d-87d9-16d8007c5599/Testo+Prassi+di+Riferimento+UNI-PdR+125-2022.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-6decf39c-f5a2-4c3d-87d9-16d8007c5599-ppXS.zz
18. CODICE ETICO SA 8000 E PARITA' DI GENERE UNI PDR 125:2022 - palingeo.it, accesso eseguito il giorno marzo 4, 2026, https://www.palingeo.it/wp-content/uploads/2024/11/CODICE-ETICO-SA8000-E-PARITA-DI-GENERE-ff.pdf
19. UNI/PdR 125:2022 Procedura antimolestie e modalità di segnalazione - Confcooperative Terre d'Emilia, accesso eseguito il giorno marzo 4, 2026, https://www.terredemilia.confcooperative.it/Portals/0/Documenti%20Utili/Procedura%20antimolestie%20e%20m

odalit%C3%A0%20segnalazioni.pdf?ver=Tk76iBZ5Cd6A9cKtR9OfqA%3D%3D
20. procedura whistleblowing ai sensi del d.lgs. 24/2023 - Avio.com, accesso eseguito il giorno marzo 4, 2026, https://www.avio.com/sites/avio.com/files/downloads/Avio%20Procedura%20Whistleblowing_def_0.pdf
21. Best Practice nelle Organizzazioni Certificate PdR 125:2022 - Dasa Raegister, accesso eseguito il giorno marzo 4, 2026, https://www.dasa-raegister.com/best-practice-nelle-organizzazioni-certificate-uni-pdr-1252022-verso-una-parita-di-genere-effettiva/
22. Parità di genere, Invisiblefarm è certificata UNI/PdR 125:2022, accesso eseguito il giorno marzo 4, 2026, https://www.invisiblefarm.it/parita-di-genere-invisiblefarm-e-certificata-uni-pdr-1252022/
23. Vademecum D.LGS. 231/01 - GVM Spa, accesso eseguito il giorno marzo 4, 2026, https://www.gvmspa.it/it-IT/Etica-e-Trasparenza/Decreto-Legislativo-231-01/Vademecum-D-LGS-231-01
24. allegato 3 modello di organizzazione, di organizzazione gestione e controllo protocolli 231, accesso eseguito il giorno marzo 4, 2026, https://www.collegiounibs.it/wp-content/uploads/2019/02/ALL.3-Protocolli-231-.pdf
25. SISTEMA DISCIPLINARE, accesso eseguito il giorno marzo 4, 2026, https://www.aqp.it/sites/default/files/2021-10/AQP%20-%20Sistema%20Disciplinare%20231%20vers%2018.1.19.pdf
26. Codice Sanzionatorio – MOG 231 Aciam S.p.a., Rev. 2, maggio 2019 Sommario, accesso eseguito il giorno marzo 4, 2026, https://www.aciam.it/wordpress/wp-content/uploads/2019/07/CODICE-SANZIONATORIO-231-ACIAM.pdf
27. Modello di Organizzazione Gestione e Controllo ex D. Lgs. 231/2001 1 - Acquedotto Pugliese, accesso eseguito il giorno marzo 4, 2026, https://www.aqp.it/sites/default/files/2020-09/MODELLO%20231%20-%20versione%2002.09.2020.pdf
28. MODELLO ORGANIZZATIVO EX D.LGS. 231/01 – PARTE GENERALE REV. 5 17 LUGLIO 2023, accesso eseguito il giorno marzo 4, 2026, https://www.dorbit.space/downloads/Modello%20231%20-%20Completo.pdf
29. Modello 231 - Business Defence, accesso eseguito il giorno marzo 4, 2026, https://www.businessdefence.it/it/modello-231
30. MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D. LGS. 8 GIUGNO 2001 N. 231 PARTE GENERALE - ATV Verona, accesso eseguito il giorno marzo 4, 2026, https://www.atv.verona.it/flex/cm/pages/ServeAttachment.php/L/IT/D/1%252F9%252Fb%252FD.db740aee6c469cbca883/P/BLOB%3AID%3D412/E/pdf?mode=download
31. Procedure per la Parità di Genere | Certificazione UNI/PdR 125:22 | - Winple.it, accesso eseguito il giorno marzo 4, 2026, https://www.winple.it/dimostrativi-esempi/uni-pdr-125-2022-parita-genere/procedure-parita-genere/
32. 231 e Organismo di Vigilanza: composizione monocratica e composizione collegiale. Quale l'indirizzo della giurisprudenza? - Studio Legale Stefanelli, accesso eseguito il giorno marzo 4, 2026, https://www.studiolegalestefanelli.it/it/approfondimenti/231-e-organismo-di-vigilanza-composizione-monocratica-e-composizione-collegiale-quale-lindirizzo-della-giurisprudenza
33. LINEE GUIDA PER LO SVOLGIMENTO DELLE FUNZIONI DELL'ORGANISMO DI VIGILANZA EX D.LGS.8GIUGNO 2001,N.231 - Commercialisti.it, accesso eseguito il giorno marzo 4, 2026, https://commercialisti.it/wp-content/uploads/2025/11/Allegato-6.pdf
34. D.Lgs. 231/2001: i requisiti dell'Organismo di Vigilanza -... - PuntoSicuro, accesso eseguito il giorno marzo 4, 2026, https://www.puntosicuro.it/sgsl-mog-dlgs-231/01-C-58/d.lgs.-231/2001-i-requisiti-dell-organismo-di-vigilanza-AR-12974/
35. MOG 231 - SISTEMA DISCIPLINARE - Valle Umbra Servizi, accesso eseguito il giorno marzo 4, 2026, https://www.valleumbraservizi.it/document/open?id=13847
36. 231.PG-Sistema sanzionatorio - STEELFORM SRL Modello Organizzativo di Gestione e Controllo ex D. Lgs. 231/2001, accesso eseguito il giorno marzo 4, 2026, https://steelformitalia.it/wp-content/uploads/2025/10/231.PG-Sistema-sanzionatorio.pdf
37. Codice Sanzionatorio 231 - Sea Risorse, accesso eseguito il giorno marzo 4, 2026, https://www.searisorse.it/allegati/Codice-Sanzionatorio-231-searisorse-spa.pdf

38. Il sistema disciplinare e sanzionatorio dei Modelli 231, accesso eseguito il giorno marzo 4, 2026, https://www.procedure231.it/sistema-di-gestione-dlgs-231/sistema-disciplinare-e-sanzionatorio/
39. sistema sanzionatorio - e disciplinare - AECOM, accesso eseguito il giorno marzo 4, 2026, https://aecom.com/wp-content/uploads/documents/compliance/it/All-3-Modello-Dlgs-231-Sistema-sanzionatorio-AECOM.pdf
40. Segnalazione violazioni - Whistleblowing - D.Lgs. 24/2023 | Casa di Cura Giovanni XXIII, accesso eseguito il giorno marzo 4, 2026, https://www.giovanni23.it/segnalazione-violazioni-whistleblowing-d-lgs-24-2023/
41. Procedura Whistleblowing per la segnalazione di illeciti Corteva Agriscience - ITALIA, accesso eseguito il giorno marzo 4, 2026, https://www.corteva.com/content/dam/dpagco/corteva/eu/it/it/files/DF_Procedura%20Whistleblowing.pdf?=1
42. Whistleblowing - www.anticorruzione.it, accesso eseguito il giorno marzo 4, 2026, https://www.anticorruzione.it/-/whistleblowing
43. INCUBATORE DEL POLITECNICO SCPA MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO ai sensi del D.lgs 231/01 MAPPA DELLE AREE A RISCHIO - I3P, accesso eseguito il giorno marzo 4, 2026, https://www.i3p.it/assets/Doc/i3p_mo_231_4.-mappatura-del-rischio.pdf
44. all. 2 mappatura del rischio potenziale e del rischio residuo - Apam, accesso eseguito il giorno marzo 4, 2026, https://www.apam.it/uploads/societa-trasparente/3055/2024-03-22_65fd47_b-all-2-mappatura-dei-rischi-apamspa-rev2024-pdf.pdf
45. D.Lgs. n. 231 del 2001 (responsabilità enti e società) - Bosetti & Gatti, accesso eseguito il giorno marzo 4, 2026, https://www.bosettiegatti.eu/info/norme/statali/2001_0231.htm
46. PROTOCOLLO OPERATIVO N. 8 GESTIONE SISTEMI INFORMATIVI 1. Obiettivo e ambito di applicazione. Il presente protocollo ha l'obiett - Amministrazione Trasparente Segrate Servizi, accesso eseguito il giorno marzo 4, 2026, https://trasparenza.segrateservizi.it/wp-content/uploads/2022/06/All.-02.8-protocollo-8-gestione-sistemi-informativi-22.pdf
47. Guida alla Segregazione dei Compiti (SoD) - Netwrix, accesso eseguito il giorno marzo 4, 2026, https://netwrix.com/it/cybersecurity-glossary/architectural-concepts/segregation-of-duties/
48. Conservazione|Agenzia per l'Italia digitale - Agid, accesso eseguito il giorno marzo 4, 2026, https://www.agid.gov.it/it/piattaforme/conservazione
49. Conservazione Sostitutiva: Come Funziona e Perché è Fondamentale - Intesa, accesso eseguito il giorno marzo 4, 2026, https://www.intesa.it/conservazione-sostitutiva-come-funziona-e-perche-e-fondamentale/
50. Osservatorio 231 - Settembre 2024 - Protiviti, accesso eseguito il giorno marzo 4, 2026, https://www.protiviti.com/sites/default/files/2024-09/osservatorio_231_settembre-2024.pdf
51. Guida alla conservazione sostitutiva: cos'è, obblighi e modalità - Blog Geobadge, accesso eseguito il giorno marzo 4, 2026, https://geo-badge.com/blog/cose-conservazione-sostitutiva-come-si-fa-su-chi-ricade-obbligo/
52. I reati informatici e la 231/01: controlli e formazione - CyberAcademy, accesso eseguito il giorno marzo 4, 2026, https://www.cyberacademy.online/blog/reati-informatici-controlli-formazione
53. parità di genere UNI PdR 125:2022 - consulenza gdpr, MOG231, ISO 27001, accesso eseguito il giorno marzo 4, 2026, https://www.maggioloconsulting.it/parit%C3%A0-di-genere-uni-pdr-125.html
54. MOG 231: Check List, Controlli e Protocolli – Guida Completa, accesso eseguito il giorno marzo 4, 2026, https://bluen.eu/modello-231-strumenti-e-fasi-operative-per-una-compliance-efficace/