VUS COM S.R.L.

CORPORATE GOVERNANCE -D.LGS. 231/2001

MODELLO ORGANIZZATIVO E DI GESTIONE

PARTE GENERALE

Approvato dall' A.U. il 2 MAGGIO 2017 – DET A.U. 6/17

MODIFICATO IL 28/3/2018 – DET A.U. 3/18

MODIFICATO IL 15 luglio 2020 con DELIBERA CDA n. 51/2020

MODIFICATO IL 15 aprile 2021 con DELIBERA CDA n. 77/2021

MODIFICATO IL 27 aprile 2022 con DELIBERA CDA n. 112/2022

MODIFICATO IL 10 gennaio 2024 con DELIBERA CDA n. 172/2024

INTRODUZIONE

IL D.LGS. 231/2001

Il D.lgs. 231/2001 è stato emanato per effetto della delega al Governo prevista dalla L. 29/9/2000 n. 300 di recepimento, tra gli altri, della Convenzione relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità europee o degli Stati membri dell'Unione europea, fatta a Bruxelles il 26/5/1997 e della Convenzione OCSE sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali fatta a Parigi il 17/12/1997.

Tale norma ha innovato il principio secondo cui le persone giuridiche non potevano delinquere e, conseguentemente, non potevano essere punite.

I fatti dimostravano che un sistema concernente la criminalità delle imprese, basato e limitato esclusivamente attorno alle persone fisiche, comportava una perdita di garanzia. La mancata espressa previsione di una forma di responsabilità della persona giuridica, per effetto di comportamenti illeciti commessi dalle persone fisiche, in linea o comunque dipendenti dalla politica aziendale, infatti, determinava, di fatto, l'insensibilità delle persone giuridiche ai deterrenti contenuti nelle norme penali.

Dal 2001 il D.lgs. 231/2001 si è comportato come un "contenitore" ove sono stati collocati, nel tempo, reati socialmente rilevanti, così accanto agli originari reati in danno alle Pubbliche Amministrazioni (malversazione, indebita percezione, truffa, concussione, corruzione), si sono aggiunti i reati di falso nummario, i reati societari, i reati con finalità di terrorismo od eversione dell'ordine democratico …

La responsabilità dell'Ente nasce da difetti di organizzazione, tanto che si semplifica definendo la responsabilità dell'Ente come l'effetto della deficienza organizzativa.

L'art. 5 della norma definisce l'ambito di responsabilità dell'Ente:

"*1. L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:*

a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; (Soggetti Apicali)

b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a) (Sottoposti).

2. L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi."

Il successivo articolo 6 precisa:

"*1. Se il reato è stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a)* (Soggetti Apicali), *l'ente non risponde se prova che:*

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;

c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;

d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b)."

Riguardo, poi, i soggetti sottoposti il successivo articolo 7 stabilisce:

"1. Nel caso previsto dall'articolo 5, comma 1, lettera b) (Sottoposti), *l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza.*

2. In ogni caso, è esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi.".

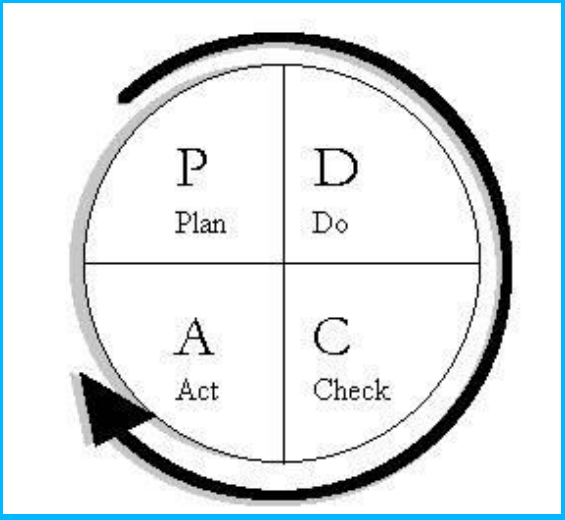
L'ente, dunque, per non assumere la responsabilità prevista dalla norma, deve dotarsi di un sistema organizzativo che sia in grado di prevenire e ridurre al minimo la possibilità che siano commessi i reati previsti dalla norma da soggetti Apicali o da sottoposti.

IL PROCESSO "231"

Col termine "processo 231" si intende il complesso di attività, conoscenze e risorse che sono organizzate tra loro in modo da soddisfare quanto previsto dal D.lgs. 231/2001 sollevando così l'Ente dalla relativa responsabilità.

Si tratta di un processo ciclico che deve essere avviato dall'organo dirigente (Art.6 comma1 lett.a) e quindi mantenuto aggiornato ed efficacemente attuato attraverso la partecipazione dell'Organismo di Vigilanza – OdV – (Art.6 comma 1 lett.b).

Il funzionamento del processo può ben essere descritto attraverso il noto ciclo di Deming (che, peraltro, è alla base degli standard di risk management)



Nella tabella che segue sono sintetizzate le macro-attività previste dal processo 231, raggruppate secondo i quattro momenti del Pianificare (Plan), Agire (Do), Controllare (Check) e Reagire (Act) (colonne "fase" e "descrizione", collegate, attraverso la colonna "chi" al segmento gerarchico dell'ente.

FASE	DESCRIZIONE	CHI
PLAN	PIANIFICARE, ovvero individuare e definire gli obiettivi, elaborare la strategia per il loro conseguimento, organizzare le risorse per darne attuazione.	ALTA AMMINISTRAZIONE. Questa fase appartiene all'organo dirigente al suo livello più alto.
DO	FARE, ovvero definire i programmi tattici e curarne l'esecuzione.	GESTIONE. In questa fase intervengono i livelli più operativi.
CHECK	CONTROLLARE, ovvero verificare il corretto funzionamento dell'ente, monitorare l'osservanza dei modelli (attuazione ed applicazione), controllare l'efficienza, l'adeguatezza, l'attualità e coerenza dei modelli.	GESTIONE ORGANISMO DI VIGILANZA
ACT	REAGIRE, ovvero adottare tutte le iniziative ed azioni opportune e necessarie sulla base delle verifiche svolte ivi inclusi i provvedimenti disciplinari. Aggiornare i modelli, individuare gli elementi di aggiornamento od aggiustamento di obiettivi, strategie e tattiche.	GESTIONE ALTA AMMINISTRAZIONE ORGANISMO DI VIGILANZA

L'illustrazione che segue schematizza le tre aree gerarchiche e decisionali dell'ente:

- Strategia ovvero l'area propria del Consiglio di Amministrazione; questa area ha la responsabilità della organizzazione dell'associazione che guida ed indirizza. Questa area esercita al massimo livello i poteri decisionali inclusi quelli di disposizione delle risorse.

- Gestione, ovvero l'area propria delle direzioni; questa area, in ragione delle competenze professionali, dei poteri gerarchici e funzionali che riceve, attua le direttive dell'alta amministrazione organizzando e vigilando le attività dell'associazione attraverso i processi ed ha il compito di definire le strategie per l'attuazione degli obiettivi dell'ente.

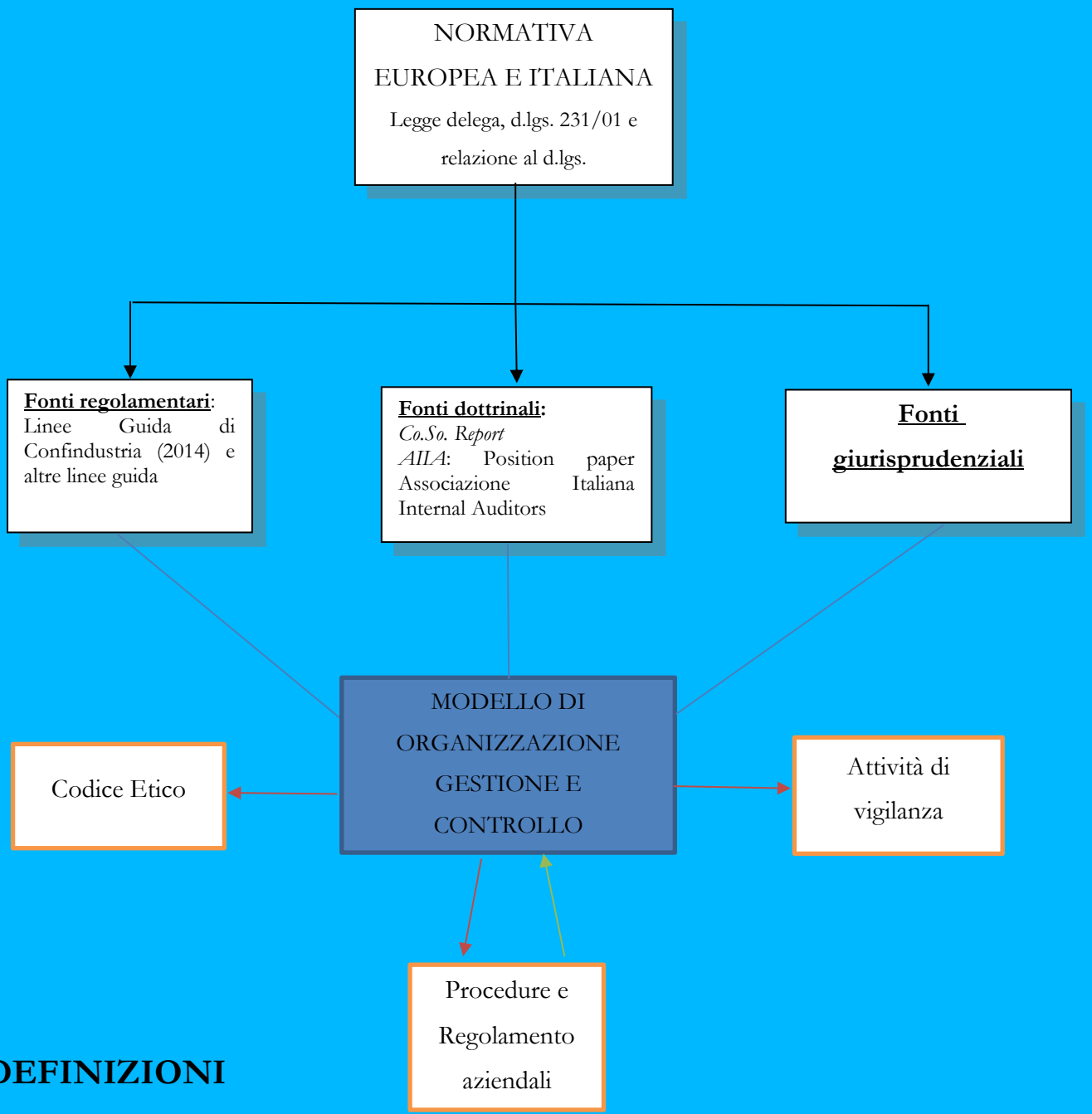
- Operatività, ovvero l'area che, in ragione delle competenze professionali, dei poteri gerarchici e funzionali che riceve, garantisce l'attuazione delle direttive ricevute controllandone la corretta esecuzione.

FIGURA DEI PIANI DECISIONALI

IL MODELLO DI ORGANIZZAZIONE E GESTIONE - MOG

Lo schema che segue illustra sinteticamente, relativamente al processo 231, la gerarchia delle fonti ed il sistema documentale adottato dall'ente.

SCHEMA GERARCHIA DELLE FONTI



DEFINIZIONI

Qui sono contenute, in ordine alfabetico, le definizioni dei termini più significativi utilizzati nel presente documento.

AUTENTICITA', si intende il requisito di sicurezza del Sistema informativo secondo il quale le informazioni devono essere riconducibili a chi le produce o le approva.

DANNO, si intende l'impatto prodotto dall'avveramento di un rischio sull'ente ed i suoi stakeholders.

DATI, si intende ogni informazione nella sua accezione più ampia, indipendentemente dal formato o dal supporto su cui essa è contenuta, sia in forma sciolta che aggregata.

DISPONIBILITA', si intende il requisito di sicurezza del Sistema informativo secondo il quale le informazioni, quando occorrono, devono essere a disposizione di chi ne ha diritto.

INTEGRITA', si intende il requisito di sicurezza del Sistema informativo secondo il quale le informazioni devono essere integre, esatte ed aggiornate.

MINACCIA, si intendono quegli eventi che, associati a debolezze (vulnerabilità) dell'ente, permettono l'avverarsi di un rischio; la minaccia si esprime in probabilità di accadimento.

MODELLO DI ORGANIZZAZIONE E GESTIONE (MOG), si intende il documento che definisce e formalizza gli obiettivi, i principi, i presupposti e le attività organizzative che l'ente, in conformità all'art.6 del D.lgs. 231/2001 adotta ed attua al fine di ridurre al minimo il rischio che soggetti da esso dipendenti (sia Apicali che Sottoposti) possano commettere reati delle specie previste dal D.lgs. 231/2001 nell'interesse od a vantaggio dell'ente medesimo.

ORGANISMO DI VIGILANZA (OdV), si intende l'organismo dell'ente, dotato di autonomi poteri di iniziativa e controllo, cui l'organo dirigente ha affidato il compito di vigilare sul funzionamento e l'osservanza del MOG e di curarne l'aggiornamento in conformità a quanto previsto dall'art.6 comma 1 lett.b) del D.lgs. 231/2001.

PROCESSO, si intende il complesso di attività e risorse tra loro organizzate al fine di produrre un determinato output partendo da un determinato input.

QUOTE, si tratta del sistema sanzionatorio previsto dall'art. 10 del D.lgs. 231/2001.

RISCHIO, si intende la possibilità che un evento non desiderato si attui arrecando un danno all'ente.

RISERVATEZZA, si intende il requisito di sicurezza dei flussi informativi secondo i quali le informazioni devono essere conosciute solo da coloro che ne hanno diritto.

SISTEMA INFORMATIVO (SI), il complesso delle risorse (risorse umane, tecnologia, applicazioni, infrastrutture, dati) organizzate dall' azienda per il trattamento delle informazioni in genere e dei dati personali in modo specifico.

FLUSSI INFORMATIVI DI VIGILANZA, il documento che definisce il contenuto delle informazioni che obbligatoriamente devono essere trasmesse all'organismo di vigilanza, individuando compiti e responsabilità.

SOGGETTI APICALI, si intendono le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché le persone che esercitano, anche di fatto, la gestione ed il controllo dell'ente medesimo, secondo quanto previsto dall'art. 5 comma 1 lett. a) del D.lgs. 231/2001.

SOGGETTI SOTTOPOSTI, si intendono le persone sottoposte alla direzione o alla vigilanza di un soggetto apicale, così come definito dall'art.5 comma 1 lett. b) del D.lgs. 231/2001.

VULNERABILITA', si intende la debolezza dell'ente rispetto specifiche ipotesi di rischio; attraverso tali debolezze le minacce determinano l'avverarsi dei rischi.

PARTE I

SEZIONE I - DICHIARAZIONI

I dati che seguono sono stati ricavati dalle interviste con gli organi ed il personale dell'ente nonché da documenti forniti dagli stessi interessati.

I.1. ENTE

L'Ente che adotta e si impegna ad efficacemente attuare il presente Modello di Organizzazione è la VUS COM S.R.L.., di seguito più brevemente denominato "VUS COM", con sede in via Gramsci 54 CAP 06034 Foligno. C.F.-P. IVA: 02635680545.

I.2. RAPPRESENTANZA LEGALE

La rappresentanza dell'Ente di fronte ai terzi ed in giudizio spetta al Presidente del Consiglio di Amministrazione.

I.3. NATURA E DESCRIZIONE

La Vus Com S.r.l nasce nel 2003 come società commerciale del Gruppo Valle Umbra Servizi, è detenuta al 100% dalla Valle Umbra Servizi S.p.a.; società a sua volta detenuta al 100% dai 22 Comuni dell'ambito territoriale n. 3 dell'Umbria. Ha come obbiettivo principale la commercializzazione di GAS METANO e la COMMERCIALIZZAZIONE DI ENERGIA ELETTRICA, a favore di clienti per utenze domestiche e per le piccole e medie imprese, per condomini, alberghi, artigiani e industria. Il suo territorio di riferimento è l'Umbria, dove sono presenti in 57 comuni. L'Azienda opera sul mercato con serietà, professionalità e trasparenza garantendo affidabilità per la commercializzazione del servizio Gas Metano e dell'Energia elettrica.

I.4. LA MISSIONE

L'obbiettivo principale dell'Azienda è la soddisfazione del cliente e la creazione, sin dall'inizio, di un rapporto chiaro e sereno. Il cliente è al centro dell'interesse per cui gli viene offerta una valida consulenza per la soluzione più idonea per ogni esigenza, come può essere la scelta di una tariffa che meglio si adatta ai consumi del cliente stesso. Esso viene informato su come si svilupperà (presumibilmente) la dinamica dei prezzi del Gas Metano e dell'energia elettrica, al fine di rendere consapevole la scelta tariffaria che verrà sottoscritta.

I.5. AMMINISTRAZIONE

La Società è amministrata dal Consiglio di Amministrazione, composto da n° 3 membri, nominato dall'Assemblea dei soci.

I.6. CONDIZIONI

L'Ente è vincolato all'osservanza, oltre che della vigente normativa italiana, dello statuto, del codice etico e dei regolamenti interni.

I.7. NORMATIVA

Questo Modello di Organizzazione e Gestione è stato sviluppato in conformità al D.lgs. 231/2001 e s.m.i.-

I.8. STANDARDS DI RIFERIMENTO

Di seguito sono riportati gli standard di riferimento utilizzati per lo sviluppo della presente documentazione:

- COSO:1992 (Committee of Sponsoring Organizations of the Treadway Commission) per quanto riguarda i principi di internal control.
- AS4360:2004 (Risk management) per quanto riguarda l'analisi dei rischi e la loro gestione.
- COBIT 4.1 (Control Objectives for Information and related Technology) per quanto riguarda la governance dei sistemi IT.
- ITIL v. 3 (Information Technology Infrastructure Library) per quanto riguarda la governance dei servizi IT.
- ISO/IEC 27001:2005 (Information Security Management Systems) per quanto riguarda gli aspetti di sicurezza del Sistema Informativo.
- Linee guida per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) – UNI-INAIL 2001.
- Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.lgs. 231/2001 – Confindustria 2004/2014.
- ISO/EC 38.5000 (IT Governance) per quanto riguarda i principi di governo del sistema informatico.

I.9. OBIETTIVI DEL MODELLO

L'Ente si propone di ridurre al minimo il rischio che soggetti da esso dipendenti (sia apicali che sottoposti) possano commettere reati delle specie previste dal D.lgs. 231/2001, nell'interesse od a vantaggio dell'ente

medesimo; ciò al fine di rispettare i principi etici che lo ispirano e lo guidano ed al fine di essere sollevato dalla responsabilità prevista dal citato D.lgs. 231/2001.

I.10. SCOPO DEL DOCUMENTO

Questo documento ha lo scopo di definire e formalizzare i principi, i presupposti, le attività ed i progetti organizzativi, che l'Ente intende adottare ed attuare al fine di raggiungere l'obiettivo sopra enunciato.
Tutti coloro i quali rivestono le figure di soggetti apicali o sottoposti come meglio definito dal D.lgs. 231/2001 sono tenuti allo scrupoloso rispetto di quanto di seguito stabilito e ciascuno, nei limiti delle proprie competenze e funzioni, è obbligato a darne immediata attuazione.

SEZIONE II – PRINCIPI

Questa sezione contiene i principi, che guidano ed ispirano il presente Modello di organizzazione e gestione.

I principi qui elencati devono essere rispettati da tutti coloro i quali operano per conto della VUS COM.

II.1. - ETICITA'

L'adozione di principi etici rilevanti ai fini della prevenzione dei reati previsti dal D.lgs. 231/2001 costituisce elemento essenziale del processo "231".

La Vus Com riconosce l'importanza della responsabilità etico-sociale nella conduzione degli affari e delle attività aziendali impegnandosi al rispetto dei legittimi interessi dei propri stakeholder e della collettività in cui opera.

Non sono etici e favoriscono l'assunzione di atteggiamenti ostili nei confronti dell'ente, i comportamenti di chiunque, singolo o organizzazione, cerchi di appropriarsi dei benefici della collaborazione altrui, sfruttando posizioni di forza.

In ogni caso il perseguimento dell'interesse dell'ente non può mai giustificare una condotta contraria ai principi di correttezza ed onestà.

II.2. - LEGALITA'

II.2.1. RISPETTO DELLE LEGGI

È condizione imprescindibile di ogni attività dell'ente il rispetto della normativa vigente ed applicabile all'ente. Per normativa si intendono la Costituzione e le Leggi italiane, le disposizioni di pari rango dell'Unione Europea, le Leggi nazionali dei Paesi in cui l'Ente opera.

II.2.2. RISPETTO DEGLI OBBLIGHI DI NATURA NEGOZIALE

La Vus Com si obbliga, altresì, a rispettare scrupolosamente tutti gli obblighi derivatigli da contratti od altri strumenti negoziali di cui è parte. Come pure a rispettare gli altri obblighi legati dal contesto sociale in cui essa opera.

II.2.3. RISPETTO DEL D.lgs. 231/2001

La Vus Com si impegna a ridurre i rischi di commissione dei reati previsti dal D.lgs. 231/2001. La riduzione dei rischi deve essere più bassa possibile ritenendo il rispetto della legge obiettivo prioritario. La revisione ed aggiornamento periodici hanno il fine di restringere il livello di rischio accettabile al più basso possibile e conferire la massima efficacia al Modello di organizzazione e gestione.

II.3. - RIGORE

Le disposizioni del presente documento, come pure le disposizioni di legge o di altra natura che sono vincolanti per l'ente devono essere interpretate in maniera rigorosa avendo come guida i fini primari del presente documento che sono il rispetto dei principi etici e delle leggi.

II.4. - GESTIONE DEI RISCHI

Le attività dell'ente e le scelte conseguenti devono essere condotte con consapevolezza secondo le migliori prassi.

Nel gestire i rischi deve essere garantito il rispetto oltre che delle leggi degli interessi degli stakeholders[1] e comunque e i rischi devono essere gestiti assegnando chiari e specifici poteri e responsabilità.

II.4.1. ANALISI DEI RISCHI

Ogni attività rilevante dell'Ente deve essere preceduta da analisi dei rischi. L'analisi dei rischi deve individuare e descrivere gli scenari di rischio in relazione alla commissione dei reti previsti dal D.lgs. 231/2001 con riferimento alla attività in esame. I ruoli, poteri e responsabilità per le analisi dei rischi devono essere chiaramente e specificamente allocate.

---

[1] Col termine stakeholder si individuano tutti i soggetti, individui od organizzazioni, attivamente coinvolti in un'iniziativa economica (progetto, azienda), il cui interesse è negativamente o positivamente influenzato dal risultato dell'esecuzione, o dall'andamento, dell'iniziativa e la cui azione o reazione a sua volta influenza le fasi o il completamento di un progetto o il destino di un'organizzazione.
Nell'ambito di un progetto, sono s. i soggetti relativi al cliente, al fornitore, alle terze parti (altre organizzazioni eventualmente coinvolte tra cliente e fornitore), i membri del team di progetto, i fruitori dei risultati in uscita dal progetto, i finanziatori (come banche e azionisti), i gruppi di interesse locali relativamente all'ambiente dove il progetto si sviluppa e l'azienda opera. Tra gli s. vi sono i soggetti senza i quali l'impresa non sopravvive, per cui il processo produttivo di un'azienda continua se sono soddisfatte soglie critiche, di costo, servizio e qualità, al di sotto delle quali il cliente cambia fornitore e manager e dipendenti si dimettono. Nell'ambito poi del cosiddetto filone etico, sono s. tutti i soggetti che influenzano o sono influenzati dall'impresa e di cui essa deve tener conto, anche in assenza di potere diretto su processi e profitti, poiché essi subiscono conseguenze a vari livelli, per es. un impatto ambientale negativo. L'analisi degli s. identifica e classifica tutti gli s. di progetto e le loro esigenze informative rispetto alle varie aree di conoscenza del project management. L'identificazione degli s. si ottiene mediante un elenco casuale e libero dei soggetti coinvolti nel progetto (tecniche di brainstorming) oppure mediante liste di controllo descrittive dell'ambiente di progetto o di progetti precedenti (check list) o infine mediante simulazioni dell'ambiente di progetto per rintracciare gli s. interni ed esterni (rappresentazione).
Per la gestione degli s., è di supporto al project management un modello di classificazione a matrice basato sulle variabili interesse e potere, vale a dire sul livello di influenza che il progetto ha sugli obiettivi, le attività e i risultati dello s. e sul livello di influenza che lo s. ha su impostazione, esecuzione e risultati del progetto. In base al valore assunto dalle variabili, lo s. si classifica come s. marginale (basso interesse, basso potere), s. istituzionale (basso interesse, alto potere), s. operativo (alto interesse, basso potere), s. chiave (alto interesse, alto potere) ed è collocato in uno dei quattro quadranti della matrice, caratterizzati da diverse strategie di gestione. *(voce Stakeholder in Enciclopedia Treccani on line).*

II.4.2. VALUTAZIONE DEI RISCHI

Nella valutazione dei rischi deve essere seguito il massimo rigore, ovvero in caso di indecisione deve essere scelta la soluzione di maggior garanzia tenuto conto dei principi etici e della legge. Il danno deve essere considerato sempre massimo indipendentemente dai criteri di valutazione qualitativi o quantitativi, poiché la commissione di un reato, seppure lieve, non può essere tollerata. La scelta delle contromisure deve essere effettuata in coerenza preferendo tra le misure quelle che offrono le maggiori protezioni e non secondo criteri di mera economicità.

Il "Rischio accettabile" deve essere valutato conformemente ai superiori principi considerando che il sistema di prevenzione deve essere tale da non poter essere aggirato se non fraudolentemente.

II.5. – CORRETTEZZA E TRASPARENZA

Le informazioni che vengono diffuse dall'ente sono complete, trasparenti, comprensibili ed accurate, in considerazione di coloro che sono i destinatari, in modo che questi ultimi possano assumere decisioni consapevoli.

Le informazioni, in considerazione della propria natura, devono soddisfare adeguati livelli di integrità e di disponibilità; alle informazioni destinate a diffusione o che possono avere impatti rilevanti sull'ente, sulle risorse umane, sugli stakeholder deve essere garantito un idoneo livello di autenticità.

Tutte le azioni e le operazioni compiute ed i comportamenti tenuti da coloro che operano per l'ente, nello svolgimento del proprio incarico o funzione, devono pertanto essere ispirate a trasparenza, correttezza e reciproco rispetto, nonché alla legittimità sotto l'aspetto sia formale che sostanziale, secondo le norme vigenti e le procedure e regolamenti interni e di gruppo.

II.6. – RISERVATEZZA

L'ente, in conformità alle disposizioni di legge, garantisce la riservatezza delle informazioni in proprio possesso, ivi inclusi i dati personali.

A coloro che operano per conto dell'ente è fatto espresso divieto di utilizzare informazioni riservate per scopi non connessi all'esercizio della propria attività professionale anche successivamente alla cessazione del rapporto che li lega all'ente.

II.7. – RISORSE UMANE

Il fattore umano costituisce allo stesso tempo la risorsa chiave dell'ente ed è la fonte da cui possono essere commessi i reati da prevenire. Ne consegue che l'ente pone la massima attenzione nella gestione delle risorse umane selezionando e mantenendo personale particolarmente qualificato. Particolare attenzione è prestata

agli aspetti motivazionali ed alle specifiche esigenze formative, tenendo conto delle potenzialità degli individui e favorendo le condizioni per un ambiente di lavoro propositivo, collaborativo, gratificante e non conflittuale. Ciò nella convinzione che un sano ambiente di lavoro irrobustisce l'ente riguardo le minacce di commissione di reato.

Coloro che operano in nome e/o per conto dell'ente devono svolgere la propria attività lavorativa ed il proprio incarico con impegno professionale, diligenza, efficienza e correttezza, utilizzando al meglio gli strumenti ed il tempo a loro disposizione ed assumendo le responsabilità connesse agli impegni assunti.

L'ente garantisce un adeguato grado di professionalità nell'esecuzione dei compiti assegnati ai propri collaboratori, impegnandosi a valorizzare le competenze delle proprie risorse, mettendo a disposizione delle medesime, idonei strumenti di formazione, di aggiornamento professionale e di sviluppo.

Tutto il personale è assunto con regolare contratto di lavoro, non essendo tollerata alcuna forma di lavoro irregolare e di sfruttamento.

Qualsiasi forma di discriminazione è evitata sia in fase di selezione che in quelle di gestione e sviluppo di carriera del personale; la valutazione dei candidati è basata unicamente sul fine del perseguimento degli interessi aziendali.

Qualsiasi azione che possa configurare abuso d'autorità e, più in generale, che violi la dignità e l'integrità psico-fisica della persona non è tollerata dall'ente.

II.8. - DOCUMENTAZIONE

Ogni operazione, transazione, azione, rilevanti ai fini del D.lgs. 231/2001 (quali ad esempio la documentazione contabile e di sicurezza) deve essere verificabile, documentata, coerente e congrua rispettando i principi di sicurezza del Sistema informativo di seguito meglio specificati.

La documentazione deve essere prodotta e mantenuta secondo idonei livelli di efficacia probatoria tenuto conto della vigente normativa.

II.9. SICUREZZA

II.9.1. SUL LAVORO

La Vus Com promuove e diffonde la cultura della sicurezza, sviluppando la consapevolezza dei rischi, promuovendo comportamenti responsabili da parte di tutti i dipendenti e collaboratori, al fine di preservarne la salute e la sicurezza.

La Vus Com garantisce un ambiente lavorativo conforme alle vigenti norme in materia di sicurezza e salute mediante il monitoraggio, la gestione e la prevenzione dei rischi connessi allo svolgimento delle attività professionali.

La gestione della salute e della sicurezza sul lavoro costituisce parte integrante della gestione generale dell'Ente.
La Vus Com adotta un sistema di gestione della salute e della sicurezza sul lavoro (SGSL).
Il SGSL integra obiettivi e politiche per la salute e la sicurezza nella progettazione e gestione di sistemi di lavoro e di produzione di beni e servizi, definendo le modalità per individuare, all'interno dell'ente, le responsabilità, le procedure, i processi e le risorse per la realizzazione della politica aziendale di prevenzione, nel rispetto delle norme di salute e sicurezza vigenti (D.lgs.. 81/2008).
Adeguate risorse sono specificamente allocate per la realizzazione dei principi sopra espressi.

II.9.2. DEL SISTEMA INFORMATIVO

Le informazioni e gli strumenti con cui sono trattate (elettronici e non, inclusi i programmi software) sono una risorsa chiave dell'Ente ed allo stesso tempo sono uno dei principali strumenti per la commissione di alcuni dei reati contemplati dal D.lgs. 231/2001 (Reati ai danni delle P.A. Gr. 1 – Reati societari Gr. 3 – Delitti contro la personalità individuale Gr. 6 — Delitti informatici Gr. 10). Per Sistema informativo si intende il complesso delle risorse organizzate ed utilizzate dall'ente per il trattamento delle informazioni, ne consegue che l'ente ritiene prioritaria la protezione del Sistema informativo.
La protezione dei dati personali, come prescritto dal D.lgs. 196/2003 e GDPR 679/2016, è parte integrante della sicurezza del Sistema Informativo.

II.9.3. DELLE RISORSE FINANZIARIE

Le risorse finanziarie sono strategiche per l'ente ed allo stesso tempo sono uno degli strumenti maggiormente interessati dalla commissione di alcuni dei reati previsti dal D.lgs.. 231/2001.
L'art. 6 co. 2 lett. c) del D.lgs. 231/2001 prescrive l'obbligo di individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati, a tal fine l'Ente si attiene scrupolosamente al rispetto della vigente normativa di settore sottoponendo le suddette attività al controllo del Collegio sindacale.

II.10 - VIGILANZA ED AGGIORNAMENTO

L'art. 6 co.1 lett. b) D.lgs. 231/2001 prevede l'obbligo di affidare ad un organismo dell'ente, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza del MOG e di curarne l'aggiornamento.
L'Ente a tal scopo ha istituito ed incaricato uno specifico Organismo di vigilanza, cui ha fornito attribuzioni di competenze e responsabilità in modo da essere dotato di autonomi poteri di iniziativa e di controllo in conformità alla legge.

All'Odv come sopra nominato spetta il compito di controllare il funzionamento e l'osservanza del MOG e di curarne l'aggiornamento.
Al fine di garantire l'efficacia ed efficienza del MOG, periodicamente, almeno una volta l'anno ed anche prima qualora intervengano rilevanti mutamenti organizzativi dell'Ente o legislativi, ad iniziativa di chi è incaricato della vigilanza (consiglieri od organismo autonomo) è promossa la revisione ed aggiornamento del MOG medesimo.

II. 10.1 L'ORGANISMO DI VIGILANZA

All'interno della gerarchia aziendale l'Organismo di Vigilanza è posto in posizione apicale e in rapporto diretto con il Consiglio di Amministrazione al quale riferisce di eventuali violazioni del Modello.
Per poter svolgere efficacemente l'attività assegnata, l'Organismo possiede al suo interno competenze tecnico-professionali adeguate e capacità specifiche in tema di attività ispettiva. Ove necessario, l'OdV si avvale dell'ausilio e delle competenze di consulenti esterni di comprovata professionalità.

II. 10.2 Informativa da e verso l'Organismo di Vigilanza - Flussi informativi verso l'Organismo di Vigilanza

L'Organismo di Vigilanza è destinatario dei flussi informativi descritti ai successivi punti *a)* e *b)*.
Tali flussi posso essere comunicati all'OdV attraverso l'utilizzo indifferente dei seguenti canali:

- posta elettronica, inviando un'e-mail all'indirizzo dell'Organismo di Vigilanza: ***odv@vuscom.it***
- consegna a mano dei documenti alla funzione di "direzione commerciale".

Nello specifico, costituiscono oggetto di segnalazione all'OdV:

a) Richieste di chiarimenti in merito all'applicazione di quanto previsto dal Modello

Tutti i dipendenti e i membri degli organi sociali della Società possono chiedere chiarimenti all'OdV in merito alla corretta interpretazione e applicazione del Modello, dei protocolli di prevenzione, delle relative procedure di attuazione e del Codice Etico.

b) Altri flussi informativi

Oltre alle segnalazioni di cui sopra, devono essere obbligatoriamente trasmesse all'OdV le seguenti tipologie di informazioni:

b.1) le informazioni riportate nell'*Allegato 4 "Regolamento Flussi informativi"* relative a specifiche attività sensibili, che i dirigenti/dipendenti della Società sono tenuti a fornire con la periodicità e nel rispetto delle scadenze ivi specificate;

b.2) le informazioni relative a operazioni sensibili gestite secondo iter procedimentali diversi da quelli descritti nel Modello e/o nelle procedure aziendali, delle quali l'OdV deve essere informato al fine di attivare i riscontri ritenuti necessari. Sono tenuti a tali segnalazioni i dirigenti e/o i responsabili di processo che si

trovano a gestire le operazioni in oggetto a causa di situazioni eccezionali, dovute a una peculiarità specifica dell'operazione sensibile o a esigenze di straordinaria urgenza o di particolare riservatezza.
L'assolvimento degli obblighi di informazione verso l'Organismo di Vigilanza rientra nel più ampio dovere di diligenza e obbligo di fedeltà del prestatore di lavoro di cui agli artt. 2104 e 2105 c.c. Il corretto adempimento dell'obbligo di informazione da parte di quest'ultimo non può dar luogo all'applicazione di sanzioni disciplinari.
Di contro, la violazione degli obblighi di informazione nei confronti dell'OdV, costituendo violazione del Modello, risulta assoggettata alle previsioni di cui al successivo *"Sistema Sanzionatorio"*.

II. 10.3 Segnalazioni di condotte illecite rilevanti ai sensi del D.Lgs. 231/2001 e violazioni del Modello di Organizzazione Gestione e Controllo - tutela Whistleblowing

VUSCOM, nell'ambito dell'istituto del Whistleblowing – oggetto di riforma ad opera del D. Lgs. n. 24/2023, in attuazione della direttiva (UE) 2019/1937 sulla protezione delle persone che segnalano violazioni del diritto dell'Unione e nazionali – ha implementato un canale interno, gestito dall'RPCT, volto alla segnalazione di comportamenti, atti od omissioni che ledono l'integrità della Società riscontrati durante la propria attività lavorativa/professionale, godendo di un sistema protezionistico basato sulla tutela della riservatezza e sul divieto di applicazione di misure ritorsive nei confronti del soggetto segnalante.
Il canale interno di segnalazione whistleblowing è - in linea con le previsioni dell'art. 6, comma 2 bis, del D.lgs. n. 231/2001 - il mezzo che consente ai soggetti apicali e subordinati di effettuare segnalazioni riguardanti condotte illecite rilevanti ai fini 231 e violazioni del Modello 231.
La Società, mediante specifica Policy, ha, inoltre, reso edotti i Segnalanti dei possibili canali mediante i quali, alle condizioni previste dal Decreto Whistleblowing, è possibile eseguire una Segnalazione:

i. canali interni da considerarsi preferenziali;
ii. un canale esterno da considerarsi residuale ai canali interni nonché da utilizzare nei casi previsti dal legislatore;
iii. divulgazione pubblica da considerarsi residuale ai primi due nonché da utilizzare nei casi previsti dal legislatore.

In via prioritaria, quindi, i Segnalanti sono incoraggiati a utilizzare i canali interni della Società e, solo al ricorrere di certe condizioni, di seguito illustrate, possono essere effettuate le Segnalazioni mediante il canale esterno o mediante la Divulgazione Pubblica.
Inoltre, come previsto dal Decreto Whistleblowing, il Segnalante potrà presentare anche denuncia direttamente all'Autorità competente.

Canali Interni

VUS.COM ha previsto *(Sentite le rappresentanze o le organizzazioni sindacali di cui all'articolo 51 del decreto legislativo n. 81 del 2015)*, in conformità al Decreto Whistleblowing, la predisposizione di canali interni dedicati alle Segnalazioni per consentire a tutti i Segnalanti la possibilità di effettuare Segnalazioni mediante:

i. piattaforma informatica dedicata al Whistleblowing, accessibile al seguente link: https://vuscom.segnalazioni.net/
ii. canale orale che consente di mandare un messaggio vocale tramite la piattaforma informatica di cui al punto i;
iii. su richiesta del Segnalante - avanzata mediante uno dei canali sopra dedicati - mediante incontro diretto fissato entro un termine ragionevole;

Come segnalare tramite il canale interno whistleblowing

Il segnalante, collegandosi all'apposita piattaforma web accessibile dal sito web della Società (sezione Whistleblowing segnalazione interna come fare una segnalazione interna), deve fornire, attraverso un percorso standard con inserimenti obbligati, tutti gli elementi utili a consentire all'RPCT di procedere alle dovute e appropriate verifiche e accertamenti a riscontro della fondatezza dei fatti oggetto di segnalazione.

È necessario che la segnalazione sia il più possibile circostanziata.

In particolare, devono risultare chiare:

- le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione;
- la descrizione del fatto;
- le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

La segnalazione non può riguardare informazioni che sono già totalmente di dominio pubblico, notizie prive di fondamento e le c.d. "voci di corridoio" e/o "dicerie".

È utile anche allegare documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione. Le segnalazioni saranno prese in considerazione solo se adeguatamente

dettagliate e circostanziate, se prive di manifesta portata strumentale ed emulativa, diffamatoria o calunniosa. Al termine dell'inserimento della segnalazione, il sistema genera in automatico un codice numerico che permette al segnalante di:

- accedere direttamente alla segnalazione;
- visualizzare lo stato di avanzamento della segnalazione;
- interloquire con l'RPCT;
- inserire/allegare ulteriori informazioni/dati che ritiene utili a completamento della segnalazione e/o richiesti dall'RPCT.

È onere del segnalante:

prendere correttamente nota del codice numerico e conservarlo con cura;

provvedere alla consultazione periodica della segnalazione sulla piattaforma web al fine di verificare il riscontro dato alla stessa.

In caso di smarrimento, il codice numerico non potrà essere recuperato o duplicato in alcun modo e quindi il segnalante sarà tenuto a effettuare una nuova segnalazione.

La piattaforma web, attraverso l'utilizzo della crittografia, garantisce la sicurezza dei dati comunicati per tutte le evidenze documentali e multimediali fornite in fase di inserimento delle segnalazioni.

La segnalazione, inoltrata attraverso la piattaforma web, sarà inviata automaticamente all'RPCT, unico destinatario in grado di ricevere e gestire la segnalazione.

Qualora la segnalazione interna sia presentata a un soggetto diverso dall'RPCT, attraverso qualsiasi diverso canale, il ricevente dovrà trasmetterla, entro sette giorni dal suo ricevimento, all'RPCT, dando contestuale notizia della trasmissione alla persona segnalante. In tal caso, al fine di godere delle tutele previste dal D.lgs. n. 24/2023, il segnalante dovrà specificare nell'oggetto che trattasi di "SEGNALAZIONE WHISTLEBLOWING".

Gestione della segnalazione interna whistleblowing

L'RPCT, ricevuta la segnalazione, svolge le attività di seguito descritte.

Rilascia alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione.

Valuta la segnalazione al fine di verificarne l'ammissibilità tra i casi di Whistleblowing.

La segnalazione è considerata inammissibile per:

- manifesta mancanza di interesse all'integrità della Società;
- manifesta incompetenza sulle questioni segnalate;
- manifesta infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti;
- accertato contenuto generico della segnalazione tale da non consentire la comprensione dei fatti, ovvero segnalazione corredata da documentazione non appropriata o inconferente;
- produzione di sola documentazione in assenza della segnalazione di condotte illecite o irregolarità;
- mancanza dei dati che costituiscono elementi essenziali della segnalazione.

L'RPCT, ricevuta la segnalazione, ove quanto denunciato non sia adeguatamente circostanziato, può chiedere al segnalante di integrarla, sempre attraverso la piattaforma web, o anche di persona, ove il segnalante acconsenta.

In caso di inammissibilità, l'RPCT comunica l'esito della valutazione al segnalante e la segnalazione si considera "chiusa".

Dà diligente seguito alle segnalazioni ricevute, attivandosi per valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate.

Non spetta all'RPCT accertare le responsabilità individuali, qualunque natura esse abbiano, né svolgere controlli di legittimità o di merito su atti e provvedimenti adottati dalla Società oggetto di segnalazione, a pena di sconfinare nelle competenze dei soggetti a ciò preposti all'interno della Società ovvero della magistratura.

Per lo svolgimento dell'istruttoria, l'RPCT può avviare un dialogo con il segnalante, chiedendo allo stesso chiarimenti, documenti e informazioni ulteriori, tramite la stessa piattaforma web o anche di persona. Ove necessario, può anche acquisire atti e documenti da altri uffici e può avvalersi del loro supporto, può coinvolgere terze persone, tramite audizioni e altre richieste, avendo sempre cura che non sia compromessa la tutela della riservatezza del segnalante, della persona coinvolta nonché del contenuto della segnalazione e della relativa documentazione.

Per svolgere l'attività di verifica e di analisi delle segnalazioni, l'RPCT può avvalersi di un gruppo di lavoro dedicato, composto da soggetti in possesso di competenze trasversali, da costituire mediante un atto formale di volta in volta costituito in ragione delle specifiche competenze richieste dall'attività istruttoria.

Nell'ipotesi in cui la segnalazione abbia rilevanza sul piano 231, l'RPCT chiede collaborazione all'Organismo di Vigilanza per lo svolgimento dell'istruttoria.
Fornisce riscontro alla segnalazione comunicando alla persona segnalante entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione – informazioni relative al seguito che viene dato o che si intende dare alla segnalazione.
Qualora, a seguito dell'attività svolta, l'RPCT ravvisi elementi di manifesta infondatezza della segnalazione, ne dispone l'archiviazione con adeguata motivazione.
Qualora, invece, ravvisi il fumus di fondatezza della segnalazione è opportuno si rivolga immediatamente agli organi preposti interni o enti/istituzioni esterne, ognuno secondo le proprie competenze, trasmettendo una relazione sulle risultanze istruttorie e le attività svolte e avendo sempre cura di tutelare la riservatezza dell'identità del segnalante.
Resta fermo che gli organi riceventi da quel momento agiranno in qualità di titolari del trattamento dei dati.

Flussi informativi verso l'Organismo di Vigilanza

L'OdV dovrà ricevere da parte di gestore della segnalazione (cfr. RPCT):

• immediata informativa su segnalazioni rilevanti in termini 231 affinché, nell'esercizio della sua attività di vigilanza, possa condividere le proprie eventuali osservazioni e partecipare all'istruttoria o comunque seguirne l'andamento;

• un aggiornamento periodico sull'attività complessiva di gestione delle segnalazioni, anche non 231, al fine di verificare il funzionamento del sistema whistleblowing e proporre all'ente eventuali necessità di suo miglioramento

Protezione dalle ritorsioni

Non si possono porre in essere ritorsioni in ragione della segnalazione inviata.
A norma del D. Lgs. n. 24/2023, soggetti tutelati dalle ritorsioni sono:

- il soggetto segnalante;
- il facilitatore (persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza viene mantenuta riservata);
- le persone del medesimo contesto lavorativo della persona segnalante e che sono legate a esso da uno stabile legame affettivo o di parentela entro il quarto grado;
- i colleghi di lavoro della persona segnalante che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
- gli enti di proprietà della persona segnalante o per i quali la stessa persona lavora, nonché agli enti che operano nel medesimo contesto lavorativo della predetta persona.

Il sistema di protezione è subordinato a due condizioni (che devono coesistere):
a) al momento della segnalazione, la persona segnalante aveva fondato motivo di ritenere che le informazioni sulle violazioni segnalate fossero vere - non sono sufficienti invece semplici supposizioni o voci di corridoio così come notizie di pubblico dominio; non rileva invece, ai fini delle tutele, la circostanza che il soggetto abbia segnalato pur non essendo certo dell'effettivo accadimento dei fatti segnalati o denunciati e/o dell'identità dell'autore degli stessi o riportando anche fatti inesatti per via di un errore autentico;
b) la segnalazione è stata effettuata in conformità alle disposizioni aziendali sull'utilizzo del canale interno whistleblowing innanzi riportate – nel caso di segnalazioni interne inviate a un soggetto diverso dal Presidente dell'Organismo di Vigilanza, tale soggetto deve trasmetterle senza ritardo al soggetto autorizzato a ricevere e gestire le segnalazioni, dando contestuale notizia della trasmissione alla persona segnalante. Al fine di consentire tale trasmissione tempestiva, il segnalante deve indicare chiaramente nell'oggetto della segnalazione (e/o sulla busta, in caso si scelga la posta ordinaria come mezzo di comunicazione) che si tratta di "SEGNALAZIONE WHISTLEBLOWING".
Quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia o, comunque, per i medesimi reati commessi

con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave, le tutele qui descritte non sono garantite e alla persona segnalante o denunciante è irrogata una sanzione disciplinare.

Cosa si intende per ritorsione

Per ritorsione si intende qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto. Di seguito sono indicate, a titolo esemplificativo e non esaustivo, talune fattispecie che costituiscono ritorsioni:

a) il licenziamento, la sospensione o misure equivalenti;

b) la retrocessione di grado o la mancata promozione;

c) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;

d) la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;

e) le note di merito negative o le referenze negative;

f) l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;

g) la coercizione, l'intimidazione, le molestie o l'ostracismo;

h) la discriminazione o comunque il trattamento sfavorevole;

i) la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;

l) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;

m) i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;

n) l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;

o) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;

p) l'annullamento di una licenza o di un permesso;

q) la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

A chi comunicare le ritorsioni subite

I soggetti tutelati possono comunicare all'ANAC, tramite i canali dalla stessa attivati (cfr. sito web ANAC), le ritorsioni che ritengono di aver subito.

L'ANAC informa l'Ispettorato Nazionale del Lavoro per i provvedimenti di propria competenza.

Al fine di acquisire elementi istruttori indispensabili all'accertamento delle ritorsioni, l'ANAC può avvalersi della collaborazione dell'Ispettorato Nazionale del Lavoro, ferma restando l'esclusiva competenza dell'ANAC in ordine alla valutazione degli elementi acquisiti e all'eventuale applicazione delle sanzioni amministrative di cui all'articolo 21 del D.lgs. n. 24/2023.

Nullità degli atti ritorsivi

Ai sensi dell'art. 19, co. 3, del D.lgs. n. 24/2023,

gli atti eventualmente assunti in violazione del divieto di ritorsione sono nulli;

se una persona viene licenziata in seguito a segnalazione/denuncia avrà diritto a essere reintegrata nel posto di lavoro.

La dichiarazione di nullità degli atti ritorsivi spetta all'autorità giudiziaria.

L'autorità giudiziaria adotta tutte le misure, anche provvisorie, necessarie ad assicurare la tutela alla situazione giuridica soggettiva azionata, ivi compresi:

il risarcimento del danno;

la reintegrazione nel posto di lavoro;

l'ordine di cessazione della condotta ritorsiva;

la dichiarazione di nullità degli atti adottati.

Inversione dell'onere della prova

Nell'ambito di procedimenti giudiziari o amministrativi o comunque di controversie stragiudiziali aventi a oggetto l'accertamento dei comportamenti, atti o omissioni vietati posti

in essere nei confronti del soggetto segnalante, si presume che gli stessi siano stati realizzati a causa della segnalazione. L'onere di provare che tali condotte o atti sono motivati da ragioni estranee alla segnalazione è a carico di colui che li ha posti in essere.

In caso di domanda risarcitoria presentata all'autorità giudiziaria dal soggetto segnalante, se tale soggetto dimostra di aver effettuato, ai sensi del D.lgs. n. 24/2023, una segnalazione, una divulgazione pubblica o una denuncia all'autorità giudiziaria o contabile e di aver subito un danno, si presume, salvo prova contraria, che il danno sia conseguenza di tale segnalazione, divulgazione pubblica o denuncia all'autorità giudiziaria o contabile.

Per ogni ulteriore specifica sull'istituto del whistleblowing si rinvia a quanto pubblicato in apposita sezione del sito web aziendale.

Apparato sanzionatorio

Sono fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente procedura, quali segnalazioni che si rivelino infondate, effettuate con dolo o colpa grave, ovvero quelle manifestamente opportunistiche e/o compiute al solo scopo di danneggiare il denunciato o altri soggetti, nonché ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione della presente Procedura.

Sono analogamente sanzionate, ai sensi dell'art. 17 del D.lgs. 24/2023, anche tutte le accertate violazioni delle misure poste a tutela del segnalante, compresi tutti gli atti discriminatori adottati dalla Società nei confronti del segnalante medesimo (rif. art. 17 co. 4 del D.lgs. 24/2023) ovvero pressioni o discriminazioni volte ad influenzare l'istruttoria.

Le sanzioni disciplinari saranno proporzionate all'entità e gravità dei comportamenti illeciti accertati e potranno anche giungere alla risoluzione del rapporto di lavoro ovvero di consulenza, nel rispetto delle disposizioni di legge applicabili nonché delle normative di CCNL del settore di riferimento.

In particolare si evidenzia che, al fine di garantire la tutela del Segnalante, il Sistema Disciplinare del Modello 231 prevede che siano sanzionati atti di ritorsione o discriminatori posti in essere nei confronti di chi abbia effettuato la segnalazione di una condotta illecita, rilevante ai fini del D.Lgs. 231/2001, o di una violazione del Modello o del Codice di Condotta così come eventuali violazioni degli obblighi di riservatezza sull'identità del Segnalante.

Per le sanzioni si richiama il Sistema disciplinare del presente Modello 231 (Cap. II.12).

II. 10.4 Flussi informativi verso il Consiglio di Amministrazione e il Collegio Sindacale

L'Organismo di Vigilanza predispone annualmente una relazione di sintesi che ha per oggetto l'attività svolta nell'anno di riferimento ed ha come destinatario il Consiglio di Amministrazione.

Tale documento riporta la descrizione delle attività programmate dall'OdV per l'anno successivo a quello in corso, unitamente al correlato budget di spesa, da sottoporre al Consiglio di Amministrazione.

Inoltre, l'OdV riferisce senza indugio al Consiglio di Amministrazione e al Collegio Sindacale in merito a circostanze e fatti significativi del proprio ufficio o a eventuali urgenti criticità del Modello emerse nell'ambito dell'attività di vigilanza.

II.11 - FORMAZIONE

L'art. 6 co. 2 lett. b) prevede l'obbligo di definire specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire.

Tutti coloro che operano per conto dell'ente devono essere informati e ricevere formazione sugli aspetti rilevanti della norma, le regole decise dall'ente in materia, le responsabilità e le conseguenze per la mancata osservanza delle regole.

La formazione è elemento primario del sistema di sicurezza e prevenzione dei reati previsti dal D.lgs. 231/2001.

Le attività di formazione devono essere programmate e diversificate tenendo conto delle necessità specifiche dei destinatari.

L'attività di formazione deve essere misurata al fine di verificarne l'efficacia.

Le responsabilità per la formazione devono essere chiaramente attribuite.

La formazione deve essere aggiornata quando intervengono modifiche rilevanti del MOG ovvero quando da controlli sull'efficacia o sui livelli di consapevolezza dei destinatari ne emerga la necessità.

II.12 - SISTEMA DISCIPLINARE

L'art. 6 co.2 lett. e) prevede l'obbligo di conformare il sistema disciplinare in modo da renderlo idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il Sistema Disciplinare prevede le azioni da assumere in caso di comportamenti scorretti rilevanti ai fini del D.Lgs. 231/2001 tenuti da: dipendenti, collaboratori, amministratori e chiunque altro opera in nome o per conto dell'Ente.

In particolare, per quanto riguarda i dipendenti, coerentemente a quanto previsto dall'art. 7 della L. 300/1970 (Statuto dei lavoratori), le conseguenze disciplinari per il mancato rispetto delle decisioni adottate dall'Ente riguardo la conformità al D.lgs. 231/2001 devono essere chiaramente e specificamente formalizzate nel Sistema Disciplinare. Le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti. Esse devono applicare quanto in materia è stabilito da accordi e contratti di lavoro di riferimento. Il datore di lavoro non può adottare alcun provvedimento disciplinare nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa.

Le responsabilità per i controlli e per le contestazioni disciplinari devono essere chiaramente e specificamente definite e portate a conoscenza con idonei mezzi a tutti gli interessati.

L'introduzione ed adozione di un sistema disciplinare idoneo a sanzionare il mancato rispetto del Modello è una delle condizioni inderogabili di idoneità del Modello medesimo e di efficacia della sua attuazione.

Le sanzioni devono essere chiare e proporzionate alla gravità dell'inosservanza del Modello, devono tenere conto di tutti i soggetti interessati dal Modello a tutti i livelli (dipendenti, dirigenti, vertici amministrativi, collaboratori, ecc.) e devono essere portate a conoscenza degli interessati con mezzi idonei.

QUADRO NORMATIVO DI RIFERIMENTO

Il presente documento è redatto in riferimento e nel rispetto delle seguenti normative:

- Codice Civile

- L.300/1970 e s.m.i. Statuto dei Lavoratori (SL)
- CCNL di riferimento
- D.lgs. 196/2003 e s.m.i. Codice della Privacy (C.PRI.)
- GDPR 679/2016 e s.m.i.
- D.lgs. 231/2001 e s.m.i. Responsabilità Amministrativa (231)
- D.lgs. 81/2008 e s.m.i. Testo Unico per la Sicurezza sul Lavoro (TUS)

AMBITO DI APPLICAZIONE

Questo regolamento si applica a tutti coloro i quali svolgono attività sensibili ai sensi del D.Lgs. 231/2001.

INTERPRETAZIONE

Il presente documento deve essere interpretato conformemente al Codice Civile ed alla normativa di settore con particolare riferimento a quella giuslavoristica ivi inclusi i CCNL di lavoro vigenti; eventuali disposizioni che dovessero essere difformi, od in contrasto o peggiorative dei diritti inderogabili dei lavoratori devono essere disapplicate e segnalate al Datore di Lavoro al fine di consentire l'aggiornamento del presente documento.
Nel prosieguo del documento con il termine "Modello" si intende il Modello di Organizzazione e Gestione adottato dall'Ente, nelle sue parti, ivi inclusi i regolamenti, le procedure ed ogni altra regola organizzativo-gestionale ad esso complementare o sussidiaria.

DIPENDENTI

Il mancato rispetto delle regole previste dal Modello, delle direttive ed istruzioni emanate in attuazione del Modello, ovvero in esecuzione di un obbligo di legge cui l'Ente è soggetto, costituisce per i dipendenti inadempimento del contratto di lavoro ai sensi dell'art. 2104 Cod. Civ. e può dar luogo alla applicazione di sanzioni disciplinari a norma dell'art. 2106 Cod. civ. in conformità a quanto previsto dall'art.7 L. 300/1970.

DIRIGENTI

Qualsiasi comportamento difforme od in violazione del Modello da parte di dirigenti, ove presenti, come pure l'inosservanza, costituisce inadempimento del contratto di lavoro e comporta l'applicazione di sanzioni disciplinari in conformità ai CCNL vigenti di riferimento.

COLLABORATORI

Coloro i quali prestano la propria opera a titolo diverso dai due punti che precedono, sono tenuti al rigoroso e puntuale rispetto del Modello, ogni violazione costituisce inadempimento del contratto da cui discende il rapporto con l'Ente.
I contratti di collaborazione devono considerare espressamente:

- che il rispetto del Modello è motivo essenziale del contratto medesimo,
- che ogni violazione del Modello costituisce inadempimento contrattuale,
- che l'Ente si riserva di controllare l'esatto adempimento con particolare riferimento al rispetto del Modello

e prevedere idonee clausole (risolutive e/o penali) atte a contrastare le eventuali violazioni.

FORNITORI DI SERVIZI

Coloro i quali svolgono forniture all'Ente, limitatamente alle attività sensibili ai sensi del D.Lgs. 231/2001, sono tenuti al rigoroso e puntuale rispetto del Modello, ogni violazione costituisce inadempimento del contratto da cui discende il rapporto con l'Ente.
I contratti di fornitura devono considerare espressamente:

- che il rispetto del Modello è motivo essenziale del contratto medesimo,
- che ogni violazione del Modello costituisce inadempimento contrattuale,
- che l'Ente si riserva di controllare l'esatto adempimento con particolare riferimento al rispetto del Modello,

e prevedere idonee clausole (risolutive e/o penali) atte a contrastare le eventuali violazioni.

PARTNER

Coloro i quali che cooperano con l'Ente, sono tenuti al rigoroso e puntuale rispetto del Modello, ogni violazione costituisce inadempimento agli accordi di cooperazione.
Gli accordi di cooperazione devono considerare espressamente:

- che il rispetto del Modello è motivo essenziale dell'accordo,
- che ogni violazione del Modello costituisce inadempimento delle intese,
- che l'Ente si riserva di controllare l'esatto adempimento con particolare riferimento al rispetto del Modello,

e prevedere idonee clausole (risolutive e/o penali) atte a contrastare le eventuali violazioni.

VERTICI AMMINISTRATIVI

I vertici amministrativi provvedono ad autoregolamentare le proprie attività in modo da assicurare il rispetto del Modello da parte dei propri membri.
Il rispetto del Modello deve essere assunto come condizione inderogabile dello status di membro dei vertici tale che l'inosservanza possa costituire valido motivo di revoca.

Gli organi di controllo (Collegio Sindacale, Revisori, Organismo di Vigilanza) segnalano ai vertici ogni violazione del Modello affinché essi possano assumere le azioni correttive idonee al caso.
In caso di inerzia dei vertici ne è data comunicazione alla Assemblea, se l'inosservanza costituisce reato, gli organi di controllo, nell'inerzia dei vertici, ne danno comunicazione alle competenti Autorità.

FUNZIONI DI CONTROLLO

Gli Organi di Controllo, nel rispetto dell'autonomia ed imparzialità che è loro propria, provvedono ad autoregolamentare le proprie attività in modo da assicurare il rispetto del Modello da parte dei propri membri.
Il rispetto del Modello deve essere assunto come condizione inderogabile dello status di

membro tale che l'inosservanza possa costituire valido motivo di revoca.

VALIDITÀ - MODIFICHE

Ogni modifica deve essere previamente approvata dalla competente autorità dell'ente.
Le modifiche sono efficaci dal momento dell'approvazione.
Le modifiche approvate devono essere portate a conoscenza dei destinatari, tempestivamente, con i mezzi più idonei.
In ogni caso alcuna sanzione potrà essere assunta se non previamente comunicata.

CHIUSURA

Per quanto non espressamente regolato si rinvia alla normativa in materia prevista dal Codice Civile, dallo Statuto dei Lavoratori, dai CCNL vigenti, da tutte le altre norme nazionali ed europee applicabili.

SOMMARIO

ALLEGATI:

1) CODICE ETICO;

2) REATI 231 E MODALITA' ATTUATIVE;

3) MIAR risk assestment;

4) REGOLAMENTO FLUSSI INFORMATIVI.