VALLE UMBRA SERVIZI S.P.A.

CORPORATE GOVERNANCE – D.L.VO 231/2001

MODELLO ORGANIZZATIVO E DI GESTIONE

PARTE I

Approvato il 15 gennaio 2013

INTRODUZIONE

IL D.L.VO 231/2001

Il D.L.vo 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.L.vo 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.

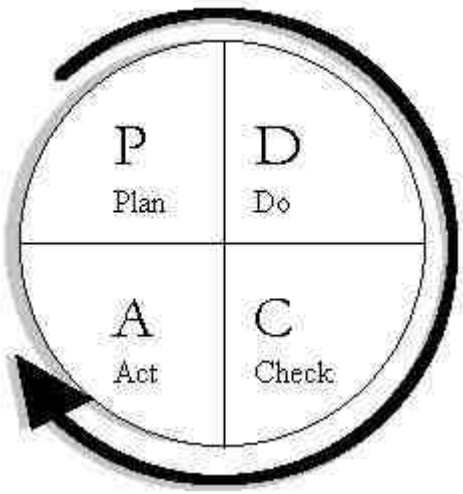
IL PROCESSO "231"

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.L.vo 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. OPERATIVO
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:

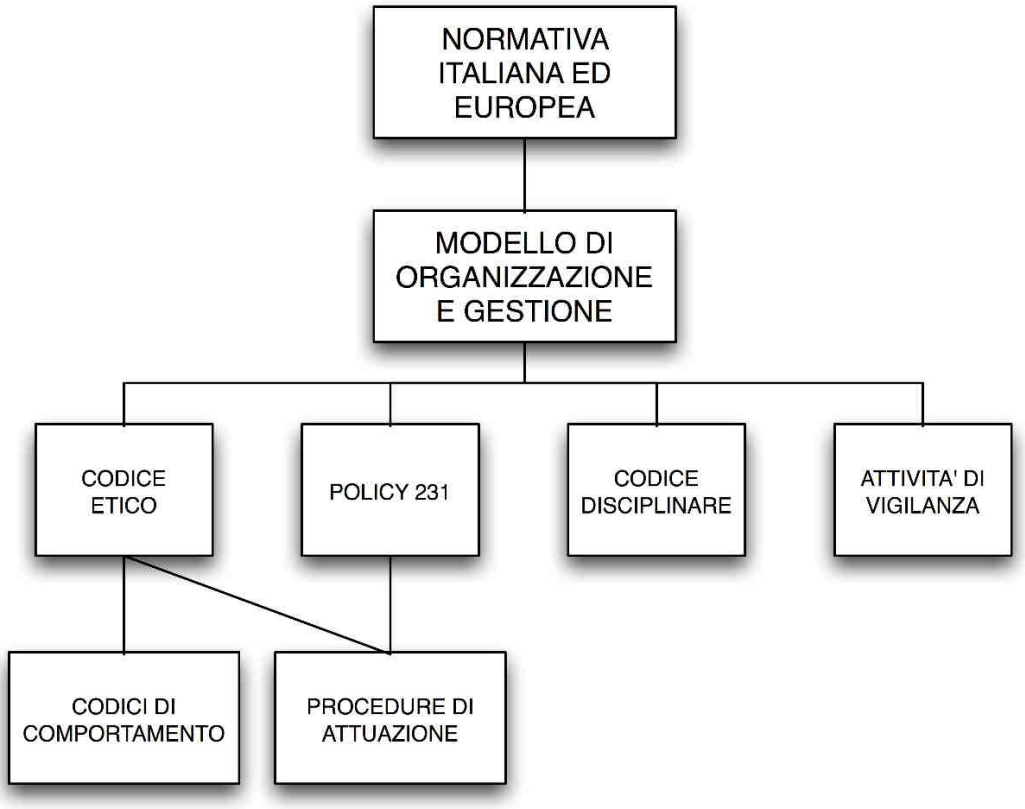
- Strategia ovvero l'area propria del Consiglio di Amministrazione; questa area ha la responsabilità della organizzazione dell'associazione che guida ed indirizza. Questa area esercita al massimo livello i poteri decisionali inclusi quelli di disposizione delle risorse.
- Gestione, ovvero l'area propria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



Il documento che segue è il Modello di Organizzazione e Gestione predisposto ed approvato da Valle Umbra Servizi in ottemperanza ed in conformità al D.L.vo 231/2001.

Esso si compone di tre parti:

I) la prima parte contiene le enunciazioni di carattere generale e di contenuto programmatico. Essa si divide in due sezioni: la prima sezione è intitolata "Dichiarazioni" in essa sono contenute le informazioni che descrivono l'ambiente in cui è stato sviluppato il MOG, la seconda parte si intitola "Principi" e contiene i principi generali che guidano l'organizzazione dell'ente coerentemente a quanto stabilito nel Codice Etico, e nel rispetto dell'ordinamento giuridico italiano.

II) La seconda parte contiene la parte di analisi e si divide in tre sezioni:
   a. la prima intitolata "Ricognizione", contiene i dati, forniti dall'ente, sui quali è stata svolta l'analisi dei rischi.
   b. La seconda sezione intitolata "Analisi", contiene la parte di analisi dei rischi inclusi gli scenari che individuano la collocazione del rischio all'interno dell'ente.
   c. La terza sezione intitolata "Riepilogo", contiene la sintesi delle risultanze dell'analisi ed evidenzia le criticità individuate.

III) La terza parte, infine, contiene gli allegati, ovvero la documentazione rilevante in materia di supporto ad una corretta organizzazione dell'ente e si divide in sei sezioni:
   a. Codice Etico, contiene i principi etici che guidano in ogni attività l'ente.
   b. Policy "231", contiene i principi e le regole per la gestione e mantenimento del processo "231".
   c. Codici di comportamento, contiene i codici che fissano le regole per i comportamenti corretti da tenere in situazioni potenzialmente critiche

agli effetti del processo "231".

d. Procedure di attuazione, contiene le procedure e la documentazione a livello di gestione ed operativo, rilevanti per la corretta ed efficace attuazione del Modello di Organizzazione e Gestione.
e. Sistema di vigilanza, contiene le disposizioni che regolano la costituzione ed il funzionamento dell'Organismo di vigilanza, con particolare riferimento all'autonomia dell'organismo rispetto gli altri organismi dell'ente.
f. Sistema disciplinare, contiene le disposizioni rilevanti ai fini del processo "231".

Tutte e tre le parti sono tra loro inscindibili e costituiscono il Modello Organizzativo e di Gestione.

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.L.vo 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.L.vo 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.L.vo 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 sanzionato rio previsto dall'art. 10 del D.L.vo 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 del Sistema informativo secondo il quale 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.

SISTEMA INFORMATIVO DI VIGILANZA (SIV), 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.L.vo 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.L.vo 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 e Gestione è la Valle Umbra Servizi S.P.A., di seguito più brevemente denominato "VUS S.p.a.", con sede in Via Antonio Busetti N 38/40, CAP 06049 SPOLETO (PG). C.F.-P. IVA: 02569060540

I.2. RAPPRESENTANZA LEGALE

La rappresentanza dell'Ente di fronte ai terzi ed in giudizio spetta al Presidente del Consiglio di amministrazione nella persona di Salari Maurizio nato a Foligno il 7 gennaio 1945, residente in Foligno via Cesare Battisti n.8.

I.3. NATURA E DESCRIZIONE

Il gruppo VUS è una realtà economica umbra fortemente radicata nel territorio, che eroga servizi pubblici nei comuni del comprensorio folignate, spoletino e della Valnerina. E' costituito dal capogruppo Valle Umbra Servizi S.p.a. e dalle aziende controllate Vus Com (100%) che si occupa dell'acquisto e vendita del gas metano per usi civili ed industriali e Vus GPL (51%) che si occupa dell'approvvigionamento e della vendita del GPL e della gestione e sviluppo di impianti e reti GPL. Valle Umbra Servizi è titolare della quota pari al 30% del capitale sociale della societa' ICT Valle Umbra s.r.l. che si occupa di servizi informatici e di telecomunicazioni.

I principali eventi che riguardano la storia della VUS Spa sono i seguenti:

- dicembre 2001: costituzione della Valle Umbra Servizi Scpa (quota paritaria tra ASE Spa ed ASM Spa)
- gennaio 2002: gestione del servizio idrico integrato per tutti i comuni dell'ATO
- luglio 2002: trasformazione della Valle Umbra Servizi Scpa in Spa. Tutti i 22 Comuni dell'ATO ne diventano i soci. Gestione del servizio gas per 8 Comuni.
- dicembre 2002: costituzione di Vus Com per la commercializzazione del gas
- dicembre 2003: incorporazione di Ase Spoleto Spa a Asm Spa
- marzo 2004: costituzione di Vus Gpl per la gestione del servizio distribuzione Gpl attraverso le reti urbane
- Settembre 2004 : acquisizione partecipazione in ICT Valle Umbra Servizi s.r.l. per la gestione dei servizi di telecomunicazione

- dicembre 2005: incorporazione della Csa Spa con acquisizione del servizio di igiene urbana in 12 Comuni dell'Ato e delle partecipazioni di Csa Spa nelle aziende Trec Spa e Centro Ambiente Spa.

- Dicembre 2008: acquisizione del controllo totale della Centro Ambiente Spa

- Febbraio 2012: fusione per incorporazione di Vus Spa e di Centro Ambiente Spa.

Le attività svolte riguardano tre settori:

Energetico: Il capogruppo Valle Umbra Servizi S.p.a. gestisce la distribuzione del gas metano, Vus Com si occupa della vendita del gas metano e Vus Gpl della vendita del Gpl. Il servizio svolto prevede tutte le attività, eseguite direttamente o tramite strutture esterne. Il servizio comprende la gestione delle infrastrutture di rete, degli impianti e dei punti di distribuzione del gas.

Idrico: la società capogruppo Vus S.p.a. che gestisce il ciclo idrico integrato che comprende la captazione, il trasporto, la distribuzione di acqua potabile fino all'utente finale, nonché la gestione delle rete fognaria e degli impianti di depurazione in base all'affidamento del servizio da parte dell'ATI n° 3 del 27/12/2001.

Il servizio svolto prevede tutte le attività, eseguite direttamente o tramite strutture esterne.

Ambientale: la società capogruppo Valle Umbra Servizi Spa si occupa della raccolta, del trasporto, e dello smaltimento dei rifiuti e dello spazzamento, e, dopo la fusione con la società controllata Centro Ambiente S.p.a. della gestione degli impianti di smaltimento dei rifiuti

I.4. LA MISSIONE

La politica aziendale per la qualità, l'ambiente e la sicurezza è la "radice" da cui si sviluppa il sistema integrato di gestione ed è espressa in uno specifico documento; questo è pubblicato utilizzando diversi supporti ed è a disposizione di chiunque ne faccia richiesta.

La dichiarazione di politica aziendale è aggiornata in funzione degli sviluppi e dei programmi aziendali fissati a medio termine; il documento è posto all'attenzione e viene portato a conoscenza di tutto il personale dell'azienda oltre che delle altre parti interessate alla materia.

La politica aziendale, partendo dall'attenzione verso i clienti e le altre parti interessate, in conformità alla regolamentazione stabilita dalle leggi nazionali e regionali per le aziende che operano nel campo dei servizi pubblici ed in particolare del servizio idrico integrato , della distribuzione di gas, e del servizio di igiene urbana, fissa gli impegni ed i principi generali ai quali il sistema di gestione si uniforma.

L'attuazione della politica aziendale si realizza attraverso quanto pianificato nel sistema di gestione per la qualità e l'ambiente; il miglioramento continuativo dei risultati aziendali, della soddisfazione del cliente e delle prestazioni ambientali è garantito con l'adozione di programmi annuali, che sono il livello operativo di pianificazione direzionale, definendo obiettivi, traguardi e risultati attesi, modalità, risorse necessarie, ruoli coinvolti, tempi previsti.

Un sistema di monitoraggio snello e completo, che riguardi la soddisfazione del cliente, i risultati ambientali, i risultati interni, i punti di forza e di debolezza, gli audit interni e le azioni di miglioramento, ci consente di conoscere lo stato del sistema di gestione e di pianificare adeguatamente il riesame direzionale.

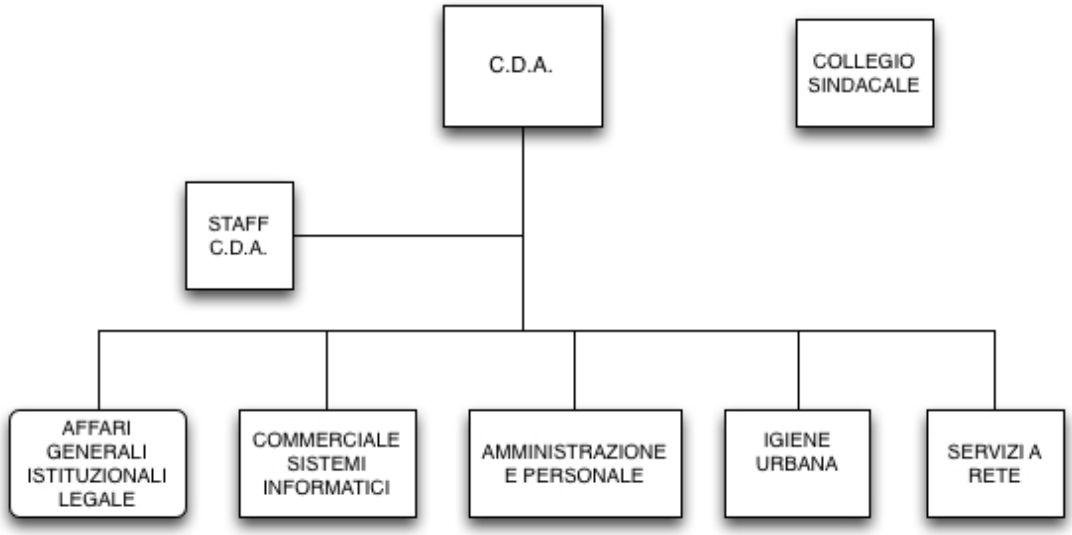
Il riesame direzionale è la cabina di regia del miglioramento continuativo; esso è il primo meccanismo per il costante adeguamento della pianificazione del sistema di gestione, con il quale si verifica l'impatto della politica, l'efficacia e l'adeguatezza del sistema di gestione e l'attuazione dei programmi stabiliti, provvedendo poi alle azioni conseguenti

ed opportune

I.5. AMMINISTRAZIONE

La società è amministrata da un consiglio di amministrazione formato da tre membri, anche non soci, ivi compreso il presidente che svolga anche le funzioni di amministratore delegato. Gli amministratori durano in carica per il periodo stabilito alla loro nomina e comunque non oltre i tre esercizi. Essi scadono in concomitanza con l'approvazione del bilancio relativo all'ultimo esercizio del loro mandato; gli stessi sono rieleggibili a norma dell'art. 2383 c.c. Il Consiglio di amministrazione potrà nominare tra i propri componenti un vicepresidente .

I.6. ORGANIGRAMMA



I.7. CONDIZIONI

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

I.8. NORMATIVA

Questo Modello di Organizzazione e Gestione è stato sviluppato in conformità al

D.L.vo 231/2001 e successive modificazioni ed integrazioni alla data del gennaio 2012.

I.9. 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.L.vo 231/2001 – Confindustria 2004.
- ISO/EC 38.5000 (IT Governance) per quanto riguarda i principi di governo del sistema informatico.

I.10. 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.L.vo

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.L.vo 231/2001.

I.11. 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.

I.12. ESTENSORI

Il documento è adottato dal Consiglio di amministrazione con l'assistenza e consulenza dell'avvocato Frillici Alessandro:

I.13. DATE E TERMINI

Questo Modello Organizzativo e di Gestione è stato sviluppato sulla base delle informazioni alla data del 12 settembre 2012.

Esso è stato approvato dal Consiglio di amministrazione in data 15 gennaio 2013, che ne ha disposto l'immediata adozione.

Tutti coloro i quali rivestono le figure di soggetti apicali o sottoposti come meglio definito dal D.L.vo 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, in conformità con il Codice Etico, 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 di della Valle Umbra Servizi S.p.a.

II.1. - ETICITA'

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

La Vus Spa, in conformità a quanto previsto nel Codice Etico, 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 Spa 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.l.vo 231/2001

La Vus Spa si impegna a ridurre i rischi di commissione dei reati previsti dal D.L.vo 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.

Il processo "231" è dettagliatamente descritto nella sezione b) della III Parte di questo documento.

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 quali ad esempio gli standard AS/NZS 4360:2004 oppure M_o_R Risk Management.

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.L.vo 231/2001 con riferimento alla attività in esame. I ruoli, poteri e responsabilità per le analisi dei rischi devono essere chiaramente e specificamente allocate.

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 indipendente 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.

[1] Col termine stakeholder si individuano i soggetti sostenitori nei confronti di una iniziativa economica.

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 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.

Le regole per la tutela dei dati personali in conformità al D.L.vo 196/2003 sono contenute nel Documento Programmatico sulla Sicurezza (DPS) cui si rinvia.

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 al 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 e 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.L.vo 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.

Il sistema di controllo e vigilanza deve documentare l'effettuazione dei controlli, anche di supervisione; il sotto-processo "documentazione di vigilanza" è parte del processo "231" contenuto nella sezione b) della III Parte di questo documento.

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 S.p.a. 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 S.p.a. 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 S.p.a. adotta un sistema di gestione della salute e della sicurezza sul lavoro (SGSL) conforme alle linee guida OHSAS.

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.L.vo 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.L.vo 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.L.vo 196/2003 è parte integrante della sicurezza del Sistema Informativo.
L'Ente organizza e gestisce la sicurezza del SI ispirata ai principi dell'ISO 27001, così come meglio definito dal DPS, i cui principi e norme sono estesi anche ai dati anonimi.

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.L.vo 231/2001.
L'art. 6 co. 2 lett. c) del D.L.vo 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 incrociato del collegio sindacale e dei revisori dei conti.

II.10 - VIGILANZA ED AGGIORNAMENTO

L'art. 6 co.1 lett. b) D.L.vo 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'art.6 co. 4 D.L.vo 231/2001

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.
Il processo "Vigilanza" è meglio definito nella sezione e) della III Parte di questo documento "Sistema di vigilanza" nel rispetto dei principi contenuti nella policy dell'Organismo di vigilanza.
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.
Il sotto-processo "Revisione" è parte del processo "231" descritto nella sezione b) della III Parte di questo documento.

II.11 - COMUNICAZIONI

L'art. 6 co. 2 lett. d) del D.L.vo 231/2001 prevede l'obbligo di organizzare un sistema di informazioni nei confronti di chi è tenuto alla vigilanza.
Tale sistema è definito nel sotto-processo "Sistema di informazioni di vigilanza" (SIV) che è parte del processo "231"
Il processo è assegnato ad un responsabile che ha l'onere di garantirne l'efficace attuazione e l'aggiornamento.
Il SIV definisce il contenuto delle informazioni che obbligatoriamente devono essere trasmesse all'Organismo di vigilanza, individuando coloro che devono effettuare le comunicazioni, le modalità ed i tempi.
Le informazioni trasmesse a chi effettua la vigilanza devono soddisfare alti livelli di integrità, disponibilità, riservatezza ed autenticità.
Devono essere individuati e stabiliti idonei canali di comunicazione verso chi effettua la

vigilanza, attraverso i quali tutti coloro che operano per l'ente possano segnalare fatti rilevanti ai fini del D.L.vo 231/2001 (quali ad esempio incidenti di sicurezza, violazioni o sospetto di violazioni delle norme previste dal MOG).
Nel caso in cui la vigilanza sia affidata ad un organismo autonomo deve essere parimenti garantito un efficace sistema di comunicazione verso i vertici dell'ente.

II.12 - 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.L.vo 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.
Il sotto-processo "formazione 231" è parte del processo "231" contenuto nella sezione b) della III Parte di questo documento.

II.13 - 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.L.vo 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.

Il Sistema Disciplinare rilevante ai fini del processo "231" è riportato nella sezione f) della III Parte di questo documento.

SOMMARIO