Piano Regionale di Prevenzione 2014 -2018

(Prorogato sino al 2020)

Programma P-7.4

Miglioramento dell'efficacia delle attività di controllo e della compliance

Pianificazione delle azioni: P-7.4.3.5: divulgazione materiale sui principali MOG SGSL

Lo S.Pre.S.A.L. dell'ASSL di Oristano con il presente documento provvede alla divulgazione, attraverso il sito Web della ASL, dei principali MOG (Modelli di Organizzazione e Gestione) e SGSL (Sistemi di Gestione per la Sicurezza sul Lavoro), della normativa di recepimento (DM 13 Febbraio 2014) delle Procedure Semplificate approvate dalla Commissione Consultiva Permanente ex art.6 D.lgs. 81/2008 per l'adozione e l'efficace attuazione dei MOG e dei SGSL nelle piccole e medie imprese, ai sensi dell'art. 30 c. 5-*bis* del D.lgs. 81/2008 al fine di contribuire a promuovere e diffondere una cultura sulla gestione sistemica delle attività di prevenzione in materia di Sicurezza e Igiene dei luoghi di lavoro.

"DAL D.LGS. 231/01 AI MODELLI DI GESTIONE, ORGANIZZAZIONE E CONTROLLO SECONDO L'ART. DEL D.LGS 81/08"

INDICE

Introduzione

Il decreto Legislativo 8 giugno 2001 n. 231 ("Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica") *rappresenta l'epilogo di un lungo cammino volto a contrastare il fenomeno della criminalità d'impresa, attraverso il superamento del principio, insito nella tradizione giuridica nazionale, "**societas delinquere non potest***[1]" [Corte di Cassazione, Sezioni Unite Penali, Sentenza 27 marzo 2008 (dep. 2 luglio 2008), n. 26654][2].

Il D.lgs.231/01 ha, infatti, introdotto, per la prima volta nell'ordinamento giuridico italiano, un regime di responsabilità amministrativa a carico degli enti per alcuni reati commessi o anche solo tentati nell'interesse o a vantaggio degli stessi o di una propria unità organizzativa, da individui che rivestono funzioni di rappresentanza, di amministrazione o di direzione o da persone sottoposte alla direzione o alla vigilanza da parte di uno dei soggetti sopraindicati.

La responsabilità amministrativa delle persone giuridiche derivante da reato penale di cui al D.lgs. n. 231/01 è perfettamente inquadrata dalla Sentenza Thyssenkrupp del 14 novembre 2011, n. 31095 [3]: "*La responsabilità delle persone giuridiche (precisamente degli "enti"), fino ad allora sconosciuta nel nostro sistema giuridico, è stata introdotta con il D.lgs. n. 231/2001, in esecuzione della Convenzione OCSE del 17/12/1997, sulla lotta alla corruzione dei pubblici ufficiali stranieri e del secondo protocollo del 19/6/1997, sulla tutela degli interessi finanziari delle Comunità Europee: entrambi atti che prevedono appunto la responsabilità della persona giuridica, in linea con quanto già stabilito in molti Stati e nell'elaborazione di reati in sede internazionale (Unione Europea, Consiglio d'Europa, Nazioni Unite). Con la legge n. 300/2000, il cui articolo 11 conteneva la delega al Governo in materia, il Parlamento ha indicato i principi fondamentali: per quanto qui rileva, la scelta di gravare gli enti di una **responsabilità amministrativa e non penale;** i diversi criteri di incolpazione a seconda che autori del reato siano i vertici ovvero semplici dipendenti; l'applicazione delle norme del codice di procedura penale, in quanto compatibili; l'irrogazione delle sanzioni da parte del Giudice che conosce il reato (commesso dalla o dalle persone fisiche*)".

La responsabilità penale è l'attribuzione materiale e psicologica ad un soggetto, di un fatto considerato penalmente illecito, con conseguente applicazione di una sanzione penale (ergastolo, reclusione, arresto, ammenda, multa). Il motivo per il quale le persone giuridiche non possono essere responsabili penalmente è indicato all'interno della nostra Costituzione all'art. 27 comma 1 che recita "*la responsabilità penale è personale*", ad indicare che ciascuno (in quanto

[1]Trad. "le persone giuridiche non possono delinquere".

[2]Corte di Cassazione, Sezioni Unite Penali, Sentenza 27 marzo 2008 (dep. 2 luglio 2008), n. 26654.

[3]Tribunale di Torino, Seconda Corte di Assise, 14 novembre 2011, n. 31095 - Sentenza Thyssenkrupp

persona fisica) è responsabile esclusivamente per le proprie azioni e che nessuno può essere punito penalmente per un reato commesso da altri; per questa ragione non è possibile punire penalmente le persone giuridiche. La nuova forma di responsabilità, introdotta dal D.lgs. n. 231/01, mira a coinvolgere nella punizione di taluni illeciti penali il patrimonio degli enti e gli interessi economici dei soci che, precedentemente, non subivano conseguenze in seguito alla realizzazione di reati commessi per interesse o a vantaggio dell'ente, da parte di soggetti apicali o sottoposti, a causa della "personalità della responsabilità penale"; pertanto tale nuova forma di responsabilità, essendo **nominalmente amministrativa**, dissimula la sua natura **sostanzialmente penale**. Essa è collegata ai cosiddetti "**reati presupposto 231**" ovvero reati di impresa commessi da soggetti apicali o sottoposti per interesse o a vantaggio dell'ente e che riguardano di conseguenza, la persona giuridica a favore della quale si riflette la condotta criminosa di persone fisiche ricollegabili all'attività dell'ente stesso. La sanzione viene irrogata, all'interno di un processo simultaneo, dallo stesso giudice penale competente per tali reati. Egli può applicare alla persona fisica le sanzioni penali e, contestualmente, le sanzioni amministrative alla persona giuridica.

Sono molteplici i reati per i quali la disciplina in esame viene applicata. In seguito all'emanazione della legge 29 settembre 2000 n° 300 (la quale, attraverso l'articolo 11, attribuiva una delega al Governo per l'emanazione un decreto legislativo avente per oggetto la disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica che non svolgono funzioni di rilievo costituzionale con l'osservanza di una serie di principi e criteri direttivi) venne emanato il D.lgs. 231/01 nel quale, inizialmente, erano state prese in considerazione le fattispecie di:

- indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico (art. 24 D.lgs. n. 231/01);
- concussione e corruzione, induzione indebita a dare o promettere utilità (art.25 D.lgs. n. 231/01).

A seguito di ulteriori interventi legislativi è stato ampliato il catalogo dei reati per i quali è applicabile il D.lgs. n. 231/01:

1. la legge 3 agosto 2007 n. 123 ("Misure in tema di tutela della salute e della sicurezza sul lavoro e delega al Governo per il riassetto e la riforma della normativa in materia") ha modificato il D.lgs. n. 231/01, introducendo l'art. 25-*septies* e estendendo l'ambito della responsabilità amministrativa degli enti ai reati di omicidio colposo e lesioni colpose gravi o gravissime commessi in violazione delle norme per la prevenzione degli infortuni sul lavoro o relative alla tutela dell'igiene e della salute sul lavoro;
2. il decreto legislativo del 7 luglio 2011 n.121 ("Attuazione della direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della direttiva 2009/123/CE che modifica la direttiva

2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni") ha introdotto delle modifiche al D.lgs. n. 231/01 (art. 25-*undecies*), nonché al codice penale (art. 727-*bis*) e al Testo Unico Ambientale (Decreto Legislativo 3 aprile 2006 n. 152), estendendo la responsabilità amministrativa degli enti anche ad una serie di reati ambientali. L'estensione è effetto delle direttive europee 2008/99/CE e 2009/123/CE, che hanno imposto la responsabilità degli enti per i reati ambientali commessi (anche) a loro vantaggio[4]. L'art. 25-*undecies* è stato successivamente ulteriormente modificato dall'entrata in vigore della Legge 22 maggio 2015, n. 68 ("disposizioni in materia di delitti contro l'ambiente") che ha previsto l'ampiamento dell'elenco dei reati presupposto della responsabilità amministrativa degli enti con i cd. "Eco-reati". La legge n. 68/2015 ha inoltre introdotto, all'interno del libro II del Codice penale, il titolo IV-*Bis* dedicato alle nuove fattispecie di reati legate all'inquinamento ambientale.

3. La legge 29 ottobre 2016 n. 199 (Disposizioni in materia di contrasto ai fenomeni del lavoro nero, dello sfruttamento del lavoro in agricoltura e di riallineamento retributivo nel settore agricolo) ha modificato l'art. 25–*quinquies* del Decreto Legislativo n. 231/01 al fine di contrastare lo sfruttamento del lavoro e dei lavoratori, attraverso azioni di contrasto, sul piano civile e penale, del lavoro nero che prevedono la confisca dei patrimoni delle aziende che commettono reati di caporalato. Tale legge ha, come nei casi sopracitati, introdotto delle modifiche anche al Codice Penale, mediante la riformulazione dell'art. 603-bis ("*Intermediazione illecita e sfruttamento del lavoro")* considerando, rispetto alla versione precedente, anche i comportamenti di sfruttamento che fanno leva sullo stato di bisogno e mediante l'introduzione degli artt. 603-bis.1 e 603-bis.2, relativi ad attenuanti del delitto di caporalato.

Soggetti giuridici destinatari della responsabilità amministrativa di cui al D.lgs. n. 231/01

L'art. 1 del D.lgs. n. 231/01 recita:

1. *il presente decreto legislativo disciplina la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato;*
2. *le disposizioni in esso previste si applicano agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica;*
3. *non si applicano allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici nonché' agli enti che svolgono funzioni di rilievo costituzionale.*

Come indicato in alto, in merito agli enti a soggettività privata forniti di personalità giuridica è applicato l'art 1 comma 2. Tale comma fa riferimento in particolar modo sia alle associazioni,

[4] Bartoccioni A.C. Il decreto legislativo n.121/2011 e la responsabilità degli enti in materia ambientale. Gazzetta Amministrativa. Uso del Territorio: Urbanistica, Ambiente e Paesaggio. Numero 1 – 2012.

fondazioni ed altre istituzioni di carattere privato alle quali, lo Stato attribuisce personalità giuridica, sia alle società cui il riconoscimento invece è conferito per effetto dell'iscrizione nel registro delle imprese, ai sensi dell'art 2331 c.c.
È questo il caso, per esempio, delle società per azioni ed accomandita per azioni, delle società a responsabilità limitata, delle società cooperative. Quindi, come si evince, le persone giuridiche sono le protagoniste indiscusse della normativa in esame.
Meno scontata, per altro verso, è invece la previsione delle Società e associazioni anche prive di personalità giuridica. Rientrano in tale ambito, le società semplici, quelle in nome collettivo, anche irregolari, le società in accomandita semplice, anche irregolare e le associazioni non riconosciute.

I soggetti ai quali non si applica il D.lgs. 231/01 sono lo Stato e gli enti pubblici territoriali (ossia le Regioni, le Province e i Comuni), gli enti non economici (enti di diritto pubblico esercitanti un pubblico servizio, come INPS. INAIL, scuole, università ecc..), le Aziende Sanitarie Locali, le aziende Ospedaliere (poiché l'estensione della responsabilità amministrativa a questi enti causerebbe un costo sociale senza adeguati benefici), enti con funzioni di rilievo costituzionale.

L'applicabilità del D.gs.231/01 alle Strutture Sanitarie Locali è oggetto di dibattito in dottrina. Le Unità Sanitarie Locali sono state infatti oggetto di un processo di "de publicizzazione" e trasformazione in Aziende Sanitarie Locali, il quale trova origine nel D.lgs. n. 502 del 1992 e nei successivi aggiornamenti allo stesso decreto apportati dal D.lgs. n. 229 del 1999, in cui è indicato che le unità sanitarie locali si costituiscono in aziende con personalità giuridica pubblica, ma sono dotate di autonomia imprenditoriale e la loro organizzazione ed il funzionamento sono disciplinati da atti aziendali di diritto privato.

Tra gli enti privati, sono da ritenersi esclusi dalla disciplina in esame, i sindacati (art. 39 Cost.) ed i partiti politici (art. 49 Cost.) che, com'è noto nel nostro ordinamento, sono sprovvisti di personalità giuridica. Il legislatore italiano si è infatti orientato per una loro esenzione della responsabilità, potendo essere ricompresi tra gli enti che svolgono funzioni di rilievo costituzionale esclusi espressamente dal comma 3 dell'art 1 del decreto legislativo 231/01.

L'esonero dalla responsabilità degli enti (di cui all'art.6. D.lgs. 231/01) dipende dall'aver **adottato ed efficacemente attuato** modelli di organizzazione, gestione e controllo, idonei a prevenire la realizzazione degli illeciti penali considerati. L'adozione dei modelli **non** è obbligatoria, pertanto la mancanza dell'adozione degli stessi non è soggetta ad alcuna sanzione, ma espone l'ente alla responsabilità derivante da illeciti realizzati da amministratori e dipendenti.

Interesse e vantaggio dell'ente

Art. 5 D.lgs. n. 231/01 – Responsabilità dell'ente

1. *L'ente è responsabile per i reati commessi nel suo interesso 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.*
    b. *da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti.*
2. *L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi.*

Il riconoscimento della responsabilità amministrativa dell'ente presuppone, di per sé, **l'esistenza di un interesse o un vantaggio dell'ente** collegati strettamente all'azione criminosa del soggetto apicale o del suo sottoposto. L'**interesse** corrisponde **all'intenzione da parte dell'autore del reato di procurare un vantaggio all'ente**. Questo è dunque un presupposto sufficiente per coinvolgere la persona giuridica nella responsabilità. Il **vantaggio** è ancorato al **beneficio che l'ente ha tratto dalla commissione dell'illecito**. Può accadere che l'interesse sussista anche senza che l'ente tragga alcun vantaggio.

ESEMPIO – condotta di istigazione alla corruzione di cui all'art. 322 c.p. *(chiunque offre o promette denaro od altra utilità ad un pubblico ufficiale o ad un altro incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri […])* attuata dal direttore generale di una società che opera con la pubblica amministrazione. In tale ipotesi anche se il fine del corruttore non viene realizzato, la consistenza dell'interesse risulta indiscutibile. Questo significa che l'interesse sarà sussistente anche nel caso in cui non si verifichi un vantaggio. Per quanto riguarda il vantaggio è necessario chiarire chi ha beneficiato del vantaggio derivante dalla condotta illecita posta in essere dalla persona fisica e il beneficio che può essere derivato per l'ente. È necessario che il vantaggio sia conseguente all'interesse. Riguardo all'interesse, qualora emerga che l'autore abbia commesso il reato nel "prevalente interesse proprio o di terzi" e l'ente non ne abbia ricavato alcun vantaggio e ne abbia ricavato un minimo vantaggio, è prevista una riduzione della sanzione pecuniaria irrogabile e l'inapplicabilità di alcune sanzioni interdittive.

Soggetti in posizione apicale e soggetti sottoposti

Il legislatore, al comma 1 lettera a) dell'art. 5 del D.lgs. n. 231/01, piuttosto che eseguire una rigida (e poco praticabile) elencazione di soggetti, ha preferito adottare una formula flessibile per individuare i soggetti in posizione apicale, considerando l'eterogeneità degli enti e delle situazioni di riferimento. In questo modo la funzione apicale si connota, sia che essa sia **formale**, sia che essa sia **di fatto**. Di conseguenza sono rilevanti sia le condotte illecite poste in essere da soggetti con funzioni di rappresentanza, amministrazione e direzione quali ad esempio il rappresentante

legale, l'amministratore unico (o delegato) e il direttore generale (nel caso di enti di medio-grandi dimensioni), sia quelle poste in essere da soggetti che esercitano sull'ente un controllo "di fatto", come per esempio l'amministratore di fatto (qualora sia provata la sua ingerenza nella gestione della società all'epoca dei fatti oggetto di contestazione) o il socio che detiene la quasi totalità di azioni all'interno di una società e che dispone dall'esterno le linee della politica aziendale o il compimento di determinate operazioni.

In materia di sicurezza sul lavoro si individuano, quali soggetti apicali, il datore di lavoro e i dirigenti, per via della loro posizione funzionale. Ricordiamo che la responsabilità amministrativa dell'ente non è legata solo ai soggetti che possiedono funzione di rappresentanza, amministrazione e direzione dell'ente stesso, ma deriva anche in seguito al comportamento illecito di soggetti che hanno le medesime funzioni all'interno di una unità organizzativa dotata di autonomia finanziaria. Spesso, infatti, accade che i soggetti dotati di una forte autonomia gestionale siano sottratti al controllo delle sedi centrali (realtà complesse). L'inclusione di questi soggetti tra gli apicali si realizza solo in riferimento ai casi in cui le unità organizzative siano dotate di autonomia finanziaria (si intende la possibilità di disporre di risorse finanziarie per il proprio settore di attività all'interno di una società, da non confondere con l'autonomia patrimoniale) e gestionale.

Nelle realtà a minore complessità, in cui le unità organizzative siano carenti dal punto di vista dell'autonomia finanziaria e funzionale, i soggetti che ne fanno parte saranno quelli cosiddetti "sottoposti" (art. 5, comma 1, lett. b).

Per quanto concerne la salute e la sicurezza sul lavoro, è necessario focalizzare il concetto secondo cui, chi ordina l'esecuzione di un lavoro senza controllare che questo sia realizzato nel rispetto della normativa antinfortunistica, sarà inevitabilmente chiamato in sede di accertamento delle responsabilità penali da danno alla persona (omicidio colposo o lesioni gravi o gravissime di cui agli artt. 589 e 590 c.p.), coinvolgendo la propria azienda nella responsabilità amministrativa da reato penale per **colpa organizzativa**[5], ai sensi del D.lgs. 231/01.

La gestione programmata della sicurezza e dell'igiene del lavoro (indicata dagli artt.15, 17 e 28 del D.lgs. 81/08) richiede il coinvolgimento attivo e operante di tutti i soggetti presenti in azienda, che sono ritenuti responsabili della propria e dell'altrui sicurezza.

Il legislatore articola nei modi seguenti la ripartizione dei compiti antinfortunistici nel luogo di lavoro: si parte con il **datore di lavoro** (soggetto apicale), che ha l'obbligo di predisporre mezzi e strutture che siano sicuri e rispondenti ai requisiti preventivi e protettivi, tecnici e igienici previsti (in riferimento anche a quanto indicato dall'art. 2087 del c.c., secondo cui il datore di lavoro è tenuto ad adottare tutte le misure per tutelare l'integrità fisica e morale del lavoratore,

[5] La **colpa organizzativa** deriva dalla *"omessa predisposizione di un insieme di accorgimenti preventivi idonei ad evitare la commissione del reato presupposto: è il riscontro di tale deficit organizzativo che consente l'imputazione all'ente dell'illecito penale realizzato nel suo ambito operativo*" [Tribunale di Novara, 26 ottobre 2010].

rispettando tutte quelle norme che si rivelino necessarie in base alla particolarità del lavoro, l'esperienza e tecnica, per poi passare ai **dirigenti** (soggetti apicali), che hanno l'onere di organizzare in modo adeguato e sicuro l'utilizzo delle strutture e delle attrezzature messe a disposizione dal datore di lavoro, a prescindere dai poteri di spesa. Il dirigente è colui che dirige e che esercita la supremazia che si estrinseca in un potere organizzativo dell'attività lavorativa, nel potere di decidere le procedure di lavoro e di organizzare opportunamente i fattori di produzione, sempre nell'ambito dei compiti e delle mansioni effettivamente devolutegli dall'organizzazione aziendale.

I dirigenti NON si sostituiscono al datore di lavoro, nonostante ne condividano oneri e responsabilità (art. 18 D.lgs. 81/08). Dai dirigenti si passa ai **preposti** (soggetti sottoposti), che corrispondono all'ultimo anello della catena gerarchica. I preposti corrispondono alle figure del capo reparto, capo sala, capo ufficio, capo turno, capo cantiere, capo macchina, supervisori, coordinatori, tutte figure che godono di una supremazia sugli altri lavoratori. A essi la legge attribuisce il compito di vigilare sulla corretta osservanza da parte dei lavoratori, delle misure di prevenzione e protezione predisposte dai vertici aziendali e di riferire ad essi stessi le eventuali situazioni pericolose e le carenze sulle misure preventive e protettive presenti all'interno dei luoghi di lavoro. Ai preposti non è riconosciuta alcuna autonomia decisionale personale, ma solo il compito di attenersi fedelmente alle istruzioni impartite dai vertici.

La cassazione sottolinea che "*la stessa formulazione della norma […] consente di ritenere che il legislatore abbia voluto rendere i dirigenti e i preposti destinatari delle norme antinfortunistiche iure proprio, prescindendo dall'eventuale delega*" (sentenza Cassazione Penale sez. IV pe. N. 11351 del 31 marzo 2006). Si è dunque dirigenti e preposti ai fini della sicurezza, in base all'organigramma aziendale, alla posizione ricoperta e agli effettivi poteri esercitati sul lavoro degli altri. Il dirigente o il preposto si identifica con chi abbia assunto una posizione di preminenza rispetto agli altri lavoratori, tale da poter impartire loro degli ordini, istruzioni o direttive da eseguire; per questi motivi egli deve considerarsi automaticamente in obbligo di attuare le misure di sicurezza e di predisporre ed esigere che esse vengano rispettate.

L'articolo 299 del decreto legislativo 9 aprile 2008 n. 81 ("Esercizio di fatto di poteri direttivi"), ha esplicitato un principio da decenni affermato dalla giurisprudenza, prevedendo che le posizioni di garanzia, (ossia l'obbligo di tutelare l'integrità fisica e la personalità morale del lavoratore) relative a datore di lavoro, dirigente e preposto "gravano" in modo peculiare "*su colui il quale, pur sprovvisto di regolare investitura, eserciti in concreto i poteri giuridici riferiti a ciascuno dei soggetti ivi definiti*" (art.299 D.lgs. 81/08).

In precedenza, si sono spesso menzionate le figure dei sottoposti, ossia tutte quelle persone assoggettate alla direzione o alla vigilanza di uno dei soggetti apicali. Questi soggetti non godono di autonomia amministrativa e organizzativa. Rientrano tra le figure dei sottoposti:

- i consulenti;
- il medico Competente;
- il preposto;
- il RSPP (Responsabile del Servizio di Prevenzione e Protezione);
- il lavoratore
- i collaboratori;
- i fornitori

Possono rientrare tra i sottoposti anche quelle figure dirigenziali a cui spettano poteri organizzativi, come per esempio la predisposizione di determinate procedure, ma che non possiedono un incisivo potere sull'ente o sull'unità organizzativa tale da rientrare fra i soggetti apicali. Tale figura prende il nome di "dirigente preposto".

Mancata identificazione / non imputabilità dell'autore del reato

Per poter attribuire all'ente una responsabilità amministrativa dipendente da reato presupposto, occorrerà che la condotta illecita posta in essere da un autore rimasto non identificato, sia collegabile alla colpa organizzativa. In questo contesto, l'autorità giudiziaria, sulla base delle emergenze investigative, dovrà dimostrare che lo stesso autore non identificato:

1) appartenga ad una delle categorie individuate dall'articolo 5 comma 1 del D.lgs. 231/01. L'analisi degli elementi oggettivi del reato–presupposto e delle procedure organizzative interne (attribuzioni, competenze, poteri e mansioni) potrebbe consentire di identificare se non l'autore stesso, almeno la categoria di appartenenza, ossia se si tratti di un apicale o di un sottoposto;
2) se il soggetto in questione abbia agito nell'interesse o a vantaggio dell'ente oppure nell'interesse esclusivo di sé stesso o di terzi, con nessun vantaggio o con vantaggio minimo dell'ente.

Mentre il vantaggio risulta facilmente dimostrabile, in quanto è sufficiente valutare in concreto il risultato della condotta, è più difficile valutare il tipo di interesse che "ex ante" ha determinato la condotta dell'autore del reato. In ogni caso, se a seguito delle indagini dell'autorità giudiziaria competente, qualora anche una sola delle due condizioni sopra richiamate venga meno, non sarà possibile attribuire la responsabilità all'ente.

Sanzioni a carico dell'ente

Il sistema sanzionatorio previsto dal D.lgs. 231/01 è particolarmente afflittivo per gli enti; il legislatore ha istituito, indicandolo nell'art. 9 (sanzioni amministrative) del medesimo decreto, un sistema che prevede sia l'applicazione di sanzioni pecuniarie, che devono essere sempre comminate e di sanzioni interdittive che, al contrario, trovano applicazione soltanto in

determinate condizioni e vanno ad inserirsi all'interno della più ampia misura delle sanzioni cautelari. Le misure interdittive incidono sul soggetto, limitandone l'attività o l'accesso a determinate risorse economiche. Sia nel caso delle sanzioni pecuniarie che nel caso delle sanzioni interdittive, l'esigenza è quella di paralizzare o ridurre l'attività dell'ente quando la prosecuzione dell'attività stessa possa protrarre o aggravare le conseguenze del reato o agevolare la commissione di altri reati.

Sanzioni pecuniarie e sistema per quote

La sanzione pecuniaria è irrogata con lo scopo di punire l'illecito commesso; al fine di adattare la risposta sanzionatoria alle reali capacità finanziarie dell'ente e alla sua posizione di mercato, il legislatore ha previsto un modello commisurativo per quote (art. 10 - *Sanzione amministrativa pecuniaria*- D.lgs. 231/01). Così, mentre il numero delle quote viene determinato in riferimento alla gravità oggettiva e soggettiva dell'illecito, il valore economico di ciascuna quota viene determinato dal giudice sulla base della capacità economica della persona giuridica.

Per quanto riguarda il calcolo dell'ammontare della sanzione pecuniaria, vengono presi in considerazione i seguenti elementi:

- **gravità oggettiva e soggettiva del fatto**: il giudice in base al comportamento tenuto dall'ente, determina il numero di quote che deve essere non inferiore a 100 e non superiore a 1000. Nel differenziare l'entità della sanzione, il giudice dovrà tenere conto del fatto che l'illecito costituisca espressione della politica aziendale (nel caso in cui il reato sia commesso da una persona ai vertici dell'azienda), oppure se derivi dalla cosiddetta "colpa organizzativa" (in quanto commesso da un subordinato). Questo significa che a carico dell'ente ci sarà un giudizio di maggiore riprovazione, qualora dalle indagini dell'autorità giudiziaria emerga che il reato sia stato commesso da un soggetto in posizione apicale;
- **capacità economica della persona giuridica**: il giudice determina il valore di ciascuna quota.
- il numero delle quote è moltiplicato per il valore unitario, determinando così l'ammontare della sanzione pecuniaria.

È possibile che l'ente manifesti la volontà di attuare degli interventi al fine di eliminare o attenuare le conseguenze del fatto illecito, o prevenire ulteriori commissioni di illeciti. In alcuni casi è possibile che si verifichino delle condizioni per cui alcune delle condotte adottate portino ad una riduzione della sanzione pecuniaria (art.12 D.lgs. 231/01).

Nei casi seguenti la sanzione pecuniaria può essere ridotta della metà qualora (art. 12 comma 1, lett. a) e b)):

a) l'autore del reato abbia commesso il fatto nel ***prevalente*** *interesse di sé stesso o di terzi* e l'ente non ne abbia ricavato alcun vantaggio o ne abbia ricavato un vantaggio minimo;
b) il danno patrimoniale è di particolare tenuità.

La sanzione può essere ridotta da un terzo alla metà se, prima della dichiarazione del dibattimento di primo grado (art. 12 comma 2, lett. a) e b)):

a) l'ente abbia risarcito il danno o abbia eliminato le conseguenze dannose o pericolose del reato oppure se si sia efficacemente adoperato in tal senso;
b) è stato adoperato e reso operativo un modello organizzativo idoneo a prevenire i reati della specie di quello verificatosi.

Per ottenere la riduzione è sufficiente che si verifichi almeno una delle condizioni e se le stesse concorrono, l'attenuazione sarà della metà ai due terzi (*Nel caso in cui concorrono entrambe le condizioni previste dalle lettere del precedente comma, la sanzione è ridotta dalla metà ai due terzi* (art. 12 comma 3)).

È importante ricordare che l'attività riparatoria deve riguardare anche la riparazione delle conseguenze dannose o pericolose del reato, anche se non hanno avuto riflessi sul patrimonio della vittima.

Sanzioni interdittive

Sono le sanzioni che hanno maggiore rilievo in quanto sono capaci di limitare e condizionare le capacità operative di una persona giuridica e di ostacolarne la presenza sul mercato. Si applicano in aggiunta alle sanzioni pecuniarie per fronteggiare le ipotesi più gravi della criminalità corporativa.

Le sanzioni interdittive previste dall'art. 9 comma 2 del D.lgs. 231/01 sono:

- interdizione temporanea o definitiva dell'esercizio dell'attività;
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- esclusione da agevolazioni, finanziamenti, contributi, sussidi ed eventuale revoca di quelli già concessi;
- divieto temporaneo o definitivo di pubblicizzare beni o servizi.

Le sanzioni interdittive si applicano per i reati per cui sono previste, quando ricorre almeno una delle seguenti condizioni:

1) l'ente ha tratto dal reato un profitto di grande entità e il reato è stato commesso da soggetti in posizione apicale o da sottoposti quando la commissione del reato è stata determinata o agevolata da forti carenze organizzative;
2) in casi di reiterazione di illeciti.

Talvolta, se sussistono i presupposti per l'applicazione di una sanzione interdittiva che determina l'interruzione dell'attività dell'ente, il giudice, in luogo dell'applicazione della sanzione, dispone la prosecuzione dell'attività dell'ente da parte di un commissario, per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata quando ricorre almeno una delle seguenti condizioni:

1) l'ente svolge un pubblico servizio o un servizio di pubblica necessità, la cui interruzione può provocare un grave pregiudizio per la collettività;
2) l'interruzione dell'attività dell'ente può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione.

Il commissario curerà l'adozione di efficaci Modelli di Gestione e di Controllo, idonei a prevenire i reati della specie di quello verificatosi. Non può compiere atti di straordinaria amministrazione senza l'autorizzazione del giudice.

Tra le sanzioni a carico dell'ente previste dal D.lgs. 231/01 si annoverano anche la pubblicazione della sentenza e la confisca. La pubblicazione della sentenza è definita dall'art. 18 Dlgs. 231/2001 che stabilisce che la pubblicazione della sentenza di condanna può essere disposta quando nei confronti dell'ente viene applicata una sanzione interdittiva; tale sanzione amministrativa ha un carattere accessorio in quanto può essere applicata solo contestualmente ad una sanzione amministrativa ed è discrezionale, in quanto è il giudice a stabilire quando applicarla. Per quanto riguarda la confisca, come stabilito dall'art. 19, "*è sempre disposta, con la sentenza di condanna, la confisca del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato. Sono fatti salvi i diritti acquisiti dai terzi in buona fede (comma 1). Quando non è possibile eseguire la confisca a norma del comma 1, la stessa può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato (comma 2)".*

Esenzione dalla Responsabilità Amministrativa mediante l'adozione di un Modello di Organizzazione, Gestione e Controllo

Come più volte anticipato in precedenza, l'ente va esente da responsabilità quando coloro che hanno commesso uno dei cosiddetti "reati-presupposto" hanno agito in interesse esclusivo proprio o di terzi. Il D.lgs. 231/01 prevede, nell'ottica di un'incentivazione o sensibilizzazione di una cultura aziendale improntata alla prevenzione del rischio di reati, una sorta di esonero dalla responsabilità, qualora, in occasione di un procedimento penale per uno dei reati-presupposto, la persona giuridica dimostri una serie di condizioni, tra cui in particolare l'adozione e l'efficace attuazione di modelli 231 di organizzazione, gestione e controllo idonei a prevenire reati della specie di quello verificatosi. È inoltre necessaria la creazione di un organo interno dotato di autonomi poteri di iniziativa e di controllo per verificare il funzionamento e la corretta ed effettiva attuazione e l'aggiornamento di detti modelli.

Implementazione e requisiti di un modello di organizzazione, gestione e controllo 231

Il modello organizzativo da implementare, per essere adeguato ai requisiti richiesti dal D.lgs. 231/01, deve essere elaborato secondo il processo del "risk–management" basato sulle seguenti fasi:

1) **identificazione dei rischi:** consiste in un'analisi del contesto aziendale volta ed evidenziare le aree, le attività e i settori che siano potenzialmente esposti alla commissione di reati previsti dalla 231 e nello studio di una modalità di attuazione.
2) **Progettazione di sistemi di controllo:** consiste nell'attuazione di un adeguato sistema di controlli che garantiscono la vigilanza sulla correttezza e sulla liceità dei processi aziendali.

Queste due fasi si trovano, rispettivamente, alle due estremità del processo; tra esse sono collocate una serie di attività intermedie che consentono all'azienda di analizzare la propria impostazione e di adottare le necessarie tutele rispetto ai requisiti imposti dalla legge. Tutto il processo va affrontato nell'ottica del "rischio accettabile", ossia l'ente viene esonerato dalla responsabilità amministrativa dell'impresa quando ha adottato un sistema prevenzionale tale da non poter essere aggirato, se non intenzionalmente. Ciò significa che l'azienda deve dotarsi di un sistema che non permetta a nessuna persona operante al suo interno di avvalersi della scusa di non essere stato informato riguardo alle direttive aziendali o che il suo operato non fosse verificato da nessuno.

Nel caso in cui si realizzi la commissione di uno dei reati-presupposto da parte degli apicali, il modello, dimostratosi sostanzialmente inadeguato ad impedire la realizzazione della condotta, sarà giudicato comunque idoneo in presenza delle condizioni di cui all'art. 6 comma 1 lett. c) e d), ossia nei casi in cui l'autore abbia agito violando **fraudolentemente** il sistema dei controlli apprestato con il modello e non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di vigilanza. Nell'ipotesi, dunque, di reato commesso da soggetto apicale la polizia giudiziaria dovrà valutare la validità degli elementi adottati dall'ente a propria difesa, mentre nell'ipotesi di reato commesso da soggetto sottoposto, la polizia giudiziaria dovrà provare l'inefficienza dei modelli adottati, ovvero il mancato rispetto degli obblighi di vigilanza da parte degli organi preposti. Il regime adottato è dunque differente a seconda del caso in cui il reato sia stato commesso da un soggetto apicale piuttosto che da un soggetto sottoposto, poiché nel primo caso l'onere della prova è attribuito all'ente, che dovrà dimostrare l'idoneità e l'efficacia del modello organizzativo, nel secondo caso l'onere della prova è attribuito all'accusa.

Il D.lgs. 231/01 dunque non esige che il modello annulli completamente il rischio che si verifichino dei reati-presupposto, ma che lo definisca e lo tenga sotto controllo **con continuità**. Il modello **deve adattarsi alla realtà aziendale** in tutte le sue particolarità e deve presentare le caratteristiche di **efficienza, praticabilità e funzionalità**, in grado di disinnescare le fonti di rischio in modo ragionevole.

Per l'implementazione del sistema di gestione 231 sono necessari diversi strumenti indicati di seguito. Innanzitutto, è fondamentale la formulazione di un **codice etico**; questo consente di sancire i contenuti e i valori guida a cui si ispira la cultura imprenditoriale, definendo le modalità di comportamento dei diversi destinatari del codice stesso. I codici etici sono documenti ufficiali dell'ente che contengono l'insieme dei diritti, dei doveri e delle responsabilità dell'ente nei confronti degli "stakeholder" (portatori d'interesse - dipendenti, fornitori, clienti, Pubblica Amministrazione, azionisti, mercato finanziario, ecc.). Tali codici mirano a raccomandare, promuovere o vietare determinati comportamenti, indipendentemente da quanto previsto a livello normativo e possono prevedere sanzioni proporzionate alla gravità delle eventuali infrazioni commesse. I codici etici sono documenti voluti ed approvati dal massimo vertice dell'ente. Il Codice etico dovrebbe focalizzarsi sui comportamenti rilevanti ai fini del decreto 231 e andrebbe distintamente formulato in relazione, da un lato, alla generalità delle fattispecie di reato doloso, dall'altro ai reati a tutela della salute e sicurezza sul lavoro e dell'ambiente.

Al fine di costruire un modello efficace sarebbe consigliabile realizzare un'analisi e una mappatura di quelli che sono i rischi potenziali di commissione dei reati pertinenti l'attività aziendale. Tale valutazione deve essere completa, esauriente e metodologicamente affidabile, basata sul controllo e sulla verifica con le figure sensibili in materia (es. soggetti apicali).
Si rende necessaria l'individuazione di procedure, di misure specifiche e protocolli di controllo che riguardano lo svolgimento delle attività aziendali e le modalità di controllo da parte dell'organo di vigilanza. Le procedure devono essere definite in modo esplicito, anche attraverso la redazione di un manuale che, partendo dal codice etico, vada ad individuare tutte le aree e i processi interni all'azienda che potrebbero essere soggetti alla realizzazione di reati presupposto e che racchiuda al suo interno l'insieme delle procedure organizzative volte ad assicurare il conseguimento degli obiettivi e delle regole fissate; alcuni esempi di tali procedure possono essere: la corretta tenuta dei registri contabili, il monitoraggio dei fornitori, il controllo delle nuove assunzioni, le verifiche di ottemperanza alle regole di anticorruzione, le procedure per eseguire gli audit sulla sicurezza ambientale, l'individuazione delle modalità di gestione delle risorse finanziare ecc..
È necessaria, inoltre, l'organizzazione di registrazioni che prevedano il rispetto delle procedure o l'effettuazione di controlli o audit. In tutti questi casi deve esistere una verbalizzazione e una documentazione che dimostri il rispetto delle procedure individuate dal sistema di gestione. Dunque, per ogni operazione vi deve essere un supporto documentale idoneo a consentire, in ogni momento, l'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione ed individuino chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa.

Un punto qualificante nella costruzione del modello è costituito dalla previsione di un adeguato **sistema sanzionatorio** per la violazione delle norme del Codice etico, nonché delle procedure previste dal modello. Infatti, per valersi dell'efficacia esimente del modello, l'ente deve

assicurarsi che questo sia adottato, ma anche efficacemente attuato. Il modello dovrebbe, pertanto, individuare nel dettaglio le misure disciplinari cui si espone chiunque non osservi le misure organizzative adottate, ricollegando a ciascuna violazione o gruppo di violazioni le sanzioni applicabili, in una prospettiva di gravità crescente.

Le sanzioni dovrebbero spaziare da misure conservative, per le infrazioni più tenui, a provvedimenti idonei a recidere il rapporto tra l'agente e l'ente, nel caso di violazioni più gravi. Secondo il consolidato orientamento della Corte Costituzionale (sent. n. 220 del 1995), l'esercizio del potere disciplinare deve sempre conformarsi ai principi di:

- **proporzione**, commisurando la sanzione irrogata all'entità dell'atto contestato;
- **contraddittorio**, assicurando il coinvolgimento del soggetto interessato: formulata la contestazione dell'addebito tempestiva e specifica, occorre dargli la possibilità di presentare giustificazioni a difesa del suo comportamento.

Infine, si possono anche prevedere, accanto alle sanzioni disciplinari, meccanismi premiali riservati a quanti coopereranno al fine dell'efficace attuazione del modello, per esempio denunciando comportamenti individuali devianti. Spesso, infatti, quando si intende promuovere il rispetto delle regole, il prospetto dei vantaggi derivanti dalla loro osservanza può risultare più efficace della minaccia di conseguenze negative per la loro violazione.

È importante, inoltre, definire all'interno del modello organizzativo adottato da ciascun ente, quali siano le funzioni aziendali deputate a valutare e disporre i provvedimenti o contestazioni disciplinari per violazioni del Codice Etico e/o del Modello 231, nonché il ruolo dell'Organismo di vigilanza (consulenziale, propositivo) nel momento dell'eventuale applicazione della sanzione.

Affinché l'istituzione del sistema disciplinare per la violazione di misure, protocolli, obblighi di informazione e registrazione, come anche dei controlli a campione o a sorpresa sulle attività sensibili, consenta realmente di verificare la corretta applicazione delle procedure, è senza dubbio indispensabile l'istituzione di una disciplina della formazione dei soggetti apicali e dei collaboratori presenti in via continuativamente significativa all'interno dell'ente. La formazione deve essere svolta in maniera efficace in modo da rendere tali soggetti consapevoli dei loro obblighi e responsabilità relativamente all'adozione del modello di gestione e del rispetto del codice etico.

Creazione di un Organismo di Vigilanza (OdV)

Come già più volte anticipato, l'art. 6 del decreto 231/01 prevede che l'ente possa essere esonerato dalla responsabilità derivante dalla commissione di reati-presupposto qualora l'organo dirigente abbia, sia adottato modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati e abbia previsto l'istituzione di un organismo di controllo al quale sia

affidato il compito di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento. Tale organismo deve essere indipendente e dotato di autonomi poteri ispettivi, di iniziativa e controllo e prende il nome di "Organismo di Vigilanza" o "OdV".
Le "linee guida della Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo", approvate il 7 marzo 2002 e aggiornate al marzo 2014, hanno precisato alcuni aspetti specifici dell'Organismo di Vigilanza relativi ai poteri e requisiti dello stesso e che sono di seguito elencati:

- **autonomia e indipendenza:** la presenza all'interno dell'Organismo di Vigilanza anche solo di un componente che non sia autonomo rispetto ai processi operativi e decisionali, può portare alla vanificazione dell'intero modello organizzativo. Il primo dei due requisiti va inteso nel senso che la posizione dell'OdV nell'ambito dell'ente deve garantire l'autonomia dell'iniziativa di controllo da ogni forma di interferenza o condizionamento da parte di qualunque componente dell'ente e, in particolare, dell'organo dirigente. Nel sistema disegnato dal decreto 231, quest'ultimo è uno dei soggetti controllati dall'Organismo di Vigilanza. Inoltre, l'OdV non dovrebbe essere influenzato a livello economico e personale, né dovrebbero esserci situazioni di conflitto di interesse anche potenziale, poiché, in tal caso, il requisito dell'autonomia verrebbe meno. Pertanto, una soluzione potrebbe essere quella di inserire l'Organismo di Vigilanza come "unità di staff" in una posizione gerarchica più elevata possibile e prevedendo il "riporto" al massimo vertice operativo aziendale, vale a dire al Consiglio di Amministrazione nel suo complesso. Per assicurare la necessaria autonomia di iniziativa e l'indipendenza è poi indispensabile che all'Organismo di Vigilanza non siano attribuiti compiti operativi. Diversamente, infatti, potrebbe esserne minata l'obiettività di giudizio come organo, all'atto delle verifiche sui comportamenti e sul Modello. Allo scopo di assicurare l'effettiva sussistenza dei requisiti descritti, sia nel caso di un Organismo di Vigilanza composto da una o più risorse interne, sia nell'ipotesi in cui esso sia composto anche da figure esterne, sarà opportuno che i membri possiedano i requisiti soggettivi formali che garantiscano ulteriormente l'autonomia e l'indipendenza richiesta dal compito, come onorabilità, assenza di conflitti di interessi e relazioni di parentela con il vertice. Tali requisiti andranno specificati nel Modello Organizzativo. Una volta istituito è opportuno che l'OdV formuli egli stesso un regolamento delle proprie attività (determinazione delle cadenze temporali dei controlli, individuazione dei criteri e delle procedure di analisi, ecc.). La redazione e l'approvazione del regolamento da parte di organi societari diversi dall'OdV, infatti potrebbero mettere in dubbio l'indipendenza dell'organismo stesso.
- **Disporre di competenze tecniche professionali necessarie all'efficace svolgimento delle attività richieste:** il modello deve esigere che i membri dell'OdV abbiano competenze in "*attività ispettiva, consulenziale, ovvero la conoscenza di tecniche specifiche, idonee a garantire l'efficacia dei poteri di controllo e del potere propositivo ad esso demandati*" (Trib. Napoli, 26 giugno 2007); per queste ragioni, durante la scelta dei membri dell'Organismo di Vigilanza, non è sufficiente un "*generico rinvio al curriculum vitae dei*

singoli", ma è indispensabile la verifica del possesso di specifiche competenze tecnico professionali, in particolare in merito all'attività ispettiva e di analisi del sistema di controllo, la giurisprudenza ha fatto riferimento, a titolo esemplificativo:

- al campionamento statistico;
- alle tecniche di analisi, valutazione e contenimento dei rischi, (procedure autorizzative, meccanismi di contrapposizione di compiti; ecc.);
- al flow-charting di procedure e processi per l'individuazione dei punti di debolezza;
- alla elaborazione e valutazione dei questionari;
- alle metodologie per l'individuazione di frodi (Trib. Milano, 20 settembre 2004).

Poiché inoltre, la disciplina in argomento ha natura sostanzialmente punitiva e il modello si prefigge di prevenire la realizzazione di reati, è consigliabile che almeno qualcuno tra i membri dell'Organismo di Vigilanza abbia competenze in materia di analisi dei sistemi di controllo e di tipo giuridico e, più in particolare, penalistico.

- **Avere continuità d'azione**, cioè l'Organismo di Vigilanza deve potersi dedicare a tempo pieno allo svolgimento dei controlli, al fine di assicurare che non si verifichino falle al sistema, determinate da controlli carenti e suscettibili di inficiare il modello. L'attività, come già detto in precedenza, deve essere priva di mansioni operative che possano portarla ad assumere decisioni con effetti economico-finanziari (cfr. Trib. Roma, 4 aprile 2003).

L'articolazione e la composizione dell'Organismo di Vigilanza sono correlate alla complessità strutturale dell'impresa (dimensioni, articolazione interna, dislocazione sul territorio ecc..) e vanno valutate caso per caso a seconda dei risultati dell'analisi dei rischi, dalla quale emergono quante aree, processi, funzioni devono essere assoggettate al controllo.

Si è osservato, in ogni caso, che le realtà medio - grandi si servono di OdV plurisoggettivi o collegiali, mentre le piccole realtà si servono di organismi monosoggettivi (o monocratici). Nelle piccole realtà è possibile che i compiti previsti dall'art. 6 comma 2 lett. b) - *prevedere protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire* - possano essere svolti direttamente dall'organo dirigente, il quale potrà avvalersi di professionisti esterni a cui affidare l'incarico di svolgere verifiche sul rispetto e l'efficacia del modello. Nelle aziende di grandi dimensioni sarebbe meglio preferire degli OdV di natura collegiale, con il ricorso a professionisti esterni che andranno ad affiancare il personale interno qualificato e non operativo, in modo tale da garantirne autonomia e professionalità.

Al momento della formale adozione del Modello l'organo dirigente dovrà:

- regolamentare gli aspetti principali relativi al funzionamento dell'OdV (es. modalità di nomina e revoca, durata in carica) e ai requisiti soggettivi dei suoi componenti;
- comunicare alla struttura i compiti dell'OdV e i suoi poteri, prevedendo eventuali sanzioni in caso di mancata collaborazione.

Nei confronti dell'Organismo di vigilanza, l'art. 6 comma 2 lett. d) prevede l'obbligo di informazione da ritenersi indirizzato alle funzioni aziendali a rischio reato. Esso riguarda le risultanze periodiche dell'attività di controllo realizzata dalle stesse funzioni aziendali succitate per dare attuazione ai modelli (report riepilogativi dell'attività svolta, attività di monitoraggio, indici consuntivi, ecc.) e le anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (un fatto non rilevante, se singolarmente considerato, potrebbe assumere diversa valutazione in presenza di ripetitività o estensione dell'area di accadimento).

Tali informazioni potranno riguardare, ad esempio:

- le decisioni relative alla richiesta, erogazione e utilizzo di finanziamenti pubblici;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura procede per i reati previsti dalla richiamata normativa;
- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al decreto 231;
- le commissioni di inchiesta o relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al decreto 231;
- le notizie relative alla effettiva attuazione, a tutti i livelli aziendali, del modello organizzativo, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- gli esiti dei controlli - preventivi e successivi - che sono stati effettuati nel periodo di riferimento, sugli affidamenti a operatori del mercato, a seguito di gare a livello nazionale ed europeo, ovvero a trattativa privata;
- gli esiti del monitoraggio e del controllo già effettuato nel periodo di riferimento, sulle commesse acquisite da enti pubblici o soggetti che svolgano funzioni di pubblica utilità.

Va chiarito che le informazioni fornite all'Organismo di Vigilanza, mirano a consentirgli di migliorare le proprie attività di pianificazione dei controlli e non ad imporgli attività di verifica puntuale e sistematica di tutti i fenomeni rappresentati. In altre parole, all'OdV non incombe un obbligo di agire ogni qualvolta vi sia una segnalazione, essendo rimesso alla sua discrezionalità (e responsabilità) di stabilire in quali casi attivarsi. È il caso di aggiungere che l'obbligo di informazione è stato probabilmente previsto anche allo scopo di conferire maggiore autorevolezza alle richieste di documentazione che si rendono necessarie all'Organismo di Vigilanza nel corso delle sue verifiche.

Successivamente si riporta brevemente il percorso da seguire per l'adozione del modello 231:

1. **analisi preliminare** del contesto aziendale, dei processi aziendali sensibili alla commissione di reati presupposto e in collaborazione con le funzioni aziendali sensibili, mappatura dei rischi di commissione dei reati-presupposto 231;
2. **progettazione** o eventualmente **acquisizione dei protocolli del sistema di controllo**, idonei a ridurre i rischi accertati e potenziali. Fra i protocolli, che devono essere diffusi presso il personale (e in merito ai quali è necessario effettuare la formazione) vanno menzionati,
   - il **codice etico comportamentale**, ossia, come già enunciato precedentemente, il codice di condotta aziendale redatto al fine di:
     - informare le persone interne all'azienda e i soggetti terzi della natura dell'impegno aziendale nel combattere reati e comportamenti illeciti;
     - aumentare la coscienza e la conoscenza dell'etica e delle politiche aziendali tra i dipendenti per ottenere il loro consenso e supporto alla lotta contro la corruzione, le frodi e la negligenza, l'imperizia e l'imprudenza in materia di sicurezza del lavoro e verso la tutela dell'ambiente;
   - la **creazione di un sistema organizzativo chiaro ed esaustivo** (in particolare per quanto riguarda l'attribuzione dei compiti e delle responsabilità, l'organigramma aziendale e il funzionigramma, il sistema delle deleghe e sub-deleghe, la descrizione chiara e definita dei compiti dei differenti soggetti aziendali);
3. **l'adozione di un sistema disciplinare** che preveda sanzioni per le inosservanze attivato, ad esempio, dal responsabile del personale o dai dirigenti, dall'OdV stesso. È importante l'adozione di un sistema di controllo sull'attuazione delle misure e sul mantenimento nel tempo della loro idoneità;
4. **l'individuazione dei criteri per la scelta e la nomina dell'OdV**, specificando la sua terziarietà e la sua indipendenza, autonomia di iniziativa e controllo e la regolamentazione dei flussi informativi verso l'OdV stesso (vedi linee guida Confindustria);
5. **l'adozione formale** del modello;
6. **l'aggiornamento continuo** del modello;
7. **il riesame del sistema ed eventuale sua modifica** da attuarsi nel momento in cui si ravvisino violazioni significative delle norme prevenzionistiche o in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

Modello di Organizzazione e Gestione secondo l'art. 30 del D.lgs. 81/08

Deve essere chiaro sin dall'inizio che **non esiste** un modello organizzativo di cui all'art. 30 del D.lgs. n. 81/08, ma solo un modello organizzativo e gestionale ai sensi dell'art. 6 comma 1 lett. a) del D.lgs. 231/01, i cui obiettivi, in questo caso specifico, sono la definizione e l'attuazione di una politica aziendale relativa alla salute e sicurezza dei lavoratori. Il Modello Organizzativo di cui alla 231/01 va dunque **ampliato** includendo i principi indicati dall'art. 30 del D.lgs. 81/08, il quale è norma aggiuntiva e integrativa, non derogatoria. L'adozione di tale modello deriva dalla necessità

di prevenire i reati di cui agli artt. 589 (omicidio colposo) e 590 (lesioni colpose gravi o gravissime) del c.p. commessi, come indicato nell'art. 25-septies 231/01, per violazioni delle norme sulla tutela della salute e della sicurezza sul lavoro (tra le quali è ricompresa anche la violazione dell'art. 2087 del c.c.) e individuati dallo stesso 231/01 quali reati-presupposto. La commissione di tali reati da parte di soggetti in posizione apicale potrebbe determinare la responsabilità amministrativa in sede penale dell'ente, il quale non risponde della stessa se è in grado di dimostrare di avere adottato ed efficacemente attuato, un modello di organizzazione e gestioni idoneo.

Si sottolinea inoltre che tali violazioni possono configurarsi come "reato proprio"[6], riferito ad un soggetto specifico (datore di lavoro, dirigente, preposto), sul quale ricade la responsabilità penale (essendo egli titolare della **posizione di garanzia**, ossia in capo ad esso è posto l'obbligo di tutela dell'integrità dei lavoratori), anche nel momento in cui la condotta sia posta in essere materialmente da altri soggetti. Pertanto, da parte di tali soggetti va sempre esercitato il potere impeditivo, diretto o indiretto di tali reati, anche mediante l'intervento di figure operative che intervengano direttamente o di segnalatori qualificati, come il RSPP (Responsabile del Servizio di Prevenzione e Protezione) o consulenti. Secondo l'art. 40 del c.p. – **rapporto di causalità**: "*nessuno può essere punito per un fatto preveduto dalla legge come reato, se l'evento dannoso o pericoloso, da cui dipende l'esistenza del reato, non è conseguenza della sua azione o omissione. Non impedire un evento che si ha l'obbligo giuridico di impedire equivale a cagionarlo*". Questo significa, per quanto riguarda la sicurezza sul lavoro, che una violazione commessa da un soggetto sottoposto è sempre potenzialmente una violazione del soggetto apicale, che deve dimostrare di aver adempiuto al proprio dovere di vigilanza previsto dall'art. 18 comma 3-bis del D.lgs 81/08 (sempre sottolineando che in caso di violazione da parte di soggetto sottoposto, è l'accusa che deve dimostrare l'omessa vigilanza da parte dei soggetti ad essa preposti).

L'art. 30 del D.lgs. 81/08 prescrive che il sistema di gestione sia adottato ed efficacemente attuato assicurando l'individuazione di un sistema aziendale atto all'adempimento di tutti gli obblighi giuridici relativi, in particolare:

1. al rispetto degli standard tecnico – strutturali di legge relativi alle attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
2. alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
3. alle attività di natura organizzative (emergenze, primo soccorso, riunioni periodiche, gestione di appalti, consultazioni degli RLS ecc.);
4. alle attività di sorveglianza sanitaria;

[6] Il reato può essere proprio o comune: è proprio il reato che può essere commesso soltanto da colui che rivesta una determinata qualifica o posizione; è comune il reato che può essere commesso da chiunque. (https://www.brocardi.it/dizionario/3241.html)

5. alle attività di informazione, formazione e addestramento dei lavoratori;
6. all'acquisizione di documentazione e certificazioni obbligatorie per legge;
7. alle verifiche realizzate per il riscontro dell'efficacia delle procedure.

Il modello deve inoltre prevedere:

1. idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui sopra;
2. un'articolazione di funzioni che assicuri le competenze tecniche per il controllo, la gestione e l'individuazione del rischio, valutata a seconda della natura e delle dimensioni dell'organizzazione;
3. un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;
4. un idoneo sistema di controllo per il mantenimento nel tempo delle condizioni di idoneità delle misure adottate;
5. il riesame e l'eventuale modifica del modello, per esempio, in occasione di mutazioni dell'organizzazione o delle attività lavorative, o in caso di violazione delle norme relative alla prevenzione degli infortuni e all'igiene del lavoro.

Per quanto concerne la materia della salute e sicurezza nei luoghi di lavoro, non esistono in questo contesto aree, mansioni, attività esenti dal rischio, ma per qualsiasi situazione sarà necessario effettuare un'approfondita valutazione dei rischi per verificare che il rischio residuo possa considerarsi accettabile ai sensi della 231/01. L'introduzione del sistema di gestione quale scriminante per la responsabilità dell'azienda per gli infortuni e le malattie professionali ha portato una forte innovazione con rilevanti aspetti positivi anche per quanto riguarda gli aspetti di produttività intrinseci all'impresa. Nel caso delle piccole e medie aziende, che spesso sono organizzate con logiche "fai da te", si rileva spesso una mancanza di struttura e di una vera e propria cultura imprenditoriale. Affinché l'applicazione di un sistema di gestione sia vincente, è necessario che i contenuti del sistema vengano innanzitutto condivisi a partire dal datore di lavoro sino all'apprendista. È inoltre necessario focalizzarsi solo ed esclusivamente sugli aspetti formali e documentali, ma il sistema va pensato, progettato ed applicato correttamente.

Gli operatori qualificati dispongono di diverse opzioni per implementare un sistema di gestione in materia di salute e sicurezza nei luoghi di lavoro. Ricordiamo che adottare un SGSL non è un obbligo di legge, ma una svolta volontaria di chi sente la responsabilità per la propria sicurezza e per quella degli altri; l'adozione di un SGSL consente di ridurre i costi per la "non sicurezza", in quanto riduce la probabilità di accadimento degli infortuni e i costi che ne conseguono.

L'art. 30 comma 5 del D.lgs. 81/08 individua degli standard ai quali ci si può riferire per l'implementazione di un Sistema di Gestione della Salute e Sicurezza sul Lavoro (SGSL), affermando quanto segue: "*in sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e*

sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti agli stessi fini. Ulteriori modelli di organizzazione e gestione aziendale possono essere indicati dalla Commissione di cui all'articolo 6".
Il comma 5-bis dello stesso articolo recita: "*la commissione consultiva permanente per la salute e sicurezza sul lavoro elabora procedure semplificate per la adozione e la efficace attuazione dei modelli di organizzazione e gestione della sicurezza nelle piccole e medie imprese. Tali procedure sono recepite con decreto del Ministero del lavoro, della salute e delle politiche sociali".*

Riepilogando quanto indicato dall'art. 30 del D.lgs. 81/08, gli standard di riferimento che è possibile adottare per l'implementazione di un idoneo modello di gestione per la sicurezza sul lavoro sono i seguenti:

1. le linee guida S.G.S.L. UNI-INAIL del 2001;
2. la norma BS OHSAS 18001:2007 (la norma ISO 45001:2018 avrebbe dovuto definitivamente sostituire la BS OHSAS 18001:2007 dal 12 marzo 2021, termine che è stato prorogato alla data 30 settembre 2021 al fine di tutelare le aziende interessate alla migrazione che stanno incontrando oggettive difficoltà a causa della crisi sanitaria causata dal Covid-19[7]. Entro il 30 settembre 2021 pertanto, si dovrà concludere il processo di migrazione delle certificazioni dei sistemi di gestione per la salute e sicurezza sul lavoro rilasciate dagli organismi accreditati; al momento attuale le due norme coesistono);
3. la norma UNI-ISO 45001:2016.

In seguito, è riportata una breve descrizione di ciascuno standard sopra citato.

[7] https://www.accredia.it/2018/04/04/nuova-norma-uni-iso-45001-tre-anni-per-completare-la-migrazione-delle-certificazioni-di-sistema-di-gestione-per-la-salute-e-sicurezza-sul-lavoro/

Le linee guida UNI-INAIL 2001

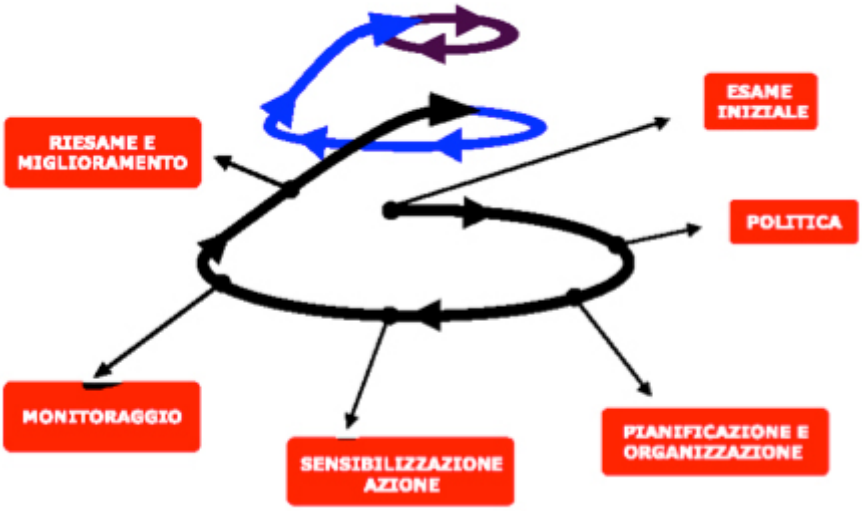

Figura 1: Ciclo di Deming

In accordo con le parti sociali (CGIL, CISL, CNA, Confagricoltura, Confartigianato, Confindustria, UNI), l'INAIL ha pubblicato le "Linee guida per un sistema di gestione della salute e sicurezza nei luoghi di lavoro" per aiutare le imprese che intendono volontariamente adottare un sistema di gestione della sicurezza.

Esse hanno validità generale e la loro applicazione va modulata secondo le caratteristiche dell'impresa. La finalità del sistema di gestione ex linee guida UNI-INAIL è quella di garantire il raggiungimento degli obiettivi di salute e sicurezza che l'impresa si è data, in un efficace prospettiva di costi/benefici.

Il sistema si propone di:

- ridurre i costi complessivi della salute e sicurezza sul lavoro, minimizzando i rischi a cui possono essere esposti i dipendenti e i terzi (clienti, fornitori, visitatori);
- aumentare l'efficienza delle prestazioni d'impresa;
- contribuire a migliorare i livelli di salute e sicurezza dell'impresa;
- migliorare l'immagine interna ed esterna dell'impresa.

I contenuti delle fasi possono essere più o meno complessi in ogni singola azienda o unità produttiva in funzione di:

- dimensione, natura, attività e relativa complessità dell'organizzazione;
- significatività dei pericoli e rischi presenti, potenziali o residui;
- soggetti potenzialmente esposti.

Il SGSL di cui alle linee guida UNI INAIL opera sulla base del "Ciclo di Deming" ossia della sequenza ciclica delle fasi di **pianificazione, attuazione, verifica e monitoraggio e riesame del sistema**, per mezzo di un processo dinamico, con il proposito del **miglioramento** continuo. Di seguito sono brevemente descritte le fasi citate precedentemente:

PIANIFICAZIONE:

Per il successo di un Sistema di Gestione occorre l'impegno di tutti i livelli e di tutte le funzioni aziendali, a partire dalla Direzione fino ad arrivare ai singoli dipendenti. Il ciclo ha inizio con la definizione da parte della Direzione della politica della sicurezza. Tale politica deve essere appropriata all'azienda, specificando gli impegni del vertice aziendale, i principi d'azione e i risultati a cui tendere per la sicurezza.

La politica per la sicurezza dovrebbe:

- comprendere l'impegno al rispetto della legislazione in tema di Sicurezza;
- essere comunicata, diffusa e disponibile per tutti i dipendenti;
- essere documentata, attuata, aggiornata e mantenuta;
- essere adeguata alla natura ed entità dei rischi presenti;
- prevedere impegno sulla disponibilità delle risorse necessarie;
- essere volta al miglioramento continuo e alla prevenzione.

L'azienda deve formulare una serie di azioni (piani, programmi) volti a dimostrare il soddisfacimento dei requisiti.

Requisiti chiave della pianificazione:

- definizione degli obiettivi e dei rispetti traguardi misurabili;
- predisposizione di un piano operativo/temporale per ogni obiettivo;
- definizione delle risorse (es.: locali, risorse umane, attrezzature, ecc.) necessarie, comprese quelle economiche. Questa pianificazione dovrebbe tener conto:
    - delle attività lavorative ordinarie e straordinarie, comprese le situazioni di emergenza, con priorità decrescente in funzione dei rischi rilevati;
    - delle attività di tutto il personale (inclusi lavoratori con contratto a tempo determinato, fornitori, clienti, visitatori, ecc.), che ha accesso ai luoghi di lavoro e/o ha interferenza con le attività lavorative svolte negli uffici e/o negli impianti e/o nei cantieri;
    - delle modifiche ed integrazioni legislative in ambito sicurezza applicabili all'organizzazione;

- delle strutture, dei luoghi e dei metodi di lavoro, delle macchine, degli impianti, delle attrezzature, delle sostanze e tecnologie utilizzate, sia che siano quelle proprie dell'azienda sia che vengano fornite da terzi.

ATTUAZIONE

L'attuazione del SGSL avviene tramite il controllo delle attività, la definizione di procedure documentate e di registrazioni formali che costituiscono il riscontro oggettivo dell'applicazione della politica per la sicurezza. Per prima cosa è necessario definire l'organizzazione con i diversi legami gerarchici e le mansioni delle singole funzioni sia dirigenziali sia operative. Il SGSL prevede di definire in modo documentato le procedure e le prassi aziendali così da consolidare ed uniformare i comportamenti e le istruzioni (CHI FA? / CHE COSA FA? /IN CHE MODO?).

Il personale, così come richiesto anche dal D.lgs. 81/08, deve essere consapevole e competente in merito ai rischi connessi al proprio lavoro. È necessario definire programmi di addestramento mirati sia ai rischi riguardanti le attività dell'Azienda in generale, sia ai rischi specifici in relazione alle mansioni svolte, registrando le singole formazioni attuate.

Identificate le condizioni e gli impianti che possono generare situazioni di emergenza, il SGSL deve prevedere attività preventive di verifica e di formazione, rivolte sia a limitare i danni in caso di avvenimento dell'emergenza, sia ad evitarne l'accadimento dello stesso. Il controllo operativo prevede che l'azienda individui e gestisca tutte quelle funzioni, attività e processi che in qualche modo hanno un impatto sulla salute e sicurezza dei lavoratori, introducendo le procedure e le istruzioni necessarie.

Una volta identificati i processi critici, ne vengono rilevate le pericolosità, le attività operative connesse con le loro interrelazioni e le regole operative per controllarli al meglio. Il controllo operativo prevede la gestione e la manutenzione degli impianti, in quanto attrezzature di lavoro efficienti, comportano minori possibilità di funzionamento anomalo e minore possibilità di accadimento di incidenti/infortuni. L'applicazione del SGSL prevede lo sviluppo di efficaci canali di informazione (es.: bacheche, circolari interne, comunicazioni audio, ecc.), interni ed esterni, riguardanti aspetti della sicurezza. Le comunicazioni devono essere attuate anche per la diffusione delle disposizioni legislative sempre in continua evoluzione.

MONITORAGGIO E VERIFICA

All'interno delle attività di monitoraggio e verifica sono comprese, sia le sorveglianze e le misurazioni delle caratteristiche delle operazioni e/o attività che possono produrre impatti significativi sulla sicurezza e salute dei lavoratori (compresa la gestione delle non conformità, azioni correttive e preventive), sia le attività di audit sul SGSL.

L'attività di monitoraggio avviene in genere mediante:

- misurazione e monitoraggio delle prestazioni;
- attivazione di procedure preventive e correttive per infortuni, incidenti e non conformità;
- registrazioni di sistema e loro gestione e conservazione;
- predisposizione e mantenimento di un programma di audit.

I risultati del SGSL (in termini di controlli eseguiti, attività legate agli obiettivi e traguardi, misure di prevenzione, ecc.) devono essere misurati, monitorati e valutati nella loro efficacia. Prioritarie sono la conduzione, la registrazione e l'archiviazione delle misurazioni previste dalle disposizioni legislative (es. rumore, polveri, ecc.). Il SGSL prevede l'identificazione di opportuni indicatori che permettono di monitorare nel tempo le prestazioni aziendali.

Le verifiche ispettive della sicurezza hanno lo scopo di assicurare che le varie aree ed attività di lavoro siano progettate, condotte e mantenute sia in modo da proteggere adeguatamente la sicurezza degli operatori, sia in conformità alle procedure interne documentate, quindi:

- verifica dell'adeguatezza ed efficacia del SGSL;
- aggiornamento valutazione rischi;
- aggiornamento o implementazione degli obiettivi;
- adeguatezza delle risorse e dei bisogni formativi;
- efficacia delle verifiche ispettive interne;
- non conformità, infortuni, incidenti, potenziali incidenti;
- analisi delle statistiche;
- gestione delle emergenze.

Dunque, periodicamente l'azienda effettua un'attività di verifica con lo scopo di valutare l'adeguatezza del Sistema Sicurezza al raggiungimento degli obiettivi previsti dalla politica aziendale, all'adempimento dei vincoli normativi, all'implementazione delle nuove tecnologie e/o lavorazioni. Questo riesame si fonda sia sull'analisi di informazioni e dati raccolti durante l'implementazione del SGSL, sia sui risultati delle verifiche ispettive e delle attività di sorveglianza e permette all'azienda di aggiornare periodicamente il proprio Sistema (anche alla luce di eventuali punti di criticità emersi durante l'esercizio dello stesso), mediante l'introduzione di opportune azioni correttive.

RIESAME DEL SISTEMA

Dopo la conclusione del ciclo di monitoraggio interno, il vertice aziendale dovrebbe sottoporre a riesame le attività del sistema di gestione della sicurezza per valutare se il sistema sia adeguatamente attuato e si mantenga idoneo al conseguimento degli obiettivi e della politica della sicurezza stabilita dall'azienda.

MIGLIORAMENTO

Concluso il riesame del SGSL il ciclo di Deming prevede un nuovo percorso PDCA permettendo all'azienda di migliorare l'efficacia degli interventi già attuati, intervenendo tramite processi correttivi ed esercitando una attività di autocontrollo finalizzata al miglioramento e non semplicemente alla pur doverosa ottemperanza alle leggi.

La norma BS OHSAS 18001:2007

La norma definisce quelli che sono i requisiti che un "Sistema di Gestione per la Salute e la Sicurezza nei Luoghi di Lavoro" deve possedere affinché, l'organizzazione che decide di adottarlo, possa perseguire in modo efficace gli obiettivi del benessere dei propri lavoratori e degli altri soggetti che operano nell'ambito dell'organizzazione. Lo standard è rivolto alle organizzazioni di tutte le dimensioni e di tutti i settori merceologici e permette di dotarsi di un SGLS finalizzato al miglioramento continuo delle prestazioni organizzative in materia di sicurezza e salute nei luoghi di lavoro.

La norma OHSAS 18001:2007 è strutturata in modo tale da potersi inserire nel più vasto sistema di gestione aziendale, integrandosi perfettamente con le norme ISO 9001 e ISO 14001.

Implementare un sistema di gestione in tal senso permette di:

1. aumentare la prevenzione ed il controllo dei luoghi di lavoro riducendo il numero degli infortuni;
2. assicurare la conformità legislativa;
3. ridurre notevolmente il rischio di incidenti gravi;
4. migliorare in modo significativo e misurabile le prestazioni in materia di sicurezza;
5. accrescere la soddisfazione del personale e migliorare il clima aziendale.

Anche il SGSL indicato dalla norma OHSAS 18001 opera secondo il ciclo di Deming (pianificazione, attuazione, verifica e riesame del sistema).

PIANIFICAZIONE

Tale fase si può suddividere in tre step:

- PRIMO STEP: identificazione dei pericoli, valutazione dei rischi e determinazione delle misure di controllo. L'organizzazione definisce una o più procedure che dovranno indicare come si ha intenzione di procedere per l'identificazione dei pericoli e le metodologie che si intendono attuare per effettuare la valutazione dei rischi. Le indicazioni contenute all'interno di queste procedure sono quelle che poi andranno a far parte del Documento di Valutazione dei rischi, di cui all'art. 28 del D.lgs. 81/08. Devono essere identificate durante questo step tutte le strategie per la gestione dei cambiamenti che possono avere un impatto sulla salute e sicurezza dei lavoratori, in modo tale che tali cambiamenti siano valutati prima di essere attuati. Una volta individuati i rischi, si deve procedere con l'identificazione delle misure di

eliminazione/contenimento dei rischi (meglio conosciute come misure di prevenzione e protezione).

- SECONDO STEP: Verifica della conformità legislativa. È necessario per l'organizzazione dotarsi di procedure volte ad individuare quali siano le norme di legge a cui è soggetta e permettere l'accesso alle stesse a tutti i soggetti interessati, comunicando le eventuali variazioni. Oltre alle norme di legge è necessario identificare e diffondere anche le disposizioni aziendali, contrattuali ecc...
- TERZO STEP: obiettivi e programma. L'organizzazione deve definire quali obiettivi sia necessario raggiungere per attuare la politica aziendale in materia di salute e sicurezza sul lavoro; tali obiettivi devono essere **misurabili** al fine di dare evidenza del loro raggiungimento. Deve essere definito un programma tenendo conto delle risorse da impiegare, dei mezzi necessari e dei compiti da svolgere. Gli obiettivi devono essere divulgati a tutto il personale con lo scopo di coinvolgere tutti i lavoratori.

ATTUAZIONE

Per poter procedere all'attuazione del sistema si deve verificare se le responsabilità in materia di salute e sicurezza sul lavoro siano state definite coerentemente con lo schema organizzativo e funzionale dell'organizzazione. Devono essere resi noti, oltre alla definizione dei compiti organizzativi e operativi della direzione, dei dirigenti, dei preposti e dei lavoratori anche quelli relativi alle attività di sicurezza di loro competenza e le responsabilità connesse all'esercizio delle stesse; ogni ruolo e le sue responsabilità devono essere documentati. Un altro requisito fondamentale, al fine della corretta attuazione del sistema, è che vengano garantiti all'interno dell'organizzazione adeguati livelli di consapevolezza circa le azioni di ciascuno rispetto alla politica ed ai requisiti del SGSL, in particolare in caso di discostamento delle stesse da quanto previsto dalle procedure e norme di sicurezza. Inoltre, l'organizzazione deve attivarsi affinché tutto il personale sia sufficientemente competente per partecipare al funzionamento del Sistema di Gestione, incoraggiando l'attiva partecipazione dei lavoratori. La formazione e l'addestramento dovrebbero essere programmati secondo il fabbisogno rilevato periodicamente anche mediante la consultazione dei lavoratori e dei loro rappresentanti. La circolazione delle informazioni all'interno dell'organizzazione è di fondamentale importanza; maggiore è la condivisione delle informazioni e maggiore è la partecipazione attiva al sistema, maggiore sarà la probabilità di prevenire gli infortuni e le malattie professionali. La direzione deve dunque definire e attuare efficaci modalità di comunicazione sulle politiche, gli obiettivi, i programmi e i risultati, incoraggiando il ritorno dell'informazione e favorire la comunicazione interpersonale per un miglioramento degli aspetti relazionali.

La documentazione riguardante il sistema di gestione (la politica, le procedure e i loro allegati e le registrazioni) deve essere mantenuta aggiornata. Essa deve rispondere alle effettive esigenze dell'organizzazione per garantire che il sistema di gestione sia efficiente, ma anche semplice e

snello. La documentazione relativa al sistema deve essere adeguatamente gestita definendo le modalità per la sua identificazione, approvazione, pubblicazione, distribuzione, eliminazione. Inoltre, devono essere predisposte delle procedure che definiscano chi ha la responsabilità della redazione e del controllo dei documenti e che contemplino la tenuta di appositi registri che indichino la documentazione ancora attiva e quella archiviata.

Il controllo operativo dei rischi prevede l'attuazione di misure di prevenzione e protezione già individuate in fase di pianificazione. La scelta delle misure dovrà seguire quanto indicato all'interno dell'art. 15 del D.lgs. 81/08 (misure generali di tutela), al fine di raggiungere la soglia del rischio accettabile. Tali misure dovranno essere soggette a controlli periodici in modo tale da verificarne l'adeguatezza e il perdurare della soglia di accettabilità del rischio.

L'organizzazione deve dotarsi anche di una procedura che permetta di identificare e gestire eventuali situazioni di emergenza. Tale procedura può coincidere, ad esempio, per quanto riguarda il rischio incendio, con il Piano di emergenza di cui al DM 10 Marzo 1998, da integrarsi con le procedure relativi alla gestione di altri tipi di emergenza (black-out, infortunio, terremoto, alluvione, rapina ecc …)

CONTROLLO

Misurazione delle prestazioni e monitoraggio: consiste nell'osservazione dell'andamento delle prestazioni per accertarsi se gli obiettivi siano stati raggiunti, se i requisiti di legge sono soddisfatti, se si sono verificati eventi che necessitano di interventi correttivi. Alcuni tipi di misurazioni possono essere di natura proattiva (verifica dell'efficacia della formazione e dell'addestramento) o reattiva (indice infortunistico). Tali verifiche e controlli possono essere svolte da personale interno all'azienda o esterno (es. audit). Tutti gli infortuni o i "near miss" devono essere segnalati da chiunque ne abbia notizia e successivamente analizzati dall'organizzazione, allo scopo di capire se vi siano state carenze a identificare le conseguenti misure correttive, preventive e valutare le opportunità di miglioramento del sistema.

Registrazioni: tutte le evidenze che possono dimostrare la corretta attuazione del sistema devono essere correttamente archiviate e gestite, anche per facilitare le attività di monitoraggio.

Audit: uno degli strumenti attraverso cui l'organizzazione valuta le prestazioni e l'efficacia del proprio sistema sono gli audit. Questi hanno lo scopo di stabilire se il sistema sia conforme a quanto pianificato, sia applicato nel modo corretto e se consenta di raggiungere gli obiettivi prefissati. Attraverso il sistema di controllo (monitoraggio e verifiche) il vertice aziendale ha la possibilità di prendere decisioni strategiche di propria competenza al fine di attuare azioni correttive e perseguire il miglioramento continuo del sistema.

RIESAME DELLA DIREZIONE

Tale fase è l'ultima e chiude il ciclo di Deming. A valle degli audit, il vertice aziendale dovrebbe sottoporre a riesame l'attività del Sistema di Gestione per valutare se esso sia adeguatamente attuato e si mantenga idoneo nel tempo al conseguimento degli obiettivi relativi alla salute e sicurezza sul lavoro prefissati. Gli elementi oggetto del riesame possono essere:

- risultati dei monitoraggi interni;
- rapporti sull'identificazione dei pericoli e sulla valutazione e controllo dei rischi;
- rapporti sull'efficacia del sistema di gestione;
- le non conformità, gli infortuni, gli incidenti e i quasi incidenti accaduti (statistiche infortuni);
  le azioni correttive e preventive intraprese e da intraprendere;
- lo stato di avanzamento degli obiettivi;
- la ridefinizione del riesame iniziale;
- i programmi di miglioramento.

Una volta concluso il riesame, oltre a valutare lo stato di conseguimento degli obiettivi prefissati, la Direzione, alla luce dei risultati forniti dal monitoraggio del sistema, dell'esecuzione delle azioni correttive e preventive e delle eventuali modifiche della situazione, dovrebbe stabilire nuovi obiettivi e piani, nell'ottica del miglioramento progressivo, considerando l'opportunità di modificare la politica, le procedure e eventuali altri elementi del sistema.

Si ricorda, come precedentemente anticipato, che i sistemi di gestione implementati secondo la norma BS OHSAS 18001:2007 dal 30 settembre 2021 non saranno più validi.

La norma UNI ISO 45001:2018

La UNI ISO 45001 è la prima norma internazionale per la salute e la sicurezza nei luoghi di lavoro. Stabilisce un quadro per migliorare la sicurezza, ridurre i rischi in ambito lavorativo e migliorare la salute e il benessere dei lavoratori, permettendo così alle organizzazioni di aumentare in modo proattivo le performance in materia di salute e sicurezza.

Il percorso di maturazione internazionale, che ha portato nel 2018 alla nascita della UNI ISO 45001, è durato più di 20 anni, esordendo nel 1996 con la BS 8800, poi seguito nel 1999 dalla OHSAS 18001. Il mercato internazionale ha dimostrato in questi anni un crescente interesse verso i SGSL e ha visto una crescente adesione delle imprese alla norma BS OHSAS 18001, pur trattandosi di uno standard britannico. Proprio tale diffusione ha posto la necessità di armonizzare i contenuti con una norma internazionale completamente integrabile nel "sistema azienda", grazie alla radice comune a tutti i sistemi (qualità – ISO 9001 e Ambiente - ISO 14001).

Per facilitare l'integrazione della ISO 45001 con altri sistemi (es. qualità, ambiente) eventualmente implementati all'interno dell'organizzazione, essa aderisce al modello HLS (High Level Structure), ossia la sua struttura è comune a quella degli altri standard internazionali gestionali. La migrazione allo standard ISO 45001: 2018 dallo standard BS OHSAS 18001:2007 determinerà per le organizzazioni che avevano già implementato il sistema secondo lo standard

britannico, delle integrazioni al sistema secondo quanto introdotto dalla nuova norma, riguardanti:

- **l'approccio metodologico basato su l'HLS** (High Level Structure), già introdotto con le nuove revisioni della ISO 9001 e della ISO 14001 e non contemplato nella norma BS OHSAS 18001:2007;

- **la valutazione dei rischi e delle opportunità attraverso risk-based thinking** (strategia basata sul rischio, ossia lo strumento per valutare e gestire gli imprevisti che si presentano nel raggiungimento degli obiettivi aziendali). Il pensiero basato sul rischio (risk-based thinking) è il concetto introdotto dalle norme di nuova generazione sui di sistemi di gestione, come la ISO 9001, la ISO 14001 e tutte le altre norme che si basano su High Level Structure (HLS). Questo rappresenta il punto di partenza per pianificare e attuare i processi del sistema di gestione, per pianificare e per implementare le azioni da intraprendere con il fine di affrontare i rischi e le opportunità e per misurare l'efficacia delle azioni intraprese. L'approccio diventa quindi proattivo, mettendo in atto misure e controlli per minimizzare preventivamente gli effetti negativi, massimizzare le opportunità (quando esse si presentano) e conseguire il miglioramento continuo.

- **l'identificazione e l'analisi del contesto dell'impresa:** l'organizzazione, infatti, è inserita all'interno di diverse "condizioni di contesto" sia interne che esterne, per questo è necessario determinare quali siano i fattori interni ed esterni che influenzano la sua capacità di conseguire i risultati attesi.

  Alcuni esempi di fattori esterni sono:
  - l'ambiente culturale, sociale, politico, legale, finanziario, tecnologico, economico e naturale di concorrenza di mercato, sia a livello internazionale e/o nazionale e/o regionale e/o locale
  - l'ingresso nel mercato di nuovi concorrenti, appaltatori, subappaltatori, fornitori di beni, introduzione di nuove tecnologie e nuove leggi;
  - nuove conoscenze sui prodotti e sui loro effetti sulla salute e sicurezza dei lavoratori;
  - tendenze che hanno un impatto sull'organizzazione.

  Alcuni esempi di fattori interni sono:
  - la struttura organizzativa, i ruoli le responsabilità;
  - le politiche, gli obiettivi e le strategie attuate per realizzarli;
  - risorse a disposizione, conoscenze e competenze (capitale, risorse umane, processi, sistemi, tecnologie);

- sistemi informativi e flussi di informazioni;
- introduzione di nuovi prodotti, strumenti, software, locali e attrezzature;
- relazioni con i lavoratori e loro percezioni e valori;
- disposizioni sull'orario di lavoro e condizioni lavorative;
- cambiamenti relativi a ciascuno degli elementi menzionati sopra.

- **La valorizzazione del concetto di leadership**: i processi aziendali devono essere governati con impegno evidente da parte del management. Si pone una maggiore enfasi sulla leadership; il ruolo del top management nei processi aziendali diviene centrale, affinché si impegni attivamente e si assuma la responsabilità per l'efficacia del sistema di gestione e nella promozione della cultura della sicurezza.

- **L'identificazione e la comprensione delle esigenze e delle aspettative degli stakeholder** che hanno influenza sulle imprese.

  Alcuni esempi di parti interessate sono:

  - lavoratori (la norma introduce una maggiore attenzione a bisogni ed aspettative dei lavoratori e delle altre parti interessate ed il coinvolgimento dei lavoratori stessi);
  - autorità legislative;
  - fornitori, appaltatori, subappaltatori;
  - organizzazioni dei lavoratori (sindacati) e organizzazioni datoriali;
  - azionisti, clienti, visitatori, comunità locale;
  - media, università, associazioni di imprese, organizzazioni non governative.

Sono inoltre ridefiniti i requisiti riguardanti la valutazione e la gestione del rischio correlato a tutti i processi in outsourcing, dalla selezione, alla qualifica, alla contrattualizzazione dei fornitori.

Un altro aspetto è quello che riguarda obiettivi e prestazioni: viene posta maggiore attenzione agli obiettivi come fattori di miglioramento e valutazione delle prestazioni.

La norma UNI ISO 45001:2018 è applicabile da **qualsiasi organizzazione** che desideri implementare, attuare e mantenere un sistema di gestione per eliminare e minimizzare i rischi, cogliere le opportunità e prendere carico delle non conformità del sistema di gestione associate alle proprie attività per la salute e sicurezza dei lavoratori (SSL). La ISO 45001 non stabilisce criteri specifici per le prestazioni in termini di salute e sicurezza sul lavoro e può essere utilizzata in tutto o in parte per migliorare in modo sistematico la gestione della salute e della sicurezza, benché sia necessario attuarla in toto per ricevere la certificazione del modello.

Gli elementi comune tra i vari sistemi di gestione

Come anticipato precedentemente i sistemi gestionali riconosciuti nelle aree della qualità, ambiente e sicurezza sono:

- per la qualità: UNI EN ISO 9001:2015;
- per l'ambiente: UNI EN ISO 14001:2015
- per la sicurezza: BS OHSAS 18001:2007 - UNI EN 45001:2018

le tre norme ISO possiedono una struttura comune che consente la progettazione di un sistema di gestione integrato, ovvero di un sistema che consenta all'organizzazione un'amministrazione unica su tutte e tre le aree principali necessarie all'organizzazione stessa per ottenere un vantaggio competitivo duraturo nel tempo. In particolare, gli elementi fondamentali e comuni dei sistemi di gestione succitati sono:

- **Organizzazione orientata al cliente:** le organizzazioni dipendono dai propri clienti e dovrebbero pertanto capire le loro esigenze presenti e future, soddisfare i loro requisiti e mirare a superare le loro stesse aspettative.
- **Orientamento alla prevenzione relativamente alle aree oggetto del sistema di gestione:** nel caso specifico del sistema di gestione relativo alla sicurezza sul lavoro, esso mirerà ad una situazione di assenza di infortuni, incidenti, malattie professionali.
- **Leadership e coinvolgimento del personale**: i vertici aziendali stabiliscono le unità di intenti e di indirizzo dell'organizzazione. Il raggiungimento degli obiettivi di miglioramento è infatti possibile solo mediante l'impegno del management. I vertici aziendali dovrebbero, inoltre, creare e mantenere un ambiente interno che coinvolga pienamente il personale nel perseguimento degli obiettivi dell'organizzazione. Sono attuati processi di formazione e addestramento e la consultazione del personale; questo consentirà al personale di comprendere ed essere motivato nel perseguimento degli obiettivi e dei traguardi dell'organizzazione. Saranno ridotti i disguidi di comunicazione tra i diversi livelli dell'organizzazione. Le persone, a tutti i livelli, costituiscono l'essenza dell'organizzazione ed il loro pieno coinvolgimento permette di porre le loro capacità al servizio dell'organizzazione.
- **Approccio basato sui processi**: un risultato desiderato si ottiene con maggior efficienza quando le relative attività e risorse sono gestite come un processo. La gestione dei processi e del sistema può essere realizzata secondo il metodo del ciclo PDCA, con un orientamento al "risk based thinking" volto a cogliere le opportunità e a prevenire i risultati indesiderabili. Un processo trasforma qualcosa che entra, l'input, in qualcos'altro che esce dal processo, l'output, utilizzando metodologie ben precise (procedure, istruzioni di lavoro ecc.) e aggiungendo del valore perché opera in condizioni controllate. Un processo è costituito da delle azioni più o meno elementari collegate in sequenza logica e temporale, tali che, prese nel loro complesso, sia possibile identificare un unico attore nel ruolo di responsabile o più attori co-responsabili.

    - Tutte le attività fanno parte dei processi;
    - Il processo è una trasformazione con valore aggiunto;
    - Ogni processo coinvolge persone e/o risorse;

- Ogni processo ha input e output (risultati);
- Ogni processo richiede controlli per assicurare stabilità;
- Occorre misurare gli input, le attività di processo, gli output.

- **Approccio sistemico alla gestione:** identificare, capire, e gestire processi tra loro correlati (come se fossero un sistema), contribuisce all'efficacia e all'efficienza dell'organizzazione nel conseguire i propri obiettivi. L'obiettivo dell'approccio sistemico è quello di passare da un'ottica divisionale ad un'ottica sistemica. Per sistema si intende un insieme di oggetti (parti, componenti, funzioni, processi) legati tra loro da relazioni di interdipendenza. Un'organizzazione per funzionare efficacemente deve identificare e gestire numerosi processi tra loro correlati ed interagenti.
- **Documentazione aziendale:** è indispensabile che i documenti connessi al sistema di gestione definiscano sempre più precisamente le responsabilità, i ruoli, le mansioni, i programmi e stabiliscano procedure e regolamenti interni.
- **Miglioramento continuo:** il miglioramento continuo delle prestazioni complessive dovrebbe essere un obiettivo permanente e dell'organizzazione. Questo significa che, dopo aver raggiunto i requisiti pianificati dal processo, l'organizzazione dovrebbe concentrare i suoi sforzi per portare in modo continuativo, le prestazioni dei processi verso livelli sempre più elevati.

  Alcuni elementi per il miglioramento potrebbero essere:

  - ridurre la burocrazia;
  - eliminare attività quali approvazioni, compilazioni di carte, che non hanno più ragion d'essere perché inutili;
  - rimuovere attività identiche ripetute più volte, o da più persone;
  - semplificare, ridurre complessità del processo mediante, ad esempio, riduzione delle fasi, degli obiettivi o delle relazioni. Ciò può significare anche rendere tutto più facile da apprendere, da fare, da comprendere.

  La metodologia P.D.C.A. può essere un utile strumento per definire, attuare e controllare le azioni correttive e per il miglioramento. Questa metodologia si applica egualmente sia ai processi strategici di alto livello, che alle semplici attività lavorative.

  Si può migliorare solo ciò che si può misurare! Un processo non misurato è un processo non gestito!

- **Decisione basate su dati e sui fatti:** le decisioni vanno sempre prese basandole sull'analisi di dati e di informazioni attendibili e concreti. È importante in questa fase assicurarsi che i dati e le informazioni siano accurati ed affidabili, rendere accessibili dati e informazioni a chi ne

ha bisogno, analizzare dati ed informazioni utilizzando metodi validi, assumere decisioni ed effettuare azioni basandosi su analisi di fatti reali, solo in assenza di essi, su esperienza ed intuizione.

- **Rispetto dei requisiti di legge:** osservando questi principi salta all'occhio che i vari sistemi di gestione, pur essendo diversi per le loro finalità, obiettivi e motivazioni hanno in comune degli elementi portanti, si rivolgono all'organizzazione coinvolgendo tutti a partire dalla direzione fino al lavoratore e la loro applicazione non è obbligatoria né vincolante. Ad oggi non esiste una norma che fornisca un modello per l'implementazione di un sistema di gestione integrato, che consenta l'implementazione di un sistema a tutto tondo.
- **Riesame della direzione – auditing interno/esterno**: al fine di valutare la funzionalità dei sistemi e metterne in luce le criticità, valutare e individuare nuove soluzioni e possibili miglioramenti è necessario effettuare un processo di **auditing** e il successivo riesame della direzione.

La parola "audit" deriva dal latino auditus, cioè l'atto dell'udire, dell'ascoltare, participio passato del verbo audire. Nella seconda metà del 1900 il termine audit si diffuse dalla gestione dell'organizzazione finanziaria a tutta l'organizzazione, interessando sia l'area dell'ambiente che quella della qualità. Per la direzione dell'azienda risultava sempre più necessario compiere verifiche non occasionali e condotte con una precisa metodologia.
Negli anni 70 presso le imprese del Nord America si diffuse l'esigenza di tali verifiche anche in tema di sicurezza e di igiene industriale, specialmente circa la costruzione di strutture critiche quali ad esempio i rettori nucleari, gli armamenti o altro. Al giorno d'oggi il termine audit si applica ad un processo ben definito che si basa:

- Sulla decisione di fare un audit (chi lo chiede?);
- Sull'identificazione dell'obiettivo dell'audit (perché lo si fa?):
- Sulla cosa si sottopone ad audit (l'oggetto dell'audit);
- Sui criteri rispetto ai quali si svolge l'audit (procedure, leggi, documentazione di riferimento, leggi cogenti ecc.);
- Su chi eseguirà l'audit (auditor);
- Sulla metodologia di esecuzione dell'audit.

La logica dell'audit risiede nel verificare se un prodotto o un processo è conforme a quanto si prende a riferimento. Se l'audit andrà a verificare un sistema di gestione il riferimento è la norma internazionale che descrive il sistema di gestione.
L'auditor, colui che conduce l'audit, andrà a valutare l'efficacia e l'efficienza di un sistema di gestione aziendale e andrà a fornire informazioni utili alle parti interessate. È uno strumento molto utile per il miglioramento delle prestazioni aziendali. Le persone che eseguono l'audit sono professionalmente preparate e in possesso di adeguate competenze, senza pregiudizi e interessi nei confronti dell'organizzazione, in modo tale che le loro valutazioni assicurino risultati trasparenti e verificabili da altri auditor. La definizione di audit secondo la norma ISO 19011:2018 che definisce le linee guida per lo svolgimento degli audit dei sistemi di gestione, è la seguente: *"Processo sistematico, indipendente*

e documentato per ottenere evidenze oggettive e valutarle con obbiettività, al fine di determinare in quale misura i criteri dell'audit sono soddisfatti".

Esistono diverse tipologie di audit:

- **Gli audit di "prima parte":** detti anche audit interni, sono effettuati per il riesame da parte della direzione e per altri fini interni, dall'organizzazione stessa, o per suo conto, e possono costituire la base per una autodichiarazione di conformità da parte dell'organizzazione;
- **Gli audit di "seconda parte":** sono effettuati da chi ha un interesse nell'organizzazione, quali i clienti, o da altre persone per conto degli stessi, solitamente a fronte di specifiche prescrizioni contrattuali (Stakeholder);
- **Gli audit di "terza parte":** sono effettuati da organismi di audit esterni indipendenti, quali quelli che rilasciano certificazioni di conformità a requisiti della ISO 9001, della ISO 14001, BS OHSAS 18001 e ISO 45001 ecc.

Per la corretta conduzione dell'audit sono necessari i seguenti elementi:

- **Programma di audit:** disposizioni per un insieme di uno o più audit, pianificati un arco di tempo definito ed orientati verso uno scopo specifico. Un programma di audit comprende tutte le attività necessarie per pianificare, organizzare ed eseguire gli audit;
- **Piano di audit:** descrizione delle attività e delle disposizioni per la conduzione di un audit;
- **Esecuzione dell'audit.**
- **Rapporto di audit:** il rapporto di audit dovrebbe essere emesso nei tempi concordati, datato, riesaminato e firmato. Lo stesso deve essere distribuito ai destinatari designati dal committente dell'audit. Il rapporto di audit è di proprietà del committente dell'audit. Il team dell'audit e tutti i destinatari del rapporto sono tenuti alla riservatezza del documento. Le risultanze indicano conformità, non conformità e se previsto opportunità di miglioramento. Le non conformità devono essere riesaminate con l'organizzazione oggetto dell'audit per fa si che quest'ultima abbia la consapevolezza che le evidenze dell'audit sono accurate e le non conformità capite. Si devono cercare di risolvere le divergenze di opinioni e segnalare i punti non risolti.
- **Azioni successive all'audit:** azioni da intraprendere da parte dell'organizzazione per correggere le non conformità e attuare piani di miglioramento al sistema di gestione.

I sistemi di gestione e le PMI

Il Decreto Ministeriale del 13 febbraio 2014 (Gazzetta Ufficiale n. 45 del 24 febbraio 2014) recepisce le "procedure semplificate per l'adozione e la efficace attuazione dei modelli di organizzazione e di gestione della sicurezza nelle piccole e medie imprese"[8] (ai sensi dell'art. 30,

[8] https://www.lavoro.gov.it/temi-e-priorita/salute-e-sicurezza/focus-on/commissione-consultiva-permanente/Documents/Documento27novembre2013-procedure-semplificate-MOG.pdf

comma 5-bis, del decreto legislativo n. 81/2008 e s.m.i.) approvate dalla Commissione Consultiva nella seduta del 27 novembre 2013. Il fine, sia del decreto che delle procedure, è quello di fornire alle piccole e medie imprese, che decidano di adottare un modello di organizzazione e gestione della salute e sicurezza, indicazioni organizzative semplificate, di natura operativa, utili alla predisposizione e alla efficace attuazione di un sistema aziendale idoneo a prevenire le conseguenze dei reati previsti dall'art. 25-septies, di cui al decreto legislativo n. 231/2001.

Le "**Procedure semplificate per l'adozione dei modelli di organizzazione e gestione (MOG) nelle piccole e medie imprese (PMI)**", approvate dalla Commissione Consultiva, affermano che la semplificazione riguarda "alcuni aspetti organizzativi e le relative modalità applicative per l'adozione e l'efficace attuazione dei modelli di organizzazione e gestione della salute e sicurezza".

Le procedure semplificate tengono conto del fatto che l'alta direzione (così come indicata dalle norme BS OHSAS 18001, le linee guida UNI INAIL, la norma ISO 45001), il datore di lavoro (così come indicato dal D.lgs. 81/08) e l'organo dirigente (così come indicato ai sensi del D. Lgs. 231/01) possano essere coincidenti, che possa esistere o meno un unico centro decisionale e di responsabilità, della presenza o meno di dirigenti, della presenza di soggetti sottoposti alla altrui vigilanza".

In particolare, le procedure semplificate "delineano una serie di scelte organizzative, descrivendone le modalità attuative", per l'adempimento di tutti gli obblighi giuridici in materia di salute e sicurezza di cui all'art. 30 del Testo Unico.

I requisiti essenziali per la costituzione di un SGSSL idoneo sono quelli previsti dall'art. 30 commi da 1 a 4 del Testo Unico e l'adozione e l'efficace attuazione di un SGSSL dotato di tali caratteristiche "dipendono della complessità dell'organizzazione aziendale più che della sua dimensione, quindi le procedure semplificate dovranno essere attuate tenendo conto di tali peculiarità". Le aziende di dimensioni e/o complessità ridotte devono valutare l'opportunità di implementare un MOG aziendale: "un MOG efficacemente attuato migliora la gestione della salute e sicurezza sul lavoro ma l'adozione, non essendo da considerarsi obbligatoria, deve essere valutata dalla Direzione aziendale in virtù delle proprie necessità ed esigenze gestionali ed organizzative".

Il documento contiene diverse schede attuative del sistema, riportate nei moduli allegati, utili a semplificare l'attuazione di alcuni dei requisiti descritti nel presente documento e che possono essere modificate ed integrate a seconda della complessità organizzativa e tecnica aziendale.

I temi affrontati nel documento approvato dalla Commissione e allegato al Decreto del 13 febbraio 2014 sono di seguito elencati:

- politica aziendale di salute e sicurezza, obiettivi e piano di miglioramento;
- rispetto degli standard tecnico strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici (art. 30, comma 1, lett. a), D.lgs. 81/2008);
- attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti (art. 30, comma 1, lett. b), D.lgs. 81/2008);
- attività di natura organizzativa, quali gestione delle emergenze e primo soccorso (art. 30, comma 1, lett. c), D.lgs. 81/2008);
- gestione appalti;
- riunioni periodiche di sicurezza e consultazione dei rappresentanti dei lavoratori per la sicurezza;
- attività di sorveglianza sanitaria (art. 30, comma 1, lett. d), D.lgs. 81/2008);
- attività di informazione e formazione dei lavoratori (art. 30, comma 1, lett. e), D.lgs. 81/2008);
- attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori (art. 30, comma 1, lett. f), D.lgs. 81/2008);
- acquisizione di documentazioni e certificazioni obbligatorie per legge (art. 30, comma 1, lett. g), D.lgs. 81/2008);
- periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate (art. 30, comma 1, lett. h), D.lgs. 81/2008);
- il modello organizzativo e gestionale di cui al c. 1 dell'art. 30, del d. lgs. n. 81/08 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1 (art. 30, comma 2, D. Lgs n. 81/2008);
- il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e del tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per: la verifica, valutazione, gestione e controllo del rischio (art. 30, comma 3, D. Lgs 81/2008);
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello (art. 30, comma 3, D.lgs. 81/2008);
- il modello organizzativo deve, inoltre, prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e dell'igiene del lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico (art. 30, comma 4, D.lgs. 81/2008).

Si conclude segnalando i vari moduli allegati al decreto:

- Allegato 1 – Scheda analisi iniziale;
- Allegato 2 – Piano di miglioramento – Modulo pianificazione obiettivi e attuazione della politica;
- Allegato 3 – Elenco normativa applicabile;
- Allegato 4 - scheda manutenzione macchina;
- Allegato 5 - scheda consegna/gestione DPI;
- Allegato 6 - Programma annuale di formazione, informazione e addestramento;
- Allegato 7 - Registro presenze partecipanti;

- Allegato 8 - Scheda formazione/informazione/addestramento lavoratore;
- Allegato 9 - Registro addestramento lavoratore;
- Allegato 10 - Elenco documentazione obbligatoria;
- Allegato 11 – Modulo rilevazione: situazione pericolosa – incidente – non conformità;
- Allegato 12 - Modulo rilevazione infortunio;
- Allegato 13 - Piano di Monitoraggio;
- Allegato 14 – Programma degli/dell'audit interno;
- Allegato 15 – Piano di audit;
- Allegato 16 – Verbale di audit;
- Allegato 17 – Riesame periodico del modello organizzativo;
- Allegato 18 – Riunione periodica.

NORMATIVA E LINEE GUIDA

- Costituzione della Repubblica Italiana.
- Codice Civile.
- Codice Penale e Procedura Penale.
- D.lgs. 9 aprile 2008, n. 81 - Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro.
- D.lgs. 8 giugno 2001, n. 231 - Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300.
- Legge 29 settembre 2000, n. 300 - Ratifica ed esecuzione dei seguenti Atti internazionali elaborati in base all'articolo K. 3 del Trattato dell'Unione europea: Convenzione sulla tutela degli interessi finanziari delle Comunità europee, fatta a Bruxelles il 26 luglio 1995, del suo primo Protocollo fatto a Dublino il 27 settembre 1996, del Protocollo concernente l'interpretazione in via pregiudiziale, da parte della Corte di Giustizia delle Comunità europee, di detta Convenzione, con annessa dichiarazione, fatto a Bruxelles il 29 novembre 1996, nonché' 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 maggio 1997 e della Convenzione OCSE sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali, con annesso, fatta a Parigi il 17 dicembre 1997. Delega al Governo per la disciplina della responsabilità amministrativa delle persone giuridiche e degli enti privi di personalità giuridica.
- UNI-INAIL-ISPESL, “Linee guida per un sistema di gestione della salute e della sicurezza sul lavoro (SGSL), 2001.
- Norma BS OHSAS 18001:2007.
- Norma UNI EN ISO 45001:2018.
- Norma UNI EN ISO 19011:2018.
- Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231, approvate il 7 marzo 2002 (aggiornate al marzo 2014).
- Circolare informativa N° 8/2018. Migrazione alla UNI ISO 45001:2018 delle certificazioni emesse sotto accreditamento ACCREDIA e transizione ai documenti IAF MD 22:2018 e ISO IEC TS 17021-10:2018
- Procedure semplificate per l’adozione de modelli di organizzazione e gestione (MOG) nelle piccole e medie imprese (PMI)

BIBLIOGRAFIA

- Dubini R., Carozzi G. (2013), I modelli organizzativi 231 e la sicurezza sul lavoro. Gestione della responsabilità amministrativa delle imprese. Necessità e vantaggi competitivi dell’adozione dei modelli (esimenti ex art. 30 D.Lgs. 81/08) di prevenzione, organizzazione, gestione e controllo, EPC Editore
- Foti A. (2018), Guida operativa per la costruzione e gestione del Modello 231. Strumenti pratici per il professionista tecnico integrati con la norma ISO 45001:2018, EPC Editore
- Rotella A. (2018), Sicurezza sul lavoro 2018. Manuale Normo Tecnico, Ipsoa
- Bartoccioni A.C. (2012), Il decreto legislativo n. 121/2011 e la responsabilità degli enti in materia ambientale. Gazzetta Amministrativa. Uso del Territorio: Urbanistica, Ambiente e Paesaggio. Numero 1 – 2012.
- Giacobbe F., Geraci D., Monila L., D.Lgs 81/2008 art. 30 – Modelli di organizzazione e gestione della Sicurezza, ISPESL dipartimento di Messina.
- Osservatorio Accredia, La sicurezza sul lavoro e la certificazione, N° 1 – 2018
- UNI – Ente Italiano Normazione, Salute e sicurezza sul lavoro UNI ISO 45001

SITOGRAFIA

- www.inail.it
- www.lavoro.gov.it
- www.puntosicuro.it
- www.accredia.it
- www.confindustria.it
- www.olympus.uniurb.it
- www.cortecostituzionale.it

SENTENZE CITATE:

- Corte Costituzionale, Sentenza n.220 del 29 Maggio 1995
  https://www.cortecostituzionale.it/actionSchedaPronuncia.do?param_ecli=ECLI:IT:COST:1995:220

- Tribunale di Napoli, GIP Saraceno, Sez. 33, Ordinanza 26 giugno 2007 - Idoneità del Modello di organizzazione e gestione per la prevenzione dei reati presupposto
  https://olympus.uniurb.it/index.php?option=com_content&view=article&id=8868:tribunale-di-napoli-gip-saraceno-sez-33-ordinanza-26-giugno-2007-idoneita-del-modello-di-organizzazione-e-gestione-per-la-prevenzione-dei-reati-presupposto&catid=134:giurisprudenza-&Itemid=138

- Tribunale di Roma, GIP Finiti, Ordinanza 4 aprile 2003 - Idoneità delle misure predisposte dall'ente al fine di scongiurare il pericolo di reiterazione di illeciti
  https://olympus.uniurb.it/index.php?option=com_content&view=article&id=8849:tribunale-di-roma-gip-finiti-ordinanza-4-aprile-2003-idoneita-delle-misure-predisposte-dallente-al-fine-di-scongiurare-il-pericolo-di-reiterazione-di-illeciti&catid=134:giurispruden&Itemid=138

- Corte di Cassazione, Sezioni Unite Penali, Sentenza 27 marzo 2008 (dep. 2 luglio 2008), n. 26654
  https://www.cortedicassazione.it/cassazione-resources/resources/cms/documents/Relazione_pen_41_14.pdf

- Tribunale di Torino, Seconda Corte di Assise, 14 novembre 2011, n. 31095 - Sentenza Thyssenkrupp
  https://olympus.uniurb.it/index.php?option=com_content&view=article&id=15475:thyssen&catid=226&Itemid=138

- Tribunale di Novara, 26 ottobre 2010 - Responsabilità dell'ente per omicidio colposo commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro: colpa gestionale ed organizzativa
  https://olympus.uniurb.it/index.php?option=com_content&view=article&id=7802:tribunale-di-novara-26-ottobre-2010-responsabilita-dellente-per-omicidio-colposo-commesso-con-violazione-delle-norme-sulla-tutela-della-salute-e-sicurezza-sul-lavoro-colpa-gestionale-ed-organizzativa&catid=134&Itemid=138

- Cassazione Penale, Sez. 4, 20 aprile 2005, n. 11351 - Colpa professionale del RSPP
  https://olympus.uniurb.it/index.php?option=com_content&view=article&id=202:cassazione-penale-sez-4-20-aprile-2005-n-11351-colpa-professionale-del-rspp&catid=17&Itemid=138

- Tribunale di Milano, GIP Secchi, ordinanza 09 novembre 2004 - Esame dell'idoneità dei modelli di organizzazione, gestione e controllo ex artt 6 e 7 d.lg. 231/2001
  https://olympus.uniurb.it/index.php?option=com_content&view=article&id=8864:tribunale-di-milano-gip-secchi-ordinanza-09-novembre-2004-esame-dellidoneita-dei-modelli-di-organizzazione-gestione-e-controllo-ex-artt-6-e-7-dlg-2312001&catid=134&Itemid=138