Sistemi di gestione della Sicurezza
Linee guida per l'attuazione della specifica OHSAS 18001

IMPORTANTE

La BSI-OHSAS 18002 non è una norma «British Standard»

La BSI-OHSAS verrà ritirata non appena i suoi contenuti vengono pubblicati in, o come, una norma «British Standard».

ICS 03.100.01; 13.100

Ringraziamenti

La preparazione di questa guida OHSAS-18002 è stata resa possibile grazie alla collaborazione delle seguenti organizzazioni:

National Standards Authority of Ireland
South African Bureau of Standards
Japanese Standards Association
British Standards Institution
Bureau Veritas Quality International
Det Norske Veritas
Lloyds Register Quality Assurance
National Quality Assurance
SFS Certification
SGS Yarsley International Certification Services
Asociación Española de Normalización y Certificación
International Safety Management Organisation Ltd
SIRIM QAS Sdn. Bhd.
International Certification Services
Japan Industrial Safety and Health Association
The High Pressure Gas Safety Institute of Japan (KHK - ISO Centre)
Technofer Ltd
The Engineering Employers Federation
Singapore Productivity and Standards Board, Quality Assessment Centre
Instituto Mexicano de Normalización y Certificación
Industrial Technology Research Institute of Taiwan
Institute of Occupational Safety and Health
TUV Rheinland / BErlin-Brandenburg

Aggiornamenti dopo la pubblicazione

Aggiorn. N°	Data	Testo interessato

Questa pubblicazione OHSAS entra in vigore dal 15 Febbraio 2000.

ISBN 0 580 33123

Indice

Premessa

Questa linea guida e la specifica OHSAS 18001:1999 (Sistemi di gestione della Sicurezza – Specifica) sono state stilate in risposta all'urgente richiesta, da parte dei clienti, di uno standard per il sistema di gestione della Sicurezza con cui confrontare i propri sistemi di gestione e successivamente certificarli, e per creare una guida sull'attuazione di un tale standard.

La OHSAS 18001 è compatibile con la ISO 9001:1994 (Sistemi di Qualità) e con la ISO 14001:1996 (Sistemi di Gestione Ambientale) in modo da facilitare l'eventuale integrazione dei sistemi di gestione della Qualità, Ambientale e della Sicurezza.

La OHSAS 18002 riporta i requisiti specifici dalla OHSAS 18001 e li fa seguire dalla relativa spiegazione. La numerazione dei paragrafi della OHSAS 18002 corrisponde a quella della OHSAS 18001.

La OHSAS 18002 verrà rivista o modificata al momento appropriato. Le revisioni verranno effettuate quando verranno pubblicate le nuove edizioni della 18001 (previste in concomitanza con la pubblicazione delle revisioni della ISO 9001 o della ISO 14001).

La OHSAS 18001 e la OHSAS 18002 verranno ritirate non appena i loro contenuti verranno pubblicati in, o come, norme internazionali.

Durante la preparazione di questa guida, sono stati presi in considerazione i seguenti documenti:

BS 8800:1996 – *Guida ai Sistemi di Gestione della Sicurezza*.
Rapporto Tecnico NPR 5001:1997 – *Guida per un Sistema di Gestione della Sicurezza.*
SGS & ISMOL ISA 2000:1997 – *Requisiti dei Sistemi di Gestione della Sicurezza*.
BVQI SafetyCert – *Norma per la Gestione della Sicurezza*.
DNV - *Norma per la Certificazione dei Sistemi di Gestione della Sicurezza (OHSMS):1997*.
LRQA SMS 8800:1998 – *Criteri per la Valutazione dei Sistemi di Gestione della Sicurezza*.
Bozza della NSAI SR 320 – *Raccomandazioni per un Sistema di Gestione della Sicurezza*.
Bozza della AS/NZ 4801 – *Sistemi di Gestione della Sicurezza – Specifica con Guida per l'uso*.
Bozza della BSI PAS 088 – *Sistemi di Gestione della Sicurezza* .
La serie UNE 81900 di pre- standards per la prevenzione dei rischi sul lavoro.

La OHSAS 18002 sostituirà alcuni di questi documenti.
La OHSAS 18001 è altamente compatibile con la UNE 81900 e tecnicamente simile.

Per il Regno Unito:
- la BSI-OHSAS 18002 non è una norma «British Standard»;
- la BSI-OHSAS 18002 verrà ritirata non appena i suoi contenuti verranno pubblicati in, o come, una norma «British Standard»;
- la BSI OHSAS è pubblicata dalla BSI, la quale mantiene la relativa proprietà e i diritti d'autore.

Il processo di sviluppo usato per la OHSAS 18002 è disponibile per altri enti che vogliono produrre documenti simili in collaborazione con la BSI, a condizione che questi enti siano disposti ad osservare per tali documenti le condizioni della BSI.

Questa pubblicazione non intende includere tutte le dettagliate disposizioni da seguire. Gli utilizzatori sono responsabili per la sua corretta applicazione.

L'osservanza di questa pubblicazione OHSAS di per sé non esime dal rispetto degli obblighi previsti dalla legge.

1 Obiettivo

Questa guida OHSAS fornisce consigli generali sull'applicazione della OHSAS 18001.

Essa spiega i principi fondamentali della OHSAS 18001 e, per ogni requisito di questa, descrive l'intento, i dati tipici di input, i processi e i dati tipici di output in modo tale da facilitarne la comprensione e l'attuazione. La OHSAS 18002 non crea nuovi requisiti oltre a quelli già specificati nella OHSAS 18001 e non prescrive modalità obbligatorie per l'attuazione della OHSAS 18001.

Questa guida è applicabile anche alla sicurezza del prodotto e dei servizi.

OHSAS 18001

1 Obiettivo
Questa specifica OHSAS fornisce i requisiti di un sistema di gestione della Sicurezza per permettere ad un'Azienda di controllare i rischi sul luogo di lavoro e migliorare le sue prestazioni. Essa non illustra un criterio di prestazione della sicurezza specifico, né fornisce dettagli specifici per la pianificazione di un sistema di gestione.

Questa specifica OHSAS è applicabile a qualsiasi Azienda che voglia:

a) stabilire un sistema di gestione della Sicurezza per eliminare o ridurre al minimo i rischi, associati alle proprie attività, sia per i dipendenti che per tutte le altre persone che potrebbero essere esposti a tali rischi;

b) attuare, mantenere e migliorare continuamente il sistema di gestione della Sicurezza;

c) assicurarsi di essere conforme alla politica di Sicurezza dichiarata;

d) dimostrare tale conformità ad altri;

e) richiedere la certificazione/registrazione del suo sistema di gestione della Sicurezza ad un ente esterno; oppure

f) fare un'autodichiarazione di conformità a questa specifica OHSAS.

Tutti i requisiti di questa specifica OHSAS possono essere incorporati in un qualsiasi sistema di gestione della Sicurezza. L'entità dell' applicazione dei requisiti dipenderà da fattori quali la politica di Sicurezza dell'Azienda, la natura e i rischi delle sue attività e le complessità delle sue operazioni.

Questa specifica OHSAS è indirizzato alla Sicurezza sul luogo di lavoro piuttosto che alla sicurezza del prodotto e dei servizi.

2 Pubblicazioni di riferimento

Altre pubblicazioni che forniscono informazioni o linee guida sono elencate nella bibliografia. È consigliabile consultare le ultime edizioni di queste pubblicazioni. In particolare, bisognerebbe tenere conto delle seguenti pubblicazioni:

OHSAS 18001:1999 – *Sistemi di Gestione della Sicurezza – Specifica.*
BS 8800:1996 – *Guida ai Sistemi di Gestione della Sicurezza*.
ISO 10011.1:1990 – *Linee Guide per Sistemi di Verifica della Qualità – Parte 1: Verifica*.
ISO 10011.2:1991 – *Linee Guide per Sistemi di Verifica della Qualità – Parte 2: Criteri di Qualifica dei Controllori dei Sistemi di Qualità*.
ISO 10011.3:1991 – *Linee Guide per Sistemi di Verifica della Qualità – Parte 3: Gestioni dei Programmi di Verifica*.
ISO 14010:1996 – *Guida per la Verifica Ambientale – Principi Generali*.
ISO 14011:1996 – *Guida per la Verifica Ambientale – Procedure di Verifica – Verifica dei Sistemi di Gestione Ambientale.*
ISO 14012:1996 – *Guida per la Verifica Ambientale – Criteri di Verifica per le Verifiche Ambientali*.

3 Termini e definizioni

3.1
incidente con infortunio
un evento non programmato che dà luogo a morte, malattia, lesioni, danni o altra perdita

3.2
verifica
un esame sistematico allo scopo di determinare se le attività ed i relativi risultati sono conformi alle disposizioni pianificate, e se queste disposizioni sono state attuate efficacemente e se sono idonee al raggiungimento della politica e degli obiettivi dell'Azienda (vd. 3.9)

3.3
miglioramento continuo
il processo di valorizzazione del sistema di gestione della Sicurezza per ottenere miglioramenti complessivi nelle prestazioni di Sicurezza, in linea con la politica di Sicurezza dell'Azienda.
N.B.: il processo non ha bisogno di aver luogo in tutte le aree di attività contemporaneamente

3.4
pericolo
una fonte o una situazione potenzialmente capace di produrre danni in termini di infortuni o malattia, danni materiali o ambientali, o una combinazione di questi

3.5
identificazione del pericolo
processo attraverso il quale si riconosce l'esistenza di un pericolo (vd. 3.4) e se ne definiscono le caratteristiche

3.6 incidente senza infortunio
evento che ha dato origine ad un incidente o che avrebbe potuto condurre ad un incidente
NOTA: un incidente senza infortunio, malattia, danno o altre perdite è anche indicato con il termine "near-miss".

3.7
parti interessate
individuo o gruppo interessato o influenzato dalle prestazioni di Sicurezza di un'Azienda

3.8
non conformità
qualsiasi deviazione dagli standards di lavoro, prassi, procedure, regolamenti, prestazioni e sistema di gestione che potrebbe direttamente o indirettamente condurre a infortuni o malattie, danni alla proprietà, danno all'ambiente o una combinazione di questi

3.9
obiettivi
traguardi, in termini di prestazione di Sicurezza, che un'Azienda si prefigge di raggiungere
N.B.: quando è possibile gli obiettivi devono essere quantificati

3.10
sicurezza e salute professionale
i fattori e le condizioni che coinvolgono il benessere dei dipendenti, lavoratori a tempo determinato, personale esterno, visitatori e ogni altra persona nel luogo di lavoro

3.11
sistema di gestione della Sicurezza
parte del sistema complessivo di gestione che facilita la gestione dei rischi associati con l'attività dell'Azienda. Questo include la struttura organizzativa e le attività di pianificazione, le responsabilità, le prassi, le procedure, i processi e le risorse per lo sviluppo, l'attuazione, il conseguimento, la revisione e il mantenimento della politica della Sicurezza dell'Azienda

3.12
Azienda
una società, operazione, ditta, impresa, istituzione o associazione, o una parte di queste, incorporata o meno, pubblica o privata, che possiede le proprie funzioni e la propria amministrazione
N.B.: nel caso di Aziende con più unità attive, una sola di queste unità può essere definita come un'Azienda

3.13
prestazione
risultati misurabili del sistema di gestione della Sicurezza relativo al controllo dei rischi dell'Azienda, basati sulla sua politica di Sicurezza e sui relativi obiettivi
N.B.: la misurazione della prestazione include la misurazione della gestione delle attività e dei risultati relativi alla sicurezza

3.14
rischio
combinazione della probabilità e della(e) conseguenza(e) che un certo evento pericoloso abbia luogo

3.15
valutazione del rischio
processo globale comprendente la determinazione della gravità del rischio e la decisione di ritenerlo o meno tollerabile

3.16
sicurezza
assenza di rischi inaccettabili (ISO/IEC Guida 2)

3.17
rischio tollerabile
rischio che è stato ridotto ad un livello tale da poter essere sopportato dall'Azienda nel rispetto dei suoi obblighi legali e della propria politica di Sicurezza

NOTA 1: Alcuni documenti di riferimento, inclusa la BS 8800, usano il termine «valutazione del rischio» per significare l'intero processo della identificazione del pericolo, della determinazione dei rischi e della selezione di misure appropriate per la riduzione o il controllo dei rischi. La OHSAS 18001 e la OHSAS 18002 trattano gli elementi individuali di questo processo separatamente e usano il termine «valutazione dei rischi» per significare solo la seconda fase di questo processo, cioè la determinazione del rischio.

NOTA 2: «Stabilire» indica un livello di permanenza ed il sistema non può essere considerato stabilito fino a quando non si può dimostrare che tutti i suoi elementi siano stati attuati. «Mantenimento» vuol dire che, una volta stabilito, il sistema continua ad operare. Questo richiede uno sforzo attivo da parte dell'Azienda. Molti sistemi iniziano bene, ma si deteriorano per mancanza di mantenimento. Molti degli elementi della OHSAS 18001 (quale il controllo , l'azione correttiva e la revisione da parte della Direzione) sono progettati per assicurare il mantenimento attivo del sistema.

4 Elementi del sistema di gestione della Sicurezza

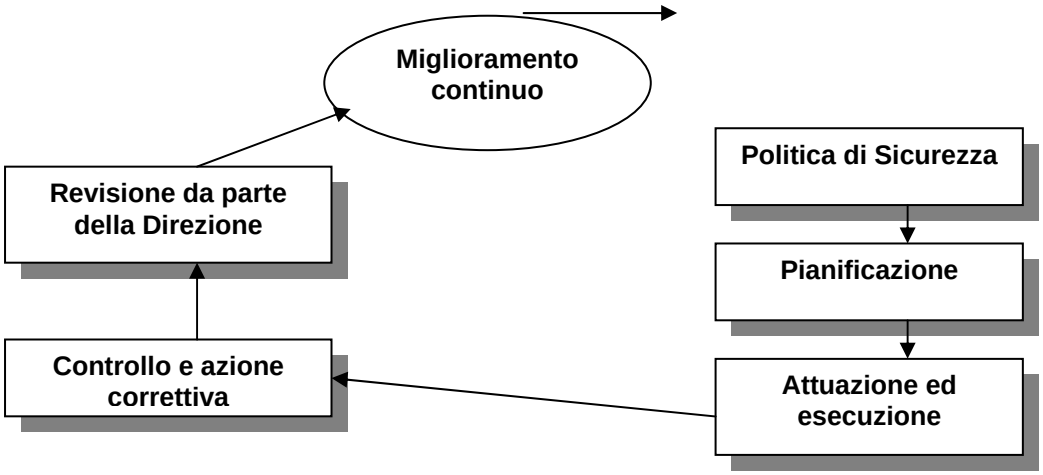

Figura 1 – Elementi di una gestione della sicurezza di successo

4.1 Requisiti generali

a) Requisito della OHSAS 18001

L'Azienda deve stabilire e mantenere un sistema di gestione della Sicurezza, i cui requisiti sono riportati nel paragrafo 4.

b) Intento

L'Azienda deve stabilire e mantenere un sistema di gestione che soddisfi tutti i requisiti della OHSAS 18001:1999. In questo modo, l'Azienda viene facilitata anche nell'osservanza degli obblighi di legge o di altre disposizioni inerenti la sicurezza.
In base all'entità dell'Azienda e alla natura delle sue attività, vengono stabiliti il grado di dettaglio e la complessità del sistema di gestione della Sicurezza, l'entità della documentazione e le risorse ad esso dedicate.

L'Azienda ha la libertà e la flessibilità di definire i suoi confini e può scegliere di applicare la OHSAS 18001 sull'intera Azienda o su sue specifiche unità operative o attività.

Nel definire i confini e lo scopo del sistema di gestione bisogna prendere delle precauzioni. Le Aziende non devono limitare il campo di applicazione in modo da escludere dalla valutazione un'operazione o un'attività necessaria per l'intera operatività dell'Azienda, o che può avere un impatto sulla sicurezza dei suoi dipendenti o di altre parti interessate.

Se la OHSAS 18001 viene applicata su una specifica unità operativa o attività, le politiche e le procedure di Sicurezza sviluppate da altre parti dell'Azienda possono essere utilizzate da quella specifica unità operativa o attività per facilitare l'ottenimento dei requisiti della OHSAS 18001. Questo potrebbe richiedere la revisione o l'aggiornamento di tali politiche o procedure di Sicurezza per assicurare che esse siano applicabili alla specifica unità operativa o attività dell'Azienda.

c) Dati tipici di input

Tutti i dati di input richiesti per l'applicazione della OHSAS 18001 sono descritti nella specifica stessa.

d) Dati tipici di output

Un dato tipico di output è un sistema di gestione della Sicurezza effettivamente applicato e mantenuto che aiuti l'Azienda nella continua ricerca di miglioramenti nella sua prestazione di Sicurezza.

4.2 Politica di Sicurezza

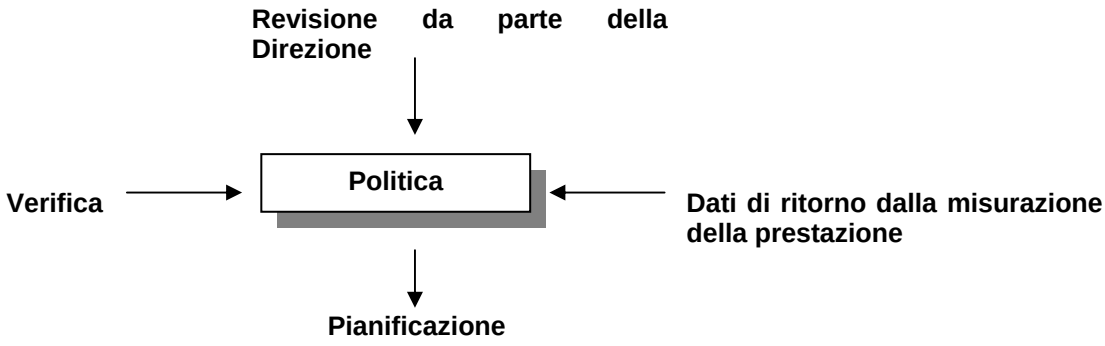

Figura 2 – Politica di Sicurezza

a) Requisito della OHSAS 18001

Ci deve essere una politica di Sicurezza autorizzata dalla Direzione Generale dell'Azienda che dichiari in modo esplicito gli obiettivi globali di Sicurezza dell'Azienda e l' impegno al miglioramento continuo della prestazione di Sicurezza.

La politica deve:

a) essere adatta alla natura e al grado dei rischi dell'Azienda;

b) includere un impegno al miglioramento continuo;

c) includere un impegno per lo meno al rispetto della legislazione in materia di Sicurezza vigente ed applicabile e di altri requisiti che l'Azienda ha sottoscritto;

d) essere documentata, attuata e mantenuta;

e) essere comunicata a tutti i dipendenti con lo scopo di renderli consapevoli dei loro obblighi individuali in materia di sicurezza;

f) essere a disposizione delle parti interessate; e

g) essere rivista periodicamente per assicurarsi che essa rimanga aggiornata e adatta all'Azienda.

b) Intento

La politica di Sicurezza stabilisce il senso generale d'orientamento e dispone i principi d'azione dell'Azienda. Fissa inoltre gli obiettivi di Sicurezza per la responsabilità e la prestazione di Sicurezza richiesti nell'Azienda. Essa rappresenta l'impegno formale dell'Azienda, in modo particolare quello della Direzione, per quanto riguarda la buona gestione della Sicurezza.

La Direzione deve produrre una documentata dichiarazione della sua politica di Sicurezza.

Nota: la politica di Sicurezza deve essere coerente con le politiche dell'Azienda per quanto riguarda le sue attività globali e con le altre discipline gestionali, ad es. la gestione della qualità o la gestione ambientale.

c) Dati di input tipici

Nello stabilire la politica di Sicurezza, la Direzione deve considerare i seguenti punti:

- la politica e gli obiettivi pertinenti alle attività dell'Azienda nel suo insieme;
- i pericoli dell'Azienda;
- i requisiti legali ed altri tipi di requisiti;
- le prestazioni di Sicurezza dell'Azienda del passato ed attuali;
- le esigenze di altre parti interessate;
- le opportunità e le necessità per un miglioramento continuo;
- le risorse di cui si ha bisogno;
- il contributo dei dipendenti;
- il contributo del personale esterno e degli appaltatori.

d) Procedura

La Direzione deve stilare e autorizzare una politica di Sicurezza tenendo conto dei punti sotto elencati. È importante che la politica di Sicurezza sia comunicata e promossa all'interno dell'Azienda dalla Direzione.
Una politica di Sicurezza formulata e comunicata in modo efficace deve:

1) essere adatta alla natura e all'entità dei rischi dell'Azienda;

   L'identificazione del pericolo, la valutazione del rischio e il controllo del rischio sono il cuore di un sistema di gestione della Sicurezza di successo e devono riflettersi nella politica di Sicurezza dell'Azienda.

   La politica di Sicurezza deve essere coerente con una visione del futuro dell'Azienda. Essa deve essere realistica e non deve né esagerare la natura dei rischi a cui l'Azienda va incontro né minimizzarli.

2) includere un impegno al miglioramento continuo;

   C'è da parte della collettività una pressante richiesta sulle Aziende di ridurre il rischio di malattia, incidenti con o senza infortunio sui luoghi di lavoro. Oltre ad affrontare le sue responsabilità legali, l'Azienda deve prefiggersi di migliorare le proprie prestazioni di Sicurezza e il proprio sistema di gestione della Sicurezza in modo efficace e efficiente, così da potersi adattare ai cambiamenti di attività e alle nuove normative.

   Il programmato miglioramento della prestazione deve essere documentato negli obiettivi di Sicurezza (vd. 4.3.3) e gestito attraverso il programma di gestione della Sicurezza (vd. 4.3.4), anche se la dichiarazione della politica di Sicurezza potrebbe includere ampie aree di azione.

3) includere un impegno di adeguamento per lo meno alle legislazioni in materia di Sicurezza vigenti ed applicabili e agli altri requisiti che l'Azienda ha sottoscritto;

Le Aziende hanno l'obbligo di conformarsi alle leggi in materia di Sicurezza applicabili e ad altri requisiti di Sicurezza. L'impegno espresso nella politica di Sicurezza è un riconoscere pubblicamente, da parte dell'Azienda, il proprio dovere ad adeguarsi a tali leggi ed ad altri requisiti, se non addirittura superarli, e l'espressione della piena intenzione di farlo.

NOTA: «altri requisiti» può significare, per esempio, politiche aziendali o di gruppo, gli standards o le specifiche interne dell'Azienda o regolamenti volontari al quale l'Azienda aderisce.

4) essere documentata, attuata e mantenuta;

La pianificazione e la preparazione costituiscono un punto chiave per un'attuazione di successo. Spesso le affermazioni della politica di Sicurezza e gli obiettivi di Sicurezza non sono praticabili perché le risorse disponibili per raggiungere tali obiettivi o non sono appropriate o sono inadeguate. Prima di fare qualsiasi dichiarazione pubblica, l'Azienda deve assicurarsi che siano disponibili i necessari fondi, capacità e risorse, e che tutti gli obiettivi di Sicurezza siano realisticamente raggiungibili entro questa struttura generale.

Per fare in modo che la politica di Sicurezza sia efficace, essa deve essere documentata, rivista periodicamente per garantire una continua adeguatezza e, se necessario, modificata o rifatta.

5) essere comunicata a tutti i dipendenti con lo scopo di rendere consapevoli questi ultimi delle loro responsabilità individuali per quanto riguarda la sicurezza.

Il coinvolgimento e l'impegno dei dipendenti sono indispensabili per una politica di Sicurezza di successo.

I dipendenti devono essere consapevoli degli effetti della gestione della Sicurezza sulla qualità del proprio ambiente di lavoro ed essere incoraggiati a contribuire attivamente a tale gestione.

I dipendenti (a tutti i livelli, inclusi quelli manageriali) difficilmente sono in grado di dare un effettivo contributo alla gestione della Sicurezza se non comprendono le proprie responsabilità e se non sono competenti per svolgere i compiti richiesti.

Questo impone all'Azienda di comunicare le politiche di Sicurezza e gli obiettivi di Sicurezza ai suoi dipendenti in modo chiaro, così che possano avere un quadro generale con il quale misurare le loro performance individuali di sicurezza.

NOTA: molti paesi hanno leggi e normative in materia che richiedono la consultazione ed il coinvolgimento dei dipendenti nei sistemi di gestione della Sicurezza dell'Azienda.

6) essere accessibile alle parti interessate;

Qualsiasi gruppo o individuo (sia interno che esterno) che si occupa della performance di Sicurezza dell'Azienda, o che è coinvolto nella stessa, dovrebbe essere particolarmente interessato alla dichiarazione della politica di Sicurezza. Perciò, dovrebbe esistere una procedura che comunichi loro tale politica. Questa procedura deve assicurare che le parti interessate ricevano su richiesta una copia della politica di Sicurezza, ma non deve necessariamente provvedere all'invio di copie non richieste.

7) essere rivista periodicamente per fare in modo che rimanga pertinente ed appropriata per l'Azienda.

I cambiamenti sono inevitabili, la legislazione evolve e le aspettative della società aumentano. Di conseguenza, devono essere rivisti periodicamente il sistema di gestione della Sicurezza e la politica di Sicurezza dell'Azienda per assicurare la loro continua adeguatezza ed efficacia.
Se vengono introdotti dei cambiamenti, questi devono essere comunicati non appena possibile.

e) Dati di output tipici

Un dato di output tipico è una politica di Sicurezza completa e comprensibile che venga comunicata all'intera Azienda.

4.3 Pianificazione

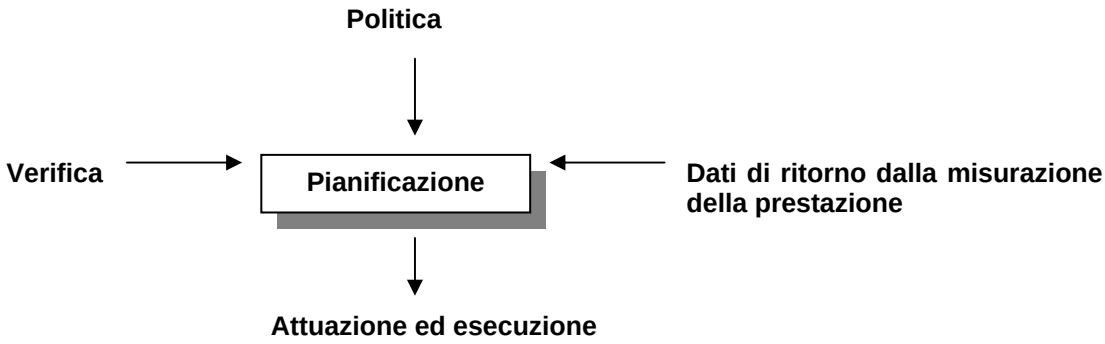

Figura 3 – Pianificazione

4.3.1 Pianificazione per l'identificazione del pericolo, valutazione e controllo dei rischi

a) Requisito della OHSAS 18001

L'Azienda stabilirà e manterrà le procedure per l'identificazione continua e la valutazione dei rischi e per l'attuazione delle necessarie misure di controllo.
Queste includeranno:

- attività ordinaria e non;
- le attività di tutto il personale che ha accesso all'ambiente di lavoro (inclusi gli appaltatori e visitatori);
- le attrezzature presenti nell'ambiente del lavoro, fornite dall'Azienda o da altri.

L'Azienda si assicurerà che i risultati di queste valutazioni e gli effetti di questi controlli vengano presi in considerazione durante la stesura degli obiettivi di Sicurezza. L'Azienda documenterà e manterrà aggiornate queste informazioni.

La metodologia dell'Azienda per l'identificazione del pericolo e la valutazione dei rischi dovrà:
- essere definita nel rispetto del suo scopo, della sua natura e dei tempi per assicurare che essa sia «proattiva» piuttosto che «reattiva»;
- provvedere alla classificazione dei rischi e all'identificazione di quelli da eliminare o controllare utilizzando le misure definite ai punti 4.3.3 e 4.3.4;
- essere conforme all'esperienza operativa e alle capacità delle misure di controllo dei rischi impiegate;
- fornire i dati utili per la definizione dei requisiti delle attrezzature, per l'identificazione di eventuali necessità di formazione del personale e/o per lo sviluppo dei controlli delle attività aziendali;
- provvedere al monitoraggio delle azioni richieste per assicurarne sia la loro efficacia che la tempestività della loro attuazione.

b) Intento

Dopo aver utilizzato i processi di identificazione del pericolo e di valutazione e controllo del rischio, l'Azienda devrebbe avere una conoscenza globale di tutti i pericoli significativi presenti nella sua sfera.

NOTA: Alcuni documenti di riferimento, inclusa la BS 8800, usano il termine «valutazione del rischio» per significare l'intero processo di identificazione del pericolo, della determinazione del rischio e della selezione di misure appropriate per la riduzione o il controllo del rischio. La OHSAS 18001 e la OHSAS 18002 trattano gli elementi individuali di questo processo separatamente e usano il termine «valutazione del rischio» per significare solo la seconda fase di questo processo, cioè la determinazione del rischio.

I processi di identificazione del pericolo, di valutazione e controllo del rischio, e i loro dati di output devono costituire la base di tutto il sistema di Sicurezza. È importante che i collegamenti fra i processi di identificazione del pericolo, valutazione e controllo del rischio, e gli altri elementi del sistema di gestione della Sicurezza siano stabiliti in modo chiaro e evidente. I paragrafi 4.3.1c**)** e 4.3.1e**)** danno una guida sui collegamenti fra i requisiti della OHSAS 18001 : 1999, 4.3.1 e gli altri requisiti della OHSAS 18001 : 1999.

Lo scopo di questa guida OHSAS è di stabilire i principi con cui l'Azienda può determinare se i processi di identificazione del pericolo, di valutazione e di controllo del rischio siano adeguati e sufficienti oppure no. Essa non ha l' intento di suggerire come queste attività debbano essere svolte.

NOTA: Per ulteriori informazioni sui processi di identificazione del pericolo, di valutazione e controllo del rischio , vd. la BS 8800.

I processi di identificazione del pericolo, di valutazione e di controllo del rischio devono permettere all'Azienda di identificare, valutare e controllare i suoi rischi in modo continuativo.

In ogni caso, si deve tenere conto sia delle operazioni ordinarie che di quelle straordinarie svolte all'interno dell'Azienda e di ogni possibile situazione di emergenza.

La complessità dei processi di identificazione del pericolo, di valutazione e di controllo del rischio dipende in larga misura da vari fattori quali la grandezza dell'Azienda, le situazioni presenti nell'ambiente di lavoro e la natura, complessità e rilevanza dei pericoli. Non è lo scopo della OHSAS 18001 : 1999, 4.3.1 di forzare piccole Aziende con pericoli molto limitati ad intraprendere complessi processi di identificazione del pericolo, di valutazione e di controllo del rischio.

I processi di identificazione del pericolo, di valutazione e di controllo del rischio devono tenere in considerazione i costi ed i tempi richiesti per condurre questi tre processi, oltre alla disponibilità di dati affidabili.
In questi processi si possono utilizzare informazioni già raccolte per adeguarsi alla legislazione o per altri scopi. L'Azienda può anche prendere in considerazione il grado di controllo pratico che essa può avere sui rischi in questione. L'Azienda deve determinare quali sono i suoi rischi, anche in base ai dati di input e di output associati alle sue attività passate e attuali, ai processi, ai prodotti e/o ai servizi.

Un'Azienda che non ha un sistema di gestione della Sicurezza può stabilire la sua condizione attuale, per quanto riguarda i rischi, svolgendo un' analisi iniziale. L'intento deve essere quello di considerare tutti i rischi affrontati dall'Azienda come base per stabilire il sistema di gestione della Sicurezza. L'Azienda può decidere di considerare i seguenti elementi nella sua analisi iniziale (senza però limitarsi a questi):

- requisiti legislativi e normativi;
- l'identificazione dei rischi affrontati dall'Azienda;
- un esame di tutte le procedure, i processi e le prassi di gestione della Sicurezza esistenti;
- una valutazione dei dati di ritorno ottenuti da un'indagine sugli incidenti con o senza infortunio e situazioni di emergenza avvenuti nel passato.

Un giusto approccio per l'analisi iniziale può includere liste di controllo, colloqui, ispezione e misurazione diretta, i risultati delle precedenti revisioni del sistema di gestione da parte della direzione o i risultati di altri riesami, a seconda della natura delle attività.
Si precisa che l' analisi iniziale non sostituisce l'attuazione dell' approccio sistematico e strutturato descritto nel resto del punto 4.3.1.

c) Dati di input tipici

I dati di input tipici comprendono i seguenti elementi:

- i requisiti legali in materia di Sicurezza ed altri requisiti (vd. 4.3.2);
- la politica di Sicurezza (vd. 4.2);
- la documentazione d'archivio di incidenti con o senza infortunio;
- le non conformità (vd. 4.5.2);
- i risultati della verifica del sistema di gestione della Sicurezza (vd. 4.5.4);
- le segnalazioni dei dipendenti e di altre parti interessate (vd. 4.4.3);
- le informazioni provenienti da consultazioni sul tema della sicurezza con i dipendenti, da attività di riesame e miglioramento nel luogo di lavoro (queste attività possono essere sia «reattive» che «proattive»);
- le informazioni sulle migliori procedure di lavoro, sui pericoli tipici associati all'Azienda, sugli incidenti con o senza infortunio accaduti in Aziende simili;

- le informazioni sulle attrezzature, sui processi e sulle attività dell'Azienda, incluse le seguenti:
    - dettagli sulle procedure di controllo delle modifiche;
    - planimetria/e dello stabilimento;
    - diagrammi di flusso del processo;
    - inventario dei materiali pericolosi (materie prime, sostanze chimiche, rifiuti, prodotti e sottoprodotti);
    - tossicità e altri dati relativi alla sicurezza;
    - dati di monitoraggio (vd. 4.5.1);
    - dati sull'ambiente di lavoro.

d) Procedura

1) Identificazione del pericolo, valutazione e controllo del rischio

i) Generalità

Le misure per la gestione del rischio devono riflettere, ove praticabile, il principio della eliminazione dei pericoli, e in seguito della riduzione del rischio (sia riducendo la probabilità che esso accada, sia riducendo la gravità potenziale dell'infortunio o del danno), tramite l'adozione, come ultima risorsa, di dispositivi di protezione individuali (DPI). I processi di identificazione del pericolo, di valutazione e di controllo del rischio sono strumenti chiave nella gestione del rischio.

I processi di identificazione del pericolo, della valutazione e del controllo del rischio variano enormemente a seconda dei settori industriali, spaziando da una semplice valutazione fino a complesse analisi quantitative corredate da un'ampia documentazione. Spetta all'Azienda pianificare ed attuare dei processi di identificazione del pericolo, di valutazione e di controllo del rischio che si adattino ai propri bisogni e alle situazioni tipiche del proprio ambiente di lavoro, e che permettano all'Azienda stessa di ottemperare ai requisiti legislativi in materia di sicurezza.

I processi di identificazione del pericolo, di valutazione e di controllo del rischio devono essere utilizzati come misure «proattive» piuttosto che «reattive», cioè devono ad esempio precedere l'introduzione di nuove o riesaminate attività o procedure. Qualsiasi necessaria riduzione del rischio e misura di controllo identificata deve essere attuata prima dell'introduzione di cambiamenti.

L'Azienda deve tenere aggiornati la documentazione, i dati e le informazioni archiviate riguardanti l'identificazione dei pericoli e la valutazione e il controllo dei rischi per le attività in corso, e deve anche ampliarli per poter includere nuovi sviluppi e nuove o modificate attività prima che le stesse vengano introdotte.

I processi di identificazione del pericolo, di valutazione e di controllo del rischio non devono essere applicati soltanto a «normali» operazioni di impianto e procedure, ma anche ad operazioni/procedure periodiche o occasionali, quali la manutenzione, la pulizia, l'avvio e lo spegnimento dell'impianto.

L'esistenza di procedure scritte per controllare un determinato lavoro pericoloso non solleva di per sé l'Azienda dalla necessità di continuare ad eseguire i processi d'identificazione del pericolo, di valutazione e controllo dei rischi per quell'operazione pericolosa.

L'Azienda non solo deve considerare i pericoli ed i rischi derivanti dalle attività svolte dal proprio personale, ma deve anche prendere in considerazione i pericoli ed i rischi derivanti dalle attività degli appaltatori e dei visitatori e dall'uso di prodotti o di servizi forniti da altri.

ii) I processi di identificazione del pericolo, di valutazione e di controllo dei rischi

I processi di identificazione del pericolo, di valutazione e controllo dei rischi devono essere documentati e devono comprendere i seguenti elementi:

- l'identificazione dei pericoli;
- la valutazione dei rischi con le esistenti (o proposte) misure di controllo in loco (occorre tener conto della esposizione a specifici pericoli, della probabilità di fallimento delle misure di controllo e della potenziale gravità delle conseguenze di un infortunio o di un danno);
- la valutazione della tollerabilità del rischio residuo;
- l'identificazione di eventuali necessarie misure di controllo del rischio aggiuntive;
- la valutazione del grado di sufficienza delle misure di controllo del rischio nel ridurre il rischio ad un livello tollerabile.

Oltre a questo, i processi devono includere la definizione dei seguenti elementi:

- la natura, i tempi, l'ampiezza e la metodologia per qualsiasi forma di identificazione del pericolo, di valutazione e di controllo del rischio che deve essere utilizzata;
- la legislazione o altri requisiti in materia di Sicurezza applicabili;
- il ruolo e l'autorità del personale responsabile per eseguirei processi;
- la competenza specifica e la necessaria formazione (vd. 4.4.2) per il personale che deve svolgere i processi. (In funzione della natura o del tipo di processo che si intende utilizzare, potrebbe essere necessario per l' Azienda avvalersi di una consulenza o servizi esterni);
- l'uso delle informazioni provenienti da consultazioni dei dipendenti su argomenti di sicurezza, dal riesame e dal miglioramento delle attività (queste attività possono essere sia di natura «reattiva» che «proattiva»);
- quale livello di considerazione riservare al rischio associato all'errore umano presente nelle attività esaminate;
- i pericoli dovuti a materiali, impianti o attrezzature soggetti all'usura col passare del tempo, in particolare quando questi materiali, impianti o attrezzature vengono tenuti in magazzino.

iii) Azioni successive

In seguito alle prestazioni dei processi di identificazione del pericolo, di valutazione e controllo dei rischi:

- ci deve essere una prova evidente che qualsiasi necessaria azione correttiva o preventiva (vd. 4.5.2) sia monitorata per assicurare il suo completamento (ciò potrebbe richiedere una ulteriore identificazione del pericolo e valutazione del rischio per tenere in conto le modifiche proposte alle misure di controllo del rischio e per definire le valutazioni dei rischi residui cambiate);
- la Direzione deve ricevere i dati di ritorno sui risultati e sullo stato di avanzamento delle azioni correttive o preventive, in modo da poterli utilizzare durante la revisione da parte della Direzione (vd. 4.6) e per stabilire dei nuovi o modificati obiettivi;
- l'Azienda deve trovarsi nella posizione di determinare se la competenza del personale che esegue specifici lavori pericolosi sia conforme con quella specificata dal processo di valutazione del rischio nella definizione dei controlli dei rischi necessari;
- i dati di ritorno dalla successiva esperienza operativa devono essere utilizzati, dove è possibile, per correggere i processi o i dati sui quali questi sono basati.

2) Riesame dell'identificazione del pericolo, della valutazione e controllo del rischio *(vd. anche 4.6)*

I processi di identificazione del pericolo, di valutazione e di controllo del rischio devono essere riveduti a intervalli di tempo prestabiliti come descritto nel documento della politica di Sicurezza o come prestabilito dalla Direzione. Questo periodo può variare in base alle seguenti considerazioni:

- la natura del pericolo;
- grandezza del rischio;
- cambiamenti nelle operazioni normali;
- cambiamenti nelle scorte di magazzino, nelle materie prime, nelle sostanze chimiche, ecc.

Il riesame deve aver luogo se i cambiamenti all'interno dell'Azienda porgono interrogativi sulla validità delle valutazioni esistenti. Tali cambiamenti possono includere :

- ampliamento, riduzione o ristrutturazione;
- ridistribuzione delle responsabilità;
- cambiamenti nei metodi di lavoro o nella modalità di comportamento.

e) Dati di output tipici

Sono necessarie delle procedure documentate per i seguenti elementi:

- identificazione dei pericoli;
- determinazione dei rischi associati ai pericoli identificati;
- indicazione del livello dei rischi associati a ciascun pericolo, e se essi siano tollerabili o meno;
- descrizione o riferimento alle misure adottate per sorvegliare e controllare i rischi (vd. 4.4.6 e 4.5.1), in particolare quelli non tollerabili;
- se necessario, gli obiettivi di Sicurezza, le azioni adottate per ridurre i rischi identificati (vd. 4.3.3) e le attività successive per monitorare il livello di riduzione del rischio;
- identificazione della competenza e i requisiti di formazione del personale per attuare le misure di controllo (vd. 4.4.2);
- necessarie misure di controllo, che devono essere dettagliate come parte dell'elemento di controllo delle attività aziendali del sistema (4.4.6);
- documenti di archivio generati da ciascuna delle procedure sopra menzionate.

NOTA: Alcuni documenti di riferimento, inclusa la BS 8800, usano il termine «valutazione del rischio» per significare l'intero processo di identificazione del pericolo, di determinazione del rischio e di selezione di misure appropriate per la riduzione o il controllo del rischio. La OHSAS 18001 e la OHSAS 18002 trattano gli elementi individuali di questo processo separatamente e usano il termine «valutazione del rischio» per significare solo la seconda fase di questo processo, cioè la determinazione del rischio.

4.3.2 Requisiti legali ed altri requisiti

a) Requisiti della OHSAS 18001

L'Azienda stabilirà e manterrà una procedura per l'identificazione e l'accesso a requisiti legali e altri requisiti inerenti la Sicurezza applicabili.
L'Azienda manterrà queste informazioni aggiornate.
L'Azienda comunicherà informazioni relative a requisiti legali (e non) ai suoi dipendenti e ad altre parti interessate.

b) Intento

L'Azienda deve essere consapevole e capire come le sue attività siano, o saranno, influenzate da applicabili requisiti legali e non, e comunicare queste informazioni al personale pertinente.

Questo requisito del 4.3.2 della OHSAS 18001 : 1999 ha lo scopo di promuovere la consapevolezza e la comprensione delle responsabilità legali. Essa non ha lo scopo di imporre all'Azienda l'obbligo di creare archivi contenenti documenti legali o di altro tipo che saranno raramente consultati o utilizzati.

c) Dati di input tipici

Tipici dati di input includono:

- informazioni sui processi di produzione o di realizzazione dei servizi svolti dall' Azienda;
- risultati dell'identificazione del pericolo, della valutazione e controllo del rischio (vd. 4.3.1);
- migliori prassi di lavoro (es. i codici e le linee di guida delle associazioni del settore);
- requisiti legali e norme governative;
- elenchi delle fonti d'informazione;
- norme nazionali, straniere, regionali o internazionali;
- requisiti interni dell'Azienda;
- requisiti delle parti interessate.

d) Procedura

Devono essere identificate le legislazioni e altri requisiti pertinenti. L'Azienda deve cercare i mezzi più appropriati per avere accesso alle informazioni, incluso il tipo di supporto (es. carta, CD, dischetti, Internet). L'Azienda deve anche valutare quali requisiti applicare e dove applicarli, chi all'interno dell'Azienda ha bisogno di ricevere informazioni e quale tipo di informazione.

e) Dati di output tipici

I dati di output tipici includono:

- procedure per l'identificazione e l'accesso alle informazioni;

- identificazione di quali requisiti applicare e dove (questo può assumere l'aspetto di un registro/i);
- requisiti (il testo effettivo, un riassunto o un'analisi, secondo il caso) disponibili in luoghi decisi dall'Azienda;
- procedure per sorvegliare l'attuazione dei controlli introdotti da nuove norme sulla sicurezza.

4.3.3 Obiettivi

a) Requisiti della OHSAS 18001

L'Azienda stabilirà e manterrà documentati obiettivi di Sicurezza per ogni funzione e livello pertinente all'interno dell'Azienda.
NOTA: Gli obiettivi, se è possibile, devono essere quantificati.

Nello stabilire e riesaminare gli obiettivi, l'Azienda deve considerare i suoi obblighi legali ed altri requisiti, i suoi rischi e pericoli, le sue opzioni tecnologiche, le sue esigenze di natura finanziaria, operativa e commerciale, e l'opinione delle altre parti interessate. Gli obiettivi devono conformarsi alla politica di Sicurezza dell'Azienda, incluso l'impegno al miglioramento continuo.

b) Intento

È necessario assicurarsi che siano stati stabiliti obiettivi di Sicurezza misurabili nel complesso dell'Azienda, in modo tale da poter soddisfare la politica di Sicurezza.

c) Dati di input tipici

I dati di input tipici includono:

- la politica e gli obiettivi pertinenti l'attività dell'Azienda nel suo insieme;
- la politica di Sicurezza, incluso un impegno al miglioramento continuo, (vd. 4.2);
- i risultati dell'identificazione del pericolo, della valutazione e del controllo del rischo (vd. 4.3.1);
- i requisiti legali e non (vd. 4.3.2);
- le opzioni tecnologiche;
- le esigenze di natura finanziaria, operativa e commerciale;
- le opinioni dei dipendenti e delle parti interessate (vd. 4.4.3);
- le informazioni provenienti da consultazioni dei dipendenti su argomenti di sicurezza, dal riesame e dal miglioramento delle attività svolte nel luogo di lavoro (queste attività possono essere sia di natura «reattiva» che «proattiva»);
- l'analisi delle prestazioni in comparazione con gli obiettivi di Sicurezza stabiliti in precedenza;
- la documentazione delle non conformità in materia di sicurezza, degli incidenti con o senza infortunio e dei danni alla proprietà accaduti nel passato;
- i risultati della revisione da parte della Direzione (vd. 4.6).

d) Procedura

I responsabili ai vari livelli devono individuare, stabilire e definire le priorità degli obiettivi di Sicurezza in base alle informazioni o ai dati provenienti dai "dati di input tipici" descritti sopra.
Nello stabilire gli obiettivi di Sicurezza, bisogna prestare molta attenzione alle informazioni o ai dati forniti dalle persone che poi saranno i diretti interessati, in modo da garantire che gli stessi obiettivi siano ragionevoli e più ampiamente accettati. E' anche utile prendere in considerazione le informazioni ed i dati forniti da fonti esterne all'Azienda, per esempio dagli appaltatori e da altre parti interessate.
Devono tenersi regolarmente delle riunioni tra i vari livelli manageriali per stabilire gli obiettivi di Sicurezza (ad es. almeno una volta all'anno). Per alcune Aziende potrebbe essere necessario documentare il processo di definizione degli obiettivi di Sicurezza.

Gli obiettivi di Sicurezza devono interessare sia temi di Sicurezza applicabili all'intera Azienda sia quelli specifici di singole funzioni e livelli al suo interno.

Devono essere definiti adeguati indicatori per ciascun obiettivo di Sicurezza. Questi indicatori devono permettere di sorvegliare l'attuazione degli obiettivi di Sicurezza.

Gli obiettivi di Sicurezza devono essere ragionevoli e realizzabili, in quanto l'Azienda deve avere l'abilità di raggiungerli e di sorvegliarne lo sviluppo. Per il raggiungimento di ciascun obiettivo di Sicurezza deve essere definito un programma relativo ai tempi di attuazione che sia ragionevole e rispettabile.

Gli obiettivi di Sicurezza possono essere suddivisi in "traguardi" separati, a seconda della grandezza dell'Azienda, della complessità dell'obiettivo di Sicurezza e dal tempo previsto per il loro raggiungimento. Ci devono essere dei chiari collegamenti fra i vari livelli dei traguardi e degli obiettivi di Sicurezza.

Alcuni esempi di obiettivi di Sicurezza sono:

- la riduzione dei livelli di rischio;
- l'introduzione di elementi aggiuntivi nel sistema di gestione della sicurezza;
- le misure adottate per migliorare gli elementi esistenti o la coerenza della loro applicazione;
- l'eliminazione o la riduzione della frequenza di accadimento di particolari eventi indesiderati.

Gli obiettivi di Sicurezza devono essere divulgati (per esempio: attraverso la formazione del personale o attraverso riunioni di gruppo; vd. 4.4.2) al personale interessato, e devono essere attuati attraverso il/i programma/i di gestione della Sicurezza (vd. 4.3.4).

e) Dati di output tipici

I dati di output tipici includono obiettivi di Sicurezza documentati e misurabili per ogni funzione dell'Azienda.

4.3.4 Programma/i di gestione della Sicurezza

a) Requisito della OHSAS 18001

L'Azienda stabilirà e manterrà uno o più programmi di gestione della Sicurezza per raggiungere i suoi obiettivi. Questo dovrà includere la documentazione relativa :

a) alle responsabilità e autorità assegnate per il raggiungimento degli obiettivi di Sicurezza ad ogni livello e funzione dell'Azienda; e

b) ai mezzi e alla tempistica con cui gli obiettivi devono essere raggiunti.

Il programma di gestione della Sicurezza va rivisto a periodi regolari e prestabiliti. Ove necessario, esso può essere modificato per adattarsi ad eventuali cambiamenti nelle attività, nei prodotti, nei servizi o nelle condizioni operative dell'Azienda.

b) Intento

L'Azienda deve cercare di attuare la sua politica di Sicurezza ed i suoi obiettivi di Sicurezza, stabilendo un programma di gestione della Sicurezza. Questo richiederà lo sviluppo di strategie e piani d' azione, che dovranno essere documentati e comunicati. Lo stato di avanzamento nel percorso di raggiungimento degli obiettivi di Sicurezza deve essere monitorato, rivisto e documentato, e le strategie ed i piani d' azione devono essere aggiornati o corretti opportunamente.

c) Dati di input tipici

I dati di input tipici includono:

- la politica di Sicurezza e gli obiettivi di Sicurezza;
- il riesame dei requisiti legali e non;
- i risultati dell'identificazione del pericolo, della valutazione e del controllo del rischio;
- i dettagli sui processi di produzione o di realizzazione dei servizi utilizzati dall'Azienda;
- le informazioni provenienti da consultazioni dei dipendenti su argomenti di sicurezza, dal riesame e dal miglioramento delle attività svolte nel luogo di lavoro (queste attività possono essere sia di natura «reattiva» che «proattiva»);
- il riesame delle opportunità offerte da nuove o da diverse opzioni tecnologiche;
- le attività di miglioramento continuo;
- la disponibilità delle risorse necessarie per raggiungere gli obiettivi di Sicurezza dell'Azienda.

d) Procedura

Il programma di gestione della Sicurezza deve identificare le persone responsabili per il raggiungimento degli obiettivi di Sicurezza (ad ogni livello). Devono essere anche indicati i vari compiti da svolgere per raggiungere ciascun obiettivo di Sicurezza.

Il programma di gestione della Sicurezza deve includere l'assegnazione adeguata, per ogni singolo compito , di responsabilità, autorità e tempo previsto di attuazione, in modo tale da rispettare la tempistica complessiva dell' obiettivo di Sicurezza ad essi associato.
Esso deve anche provvedere all'assegnazione, per ciascun compito, delle risorse adatte (es. risorse finanziarie, umane, logistiche e in termini di attrezzature).

Il programma di gestione di Sicurezza può anche essere associato a specifici programmi di formazione del personale (vd. 4.4.2). I programmi di formazione provvederanno inoltre alla divulgazione dell'informazione e a coordinare le attività di supervisione.

Quando si prevedono importanti alterazioni o modifiche nelle prassi, nei processi, nelle attrezzature o nel materiale di lavoro, il programma di gestione della Sicurezza deve provvedere a nuovi cicli di identificazione del pericolo e valutazione del rischio. Il programma di gestione della Sicurezza deve anche provvedere alla consultazione del personale pertinente circa i cambiamenti previsti.

e) Dati di output tipici

I dati di output tipici includono un programma di gestione della Sicurezza definito e documentato.

4.4 Attuazione ed esecuzione

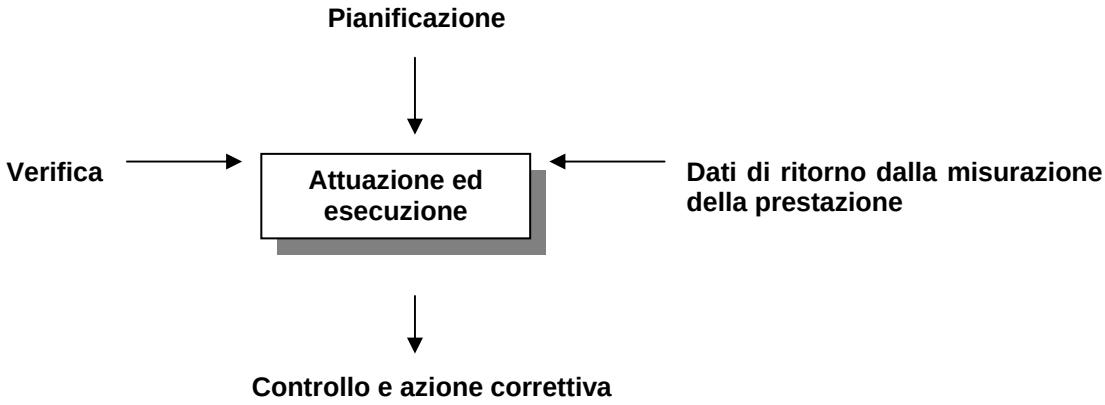

Figura 4 - Attuazione ed esecuzione

4.4.1 Struttura e responsabilità

a) Requisito della OHSAS 18001

I ruoli, le responsabilità e l' autorità del personale addetto alla gestione, all'esecuzione e alla verifica delle attività che hanno ripercussioni sui rischi insiti nelle operazioni, negli impianti e nelle procedure dell'Azienda devono essere definiti, documentati e divulgati per facilitare la gestione della Sicurezza.

La responsabilità massima in materia di sicurezza è della Direzione. L'Azienda nominerà un membro della Direzione (ad es., in una grande Azienda, un membro del consiglio di amministrazione o del comitato esecutivo) che abbia particolare responsabilità nel garantire che, in tutti i livelli e luoghi operativi all'interno dell'Azienda, il sistema di gestione della Sicurezza sia attuato e sia conforme ai requisiti.

La Direzione deve provvedere alle risorse essenziali per l'attuazione, il controllo ed il miglioramento del sistema di gestione della Sicurezza.

Nota: tra le risorse sono comprese le risorse umane e le competenze specializzate, le risorse tecnologiche ed economiche.

La persona designata dalla Direzione deve avere ruoli, responsabilità e autorità ben definite per:

a) assicurarsi che i requisiti del sistema di gestione della Sicurezza siano stabiliti, attuati e mantenuti in linea con le specifiche OHSAS;

b) assicurarsi che le relazioni sulle prestazioni del sistema di gestione della Sicurezza vengano sottoposte alla Direzione per la revisione e per essere utilizzate come base per definire un miglioramento del sistema di gestione della Sicurezza.

Tutto il personale con responsabilità di gestione dovrà mostrare il proprio impegno per un miglioramento continuo delle prestazioni di Sicurezza.

b) Intento

Per facilitare un'efficace gestione della Sicurezza è necessario che i ruoli, le responsabilità e le autorità siano definite, documentate e comunicate, e che vengano messe a disposizione risorse adeguate per permettere l' esecuzione di compiti inerenti alla Sicurezza.

c) Dati di input tipici

Tipici dati di input includono:

- la struttura/organigramma organizzativo;
- i risultati dell'identificazione del pericolo, della valutazione e del controllo del rischio;
- gli obiettivi di Sicurezza;
- i requisiti legali e non;
- la descrizione dei compiti;
- l'elenco del personale qualificato.

d) Procedura

1) Quadro generale

Devono essere definite le responsabilità e l'autorità di tutte le persone che svolgono mansioni che fanno parte del sistema di gestione della Sicurezza, specificando anche le responsabilità di interfaccia fra le diverse funzioni.

Tali definizioni possono essere richieste, per esempio, per le seguenti persone:

- la Direzione;
- i responsabili a tutti i livelli dell'Azienda;
- operatori di processo e la forza lavoro in generale;
- coloro che gestiscono la Sicurezza degli appaltatori;
- gli addetti responsabili della formazione, in materia di Sicurezza, del personale;
- gli addetti responsabili dell'attrezzatura critica dal punto di vista della Sicurezza;
- i dipendenti con qualifiche in materia di Sicurezza o specialisti di Sicurezza interni all'Azienda;
- i rappresentanti dei lavoratori per la Sicurezza nelle riunioni di consultazione.

Ad ogni modo, l'azienda deve comunicare e promuovere l'idea che la Sicurezza è responsabilità di tutti all'interno dell'Azienda, e non solo di coloro che hanno compiti definiti nel sistema di gestione della Sicurezza.

2) Definizione delle responsabilità della Direzione

Tra le responsabilità della Direzione è compresa la definizione della politica di Sicurezza dell'Azienda e l'essere garante che il sistema di gestione della Sicurezza sia attuato. Come parte di questo impegno, la Direzione deve incaricare una persona specifica, con responsabilità e autorità definite, per attuare il sistema di gestione della Sicurezza. (In Aziende grandi e complesse, ci può essere più di una persona incaricata.)

3) Definizione delle responsabilità della persona incaricata dalla Direzione

La persona incaricata per la gestione della Sicurezza dalla Direzione deve essere un membro della Direzione stessa. La persona designata può essere coadiuvata da altro personale con responsabilità delegata per il monitoraggio del funzionamento dell'operazione Sicurezza nel suo complesso. Comunque, l'incaricato dalla Direzione deve essere regolarmente informato sulla prestazione del sistema di gestione della Sicurezza e deve continuare ad essere attivamente coinvolto nei riesami periodici e nella stesura degli obiettivi di Sicurezza. Si deve garantire che qualsiasi altro compito o mansione assegnata a questo personale non entri in conflitto con l'adempimento delle loro responsabilità per quanto riguarda la Sicurezza.

4) Definizione delle responsabilità dei capi reparto

Tra le responsabilità dei capi reparto c'è quella di garantire la Sicurezza sia gestita nella propria area di competenza. Nel caso che le responsabilità primarie per questioni di Sicurezza ricadano sui capi reparto, devono essere definiti in modo appropriato ruolo e responsabilità di qualsiasi specialistica funzione di Sicurezza presente nell'Azienda, per evitare ambiguità per quanto riguarda responsabilità e autorità. Ciò deve includere accordi, a tutti i livelli fino al più alto livello direzionale, per risolvere eventuali conflitti fra questioni di Sicurezza e considerazioni di produzione.

5) Documentazione dei ruoli e delle responsabilità

Le responsabilità e autorità in materia di Sicurezza devono essere documentate in un modo adeguato all'Azienda. La documentazione può presentarsi sotto una o più delle seguenti forme, o comunque in forme alternative scelte dall'Azienda:

- manuali del sistema di gestione della Sicurezza;
- procedure di lavoro e descrizione dei compiti;
- descrizione delle mansioni;
- programma di formazione per i neoassunti.

Se l'Azienda decide di emettere descrizioni delle mansioni in forma scritta, che coprano altri aspetti dei ruoli e delle responsabilità dei dipendenti, allora devono essere incorporate in tali descrizioni anche le responsabilità di Sicurezza.

6) Comunicazione dei ruoli e delle responsabilità

Le responsabilità e autorità in materia di Sicurezza devono essere effettivamente comunicate a tutti i diretti interessati, ai vari livelli dell'Azienda. Ciò deve assicurare che le persone comprendano il campo d'azione e le interfacce tra le varie funzioni, e i canali da utilizzare per intraprendere delle azioni.

7) Risorse

La Direzione deve garantire che siano disponibili risorse adeguate (incluse le attrezzature, le risorse umane, la competenza e la formazione del personale) per mantenere il luogo di lavoro sicuro.
Le risorse possono essere considerate adeguate se sono sufficienti per svolgere i programmi e le attività di Sicurezza, compresi il monitoraggio e la misurazione della prestazione.

Per le Aziende con sistemi di gestione della Sicurezza già in essere, l'adeguamento delle risorse può essere almeno parzialmente valutato confrontando il previsto grado di raggiungimento degli obiettivi di Sicurezza con i risultati reali.

8) L'impegno della Direzione

I dirigenti devono mostrare in modo tangibile il loro impegno nella Sicurezza. Ad esempio effettuando visite e ispezioni nei luoghi di lavoro, partecipando alle indagini sugli incidenti con infortunio e fornendo risorse per le azioni correttive, assistendo agli incontri di Sicurezza ed emettendo messaggi di sostegno.

e) Dati di output tipici

Tipici dati di output includono:

- le definizioni delle responsabilità e autorità in materia di Sicurezza per tutto il personale interessato;
- la documentazione dei ruoli/responsabilità in manuali, procedure scritte e programmi di formazione del personale;
- la procedura per la comunicazione dei ruoli e delle responsabilità a tutti i dipendenti e alle altre parti interessate;
- la partecipazione attiva e il sostegno della Direzione per la Sicurezza, a tutti i livelli.

4.4.2 Formazione, informazione e competenza

a) Requisiti della OHSAS 18001

Il personale dovrà avere le competenze adatte per lo svolgimento dei compiti che possono avere un impatto sulla Sicurezza nell'ambiente di lavoro. Le competenze dovranno essere definite in termini di istruzione, formazione e/o esperienza idonea.

L'Azienda deve stabilire e mantenere delle procedure per garantire che gli addetti di ciascuna funzione e livello pertinente siano consapevoli:

- dell'importanza della conformità alla politica e alle procedure di Sicurezza, ed ai requisiti del sistema di gestione della Sicurezza;
- delle conseguenze, reali o potenziali, delle loro attività lavorative e dei benefici di un miglioramento della loro prestazione individuale sulla Sicurezza;
- i loro ruoli e responsabilità nel raggiungimento della conformità alla politica e alle procedure di Sicurezza, ed ai requisiti del sistema di gestione della Sicurezza, inclusi i requisiti di preparazione e di risposta all'emergenza (vd. 4.4.7);
- le conseguenze potenziali di una deviazione dalle procedure operative specifiche.

Le procedure di formazione del personale devono tener conto dei diversi livelli di:

- responsabilità, abilità ed istruzione; e
- rischio.

b) Intento

Le Aziende devono avere delle procedure efficaci per garantire che il personale abbia la necessaria competenza per svolgere le funzioni ad esso assegnate.

c) Dati di input tipici

Tipici dati di input includono:

- le definizioni dei ruoli e delle responsabilità;
- le descrizioni delle mansioni (incluso i particolari dei compiti pericolosi da svolgere);
- le valutazioni sulle prestazioni dei lavoratori;
- i risultati dell'identificazione del pericolo, della valutazione e del controllo del rischio;
- le procedure e le istruzioni operative;
- la politica di Sicurezza e gli obiettivi di Sicurezza;
- i programmi di Sicurezza.

d) Procedura

I seguenti elementi devono essere inclusi nella procedura:

- un'identificazione sistematica dell' informazione e della competenza richiesta ad ogni livello e funzione dell'Azienda in materia di Sicurezza;

- le misure per individuare e trovare rimedio ad eventuali scostamenti fra i livelli individuali di informazione e competenza in materia di Sicurezza effettivamente presenti e quelli richiesti;

- l'effettuazione, in modo sistematico ed opportuno, dei corsi di formazione necessari;

- la valutazione degli individui allo scopo di assicurarsi che essi abbiano acquisito e che mantengano l' informazione e la competenza richiesta;

- la conservazione della documentazione adeguata relativa alla formazione e competenza degli individui.

Un programma di formazione e di informazione di Sicurezza deve essere stabilito e mantenuto per trattare le seguenti aree:

- la comprensione delle disposizioni aziendali di Sicurezza e delle responsabilità e dei ruoli specifici dell'individuo relativi a dette disposizioni;

- un programma sistematico per i neoassunti e di formazione continua dei dipendenti e di chi compie un cambiamento di funzione, area, reparto, lavoro e mansione all'interno dell'Azienda;

- la formazione a proposito di disposizioni di Sicurezza locali, dei pericoli, dei rischi, delle precauzioni da adottare e delle procedure da seguire (tale formazione va fatta prima di iniziare il lavoro);

- la formazione per eseguire l'identificazione del pericolo, la valutazione e il controllo del rischio (vd. 4.3.1d);

- la formazione specifica, interna od esterna, per gli addetti con ruoli specifici nel sistema di gestione della Sicurezza, inclusi i rappresentanti di Sicurezza dei lavoratori;

- la formazione relativa alla responsabilità di Sicurezza per il personale che gestisce i dipendenti, gli appaltatori ed altri (es. lavoratori a tempo determinato). Questo serve ad assicurare che sia i responsabili sia le persone sotto la loro dipendenza capiscano i pericoli ed i rischi legati alle operazioni di cui sono responsabili, ovunque siano svolte. Inoltre, questo serve per garantire che il personale abbia le competenze necessarie per svolgere le attività in modo sicuro, seguendo le procedure di Sicurezza;

- i ruoli e le responsabilità della Direzione (incluse le responsabilità legali dell'individuo e dell'Azienda) per assicurare che il sistema di gestione della Sicurezza funzioni in modo idoneo a controllare i rischi ed minimizzare i casi di malattia, di infortunio e di altri danni per l'Azienda;

- i programmi di consapevolezza e di formazione per gli appaltatori, lavoratori a tempo determinato e visitatori, in base al livello di rischio a cui sono esposti.

Devono essere valutati l'efficacia della formazione ed i livelli effettivi di competenza. Questo può coinvolgere valutazioni durante i programmi di formazione e/o controlli adeguati in sito per stabilire se il livello di competenza è stato raggiunto, oppure per monitorare l'effetto a lungo termine della formazione ricevuta.

e) Dati di output tipici

Tipici dati di output includono:

- richieste di competenza per i singoli ruoli;
- analisi delle necessità di formazione;
- i programmi/piani di formazione per i singoli dipendenti;
- una gamma di corsi/sussidi di formazione disponibili all'interno dell'Azienda;
- documentazione relativa alla formazione svolta e alla valutazione dell'efficacia della stessa.

4.4.3 Consultazione e comunicazione

a) Requisiti della OHSAS 18001

L'Azienda deve avere delle procedure per accertarsi che la pertinente informazione in materia di Sicurezza sia fornita/ricevuta a/dal personale e a/da altre parti interessate.
Le disposizioni di consultazione e di coinvolgimento del personale devono essere documentate e divulgate alle parti interessate.

I dipendenti devono essere:

- coinvolti nello sviluppo e nel riesame delle politiche e delle procedure di gestione rischi;
- consultati quando si verificano cambiamenti che possono avere un impatto sulla Sicurezza del luogo di lavoro;
- rappresentati in materia di Sicurezza
- informati su chi è il loro rappresentante per la Sicurezza e il delegato della Direzione in materia di Sicurezza (vd. 4.4.1).

b) Intento

L'Azienda deve incoraggiare, attraverso un processo di consultazione e di comunicazione, la partecipazione nelle buone prassi di Sicurezza e il sostegno per la sua politica ed i suoi obiettivi di Sicurezza, da parte di tutti quelli coinvolti nelle sue attività.

c) Dati di input tipici

Tipici dati di input includono:

- la politica di Sicurezza e gli obiettivi di Sicurezza;
- la documentazione attinente al sistema di gestione della Sicurezza;
- i processi di identificazione del pericolo, di valutazione e di controllo del rischio;
- la definizione dei ruoli e delle responsabilità di Sicurezza;
- i risultati delle consultazioni formali in materia di Sicurezza fra i dipendenti e la Direzione;
- le informazioni provenienti dalle consultazioni dei lavoratori in materia di Sicurezza, dalle attività di riesame e miglioramento nell'ambiente di lavoro (queste attività possono essere sia di natura "reattiva" che "proattiva");
- i particolari sui programmi di formazione.

d) Procedura

L'Azienda deve documentare e promuovere misure per la consultazione e la comunicazione di pertinenti informazioni di Sicurezza ai suoi dipendenti e ad altre parti interessate (es. appaltatori, visitatori, ecc.) e per ricevere le informazioni dagli stessi.

Devono essere comprese anche le disposizioni per coinvolgere i dipendenti nelle seguenti procedure:

- la consultazione circa lo sviluppo e il riesame delle politiche e degli obiettivi di Sicurezza, le decisioni relative all'attuazione dei processi e delle procedure per gestire i rischi, compresa l' identificazione del pericolo, e per il riesame delle valutazioni e dei controlli dei rischi legati alle loro attività;

- la consultazione sui cambiamenti che possono avere ripercussioni sulla Sicurezza nell'ambiente di lavoro, come l'introduzione di materiali, sostanze chimiche, attrezzature, tecnologie, processi, procedure o prassi di lavoro nuove o modificate.

I dipendenti devono essere rappresentati su questioni di Sicurezza e devono essere informati su chi sia il loro rappresentante e il responsabile di Sicurezza incaricato dalla Direzione.

e) Dati di output tipici

Tipici dati di output includono:

- consultazioni formali tra la Direzione e i dipendenti tramite comitati di Sicurezza o simili strutture;

- il coinvolgimento dei dipendenti nell'identificazione del pericolo, nella valutazione e nel controllo del rischio;

- iniziative per incoraggiare la consultazione dei dipendenti su argomenti inerenti la Sicurezza, le attività di riesame e miglioramento nell'ambiente di lavoro, ed il ritorno alla Direzione di informazioni relative alla sicurezza;

- definizione di ruoli e meccanismi di comunicazione dei rappresentanti dei lavoratori per la Sicurezza con la Direzione, incluso, ad esempio, il coinvolgimento nelle indagini sugli incidenti con o senza infortunio, nelle ispezioni di Sicurezza sul campo, ecc.;

- incontri in materia di Sicurezza per i dipendenti ed altre parti interessate (es. appaltatori o visitatori);

- bacheche contenenti i dati sulle prestazioni di Sicurezza e altre informazioni di Sicurezza utili;

- circolari di Sicurezza;

- manifesti su temi della Sicurezza.

4.4.4 Documentazione

a) Requisiti della OHSAS 18001

L'Azienda deve stabilire e mantenere, utilizzando il sussidio più idoneo (cartaceo, elettronico, ecc.), informazioni che:

a) descrivano gli elementi chiave del sistema di gestione della Sicurezza e della loro interazione

b) forniscano indicazioni sulla documentazione collegata.

NOTA: è importante che la documentazione sia di dimensioni più ridotte possibili per essere efficiente ed efficace.

b) Intento

L'Azienda deve documentare e tenere aggiornata la documentazione sufficiente per assicurare che il suo sistema di gestione della Sicurezza possa essere adeguatamente capito ed applicato in modo efficace ed efficiente.

c) Dati di input tipici

Tipici dati di input includono:

- i dettagli dei sistemi di documentazione e di informazione che l'Azienda sviluppa per sostenere il suo sistema di gestione della Sicurezza e le attività di Sicurezza, e per adempiere ai requisiti della OHSAS 18001 : 1999;

- definizione di responsabilità e autorità;

- le informazioni sulle aree nelle quali la documentazione e/o l'informazione viene utilizzata, e sulle limitazioni derivanti dalla natura fisica della documentazione, o dall'uso di mezzi elettronici o di altro tipo.

d) Procedura

L'Azienda deve riesaminare le proprie necessità di documentazione e d'informazione nell'ambito del sistema di gestione della Sicurezza, prima di sviluppare la documentazione necessaria per supportare la propria attività di Sicurezza.
Non è obbligatorio sviluppare la documentazione in una forma particolare per essere conformi alla OHSAS 18001, né è necessario sostituire la documentazione esistente, quale manuali, procedure scritte o istruzioni di lavoro, se essa descrive in modo adeguato le disposizioni in atto.
Se l'Azienda già dispone di un sistema di Gestione della Sicurezza ben stabilito e documentato, potrebbe essere più comodo ed efficace sviluppare, per esempio, un documento di riesame che descriva l'interazione tra le procedure esistenti ed i requisiti della OHSAS 18001 : 1999.

Bisogna considerare i seguenti fattori:

- le responsabilità e le autorizzazioni di chi utilizza la documentazione e le informazioni, visto che ciò porta a considerare il grado di sicurezza e di accessibilità che è necessario imporre (in particolare se si usano mezzi elettronici) e i controlli sulle modifiche (vd. 4.4.5);

- il modo e l'ambiente in cui la documentazione viene utilizzata, dato che questi potrebbero influenzare il tipo di formato da utilizzare. Simili considerazioni vanno fatte sull'utilizzo di attrezzature elettroniche per i sistemi di informazione.

e) Dati di output tipici

Tipici dati di output includono:

- il documento, o manuale, contente la visione d'insieme della documentazione del sistema di gestione della Sicurezza;
- i registri, gli elenchi generali e gli indici dei documenti;
- le procedure scritte;
- le istruzioni di lavoro.

4.4.5 Controllo dei documenti e dei dati

a) Requisito della OHSAS 18001

L'Azienda deve stabilire e mantenere procedure atte a controllare tutti i documenti e i dati richiesti da questa specifica OHSAS per accertarsi che :

a) essi possano essere localizzati;
b) essi siano periodicamente riesaminati e se necessario rivisti, e che la loro adeguatezza venga approvata da personale autorizzato;
c) versioni correnti dei documenti e dei dati pertinenti siano disponibili in tutti i luoghi di lavoro dove vengono svolte le operazioni essenziali per un funzionamento efficace del sistema di gestione della Sicurezza;
d) vecchi documenti e dati siano ritirati immediatamente da tutti i punti di emissione e di uso, o comunque non sia possibile un loro uso involontario; e
e) i documenti ed i dati archiviati e conservati per scopi legali o di consultazione, o per entrambi i motivi, siano identificati in modo adeguato.

b) Intento

Tutti i documenti e i dati contenenti informazioni critiche per il funzionamento del sistema di gestione della Sicurezza e per la prestazione delle attività di Sicurezza dell'Azienda devono essere identificati e controllati.

c) Dati di input tipici

Tipici dati di input includono:

- dettagli dei sistemi di documentazione e dei dati sviluppati dall'Azienda per supportare il proprio sistema di gestione e le relative attività di Sicurezza, e per soddisfare i requisiti della OHSAS 18001 : 1999;

- dettagli delle responsabilità e autorità.

d) Procedura

Le procedure scritte devono definire i controlli per l'identificazione, l'approvazione, l'emissione ed il ritiro della documentazione di Sicurezza, ed il controllo dei dati di Sicurezza (in linea con i relativi requisiti della OHSAS 18001, vd. punto 4.4.5 di cui sopra). Queste procedure devono definire con chiarezza le categorie di documentazione e i dati alle quali si applicano.
La documentazione ed i dati devono essere disponibili ed accessibili all'occorrenza, sia in condizioni normali che non, incluse le emergenze. Per esempio, deve essere garantito che tutta la documentazione aggiornata, quale la planimetria, le schede informative delle sostanze pericolose, le procedure e le istruzioni, sia accessibile ai processisti e a tutti quelli che li richiedono in situazioni di emergenza.

e) Dati di output tipici

Tipici dati di output includono:

- la procedura di controllo dei documenti, incluse le responsabilità ed autorità designate;

- i registri dei documenti, gli elenchi generali o gli indici;
- un elenco della documentazione di controllo e la sua ubicazione;

- l'archivio dei documenti (alcuni dei quali dovranno essere conservati per adempiere ai requisiti legali od altro).

4.4.6 Controllo delle attività aziendali

a) Requisito della OHSAS 18001

L'Azienda deve individuare quelle operazioni e quelle attività, associate ai rischi identificati, che richiedono determinate misure di controllo. L'Azienda dovrà pianificare queste attività, inclusa la manutenzione, per assicurare che queste vengano effettuate sotto specifiche condizioni:

a) stabilendo e mantenendo procedure documentate per far fronte a situazioni dove la loro assenza potrebbe portare a deviazioni dalla politica e dagli obiettivi di Sicurezza;

b) stipulando criteri operativi nelle procedure;

c) stabilendo e mantenendo procedure relative agli identificati rischi delle merci, delle attrezzature, e dei servizi acquistati e/o utilizzati dall'Azienda, e comunicando le relative procedure e requisiti ai fornitori e agli appaltatori;

d) stabilendo e mantenendo procedure relative alla progettazione dell'ambiente di lavoro, dei processi, delle installazioni, dei macchinari, delle procedure operative e dell'organizzazione del lavoro, inclusa la loro adattabilità alle capacità umane, per eliminare o ridurre i rischi alla fonte.

b) Intento

L'Azienda deve stabilire e mantenere le disposizioni per garantire l'efficace applicazione delle misure di controllo e delle contromisure , ovunque queste siano richieste per monitorare i rischi operativi, per soddisfare la politica di Sicurezza e gli obiettivi di Sicurezza, e per conformarsi ai requisiti legali e non.

c) Dati tipici di input

Tipici dati di input includono:

- la politica di Sicurezza e gli obiettivi di Sicurezza;
- i risultati dell'identificazione del pericolo, della valutazione e del controllo del rischio;
- i requisiti, legali e non, identificati .

d) Procedura

L'Azienda deve stabilire le procedure per controllare i rischi identificati (inclusi quelli che potrebbero essere introdotti dagli appaltatori o dai visitatori), fornendo documentazione nei casi dove la mancanza dei controlli potrebbe condurre ad incidenti con o senza infortunio o ad altre deviazioni dalla politica di Sicurezza e gli obiettivi di Sicurezza. Le procedure di controllo del rischio devono essere riesaminate periodicamente per garantire la loro adeguatezza ed efficacia, e devono essere attuati gli eventuali cambiamenti divenuti necessari.
Le procedure devono considerare quelle eventuali situazioni in cui i rischi si potrebbero estendere agli stabilimenti o alle aree controllate da clienti o terzi: per esempio, quando i dipendenti dell'Azienda lavorano presso uno stabilimento del cliente. A volte, in queste circostanze, può essere necessario consultare le parti esterne all'Azienda riguardo alle problematiche di Sicurezza.

Qui di seguito vengono descritti alcuni esempi di aree in cui tipicamente sorgono dei rischi e delle misure di controllo per prevenirli.

1) Acquisto o trasferimento di merci e servizi, e l'uso di risorse esterne

Questo punto include i seguenti temi:

- l'approvazione dell'acquisto o del trasferimento di sostanze chimiche, materiali e sostanze pericolosi;
- il possesso della documentazione per la movimentazione sicura dei macchinari, delle attrezzature, dei materiali o delle sostanze chimiche al momento dell'acquisto, o la necessità di ricevere tale documentazione;
- la valutazione e la rivalutazione periodica delle competenze degli appaltatori;
- l'approvazione della progettazione dei dispositivi di Sicurezza per nuovi impianti od attrezzature.

2) Lavori pericolosi

Questo punto include i seguenti temi:

- l'identificazione dei lavori pericolosi;
- la predeterminazione e l'approvazione dei metodi di lavoro;
- la prequalifica del personale addetto a lavori pericolosi;
- i sistemi del "permesso di lavoro" e le procedure che controllano l'entrata e l'uscita del personale nei luoghi dove si svolgono lavori pericolosi.

3) Materiali pericolosi

Questo punto include i seguenti temi:

- l'identificazione degli inventari e dei luoghi di stoccaggio;
- le disposizioni per uno stoccaggio sicuro e il controllo delle vie d' accesso;
- la disponibilità e l'accesso ai dati sulla sicurezza dei materiali e ad altre informazioni pertinenti;

4) Manutenzione della sicurezza di impianti ed attrezzature

Questo punto include i seguenti temi:

- la disponibilità, il controllo e la manutenzione degli impianti e dell'attrezzatura dell'Azienda;
- la disponibilità, il controllo e la manutenzione dei dispositivi di protezione individuale (DPI);
- l'isolamento ed il controllo delle vie d' accesso;
- l'ispezione e la prova di dispositivi di sicurezza e di sistemi critici, quali:
- i sistemi di protezione degli operatori;
- i carter e le protezioni fisiche;
- i sistemi di interruzione;
- i dispositivi antincendio;
- l'attrezzatura per la movimentazione (gru, muletti, paranchi ed altri mezzi di sollevamento);
- le fonti di radiazione e le relative protezioni;
- i dispositivi essenziali di monitoraggio;

- i sistemi locali di ventilazione;
- le attrezzature e disposizioni sanitarie.

e) Dati di output tipici

Tipici dati di output includono:

- le procedure;
- le istruzioni di lavoro.

4.4.7 Preparazione e risposta all'emergenza

a) Requisito della OHSAS 18001

L'Azienda deve stabilire e mantenere i piani e le procedure per individuare la potenzialità di incidenti e di situazioni d'emergenza, e le relative risposte, e per prevenire e limitare i possibili casi di malattia e di infortunio associati ad essi.

L'Azienda deve riesaminare i suoi piani e le sue procedure di preparazione e di risposta all'emergenza; in particolare dopo l'insorgenza di incidenti o il verificarsi di situazioni d'emergenza.

Quando è possibile, l'Azienda deve anche verificare queste procedure periodicamente.

b) Intento

L'Azienda deve attivamente analizzare gli incidenti potenziali e le risposte all'emergenza necessarie, pianificare in che modo attuare quest' ultime, sviluppare le procedure e i processi per affrontare gli incidenti, verificare le risposte pianificate e cercare di migliorarne l'efficacia.

c) Dati di input tipici

Tipici dati di input includono:

- i risultati dell'identificazione del pericolo, della valutazione e del controllo del rischio;
- la disponibilità dei servizi di emergenza locali, e i dettagli delle disposizioni concordate per la risposta all'emergenza e per le eventuali consultazioni;
- i requisiti legali e non;
- le esperienze relative a incidenti con o senza infortunio e situazioni d'emergenza avvenuti nel passato;
- le esperienze relative a incidenti con o senza infortunio e situazioni d'emergenza avvenuti in Aziende simili nel passato (lezioni apprese, prassi migliori);
- il riesame della risposta all'emergenza e delle esercitazioni condotte, ed i risultati delle azioni successive.

d) Procedura

L'Azienda deve sviluppare un piano (o dei piani) di emergenza, individuare e fornire un'attrezzatura d'emergenza adeguata e verificare regolarmente attraverso le esercitazioni la sua capacità di risposta.

Le esercitazioni pratiche devono avere come fine la verifica dell'efficacia delle parti più critiche del/i piano/i d'emergenza e la verifica della completezza del processo di pianificazione dell'emergenza. Mentre gli esercizi teorici possono essere utili durante il processo di pianificazione, le esercitazioni pratiche devono essere il più possibile realistiche per essere efficaci. Questo richiede lo svolgimento di simulazioni di incidenti in scala reale.

I risultati delle emergenze e delle esercitazioni devono essere valutati e si devono attuare i cambiamenti che si sono riscontrati essere necessari.

1) Piano d'emergenza

Il piano d'emergenza deve delineare le azioni da prendersi quando si verificano determinate situazioni d'emergenza, e deve includere:

- l'identificazione degli incidenti e delle emergenze possibili;
- l'identificazione della persona responsabile durante l'emergenza;
- i dettagli delle azioni che dovranno essere intraprese dal personale durante un'emergenza, incluso quello esterno che si trova sul luogo dell'emergenza, quali appaltatori o visitatori (per es. potrebbe venire chiesto loro di spostarsi verso specifici punti di raccolta);
- la responsabilità, l'autorità e i doveri del personale con ruoli specifici durante l'emergenza (es. gli addetti antincendio, gli addetti al pronto soccorso, gli specialisti per perdite di materiale nucleare/tossico);
- le procedure di evacuazione;
- l'identificazione e l'ubicazione dei materiali pericolosi, e le azioni d'emergenza richieste;
- l'interfaccia con i servizi d'emergenza esterni;
- la comunicazione con le autorità;
- la comunicazione con i vicini e la comunità;
- la protezione di documenti ed attrezzature importanti;
- la disponibilità delle informazioni necessarie durante l'emergenza, ad esempio: la planimetria, i dati relativi a materiali pericolosi, le procedure, le istruzioni di lavoro ed i numeri di telefono da contattare.

Il coinvolgimento di enti esterni nella pianificazione dell'emergenza e nella risposta a quest'ultima, deve essere documentato in modo chiaro. Queste enti devono essere messi al corrente delle circostanze nelle quali potrebbero essere contattati, e occorre fornire tutte le informazioni da loro richieste per facilitare il loro intervento nelle attività di risposta.

2) Attrezzatura d'emergenza

Va identificata l'attrezzatura d'emergenza necessaria ed essa deve essere fornita in quantità adeguata. Deve essere controllata ad intervalli definiti per comprovarne la sua efficienza. Alcuni esempi sono:

- i sistemi d'allarme;
- le luci e le alimentazioni d'emergenza;
- le uscite di sicurezza;
- i rifugi sicuri;
- le valvole di isolamento, gli interruttori ed i selezionatori critici;
- l'attrezzatura antincendio;
- i mezzi di pronto soccorso (incluse le docce d'emergenza, le vaschette lavaocchi, ecc.);
- i mezzi di comunicazione.

3) Esercitazioni

Le esercitazioni devono essere svolte in base ad un programma prefissato. Se è opportuno e praticabile, bisogna promuovere la partecipazione a queste esercitazioni di servizi d'emergenza esterni.

e) Dati di output tipici

Tipici dati di output includono:

- la documentazione dei piani e delle procedure d'emergenza;
- un elenco delle attrezzature d'emergenza;
- la documentazione delle prove fatte sulle attrezzature d'emergenza;
- la documentazione inerente:
- le esercitazioni pratiche;
- il riesame delle esercitazioni pratiche;
- le azioni raccomandate a seguito dei riesami effettuati;
- lo stato di avanzamento delle azioni raccomandate.

4.5 Controllo e azione correttiva

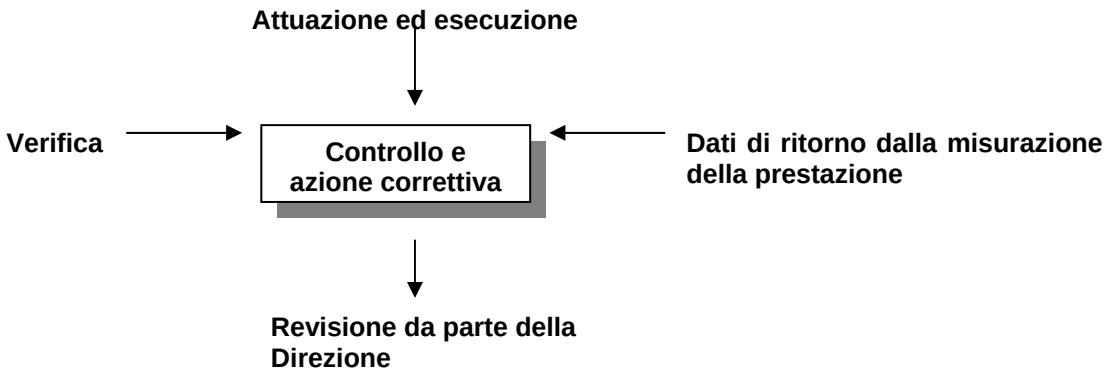

Figura 5 - Controllo e azione correttiva

4.5.1 Misura e monitoraggio delle prestazioni

a) Requisito della OHSAS 18001

L'Azienda deve stabilire e mantenere procedure atte a monitorare e misurare periodicamente le prestazioni di Sicurezza. Queste procedure devono prevedere:

- misure, sia qualitative che quantitative, adeguate alle necessità dell'Azienda;
- il monitoraggio del grado di ottenimento degli obiettivi di Sicurezza dell'Azienda;
- misure "proattive" di prestazione, che controllano la conformità al programma di gestione della Sicurezza, ai criteri operativi e ai requisiti legislativi e normativi applicabili;
- misure "reattive" di prestazione che controllano gli incidenti con infortunio, le malattie, gli incidenti senza infortunio (inclusi i «near-misses») ed altre prove storiche di lacune nella prestazione di Sicurezza;
- l' archiviazione dei dati e dei risultati di monitoraggio e di misura sufficienti per facilitare le analisi delle successive azioni correttive e preventive.

Se è richiesta un'attrezzatura di monitoraggio per la misura e il controllo delle prestazioni, l'Azienda deve stabilire e mantenere le procedure per la taratura e la manutenzione di tali attrezzature.

La documentazione delle attività e dei risultati di taratura e manutenzione deve essere conservata.

b) Intento

L'Azienda deve individuare i parametri chiave della sua prestazione di Sicurezza, da applicare in tutte le sue parti. Questi includono, ma non si limitano a, parametri che determinano se:

- la politica e gli obiettivi di Sicurezza sono stati raggiunti;
- i controlli dei rischi sono stati effettuati e sono efficaci;
- sono state apprese le lezioni da mancanze del sistema di gestione della Sicurezza, inclusi gli eventi pericolosi (incidenti, «near-misses» e casi di malattia);
- i programmi per i dipendenti e le parti interessate relativi alla consapevolezza, alla formazione, alla comunicazione e alla consultazione sono efficaci;
- sono state prodotte e vengono utilizzate le informazioni utili per il riesame e/o il miglioramento degli aspetti del sistema di gestione della Sicurezza.

c) Dati di input tipici

Tipici dati di input includono:

- i risultati dell'identificazione del pericolo, della valutazione e del controllo del rischio (vd. 4.3.1);
- i requisiti legali, le norme e le prassi migliori (se esistono);
- la politica di Sicurezza e gli obiettivi di Sicurezza;

- la procedura per far fronte alle non conformità;
- l' archiviazione delle verifiche e tarature delle attrezzature (incluse quelle degli appaltatori);
- la documentazione d'archivio relativa alla formazione del personale (inclusa quella prodotta dagli appaltatori);
- le relazioni fatte alla Direzione.

d) Procedura

1) Monitoraggio "proattivo" e "reattivo"

Un sistema di gestione della Sicurezza dell'Azienda deve incorporare sia il monitoraggio "proattivo" che quello "reattivo", come descritto di seguito:

- il monitoraggio "proattivo" deve essere utilizzato per verificare la conformità alle attività di Sicurezza dell'Azienda al suo programma di Sicurezza, ad esempio, controllando la frequenza e l'efficacia delle ispezioni di Sicurezza;
- il monitoraggio "reattivo" deve essere utilizzato per indagare, analizzare e documentare eventuali mancanze del sistema di gestione della Sicurezza - inclusi incidenti con o senza infortunio (compresi i «near-misses»), casi di malattia e i danni alla proprietà.

I dati di entrambi i tipi di monitoraggio - "proattivo" e "reattivo" - spesso vengono utilizzati per vedere se gli obiettivi di Sicurezza sono stati raggiunti (per ulteriori informazioni vd. BS 8800 : 1996, E.3.2 e E.3.3).

2) Le tecniche di misurazione

Si riportano di seguito alcuni esempi dei metodi utilizzabili per misurare la prestazione di Sicurezza:

- i risultati dei processi d' identificazione del pericolo, di valutazione e di controllo del rischio;
- ispezioni sistematiche del posto di lavoro con l'ausilio di liste di controllo;
- ispezioni di Sicurezza - per esempio sotto forma di "camminate di Sicurezza" nel luogo di lavoro);
- valutazioni preliminari di nuovi impianti, attrezzature, materiali, sostanze chimiche, tecnologie, processi, procedure o prassi di lavoro;
- ispezioni di macchinari ed impianti specifici allo scopo di controllare che le parti pertinenti alla sicurezza siano state installate e siano in buone condizioni;
- campionamento della sicurezza: esame di aspetti specifici della Sicurezza;
- campionamento ambientale: misurare l'esposizione a sostanze chimiche, biologiche o ad agenti fisici (ad esempio, rumore, particelle organiche volatili, legionella) e confrontarla con le norme riconosciute;
- la possibilità e l'efficacia di avvalersi di personale con esperienza di Sicurezza riconosciuta o con qualifiche formali;
- campionamento del comportamento: valutare il comportamento dei dipendenti per individuare prassi di lavoro non sicure che potrebbero richiedere delle correzioni;
- analisi della documentazione e del materiale d'archivio;
- confronto con le buone prassi di Sicurezza di altre Aziende;
- indagini per determinare le attitudini del personale nei confronti del sistema di gestione della Sicurezza, delle prassi di Sicurezza e dei processi di consultazione dei dipendenti.

Le Aziende devono decidere cosa controllare e a quali intervalli di tempo in base al livello di rischio (vd. 4.3.1). La frequenza delle ispezioni agli impianti e alle macchine può essere definita dalla legge (ad es. nel caso di polmoni d'aria, impianti a vapore ed attrezzatura di sollevamento). Deve essere preparato, come parte del sistema di gestione della Sicurezza, un programma di ispezione basato sui risultati dell'identificazione del pericolo e della valutazione del rischio, sulla legislazione e sulle normative in materia

I capi reparto o i quadri responsabili devono svolgere un abituale monitoraggio di Sicurezza dei processi, degli ambienti di lavoro e delle prassi di lavoro ad intervalli prefissati in base ad un piano documentato. Tutti i capi reparto devono eseguire controlli saltuari dei compiti critici per garantire conformità alle procedure di Sicurezza ed ai regolamenti di esercizio. Per facilitare lo svolgimento delle ispezioni sistematiche ed il monitoraggio, possono essere utilizzate delle liste di controllo.

3) Ispezioni

i) Attrezzatura Deve essere stilato un inventario (utilizzando codici univoci di identificazione) di tutte le attrezzature soggette ad ispezione legale o tecnica da parte di personale addetto (proveniente anche da enti esterni). Tali attrezzature devono essere ispezionate nei modi prestabiliti, e devono essere incluse nei piani di ispezione.

ii) Condizioni di lavoro Devono essere stabiliti e documentati criteri che specifichino le condizioni accettabili del luogo di lavoro. Ad intervalli prefissati, i direttori devono ispezionare la conformità a questi criteri. Si può utilizzare allo scopo un lista di controllo che fornisca i dettagli dei criteri e di tutti gli elementi da ispezionare.

iii) Ispezioni di verifica Devono essere svolte le ispezioni di verifica, ma ciò non esonera i capi reparto dal loro obbligo di svolgere regolari ispezioni o di individuare i pericoli.

iv) Archiviazione della documentazione d'ispezione Deve essere tenuta una documentazione per ogni ispezione di Sicurezza svolta. La documentazione deve indicare se sono state osservate le procedure di Sicurezza, oppure no. Bisogna fare un campionamento della documentazione relativa a ispezioni di Sicurezza, dei giri d'ispezione, delle indagini e delle verifiche del sistema di gestione della Sicurezza per poter individuare le cause alla base di non conformità e di pericoli ripetitivi. Deve essere presa ogni azione preventiva necessaria. Condizioni non conformi e situazioni ed elementi non sicuri, individuati durante le ispezioni, devono essere registrati come non conformità, valutati come un rischio e corretti utilizzando le procedure di non conformità.

4) Strumentazione per le rilevazioni

L' attrezzatura di misurazione utilizzata per valutare le condizioni di Sicurezza (es. misuratori di livello sonoro, fotometri, campionatori d'aria) devono essere elencati, identificati in modo univoco e controllati. Bisogna sapere la precisione di questa strumentazione. Quando è necessario, dovrebbero essere disponibili procedure scritte che descrivono come vengono eseguite le misurazioni. La strumentazione utilizzata per la misurazione deve essere conservata e mantenuta in modo opportuno, e deve essere in grado di effettuare le misure con la precisione richiesta.

Deve essere documentato, ove richiesto, un programma di taratura della strumentazione di misurazione. Questo programma deve includere i seguenti elementi:

- la frequenza della taratura;
- i riferimenti, dove applicabile, alla metodologia di verifica;
- i dati di identificazione degli strumenti da utilizzare per la taratura;
- le azioni da intraprendere quando l'attrezzatura di misura specifica risulta fuori taratura.

La taratura deve essere svolta in condizioni idonee. Vanno preparate delle procedure per le tarature critiche o difficili.

Gli strumenti utilizzati per la taratura devono essere conformi alle eventuali norme nazionali. Se tali norme non esistono, devono essere documentate le basi per i livelli adottati.
La documentazione di tutte le tarature, delle attività di manutenzione e dei risultati deve essere conservata. La documentazione deve fornire dettagli delle misure prima e dopo le eventuali regolazioni.
Lo stato di taratura della strumentazione di misura deve essere chiaramente indicato all'utilizzatore. L'attrezzatura di misura di cui non si sa lo stato di taratura o che è fuori taratura non deve essere utilizzata. Inoltre, va rimossa dall'utilizzo e chiaramente contrassegnata, etichettata o segnalata in altro modo, per prevenirne un uso improprio. Tali identificazioni devono essere eseguite in accordo con procedure scritte. Le procedure devono includere l'identificazione dello stato di taratura dello strumento. Bisogna emettere un rapporto di non conformità per documentare le azioni da prendere. Le procedure devono includere un piano d'azione nel caso venga individuato uno strumento fuori taratura.

5) Strumentazione dei fornitori (appaltatori)

La strumentazione di misura utilizzata dagli appaltatori deve essere soggetta agli stessi controlli dell'attrezzatura dell'Azienda. Agli appaltatori va chiesto di fornire un impegno formale a garantire che la loro attrezzatura sia conforme a tali requisiti. Prima di iniziare il lavoro, il fornitore deve fornire una copia dei documenti relativi alle verifiche di tutte le attrezzature identificate come critiche che necessitano di avere tale documentazione. Se dei compiti richiedono una formazione speciale, la relativa documentazione di formazione va fornita al cliente per un controllo.

6) Tecniche di analisi statistica e inferenziale

Qualsiasi tecnica di analisi statistica o inferenziale utilizzata per valutare una situazione dal punto di vista della Sicurezza, per indagare un incidente senza infortunio o una mancanza nel campo della Sicurezza, o per aiutare a prendere decisioni attinenti la Sicurezza, deve essere basata su principi scientifici solidi. Il delegato di Sicurezza della Direzione deve assicurare che sia individuato l'effettivo bisogno dell'adozione di tali tecniche. Se necessario, devono essere fornite delle linee guide per il loro impiego, specificando le circostanze in cui è appropriato il loro utilizzo.

e) Dati di output tipici

Tipici dati di output includono:

- la/le procedura/e per il monitoraggio e la misurazione;
- i programmi di ispezione e le liste di controllo;
- gli elenchi delle strumentazioni "critiche";
- le liste di controllo per l'ispezione delle strumentazioni;
- le condizioni standard dell'ambiente di lavoro e le liste di controllo per la loro ispezione;
- gli elenchi delle strumentazioni di misurazione;
- le procedure di misurazione;
- i programmi di taratura e le documentazioni delle verifiche di taratura;
- le attività di manutenzione ed i risultati;
- le liste di controllo complete, le relazioni delle ispezioni (dati di output della verifica del sistema di gestione della Sicurezza, vd. 4.5.4);
- le relazioni di non conformità;
- prova dei risultati dell'applicazione di tali procedure.

4.5.2 Incidenti con o senza infortunio, non conformità ed azioni correttive/preventive

a) Requisito della OHSAS 18001

L'Azienda stabilirà e manterrà delle procedure per definire le responsabilità e l' autorità per:

a) il trattamento e l'indagine dei:

- incidenti con infortunio;
- incidenti senza infortunio;
- non conformità;

b) prendere azioni per mitigare qualsiasi conseguenza derivante dagli incidenti con o senza infortunio o dalle non conformità;

c) l'inizio ed il completamento delle azioni correttive e preventive;

d) la conferma dell'efficacia delle azioni correttive e preventive adottate.

Queste procedure richiederanno che tutte le azioni correttive e preventive proposte, prima della loro attuazione, vengano riesaminate attraverso il processo di valutazione del rischio.

Tutte le eventuali azioni correttive e preventive introdotte per eliminare le cause delle non conformità, effettive o potenziali, devono essere adeguate all'entità dei problemi e proporzionate ai rischi riscontrati.

L'Azienda attuerà e documenterà qualsiasi cambiamento, derivante dalle azioni correttive e preventive, nelle procedure documentate.

b) Intento

Le Aziende devono avere delle procedure efficaci per segnalare, valutare ed indagare gli incidenti con o senza infortunio e le non conformità. Lo scopo primario delle procedure è di prevenire la ripetizione di tali eventi, individuando ed eliminando la/e causa/e originaria/e. Inoltre, le procedure devono agevolare la rivelazione, l'analisi e l'eliminazione delle potenziali cause delle non conformità.

c) Dati di input tipici

Tipici dati di input includono:

- le procedure (in generale);
- i piani d'emergenza;
- le relazioni sull'identificazione del pericolo, sulla valutazione e sul controllo del rischio;
- le relazioni sulla verifica del sistema di gestione della Sicurezza, incluse i rapporti di non conformità;
- le relazioni sugli incidenti con o senza infortunio e/o sui pericoli;
- le relazioni sulla manutenzione ordinaria ed straordinaria;

d) Procedura

All'Azienda viene chiesto di preparare procedure documentate per assicurare che si indaghi sugli incidenti con o senza infortunio e sulle non conformità (vd. il punto 3) più avanti) e che vengano introdotte le azioni correttive e preventive adeguate. Deve essere controllato lo stato di avanzamento delle azioni correttive e preventive, e riesaminata la loro efficacia.

1 Procedure

Le procedure devono includere considerazioni sui seguenti temi:

i) Generalità

La procedura deve:

- definire le responsabilità e l'autorità delle persone coinvolte nell'attuazione, nella stesura delle relazioni, nelle indagini, nelle fasi successive e nel monitoraggio delle azioni correttive e preventive;
- richiedere che vengano segnalate tutte le non conformità, gli incidenti con o senza infortunio e i pericoli;
- essere applicata a tutto l'organico (ad es. dipendenti, lavoratori a tempo determinato, personale alle dipendenze degli appaltatori, visitatori e qualsiasi altra persona che si trova nel luogo di lavoro);
- prendere in considerazione i danni alla proprietà;
- assicurare che nessun dipendente venga discriminato per aver segnalato incidenti con o senza infortunio o non conformità;
- definire chiaramente il piano d'azione da intraprendere a seguito delle non conformità nel sistema di gestione della Sicurezza emerse.

ii) Azioni immediate

L'azione immediata da prendere a seguito dell'osservazione di non conformità, incidenti con o senza infortunio o pericoli deve essere conosciuta da tutte le parti. Le procedure devono:

- definire la modalità di segnalazione;
- includere, ove opportuno, la coordinazione con le procedure ed i piani d'emergenza;
- definire l'entità dello sforzo investigativo in relazione al danno effettivo o potenziale (ad es. coinvolgere la Direzione nelle indagini per incidenti gravi).

iii) Archiviazione della documentazione

Devono essere impiegati mezzi adatti per documentare i fatti ed i risultati dell'indagine immediata e della successiva approfondita investigazione. L'Azienda deve assicurarsi che vengano seguite le procedure per:

- documentare i dettagli delle non conformità, degli incidenti e dei pericoli;
- definire dove la documentazione deve essere archiviata e chi ne ha la responsabilità.

iv) Indagine

Le procedure devono definire come deve essere svolta l'indagine. Esse devono specificare:

- il tipo di eventi da investigare (es. gli incidenti senza infortunio che avrebbero potuto avere gravi conseguenze);

- lo scopo delle indagini;

- chi deve condurre le indagini, l' autorità degli investigatori, le qualifiche richieste (se necessario includere anche i capi reparto);

- la/e causa/e prima/e delle non conformità;

- le disposizioni per i colloqui con i testimoni;

- le questioni di natura pratica, quale la disponibilità di videocamere e la conservazione delle prove;

- le disposizioni, inclusi i requisiti legali, per la stesura dei rapporti d'indagine.

Il personale investigativo deve iniziare le analisi preliminari dei fatti mentre vengono raccolte ulteriori informazioni. La raccolta e l'analisi dei dati deve continuare fino a quando si giunge ad una spiegazione adeguata e sufficientemente esauriente.

v) Azioni correttive

Le azioni correttive sono misure che vanno introdotte per eliminare la/e causa/e prima/e delle non conformità e degli incidenti con o senza infortunio, e per poter prevenirne la ripetizione. Esempi di elementi da considerare nello stabilire e mantenere le procedure per le azioni correttive sono:

- l'identificazione e l'attuazione di misure correttive e preventive sia a lungo che a breve termine (questo può anche includere l'utilizzo di appropriate fonti d'informazione, quali i suggerimenti dei dipendenti con esperienza nel campo della Sicurezza);

- la valutazione di eventuali impatti sui risultati dell'identificazione del pericolo e la valutazione del rischio (e qualsiasi necessità di aggiornamento delle relazioni relative ai processi di identificazione del pericolo, della valutazione e del controllo del rischio);

- la documentazione di eventuali cambiamenti nelle procedure risultanti dalle azioni correttive o dall'identificazione del pericolo, dalla valutazione e dal controllo del rischio;

- l'applicazione dei controlli del rischio o la modifica dei controlli del rischio esistenti per far sì che vengano adottate azioni correttive e che queste siano efficaci.

vi) Azioni preventive

Esempi di elementi da considerare nello stabilire e mantenere procedure relative alle azioni preventive sono:

- l'utilizzo di fonti di informazione adatte (l'andamento nella frequenza degli incidenti senza infortunio, le relazioni sulle verifiche del sistema di gestione della Sicurezza, documenti d'archivio, aggiornamento delle analisi del rischio, nuove informazioni sui materiali pericolosi, "camminate di sicurezza", suggerimenti forniti da dipendenti con esperienza nel campo della Sicurezza, ecc.);

- l'identificazione di eventuali problemi che richiedono azioni preventive;

- l'introduzione e l'attuazione di azioni preventive e l'applicazione dei controlli per garantire che esse sia efficaci;

- la documentazione di eventuali cambiamenti nelle procedure derivanti dalle azioni preventive e delle relative richieste di approvazione.

vii) Azioni conseguenti

Le azioni correttive e preventive adottate devono essere se possibile durature ed efficaci.
Devono essere eseguiti controlli sull'efficacia delle azioni correttive e preventive adottate.
Le azioni sospese o in ritardo devono essere segnalate alla Direzione il prima possibile.

2) Analisi delle non conformità e degli incidenti con o senza infortunio

Le cause identificate delle non conformità e degli incidenti con o senza infortunio devono essere classificate ed analizzate regolarmente. La frequenza e l'indice di severità degli incidenti deve essere calcolata in base alle prassi industriali riconosciute per poter avere un termine di paragone.

Deve essere condotta una classificazione e un'analisi dei seguenti elementi:

- la frequenza e l'indice di severità dei casi di malattia/infortunio con conseguente assenza dal lavoro;

- il luogo, il tipo di infortunio, la parte anatomica interessata, l'attività coinvolta, l'azione coinvolta, il giorno, l'ora (se appropriati);

- il tipo e l'entità del danno alla proprietà;

- le cause prime e dirette.

Bisogna fare particolare attenzione agli incidenti che coinvolgono danni alla proprietà. Le documentazioni relative a riparazioni possono essere degli indicatori di danni causati da un incidente non segnalato.

I dati e le informazioni sugli incidenti con infortunio e sulle malattie professionali sono cruciali perché possono costituire un indicatore diretto delle prestazioni di Sicurezza. Comunque, bisogna essere cauti nell'utilizzo di tali dati, e vanno considerati i seguenti aspetti:

- molte Aziende hanno troppo pochi incidenti con infortunio o casi di malattia professionale per poter distinguere la tendenza reale dagli effetti casuali;

- se viene svolto maggior lavoro da uno stesso numero di persone nello stesso tempo, il solo aumento del carico di lavoro può determinare un incremento nella frequenza degli incidenti con infortunio;

- la durata dell'assenza dal lavoro, dovuta a infortunio o a malattia professionale, può essere influenzata da fattori diversi dalla gravità di infortunio o malattia professionale, per esempio dal morale basso, dalla monotonia del lavoro o da cattivi rapporti fra la direzione e l'organico;

- spesso gli incidenti con infortunio non vengono segnalati in modo dettagliato (e occasionalmente sono relazionati in modo esagerato). Il grado di segnalazione può variare e potrebbe migliorare a seguito di un aumento della consapevolezza dell'organico e di sistemi migliori di segnalazione e di documentazione;

- trascorrerà un certo lasso di tempo fra il fallimento del sistema di gestione della Sicurezza e i conseguenti effetti dannosi. Inoltre, molte malattie professionali hanno lunghi periodi di latenza. Non è consigliabile aspettare che il danno si manifesti prima di valutare se i sistemi di gestione della Sicurezza funzionino.

Bisogna giungere a delle valide conclusioni e adottare le azioni correttive adeguate. Almeno una volta all'anno queste analisi vanno trasmesse alla Direzione e incluse nella revisione svolta dalla Direzione (vd. 4.6).

3) Controllo e comunicazione dei risultati

Bisogna valutare l'efficacia delle segnalazioni e delle indagini di Sicurezza. Questa valutazione deve essere oggettiva e deve produrre, se possibile, un risultato quantitativo.

L'Azienda, in base ai risultati dell'indagine, deve:

- individuare le cause originarie delle carenze nel sistema di gestione della Sicurezza e nella gestione generale dell'Azienda, se applicabile;
- comunicarne i risultati e le raccomandazioni alla Direzione ed alle pertinenti parti interessate (vd. 4.4.3);
- includere i risultati e le raccomandazioni derivanti dall'indagine, nel processo continuo di riesame del sistema di Sicurezza;
- sorvegliare l' attuazione delle azioni correttive e la loro successiva efficacia nel tempo;
- applicare all'Azienda nel suo complesso le lezioni apprese dalle indagini delle non conformità, concentrandosi sui principi fondamentali, piuttosto che limitandosi alle azioni specifiche per evitare la ripetizione di un evento identico nella stessa area dell'Azienda.

4) Archiviazione

L'archiviazione può essere effettuata rapidamente e con un minimo di pianificazione formale, o può costituire una più complessa e duratura attività. La documentazione associata deve essere inerente al livello di azione correttiva.
Suggerimenti e segnalazioni devono essere indirizzati, per l'analisi e l'archiviazione, al delegato della Direzione e, dove è il caso, al rappresentante dei lavoratori per la Sicurezza.

L'Azienda deve tenere un registro di tutti gli incidenti con infortunio. In questo registro devono essere inclusi anche quelli che avevano il potenziale per delle conseguenze di Sicurezza rilevanti. Tale registro spesso viene richiesto per legge*.

e) Dati di output tipici

Tipici dati di output includono:

- le procedure per incidenti con infortunio e le non conformità;
- le segnalazioni di non conformità;
- il registro delle non conformità;
- i rapporti d'indagine;
- la documentazione aggiornata relativa all'identificazione del pericolo, alla valutazione e al controllo del rischio;
- dati utilizzati nella revisione da parte della Direzione;
- prova delle valutazioni dell'efficacia delle azioni correttive e preventive adottate.

* *nota del traduttore: in Italia il registro INAIL.*

4.5.3 Documenti e loro gestione

a) Requisito della OHSAS 18001

L'Azienda deve stabilire e mantenere le procedure per l'individuazione, il mantenimento e la disponibilità dei documenti di Sicurezza, come pure i risultati delle attività di verifica e di riesame.

I documenti di Sicurezza devono essere leggibili, identificabili, rintracciabili per le attività interessate. Questi documenti di Sicurezza vanno conservati e mantenuti in modo da essere immediatamente reperibili e protetti contro qualsiasi danno, deterioramento o perdita. Il loro periodo di conservazione deve essere stabilito e documentato.

La documentazione deve essere mantenuta nel modo appropriato al sistema di gestione della Sicurezza e all'Azienda per dimostrare la conformità a questi requisiti OHSAS.

b) Intento

La documentazione deve essere mantenuta per dimostrare che il sistema di gestione della Sicurezza opera in modo efficace e che i processi sono stati svolti in condizioni di sicurezza. La documentazione di Sicurezza che documenta il sistema di gestione della Sicurezza e la conformità ai requisiti, deve essere preparata, mantenuta, leggibile ed adeguatamente identificata.

c) Dati di input tipici

I documenti (utilizzati per dimostrare la conformità ai requisiti) da conservare comprendono:

- la documentazione relativa alla formazione del personale;
- la documentazione relativa alle indagini di Sicurezza;
- la documentazione relativa alle verifiche del sistema di gestione della Sicurezza;
- la documentazione relativa alle consultazioni;
- la documentazione relativa agli incidenti con o senza infortunio;
- la documentazione relativa all' attività svolta a seguito di incidenti con o senza infortunio;
- i verbali delle riunioni di Sicurezza;
- la documentazione relativa ai test clinici;
- la documentazione relativa alla sorveglianza sanitaria;
- la documentazione relativa ai dispositivi di protezione individuale e alla loro manutenzione;
- la documentazione relativa alle esercitazioni d'emergenza;
- la verifica da parte della Direzione;
- la documentazione relativa all' identificazione del pericolo e alla valutazione e controllo del rischio.

d) Procedura

Il requisito della OHSAS 18001 è piuttosto chiaro. Tuttavia si possono fare ulteriori considerazioni per quanto riguarda i seguenti temi:

- l'autorità per la disposizione della documentazione di Sicurezza;
- la riservatezza della documentazione di Sicurezza;

- i requisiti, legali e non, circa la conservazione della documentazione di Sicurezza;

- problemi inerenti l'uso degli archivi elettronici.

La documentazione di Sicurezza deve essere compilata in modo completo, leggibile ed adeguatamente identificata. Devono essere definiti i tempi di conservazione della stessa. La documentazione deve essere archiviata in un luogo sicuro, facilmente raggiungibile e protetta da qualsiasi rischio di deterioramento. La documentazione di Sicurezza critica deve essere opportunamente protetta da un eventuale incendio e da altri tipi di danno, oppure come richiesto dalle leggi vigenti.

e) Dati di output tipici

Tipici dati di output includono:

- le procedure (per l'identificazione, mantenimento e disponibilità dei documenti di Sicurezza);

- la documentazione di Sicurezza adeguatamente conservata e facilmente accessibile.

4.5.4. Verifica

Requisito della OHSAS 18001

L'Azienda deve stabilire e mantenere un programma di verifica e le relative procedure per le verifiche periodiche del sistema di gestione della Sicurezza da svolgere per poter:

a) determinare se il sistema del gestione della Sicurezza:

   1) è conforme alle disposizioni previste per la gestione della Sicurezza, inclusi i requisiti di questa specifica OHSAS;
   2) è stato attuato e mantenuto in modo appropriato; e
   3) è efficace nel raggiungere gli obiettivi e la politica di Sicurezza dell'Azienda;

b) riesaminare i risultati delle precedenti verifiche;

c) fornire alla Direzione informazioni sui risultati delle verifiche.

Il programma di verifica, incluso eventuali piani di programmazione, devono essere basati sui risultati della valutazione dei rischi inerenti le attività dell'Azienda, e sui risultati di precedenti verifiche. Le procedure di verifica dovranno comprendere l'entità, la frequenza, le metodologie e le competenze, come pure le responsabilità ed i requisiti per l'esecuzione delle verifiche e per la documentazione dei risultati.

Dove è possibile, le verifiche devono essere condotte da personale indipendente da chi ha responsabilità diretta sulle attività esaminate[*].

NOTA: la parola "indipendente" qui non significa necessariamente estraneo all'Azienda.

b) Intento

La verifica del sistema di gestione della Sicurezza è un processo attraverso il quale le Aziende possono riesaminare e valutare in continuazione l'efficacia del loro sistema di gestione della Sicurezza. In generale, le verifiche del sistema di gestione della Sicurezza devono necessariamente considerare le procedure e la politica di Sicurezza, oltre alle condizioni e alle prassi del luogo di lavoro.
Deve essere stabilito un programma interno per la verifica del sistema di gestione della Sicurezza, in modo da consentire all'Azienda di riesaminare la conformità del suo sistema di gestione della Sicurezza ai requisiti OHSAS 18001. Le verifiche pianificate del sistema di gestione della Sicurezza devono essere svolte da personale interno all'Azienda e/o da personale esterno, selezionato dall'Azienda, per stabilire il grado di conformità alle procedure di Sicurezza e per valutare se il sistema è efficace nel raggiungere gli obiettivi di Sicurezza dell'Azienda. In entrambi i casi, il personale che esegue le verifiche del sistema di gestione della Sicurezza deve trovarsi in una posizione tale da poterle svolgere in modo imparziale ed oggettivo.

NOTA: Le verifiche interne del sistema di gestione della Sicurezza si concentrano sulla prestazione del sistema di gestione della Sicurezza. Esse non devono essere confuse con le ispezioni di Sicurezza[*].

c) Dati di input tipici

Tipici dati di input includono:

- la dichiarazione della politica di Sicurezza dell'Azienda;
- gli obiettivi di Sicurezza;

[*] *Nota del traduttore : questa tecnica viene talora denominata Non-Process-Quality-Control, cioè controllo di qualità non di processo.*

[*] *Nota del traduttore : Cfr. Piano aziendale di sicurezza, ottobre '90, Documento 5, Annesso 5.2, pag. 18.*

- le procedure di Sicurezza e le istruzioni di lavoro;
- i risultati dell'identificazione del pericolo, della valutazione e del controllo del rischio;
- la legislazione e le prassi migliori (se applicabili);
- i rapporti di non conformità;
- le procedure di verifica del sistema di gestione della Sicurezza;
- la nomina di un verificatore (o più di uno) competente, "indipendente", interno o esterno;
- la procedura per le non conformità.

d) Procedura

1) Verifiche

Le verifiche del sistema di gestione della Sicurezza forniscono una valutazione esauriente e formale della conformità dell'Azienda alle procedure e prassi di Sicurezza.

Le verifiche del sistema di gestione della Sicurezza devono essere svolte in accordo alle disposizioni prefissate. Ci può essere bisogno di ulteriori verifiche in base alle circostanze.

Le verifiche del sistema di gestione della Sicurezza devono essere svolte soltanto da personale competente e "indipendente".

I dati di output di una verifica del sistema di gestione della Sicurezza devono includere la valutazione dettagliata dell'efficacia delle procedure di Sicurezza, il grado di conformità alle procedure e alle prassi e devono, ove necessario, individuare le azioni correttive. I risultati delle verifiche del sistema di gestione della Sicurezza devono essere documentate e segnalate alla Direzione nel modo opportuno.
La Direzione deve rivedere i risultati ed adottare, se necessario, efficaci azioni correttive.

NOTA: I principi generali e le metodologie descritte nella ISO 10011 - 1, ISO 10011 - 2, ISO 10011 - 3, ISO 14010, ISO 14011, ISO 14012 o la BS 8800 : 1996, allegato F, sono applicabili per la verifica del sistema di gestione della Sicurezza.

2) Programmazione

Deve essere preparato un piano annuale per svolgere le verifiche interne del sistema di gestione della Sicurezza. Le verifiche del sistema di gestione della Sicurezza devono considerare l'intera operazione soggetta al sistema di gestione della Sicurezza e valutare la conformità ai requisiti della OHSAS.

La frequenza e l'oggetto delle verifiche del sistema di gestione della Sicurezza devono essere decisi in base ai rischi associati alle lacune dei vari elementi del sistema di gestione della Sicurezza, ai dati disponibili sulla prestazione del sistema di gestione della Sicurezza, ai dati di output provenienti dai riesami della Direzione, ed in base al grado con cui il sistema di gestione della Sicurezza o l'ambiente nel quale esso è operativo siano soggetti a cambiamenti.

Ulteriori, non pianificate verifiche del sistema di gestione della Sicurezza possono essere necessarie in seguito al verificarsi di situazioni particolari, per esempio dopo un incidente con infortunio.

3) Sostegno della Direzione

Affinché le verifiche del sistema di gestione della Sicurezza siano utili, è necessario che la Direzione si impegni appieno nella verifica del sistema di gestione della Sicurezza e nella sua efficace attuazione in tutta l'Azienda. La Direzione deve tenere in debita considerazione i risultati e le raccomandazioni delle verifiche del sistema di gestione della Sicurezza e deve intraprendere l'azione appropriata in un arco di tempo ragionevole. Una volta dato il consenso perché si effettui una verifica del sistema di gestione della Sicurezza, questa deve essere completata in modo imparziale.

Tutto il personale interessato dalla verifica deve essere informato sugli scopi della verifica del sistema di gestione della Sicurezza e sui benefici che essa apporterà. Il personale deve essere incoraggiato a cooperare appieno con i verificatori e rispondere onestamente alle loro domande.

4) Verificatori

Una o più persone possono eseguire le verifiche. L'utilizzo di una squadra può ampliare l'interesse e migliorare la cooperazione, e può anche consentire l'utilizzo di una gamma più estesa di competenze.

I verificatori non devono essere dipendenti dalla sezione dell'Azienda o dall'attività sotto esame.

I verificatori devono capire quali sono i loro compiti e devono possedere le competenze necessarie per svolgerli. Devono possedere l'esperienza e la conoscenza specifica delle norme e dei sistemi relativi a ciò che devono verificare, per poter valutare la prestazione ed individuare eventuali mancanze. I verificatori devono conoscere i requisiti contenuti nelle legislazioni applicabili. Inoltre, i verificatori devono essere consapevoli e avere accesso alle norme e alle linee guida pertinenti il lavoro che stanno svolgendo.

5) L'interpretazione e la raccolta dei dati

Le tecniche e i mezzi utilizzati per la raccolta delle informazioni dipenderanno dalla natura della verifica del sistema di gestione della Sicurezza in questione. La verifica del sistema di gestione della Sicurezza deve garantire il controllo di un campione rappresentativo delle attività essenziali e l'intervista del personale pertinente (inclusi i rappresentanti dei lavoratori per la Sicurezza, ove richiesto). Si deve esaminare la documentazione relativa. Questa include i seguenti documenti:

- la documentazione del sistema di gestione della Sicurezza;
- la documentazione della politica di Sicurezza;
- gli obiettivi di Sicurezza;
- le procedure relative alla Sicurezza e all' emergenza;
- sistemi e procedure per il permesso di lavoro;
- i verbali delle riunioni di Sicurezza;
- la documentazione e le segnalazioni degli incidenti con o senza infortunio;
- eventuali segnalazioni o comunicazioni delle autorità che si occupano di Sicurezza o di altri enti (es. verbali, lettere, circolari, ecc.);
- registri e certificati legali;
- la documentazione relativa alla formazione del personale;
- la documentazione relativa a precedenti verifiche del sistema di gestione della Sicurezza;
- le richieste per azioni correttive;
- documentazione relativa alle non conformità.

Dove possibile, devono essere incorporati nelle procedure di verifica del sistema di gestione della Sicurezza dei controlli per evitare un'interpretazione scorretta o un errato utilizzo dei dati raccolti, delle informazioni e di altre segnalazioni.

6) Risultati delle verifiche

Il contenuto della relazione finale della verifica del sistema di gestione della Sicurezza deve essere chiaro, preciso e completo. Il verificatore dovrà datare e firmare la relazione. La relazione deve contenere, se applicabili, i seguenti elementi:

- gli obiettivi e lo scopo della verifica del sistema di gestione della Sicurezza;

- i particolari del programma di verifica del sistema di gestione della Sicurezza, l'individuazione dei membri della squadra della verifica, i rappresentanti delle attività da esaminare, le date e l'identificazione delle aree soggette alla verifica;

- l'individuazione dei documenti di riferimento utilizzati per svolgere la verifica del sistema di gestione della Sicurezza (es. OHSAS 18001 ed il manuale della gestione della Sicurezza);

- i dettagli delle non conformità identificate;

- la valutazione del verificatore del grado di conformità alla OHSAS 18001;

- l'abilità del sistema di gestione della Sicurezza nel raggiungere gli obiettivi di gestione della Sicurezza dichiarati;

- la distribuzione della relazione finale della verifica del sistema di gestione della Sicurezza.

I risultati delle verifiche del sistema di gestione della Sicurezza devono essere forniti a tutte le parti interessate il più presto possibile, per permettere l'introduzione delle azioni correttive relative.
Deve essere redatto un piano d'azione contenente le azioni correttive concordate, l'identificazione delle persone responsabili della loro attuazione, le date di completamento ed i requisiti di documentazione. Devono essere stabilite le disposizioni per il controllo successivo, per garantire una attuazione soddisfacente delle raccomandazioni.

Occorre tenere conto del grado di riservatezza delle informazioni contenute nelle relazioni finali della verifica del sistema di gestione della Sicurezza.

e) Dati di output tipici

Tipici dati di output includono:

- i piani/programmi di verifica del sistema di gestione della Sicurezza;

- le procedure per la verifica del sistema di gestione della Sicurezza;

- la documentazione della verifica del sistema di gestione della Sicurezza, incluse le segnalazioni di non conformità, le raccomandazioni e le richieste di azioni correttive;

- la documentazione delle non conformità firmate e completate;

- la prova che i risultati della verifica del sistema di gestione della Sicurezza sono stati comunicati alla Direzione.

4.6 Revisione da parte della Direzione

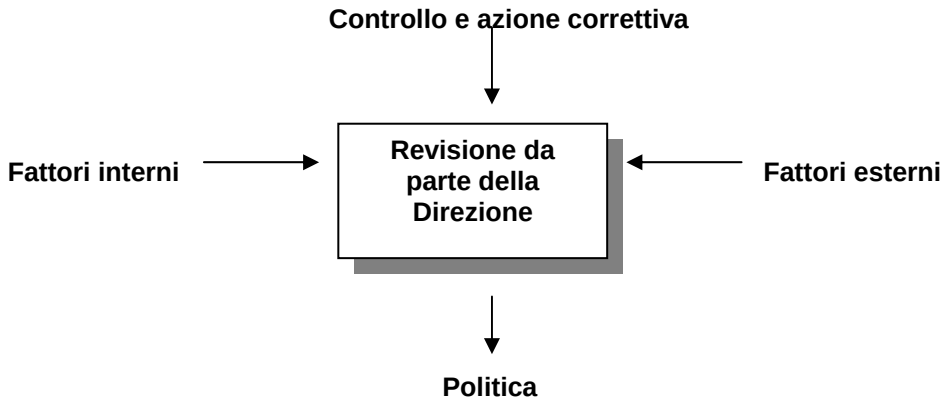

Figura 6 - Revisione da parte della Direzione

a) Requisito della OHSAS 18001

La Direzione dell'Azienda deve, ad intervalli da lei scelti, riesaminare il sistema di gestione della Sicurezza, per garantire una sua continua idoneità, adeguatezza ed efficacia. Il processo di revisione da parte della Direzione deve garantire che siano raccolte le informazioni necessarie per permettere alla Direzione di svolgere la valutazione. Questa revisione deve essere documentata.

La revisione da parte della Direzione deve considerare l' eventuale necessità di apportare modifiche alla politica, agli obiettivi e ad altri elementi del sistema di gestione della Sicurezza, alla luce dei risultati della verifica del sistema di gestione della Sicurezza, delle circostanze modificate e dell'impegno per un miglioramento continuo.

b) Intento

La Direzione deve riesaminare l'applicazione del sistema di gestione della Sicurezza, per valutare se sia stato pienamente attuato e per far sì che rimanga idoneo alla politica di Sicurezza e al raggiungimento dei dichiarati obiettivi di Sicurezza.

La revisione deve anche considerare se la politica di Sicurezza continua ad essere appropriata. Deve stabilire degli obiettivi di Sicurezza nuovi o aggiornati per un miglioramento continuo, che siano adatti per il periodo imminente, e deve considerare se c'è la necessità di attuare cambiamenti ad alcuni elementi del sistema di gestione della Sicurezza.

c) Dati di input tipici

Tipici dati di input includono:

- i dati statistici degli incidenti con infortunio;
- i risultati delle verifiche interne ed esterne del sistema di gestione della Sicurezza;
- le azioni correttive adottate nel sistema di gestione della Sicurezza dopo la precedente revisione;
- la documentazione relativa alle emergenze (reali o da esercitazione);
- la relazione del delegato di Sicurezza della Direzione sulle prestazioni generali del sistema;
- le relazioni dei singoli capi reparti sull'efficacia locale del sistema;
- la documentazione relativa all' attività di identificazione del pericolo, della valutazione e del controllo del rischio.

d) Procedura

La revisione deve essere svolta dalla Direzione a cadenza regolare (ad esempio, annualmente). La revisione deve focalizzarsi sulle prestazioni globali del sistema di gestione della Sicurezza e non su specifici dettagli, dato che questi sono già considerati dalle normali procedure del sistema di gestione della Sicurezza.
Nel pianificare tale revisione, bisogna tenere conto dei seguenti aspetti:

- gli argomenti principali da trattare;
- chi deve presenziare (i direttori, gli specialisti in Sicurezza, altro personale);
- le responsabilità dei singoli partecipanti per quanto riguarda la revisione;
- le informazioni da utilizzare nella revisione.

La revisione deve includere i seguenti argomenti:

- l'idoneità della politica di Sicurezza attuale;
- la stesura o l'aggiornamento degli obiettivi Sicurezza per un miglioramento continuo nel periodo imminente;
- l'adeguatezza delle attuali attività di identificazione del pericolo, della valutazione e del controllo del rischio;
- gli attuali livelli di rischio e l'efficacia delle misure di controllo esistenti;
- l'adeguatezza delle risorse (economiche, umane e materiali);
- l'efficacia delle procedure d'ispezione di Sicurezza;
- l'efficacia delle procedure per la segnalazione del pericolo;
- i dati relativi agli incidenti con o senza infortunio occorsi;
- casi segnalati di procedure non efficaci;
- i risultati delle verifiche interne ed esterne del sistema di gestione della Sicurezza, svolte dopo la precedente revisione, e la loro efficacia;

- lo stato di preparazione all'emergenza;

- i miglioramenti da apportare al sistema di gestione della Sicurezza (es. nuove iniziative da introdurre o l'espansione di iniziative esistenti);

- i risultati di ogni indagine sugli incidenti con o senza infortunio;

- una valutazione degli effetti dei cambiamenti futuri richiesti dalla legge o da tecnologie.

Il delegato di Sicurezza della Direzione deve fornire, durante la riunione, un resoconto sulle prestazione generali del sistema di gestione della Sicurezza.

Se necessario devono essere tenuti riesami parziali della prestazione del sistema di gestione della Sicurezza ad intervalli più frequenti.

e) Dati di output tipici

Tipici dati di output includono:

- i verbali della revisione;

- revisioni alla politica di Sicurezza e agli obiettivi di Sicurezza;

- le specifiche azioni correttive per i singoli responsabili e le scadenze per il loro completamento;

- azioni specifiche di miglioramento, le responsabilità designate e le scadenze per il loro completamento;

- le date per il riesame delle azioni correttive;

- le aree cruciali da sottolineare nella pianificazione di future verifiche interne del sistema di gestione della Sicurezza.

Allegato A (Informativo)

Collegamenti tra la OHSAS 18001, la BS EN ISO 9001 (Sistemi di Qualità) e la BS EN ISO 14001 (Sistema di Gestione Ambientale)

I principi base della gestione sono comuni indipendentemente dal tema gestito, sia esso la qualità, l'ambiente, la sicurezza e salute professionale od altre attività aziendali. Alcune Aziende trarranno vantaggi da un sistema di gestione integrato, mentre altre preferiranno l'adozione di sistemi diversi basati sugli stessi principi di gestione. La tavola A.1 riporta i collegamenti fra la OHSAS 18001 e la BS EN ISO 9001 e la BS EN ISO 14001 per le Aziende che già usano l'una o l'altra di queste norme internazionali per i sistemi di gestione, e che ora vogliono integrare la Sicurezza nei loro sistemi di gestione esistenti. Si illustrano i collegamenti solo a titolo informativo.

Tabella A.1 - Collegamenti tra la OHSAS 18001:1999, la ISO 14001:1996 e la ISO 9001:1994

Art.	OHSAS 18001	Art.	ISO 14001 : 1996	Art.	ISO 9001:1994
1	Obiettivo	1	Obiettivo	1	Obiettivo
2	Pubblicazioni di riferimento	2	Riferimenti normativi	2	Riferimenti normativi
3	Definizioni	3	Definizioni	3	Definizioni
4	Elementi dei sistemi di gestione della Sicurezza	4	Requisiti dei sistemi di gestione ambientale	4	Requisiti del sistema qualità
4.1	Requisiti generali	4.1	Requisiti generali	4.2.1	Generalità (solo la 1a frase)
4.2	Politica di Sicurezza	4.2	Politica ambientale	4.1.1	Politica della qualità
4.3	Pianificazione	4.3	Pianificazione	4.2	Sistema della qualità
4.3.1	Pianificazione per l'identificazione del pericolo, la valutazione ed il controllo del rischio	4.3.1	Aspetti ambientali	4.2	Sistema della qualità
4.3.2	Requisiti legali e altri requisiti	4.3.2	Requisiti legali e non		--------
4.3.3	Obiettivi	4.3.3	Obiettivi e traguardi	4.2	Sistema della qualità
4.3.4	Programma/i di gestione della Sicurezza	4.3.4	Programma/i di gestione ambientale	4.2	Sistema della qualità
4.4	Attuazione ed esecuzione	4.4	Attuazione ed esecuzione	4.2 4.9	Sistema della qualità Controllo del processo
4.4.1	Struttura e responsabilità	4.4.1	Struttura e responsabilità	4.1 4.1.2	Responsabilità della Direzione Azienda
4.4.2	Formazione, informazione e competenza	4.4.2	Formazione, consapevolezza e competenza	4.18	Formazione
4.4.3	Consultazione e comunicazione	4.4.3	Comunicazione		-------
4.4.4	Documentazione	4.4.4	Documentazione del sistema di gestione ambientale	4.2.1	Generalità (esclusa la 1a frase)
4.4.5	Controllo dei documenti e dei dati	4.4.5	Controllo dei documenti	4.5	Controllo dei documenti e dati

4.4.6	Controllo delle attività aziendali	4.4.6	Controllo delle attività aziendali	4.2.2 4.3 4.4 4.6 4.7 4.8 4.9 4.15 4.19 4.20	Procedure del sistema di qualità Riesame dei contratti Controllo della progettazione Acquisiti Prodotti forniti dai clienti Identificazione e rintracciabilità dei prodotti Controllo del processo Movimentazione, stoccaggio, imballaggio, conservazione e consegna Manutenzione Tecniche statistiche
4.4.7	Preparazione e risposta all'emergenza	4.4.7	Preparazione e risposta all'emergenza		-------
4.5	Controllo e azione correttiva	4.5	Controllo e azione correttiva		-------
4.5.1	Misurazione e monitoraggio delle prestazioni	4.5.1	Controllo e misurazione	4.10 4.11 4.12	Ispezione e collaudo Controllo dell'attrezzatura di ispezione, misurazione e collaudo Stato della ispezione e del collaudo
4.5.2	Incidenti con o senza infortunio, non conformità ed azioni correttive/ preventive	4.5.2	Non conformità ed azione correttiva e preventiva	4.13 4.14	Controllo di prodotti non conformi Azione correttiva e preventiva
4.5.3	Documenti e loro gestione	4.5.3	Documenti	4.16	Controllo della documentazione di qualità
4.5.4	Verifica	4.5.4	Verifica del sistema di gestione ambientale	4.17	Verifica interna di qualità
4.6	Revisione da parte della Direzione	4.6	Revisione da parte della Direzione	4.1.3	Revisione da parte della Direzione
Allegato A	Collegamenti con la ISO 14001 e ISO 9001	Allegato B	Collegamenti con la ISO 9001		-------
	Bibliografia	Allegato B	Bibliografia	Allegato A	Bibliografia
	(OHSAS 18002)	Allegato A	Guida all'uso della specifica		-------

Bibliografia

ISO 9001 : 1994, *Sistemi di Qualità: Modello per il Controllo della Qualità nelle attività di progettazione, sviluppo, produzione, installazione e manutenzione*.

ISO 14001 : 1996, *Sistemi di gestione ambientale - Specifica con guide all'uso*.

Supplemento per il Regno Unito

Pubblicazioni BSI standard

BRITISH STANDARDS INSTITUTION, LONDON W4 4AL

BS 8800 : 1996	*Guida ai Sistemi di Gestione della Sicurezza e Salute Professionale*
BS EN 30011 - 1 : 1993	*Guida alla Verifica di Sistemi di Qualità - Parte 1: Verifica*
BS EN 30011 - 2 : 1993	*Guida alla Verifica di Sistemi di Qualità - Parte 2: Criteri per le Qualifiche degli Ispettori di Verifica*
BS EN 30011 - 3 : 1993	*Guida alla Verifica di Sistemi di Qualità - Parte 3: Gestione di un Programma di Verifica*
BS EN ISO 9001 : 1994	*Sistemi di Qualità: Modello per il Controllo della Qualità nelle attività di progettazione, sviluppo, produzione, installazione e manutenzione*
BS EN ISO 14001 : 1996	*Sistemi di Gestione Ambientali - Specifica con Guida all'Uso*

Pubblicazioni della Commissione/Esecutivo di Sicurezza e Salute

(1) COMMISSIONE SICUREZZA E SALUTE - *Gestione della Sicurezza e Salute Professionale*. 1992. London: The Stationery Office

(2) ESECUTIVO SICUREZZA E SALUTE - *Gestione Valida di Sicurezza e Salute*: HS(G) 65. 1997. London: The Stationery Office

L'indirizzo del centro a cui il pubblico può rivolgersi è:

HSE information Centre
Broad Lane
Sheffield 53 7HQ

Tel.: +44.0114 289 2345
Fax: +44.0114 289 2333

Le pubblicazioni HSE, sia gratis che a pagamento, sono disponibili da:

HSE Books
PO Box 199
Sudbury
Suffolk CI0 6FS

Tel: +44.0178 788 1165
Fax: +44. 0178 731 1995

BSI — British Standards Institution

La BSI è un ente nazionale indipendente con la responsabilità di preparare le specifiche "British Standard". La BSI rappresenta il Regno Unito per quanto riguarda le norme in Europa e a livello internazionale. È costituita mediante Statuto Reale.

Revisioni
Le specifiche "British Standard" vengono aggiornate mediante emendamenti e revisioni. Gli utenti devono assicurarsi di possedere gli ultimi emendamenti o le ultime edizioni.

La BSI mira costantemente a migliorare la qualità dei suoi prodotti e dei suoi servizi e sarà grata a coloro che, usando le sue specifiche e trovando qualche inesattezza o qualche ambiguità, volessero informarci della stessa.
Tel.: +44.020 8996 9000, Telefax: +44.020 8996 7400.

La BSI offre ai soci un servizio individuale di aggiornamento chiamato PLUS; questo assicura che gli abbonati ricevano automaticamente l'ultima edizione delle sue specifiche.

Acquisto delle specifiche
Indirizzare tutte le ordinazioni per le specifiche "British Standard" o internazionali al nostro Customer Service.
Tel.: +44.020 8996 7000, Telefax: +44.020 8996 7001.

Quando si ordinano specifiche internazionali, è uso della BSI di fornire la versione BSI di quella pubblicata come specifiche "British Standard", se non altrimenti richiesto.

Informazioni sulle specifiche
La BSI offre una vasta gamma d'informazioni sulle specifiche europee e internazionali attraverso la sua Libreria ed il suo Servizio di Assistenza Tecnica ai Esportatori. Vari servizi elettronici sono disponibili con dettagli di tutti i prodotti e servizi offerti dalla BSI. Contattare il Reparto Informazioni.
Tel.: +44.020 8996 7111, Telefax: +44. 020 8996 7048.

Gli abbonati sono tenuti al corrente degli aggiornamenti mediante gli sviluppi delle specifiche e ricevono grossi sconti sul prezzo d'acquisto delle specifiche stesse. Per i dettagli di questi e di altri vantaggi, contattare Membership Admisitration.
Tel.: +44.020 8996 7002, Telefax: +44.020 8996 7001.

Diritti d'autore

BSI
389 Chiswick High Road
London
W4 4AL