



SEMINARIO

Le nuove responsabilità negli Enti ed Imprese con l'introduzione della AI



Ing. Roberto Francini

***Presidente Commissione 231 e modelli organizzativi
Ordine degli Ingegneri della Provincia di Roma***

seminario 31 marzo 2026

Industry 4.0 towards Industry 5.0

Partiamo da un caso reale

Lo stabilimento Siemens di Amberg mostra bene il passaggio da Industria 4.0 a Industria 5.0. In ottica 4.0, la fabbrica integra automazione, IoT, analisi dei dati e sistemi digitali per ottimizzare produzione, qualità ed efficienza.

In ottica 5.0, invece, queste stesse tecnologie vengono orientate anche al benessere delle persone, alla collaborazione uomo-macchina, alla sostenibilità ambientale e alla resilienza del sistema produttivo. Circa **il 75% della catena del valore sarà gestito automaticamente da macchine e robot**, mentre gli operatori supervisionano e ottimizzano i processi.

L'investimento di circa 200 milioni di euro mira a rispondere alla crescente domanda di prodotti elettronici ad alta tecnologia potenziando la flessibilità operativa attraverso l'integrazione di sistemi digitali e automatizzati.





PRINCIPI GENERALI DI RESPONSABILITA' DEL MANAGEMENT

Il passaggio da Industria 4.0 a Industria 5.0 è già in corso, vediamo come si adeguano le responsabilità degli Enti e le responsabilità dei manager d'impresa ai sensi del DLGS 231/01

Ripercorriamo inizialmente come sono normalmente suddivise le responsabilità , civili e penali in ambito aziendale

Successivamente come dovranno adeguarsi in funzione dell'introduzione della A.I. in azienda

PRINCIPI GENERALI DI RESPONSABILITA' DEL MANAGEMENT

ENTE / IMPRESA (Organizzazione)

- ☐ Responsabilità organizzativa e di governance
- ☐ Sistema di controllo e compliance
- ☐ Responsabilità amministrativa dell'ente
- ☐ Modelli organizzativi e procedure MOG 231.

MANAGER / DIRIGENTI

- ☐ Decisioni operative e gestione attività
- ☐ Vigilanza su personale e processi
- ☐ Attuazione delle procedure aziendali
- ☐ Responsabilità civile e penale personale



FUNZIONI OPERATIVE / DIPENDENTI

- Esecuzione attività operative
- Rispetto procedure e istruzioni
- Segnalazione anomalie o rischi
- Responsabilità disciplinare e operativa

SECTION

2 cenni di richiamo sul DLGS 231
E Modello Organizzativo Gestionale –MOG-

02

Obiettivo del DLGS 231/01



Il D.lgs. n. 231/2001 introdusse una grande novità per il diritto d'impresa, ponendo a carico delle società una responsabilità amministrativa/penale per

1. una serie di reati commessi da propri amministratori, dirigenti, dipendenti o terzi mandatari, definiti apicali
2. qualora siano stati realizzati nell'interesse o a vantaggio dell'impresa e
3. siano stati resi possibili da carenze della struttura organizzativa dell'impresa stessa.

Le società possono sottrarsi a responsabilità – e quindi alle relative sanzioni – qualora abbiano adottato, prima della commissione del fatto-reato, un idoneo Modello Organizzativo e Gestionale, predisposto ai sensi del Decreto 231 (in breve MOG231) , **dimostrando di aver fatto il possibile per evitare il reato.**



Responsabilità dell'Ente

Come può l'ente/azienda dimostrare di non essere responsabile per un reato commesso da un suo dipendente apicale ?

- L'ente potrebbe essere **esente da responsabilità** se prova, di aver adottato un modello ("MOGC") adeguato, o se la persona che ha commesso il reato è riuscita a commetterlo eludendo fraudolentemente il modello.
- **Le sanzioni potrebbero essere evitate**, in altri, notevolmente ridotte se l'ente si è adoperata per recuperare rapidamente le carenze ad essa contestate con le conseguenze provocate dall'illecito/reato .
- Appare evidente che nei reati 231 la dimostrazione di aver adottato le **misure logiche e organizzative idonee è fondamentale**.



RECENTI SENTENZE DI RESPONSABILITA' DEL MANAGEMENT

In caso di infortunio sul lavoro, il vantaggio dell'ente può consistere anche nel risparmio derivante dall'omessa formazione e informazione dei lavoratori, *“sia in termini di mancata sopportazione dei relativi costi, sia per effetto della circostanza che i dipendenti, ove impegnati nella frequenza dei corsi, sono distolti dall'attività lavorativa”*. Inoltre, può costituire un indebito vantaggio anche la mancata attuazione di un sistema disciplinare idoneo a sanzionare la violazione dei protocolli aziendali di prevenzione.

Lo afferma la Cassazione, con [sentenza n. 7563 del 25 febbraio scorso](#), con cui è stato dichiarato inammissibile il ricorso presentato da una società agricola semplice, condannata per l'infortunio mortale di un lavoratore, investito da un trattore che procedeva in retromarcia nel capannone dell'azienda.



RECENTI SENTENZE DI RESPONSABILITA' DEL MANAGEMENT

La Cassazione nella recente [sentenza n. 8034, depositata lo scorso 2 marzo](#), ha confermato la responsabilità penale, tra gli altri, del titolare dell'impresa che aveva appaltato le attività di smontaggio di una caldaia in una raffineria, nel corso delle quali un lavoratore dell'azienda affidataria rimaneva schiacciato dal braccio telescopico di una gru.

Per la Corte, infatti, *“il committente viene reso corresponsabile dell'effettiva attuazione delle cautele funzionali alla gestione del rischio interferenziale”* e l'obbligo di nominare CSP e CSE rappresenta lo strumento per realizzare, con l'ausilio di esperti della sicurezza,

Le denunce di infortunio sul lavoro pervenute all'Inail per il 2025 risultano, in via provvisoria, 598mila, con un incremento dell'1,4% rispetto alle 590mila dell'anno precedente, 8mila casi in più.
1093 i decessi riportati dall'INAIL nel 2025



RECENTI SENTENZE DI RESPONSABILITA' DEL MANAGEMENT

In caso di infortunio mortale di un dipendente, non si può dichiarare la colpevolezza di un Datore, nè di un ente ex art. 25 septies D.Lgs. 231/2001, basandosi sulla *"distorsione retrospettiva del 'senno di poi' (hindsight bias), mediante la quale si tende a ritenere prevedibile un evento, una volta che l'evento è ormai noto, e a costruire di conseguenza la regola cautelare (nel caso individuata nella "procedimentalizzazione" della lavorazione) che avrebbe potuto impedirlo"*.

Così la Cassazione ha annullato con rinvio una condanna pronunciata nei confronti di una s.r.l. e del suo titolare per un incidente ad un lavoratore esperto, rimasto folgorato nel corso di alcune operazioni di precollaudo di un trasformatore ([sentenza n. 37972 del 24 novembre scorso](#)).

SECTION

PRINCIPIO DI RESPONSABILITA'

04

Principio generale di responsabilità del management (DLgs. 231/01)

Quando il management adotta un sistema di controllo predittivo (anche basato su **AI**), **non delega la responsabilità alla tecnologia**.

👉 Il sistema è uno **strumento di supporto**, non un soggetto decisionale.

Il management resta responsabile per:

- **scelte organizzative**
- **adeguatezza dei controlli**
- **vigilanza sul funzionamento del sistema**

a) Responsabilità di scelta (culpa in eligendo)

Il management è responsabile di:

- selezionare una soluzione **tecnicamente adeguata** allo scopo
- verificare che il sistema sia coerente con:
 - processi produttivi
 - rischi HSE
 - requisiti normativi

⚠ Rischio 231: adozione di sistemi non validati o “black box” senza controlli.

b) Responsabilità di configurazione e governance

Il management deve assicurare:

- corretta **definizione delle soglie decisionali**
- chiara **assegnazione delle responsabilità operative**
- presenza di **procedure formali** su:
 - uso del sistema
 - gestione degli alert
 - escalation dei guasti

⚠ Rischio 231: uso improprio del sistema o decisioni automatizzate non presidiate.

c) Responsabilità di vigilanza (culpa in vigilando)

Anche dopo l'adozione, il management deve:

- ✓ monitorare le performance del sistema
- ✓ verificare errori sistemici o falsi negativi
- ✓ aggiornare modelli e dati

⚠ Rischio 231: affidamento acritico alla tecnologia ("automation bias").

d) Responsabilità in materia di salute e sicurezza sul lavoro

Se il sistema:

- ✓ **non segnala correttamente un rischio**
- ✓ o il management **ignora un alert** e si verifica un infortunio:

👉 possibile responsabilità per:

1. lesioni colpose
2. omicidio colposo (art. 25-septies DLgs. 231)

Esempio di Responsabilità in caso di evento dannoso Scenario tipico

- Il sistema predittivo segnala rischio di guasto.
- L'intervento viene rinviato per motivi produttivi.
- Si verifica incidente o fermo grave.

Responsabilità ricade su:

- management (decisione di non intervenire)
- **non sul sistema AI.**



Principio chiave (DLgs. 231/01)

La tecnologia è uno **strumento di supporto**, non sostituisce la responsabilità decisionale.

La responsabilità resta in capo al management.

- 📌 L'AI può **attenuare** la responsabilità solo se SI DIMOSTRA che è stata:
 - ✓ correttamente progettata
 - ✓ correttamente utilizzata
 - ✓ correttamente supervisionata



PRINCIPI GENERALI DI RESPONSABILITA' DEL MANAGEMENT

RIASSUMENDO

Il management è responsabile di:

Scelta del sistema

(adeguatezza tecnica, affidabilità, coerenza con i rischi aziendali)

Governance e configurazione

- definizione soglie di allarme
- regole di utilizzo
- ruoli e responsabilità operative

Decisioni conseguenti agli alert

- intervento
- rinvio
- accettazione del rischio



Il sistema AI non assorbe né trasferisce la responsabilità.



PRINCIPI GENERALI DI RESPONSABILITA' DEL MANAGEMENT

RIASSUMENDO

Il MOG 231 per mantenere il valore esimente in caso di reato commesso da una figura apicale dell' Ente

Il management deve dimostrare che:

Nel sistema di gestione è presente un **Modello Organizzativo e Gestionale 231 aggiornato, ed esistono debitamente archiviate:**

- **procedure**
- **controlli**
- **formazione**
- **Audit**

l'OdV è presente , informato e coinvolto.

In questo caso:

👉 possibile **effetto esimente o attenuante** della responsabilità dell'Ente in caso di procedimento processuale a carico.

SECTION IA IN AZIENDA

04



LEGGE N°132 /2025

25-9-2025

GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA

Serie generale - n. 223

LEGGI ED ALTRI ATTI NORMATIVI

LEGGE 23 settembre 2025, n. 132.

Disposizioni e deleghe al Governo in materia di intelligenza artificiale.

La Camera dei deputati ed il Senato della Repubblica hanno approvato;

IL PRESIDENTE DELLA REPUBBLICA

PROMULGA

principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità.

2. Lo sviluppo di sistemi e di modelli di intelligenza artificiale per finalità generali avviene su dati e tramite processi di cui devono essere garantite e vigilate la correttezza, l'attendibilità, la sicurezza, la qualità, l'appropriatezza e la trasparenza, secondo il principio di proporzionalità in relazione ai settori nei quali sono utilizzati.

Nella giornata del 25 settembre 2025, è stata pubblicata in Gazzetta Ufficiale la [Legge 23 settembre 2025 n. 132](#), con

“Disposizioni e deleghe al Governo in materia di Intelligenza Artificiale”, che è entrata in vigore il 10 ottobre.

La norma assegna delega al Governo affinché dia
“precisazione dei criteri di imputazione della responsabilità penale delle persone fisiche e amministrativa degli enti per gli illeciti inerenti a sistemi di Intelligenza Artificiale, che tenga conto del livello effettivo di controllo dei sistemi predetti da parte dell’agente”.

La Legge apporta modifiche ad alcune fattispecie che rientrano di una specifica aggravante per il caso in cui siano commessi mediante l’impiego di sistemi di Intelligenza Artificiale.

Ing. Relatore

seminario 31 marzo 2026

Data



Legge 132/2025

La nuova legge rappresenta un momento fondamentale nella regolazione nazionale dell'intelligenza artificiale, **colmando le lacune dell'AI Act europeo**:

Introduce norme su AI e salute, tutela dei minori, coordinamento istituzionale e reati informatici.

Il secondo comma dell'articolo 14 introduce il principio più importante e garantista dell'intero impianto normativo per la PA:

il principio di non sostituzione.

La legge stabilisce che:

“L'utilizzo dell'intelligenza artificiale avviene in funzione strumentale e di supporto all'attività provvedimentale, nel rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale.”

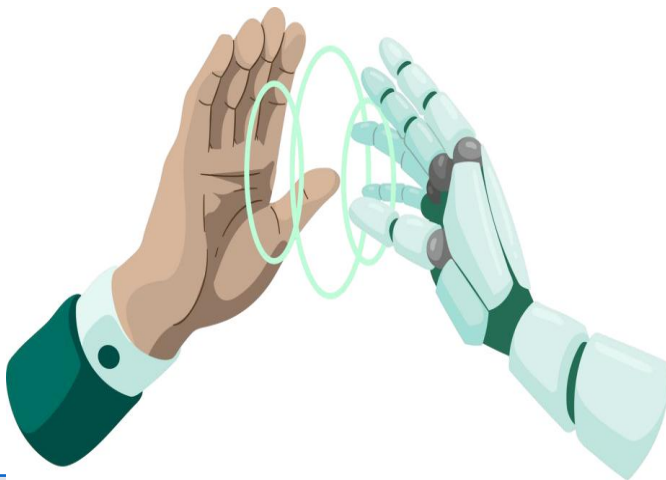


L'IA in azienda

Quando l'azienda (*deployer*) decide di introdurre uno o più sistemi di IA, deve sapere che ne deve fare

utilizzo corretto, trasparente
e responsabile (art. 1 L.132/2025)

1. avere consapevolezza dell'importanza dei dati
2. applicare tecniche appropriate di *data governance*
3. conoscere e valutare i rischi



Violazione di principi etici
Atti illeciti
Reati

Vediamo qui di seguito alcuni esempi di
RISCHI/REATI presupposto indotti dalla IA





L'IA in azienda

I dati in entrata

IA addestrata su dati distorti, crea risultati distorti

Per il momento, qualsiasi sistema di IA si basa su quello che «vede», dai dati di input. Qualora i dati di input siano viziati o non aggiornati (ovvero soggetti a bias - distorsioni) il processo di elaborazione può essere condizionato da questa “*falla*” *ab origine* del sistema.

Bias di esclusione:

un addestramento eseguito dalla Direzione Commerciale / Marketing, basato su dati storici, che non tiene conto dei cambiamenti del mercato o delle preferenze dei consumatori

rischio per l'ente: previsioni errate sulle vendite e conseguente danno economico

Bias cognitivo:

un addestramento su un gruppo demografico ristretto per la selezione di CV, pur in assenza di pregiudizi, può portare a escludere alcune categorie di candidati, negando opportunità a determinati gruppi di persone

rischio per l'ente : danno reputazionale / violazione di principi etici



L'IA in azienda

L'attenzione ai dati in entrata non riguarda solo dati eventualmente viziati o errati: anche in casi di inserimento di dati corretti si potrebbe configurare un rischio per l'azienda.

Esempio:

l'addestramento di una IA con informazioni esatte, ma tutelate dalla legge sul diritto d'autore (a prescindere dal fatto che l'output sia identico e/o simile a lavori precedentemente esistenti di un artista, da cui il sistema di IA ha attinto per la creazione di un nuovo risultato)



L'IA in azienda: cosa monitorare altro esempio

Facciamo il caso di dipendenti che inseriscono dati personali e/o informazioni riservate su un sistema IA che però li condivide in rete

Rischi per l'ente : violazione della normativa privacy, divulgazione di informazioni riservate e/o segreti

Per questo è importante :

1. integrare algoritmi di investigazione, utili per individuare anomalie all'interno dei dati raccolti;
2. capire se, dove o con chi l'IA eventualmente condivide i dati;
3. adottare ulteriori misure tecniche e organizzative per prevenire la perdita dei dati personali e delle informazioni aziendali;



L'IA in azienda: cosa monitorare esempio ambito manifattura

I sistemi di IA possono produrre risposte non consone, anche se basati su dati rappresentativi e/o su di un addestramento efficace.

È per questo necessario adottare misure preventive nell'uso degli output, **introducendo come prassi la verifica dei risultati ottenuti.**

ESEMPIO

Azienda leader nel settore del fashion introduce piattaforma di IA per l'aiuto nello sviluppo di nuove collezioni

L'azienda utilizza la piattaforma di IA, crea una nuova collezione e la presenta al pubblico.



Immediatamente dopo la presentazione, riceve una diffida in quanto un abito indossato da una modella interferisce con la creazione di un altro designer

rischio per l'ente: interferenza con un diritto di proprietà intellettuale / danno reputazionale



L'IA in azienda: rischi da monitorare

Il rischio «sistemico»

Un errore o una condotta illecita di un uomo tendono a restare isolati, ma se il sistema di IA è mal addestrato o manipolato, l'errore che produce può propagarsi automaticamente in altri processi, sistemi, documenti o decisioni dell'azienda.

ESEMPIO un errore negli automatismi contabili può riflettersi su migliaia di registrazioni.

Rischi per l'ente

- ❖ reati societari di cui all'art. 25 *ter* D.Lgs. 231/2001 – per es: falso in bilancio, false comunicazioni sociali
- ❖ frodi informatiche per applicazione di operazioni illecite da parte dell'algoritmo

Il rischio «opaco»

Se un dipendente sbaglia, è probabile che si possa ricostruire il processo che ha portato a tale errore (con documenti, email, testimonianze).

Con i sistemi di IA complessi (es. deep learning) la logica è spesso una “*black box*”, cioè non è chiaro perché una decisione sia stata presa.

➡ Problemi di responsabilità in un eventuale procedimento penale

ESEMPIO : Sistema di IA che rifiuta un cliente ritenuto rischioso, o un candidato senza spiegarne il motivo.

Rischio per l'ente: impossibilità di spiegare il processo decisionale, mancanza di trasparenza. Ricorsi legali



L'IA in azienda: rischi da monitorare

Possibili reati presupposto ex 231/01

Qualche **esempio** di reati presupposto ex D.Lgs. 231/2001 che possono essere commessi tramite l'uso dell'IA

Reati in violazione delle norme sulla salute e sicurezza dei lavoratori

La presenza dell'IA nelle attrezzature, se non opportunamente governata, ne può determinare il malfunzionamento (o il funzionamento diverso) rispetto alle previsioni originarie, mettendo a rischio la sicurezza delle persone e la qualità e sicurezza dei prodotti oggetto di lavorazione.

Reati Ambientali

L'IA può essere utilizzata per eludere controlli e comunicare dati ambientali falsi, ad esempio, attraverso la manipolazione di dati relativi alle emissioni

Frode informatica / delitti informatici

L'IA può essere utilizzata per attacchi di phishing, per manipolare i dati, per accedere abusivamente a sistemi informatici (art. 24-bis DLGS 231/01)

SECTION

ED INFINE :

- ❖ NUOVE FUNZIONI
- ❖ NUOVE RESPONSABILITA'

04



Che succede se il MOGC è stato redatto e aggiornato da una AI generativa o agentic AI ?

Per esempio cerchiamo di comprendere le conseguenze dell'utilizzo di software *AI* nel settore della *compliance* aziendale, quindi la disciplina in tema di "colpa d'organizzazione" dell'ente.

?

Come si configura la responsabilità da colpa di organizzazione dell'ente che abbia affidato la **gestione/revisione/aggiornamento** del proprio modello organizzativo e di gestione ad un *software AI*,

!

Indispensabile una dedicata **Risk Analysis** che prevede,

- ❖ definizione puntuale dei ruoli e responsabilità, dei processi,
- ❖ delle regole e dei divieti per l'adozione,
- ❖ l'utilizzo e l'acquisto di AI,
- ❖ un'attività di revisione ed eventuale aggiornamento degli stessi (es., Fastweb prevede una review e aggiornamento ogni 6 mesi).

AI Governance

Per la mitigazione dei rischi, è fondamentale che l'organigramma preveda un'adeguata AI Governance basata su più pilastri:

- **Policy e Procedure**

Implementare e continuamente aggiornare Linee guida, Policy e Procedure per garantirne compliance normativa ed etica.

- **Ruoli e responsabilità**

Definizione di ruoli e responsabilità, creando inoltre nuove posizioni per la gestione dei modelli di AI e lo sviluppo di competenze specifiche per l'AI.

- **Processi e controlli**

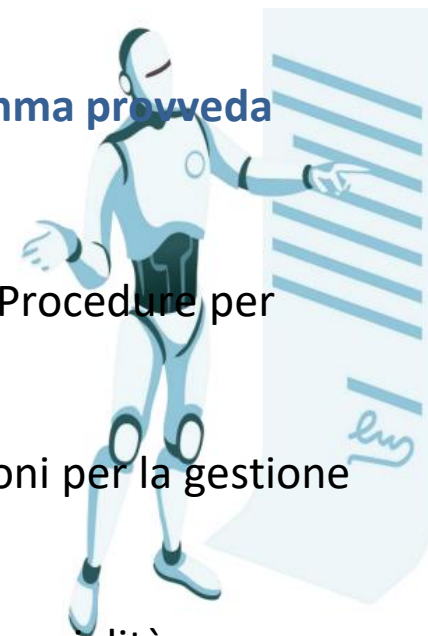
Predisporre processi e controlli volti a garantire l'affidabilità, l'imparzialità e l'accuratezza dei modelli di AI, ad esempio per la valutazione e approvazione degli «use case» con definizione di metodologie etiche per sviluppo, test e procurement.

- **Monitoring**

È necessario un monitoraggio costante dei processi di controllo interno, dei modelli di AI, dei rischi e degli «incidenti», per garantirne la conformità alle normative e agli standard etici. Inoltre, è fondamentale testare la qualità dei dati.

- **Comunicazione e formazione**

Una comunicazione chiara e una formazione mirata per assicurarsi che i dipendenti comprendano il ruolo dell'AI nell'organizzazione e come questa influenzi il loro lavoro.



Esempio di possibile applicazione pratica

Definizione ruoli e responsabilità



**E l'ODV 231
dove si
colloca in
questo
contesto ?**

Funzione legale § compliance

- Analisi normativa vigente in materia AI
- Valutazione del sistema AI sul codice Etico
- Implementazione AI coerente rispetto le policy aziendali

Funzione IT :

- Test e verifiche tecniche sui sistemi AI
- Identificazione dei rischi di sicurezza informatica legati a AI

H.R.

- Formazione all'uso di AI

Funzione Approvvigionamenti

- Acquisto di nuovi modelli AI in linea con le esigenze aziendali

Comitato di Governance di AI

- Valutazione MULTIDISCIPLINARE di rischi ed opportunità delle iniziative AI
- Gestione errori e reclami
- Supervisione aggiornamento «policy e procedure»

Alfabetizzazione : Cosa prevede l' AI Act art. 4

L'articolo 4 dell'AI Act introduce **un obbligo specifico di garantire un adeguato livello di alfabetizzazione all'AI per il personale coinvolto nell'utilizzo dei sistemi di AI**.

Il regolamento impone infatti che fornitori e utilizzatori (deployer) di AI adottino misure per garantire che il personale rilevante, ossia che usa l'IA, abbia un "livello sufficiente di alfabetizzazione all'IA", tenendo conto del contesto e delle persone potenzialmente interessate dal sistema di AI in uso.

Nel regolamento dell'UE, la **nozione di "alfabetizzazione all'IA" è definita come il possesso delle competenze, conoscenze e comprensione adeguate per procedere ad una diffusione informata dei sistemi di AI** ed essere consapevoli delle opportunità e dei rischi associati all'AI.

La principale incognita è definire cosa si intende per un "livello sufficiente" di alfabetizzazione, previsto dal Regolamento.

Fornire una formazione adeguata è obbligo e responsabilità del datore di lavoro o HR per delega

Obblighi applicabili
dal 2 agosto 2025.





DA RITENERE SEMPRE IN MENTE

Presidi richiesti e ruolo del MANAGEMENT

Per ridurre il rischio e rafforzare la funzione esimente del MOG 231

- ✓ **Human-in-the-loop**
decisione finale sempre umana
- ✓ **Procedure formalizzate**
gestione alert
escalation
tracciabilità delle decisioni
- ✓ **Aggiornamento del Modello 231**
integrazione dei sistemi predittivi
informativa all'OdV
- ✓ **Formazione e audit periodici**



Relatore

Ing ROBERTO FRANCINI

Presidente Commissione 231 e Modelli Organizzativi



3332214541

PRINCIPI GENERALI DI RESPONSABILITA' DEL MANAGEMENT: esempio

CONSIGLIO DI AMMINISTRAZIONE / DATORE DI LAVORO

Responsabilità di indirizzo e delega (art. 2087 c.c. ; D.Lgs. 81/2008 , art 18)



DIRIGENTI / MANAGER TECNICI
(Ingegneri – Operations – Plant Manager ,etc.)



RESPONSABILE HSE

- Valutazione dei rischi e prevenzione incidenti
- Applicazione normativa
- Sicurezza e ambiente
- Formazione e informazione
- Segnalazione pericoli e fermo produzione se nec.



RESPONSABILE PRODUZIONE

- Produzione
- Sicurezza e integrità degli impianti
- Procedure operative sicure
- Controllo delle condizioni di lavoro
- Segnalazione anomalie e stop produzione
- Supervisione personale operat.



RESPONSABILE MANUTENZIONE

- Manutenzione impianti e continuità esercizio
- Gestione guasti critici
- Prevenzione incidenti tecnici
- Verifica idoneità macchinari