


**CORSO DI FORMAZIONE SULLA
SICUREZZA ANTICRIMINE**

Modulo giuridico-normativo
e modulo formativo sulla prevenzione
dei rischi di origine criminosa

Docente: <nome>


1

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata




Il docente dovrà presentarsi e descrivere brevemente le proprie esperienze professionali. Successivamente, chiederà ai partecipanti di fare altrettanto, dichiarando, in particolare, le loro **aspettative in merito alla frequentazione dell'incontro formativo**. La conoscenza dei discenti è importante per organizzare al meglio l'attività didattica e affrontare tematiche che possano risultare di interesse per i partecipanti o che rispondano a loro eventuali dubbi o esigenze specifiche; può essere utile chiedere se abbiano già seguito altri corsi di contenuto simile e quanto tempo prima: il feedback ricevuto permetterà di orientare il percorso formativo nella direzione più proficua e costruttiva per l'aula.

ATTENZIONE: nella personalizzazione delle slide, il titolo (o sottotitolo) del corso potrà essere modificato per meglio aderire alle esigenze dei fruitori o per concentrarsi su specifici rischi di origine criminosa (ad esempio: “Corso di formazione sulla sicurezza anticrimine nelle imprese del commercio - L'attività antitaccheggio” o “Corso di formazione sulla sicurezza anticrimine in ambito bancario - La gestione del contante” o ancora “Corso di formazione sulla sicurezza anticrimine nella Grande Distribuzione Organizzata - La vigilanza antirapina”. Questo consentirà, da subito, di rendere espliciti gli obiettivi e il programma del corso. È fondamentale che i discenti si riconoscano nelle tematiche che verranno affrontate durante l'incontro formativo, per stimolare la loro partecipazione e tenere alto il livello di interesse.




Schema generale del corso



1. Il contesto giuridico-normativo

Il D.Lgs. 81/2008 e le altre fonti legislative




2. La formazione sulla sicurezza anticrimine

Sicurezza e Prevenzione

I rischi di origine criminosa

Le soluzioni difensive: strumenti e comportamenti

Il Security Coaching e la cultura della sicurezza aziendale

2Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata

Questa slide sintetizza il programma del corso e va personalizzata secondo gli obiettivi formativi che si intendono perseguire. Dato che l'apprendimento richiede la partecipazione attiva dei discenti, un aspetto di fondamentale importanza per costruire una proficua relazione docente-allievi è la definizione del c.d. **“contratto formativo d’aula”**, inteso come un processo libero e condiviso di negoziazione sugli impegni che si è disposti ad assumersi per l'accrescimento delle proprie conoscenze in materia di sicurezza. Il contratto d’aula:

- chiarisce le esigenze formative dell’aula e permette di progettare e gestire la lezione in modo interattivo, affrontando temi di reale interesse dei partecipanti;
- sviluppa la motivazione, la curiosità e il coinvolgimento attivo, in quanto chiede ai partecipanti la loro convinta adesione alla proposta formativa, dopo aver valutato e concordato gli obiettivi, il percorso e la metodologia da seguire;
- sviluppa le capacità cooperative dei discenti, con i quali si condivide la proposta educativa, strutturandola in maniera chiara sulla base di ciò che è utile per la loro formazione e può contribuire a migliorarli sotto il profilo personale e professionale;
- promuove una mentalità consapevole e responsabile nell'affrontare le problematiche che attengono alla sicurezza sui luoghi di lavoro (secondo un approccio di Security Coaching);
- consente di gestire in maniera democratica le principali dinamiche di gruppo e di predisporre l’aula all’ascolto partecipativo.



Definizioni

Cosa si intende per sicurezza?

SICUREZZA


Condizione - reale o percepita - di tranquillità,
di assenza di pericoli o rischi, di protezione da avversità

o

che permette di prevenire, eliminare o rendere meno gravi
evenienze spiacevoli e imprevisti

3

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



L'incontro formativo si apre presentando adeguatamente il **concetto di sicurezza**.

La **SICUREZZA** ha acquisito rilievo crescente nel contesto quotidiano, a fronte di fenomeni di varia natura che hanno provocato rapidi mutamenti e sollevato rilevanti problematiche, mettendo, talvolta, in discussione la stabilità e gli equilibri della coesione sociale.

Espressione di una condizione - reale o percepita - di tranquillità, assenza di pericoli e protezione da avversità o imprevisti, il termine italiano "sicurezza" riassume in sé i concetti assimilabili della tradizione anglosassone di "**SAFETY**", intesa come tutela da minacce di origine naturale, accidentale, igienico-sanitaria o derivanti da errori umani, e di "**SECURITY**", orientata invece alla prevenzione dei rischi criminosi. In qualunque contesto occupazionale organizzato, indipendentemente dalla dimensione e dalla tipologia di attività, la sfera di competenza e la fisionomia di queste due discipline appaiono sempre più sfumati e complementari nell'ambito del sistema prevenzionistico aziendale. Il perimetro della sicurezza non ha contorni netti ed esprime una realtà più sfaccettata e fluida, che ricomprende molteplici variabili (non soltanto tecniche ma anche e soprattutto umane) e fattori di rischio che possono ledere beni e, soprattutto, la salute delle persone.

Appare, comunque, indubbio che l'evoluzione del concetto stesso di sicurezza rende i confini tra le varie discipline sempre meno netti: il più delle volte le esigenze dell'una vanno a interfacciarsi con quelle dell'altra, e viceversa. Si fa strada l'idea di "sicurezza integrata". È quella che si definisce la "**VISIONE OLISTICA DELLA SICUREZZA**": con il contributo di tutti, nell'interesse di tutti,

in un'ottica di qualità e miglioramento continuo orientato all'eccellenza, di creazione e protezione del valore aziendale.



Definizioni

Qualche definizione, prima di iniziare

IL MACROSISTEMA TRADIZIONALE DELLA SICUREZZA AZIENDALE

Sicurezza anticrimine

(Physical Security & Intelligence Analysis)

Sicurezza antinfortunistica

(Safety)

Sicurezza logica o informatica


(IT & Network Security)

4

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



Il tema della **sicurezza** è certamente uno dei più dibattuti degli ultimi anni ed è caratterizzato da una straordinaria varietà e molteplicità di aspetti e fattori, che si prestano a interpretazioni e utilizzi altrettanto numerosi, eterogenei e variegati. L'aspirazione a vivere liberi dalla paura ha progressivamente ampliato la nozione di sicurezza, nella quale rientrano ormai una pluralità di eventi - soprattutto di natura preventiva - in grado di incidere sulla tranquillità sociale, sulla pacifica convivenza e sulla qualità globale di vita. Emerge una definizione del concetto di sicurezza complessa e ampia. Per tale motivo, prima di affrontare nel dettaglio gli argomenti del corso, il docente illustrerà brevemente le funzioni proprie della **SICUREZZA ANTICRIMINE** (Sicurezza Fisica o Security) e quelle invece rientranti nella sfera di competenza della **SICUREZZA ANTINFORTUNISTICA** (Safety) e della **SICUREZZA INFORMATICA** (Sicurezza Logica o ICT Security). Questa premessa terminologica consentirà di delineare e circoscrivere le *core competence* delle tre discipline e di individuarne i punti di contatto e di correlazione che verranno meglio illustrati nel prosieguo del corso. Dovrà, inoltre, risultare evidente come questi tre approcci consentano di elaborare strategie che, pur nella diversità dei contenuti, devono interfacciarsi e collimare verso un unico obiettivo di sicurezza aziendale. La sicurezza - non dimentichiamolo - è un processo, un percorso in continua evoluzione, non un prodotto o un punto di arrivo e richiede il contributo congiunto di più attori e un approccio multidisciplinare. **Physical Security, Safety e Information & Network Security, integrandosi fra loro, vanno a costruire il MACROSISTEMA TRADIZIONALE DELLA SICUREZZA AZIENDALE.**



Definizioni


Sicurezza anticrimine

(Physical Security & Intelligence Analysis)

La **Security** è l'attività volta a prevenire, fronteggiare e superare gli eventi derivanti da azioni prevalentemente illecite
(condotte antigiuridiche + violazione procedure organizzative)
che espongono le persone e i beni (materiali e immateriali) a potenziali
effetti lesivi e/o dannosi

5

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



Si introduce il concetto di Security riportando l'autorevole definizione contenuta nella **Norma UNI 10459:2017**, che definisce i requisiti del professionista incaricato del processo di security, ossia la persona le cui competenze, conoscenze e abilità assicurano e garantiscono la gestione complessiva del processo stesso.

La Norma UNI 10459:2017 sottolinea che, indipendentemente dall'ambito di attività e dalle dimensioni, ogni organizzazione è costantemente esposta a minacce di natura dolosa, colposa o accidentale; ciò in relazione ai processi produttivi, alle azioni dei dipendenti, ai rapporti con l'esterno e all'appartenenza a un sistema globalizzato sempre più incerto e conflittuale. Le organizzazioni devono porsi l'obiettivo di tutelare le risorse patrimoniali (tangibili e intangibili) e, soprattutto, le **persone**: ciò costituirà la base dei processi di **creazione e protezione del valore**, assicurando il mantenimento della capacità reddituale nel tempo e di profittabilità del business. Questa finalità si realizza anche attraverso il ricorso a tecniche di gestione di eccellenza, per il contributo che possono fornire sia alla riduzione dei costi, sia alla qualità di prodotti e servizi forniti agli stakeholders (ossia, i portatori di interesse a vario titolo nella vita dell'organizzazione).

Il docente richiamerà l'attenzione sulle definizioni di:

- **RISK ASSESSMENT**: processo complessivo di IDENTIFICAZIONE, ANALISI E PONDERAZIONE dei rischi e delle minacce.
- **VULNERABILITY ASSESSMENT**: valutazione dell'impatto su persone e beni al verificarsi di un determinato scenario di minaccia.



Definizioni

Sicurezza antinfortunistica

(Safety)

La **Safety** riguarda la salvaguardia dell'igiene, della salute e dell'incolumità psico-fisica delle persone, prevenendo gli infortuni e garantendo un livello di "sicurezza socialmente accettabile"


6

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



Mentre il Professionista della Security (o Security Manager) deve prevenire e fronteggiare eventi negativi di natura dolosa o colposa intenzionalmente diretti a danneggiare le risorse aziendali, il professionista della sicurezza antinfortunistica (o **Safety Manager**) deve confrontarsi con eventi dannosi di origine accidentale o casuale, che incidono direttamente sull'incolumità, sulla salute o sullo stato fisico, psicologico e morale delle persone. Appare chiaro che l'evoluzione del concetto stesso di sicurezza rende i confini tra Security e Safety sempre meno netti: il più delle volte, le esigenze dell'una vanno a interfacciarsi con quelle dell'altra. Si fa strada l'idea di "sicurezza integrata". Si citi come esempio la sentenza 22 marzo 2002, n. 4129 della Corte di Cassazione Civile: l'obbligo dell'imprenditore di tutelare l'integrità psicofisica dei dipendenti impone l'adozione e il mantenimento non solo di misure di tipo igienico-sanitario o antinfortunistico, ma anche di misure atte, secondo le comuni tecniche di sicurezza, a preservare i lavoratori dalla lesione di detta integrità nell'ambiente o in costanza di lavoro in relazione ad attività pur se allo stesso non collegate direttamente come le aggressioni conseguenti all'attività criminosa di terzi, giustificandosi l'interpretazione estensiva della predetta norma alla stregua sia del rilievo costituzionale del diritto alla salute (art. 32 Cost.) sia dei principi di correttezza e buona fede (artt. 1175 e 1375 C.C.) cui deve ispirarsi anche lo svolgimento del rapporto di lavoro (cfr. Cass. 20 aprile 1998 n. 4012).

Security e Safety devono, comunque, mantenere competenze complementari ma differenziate, in quanto si trovano ad affrontare situazioni diverse, che vanno gestite con diversi strumenti e metodologie.



Definizioni

Sicurezza logica o informatica

(IT & Network Security)

Il termine **Information & Network Security** fa riferimento


alla sicurezza e alla salvaguardia

dei dati, delle reti e delle informazioni

trattati mediante strumenti informatici

7

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



Il professionista dei processi di **Sicurezza Informatica** dovrà essere valorizzato per le sue conoscenze di natura tecnica e informatica. L'**ICT Security Manager** ha il compito di garantire la sicurezza dei sistemi informatici in modo da non subire attacchi da esterni, occupandosi anche della relativa protezione delle informazioni e dei dati. Sono aspetti delicati che toccano in molti casi i delicati aspetti della privacy.

Al professionista della Sicurezza Anticrimine è richiesta la generica comprensione delle diversificate problematiche tecniche che attengono a tale settore, al fine di poter tempestivamente individuare eventuali pericoli provenienti dal fronte tecnologico-informatico e concordare mirati interventi di difesa, nell'ottica di una politica di sicurezza aziendale globale e integrata.

Questa slide, nel delineare le funzioni dell'ICT Security Manager, permette di evidenziarne i punti di contatto sia con il Physical Security Manager che con la nuova figura professionale del Privacy Officer, garante della riservatezza e della protezione dei dati personali. L'interazione fra Security e Privacy verrà ripresa più avanti nel corso.

La **Norma UNI 11506:2017**, relativa alle "Attività professionali non regolamentate - Figure professionali operanti nel settore ICT - Definizione dei requisiti di conoscenza, abilità e competenze", definisce i criteri generali delle figure professionali riconosciute e operanti nel settore ICT (indipendentemente dalle modalità lavorative e dalla tipologia del rapporto di lavoro) e stabilisce i requisiti fondamentali e i criteri specifici di conoscenze, abilità e competenze che le contraddistinguono. La Norma offre la possibilità di parlare un linguaggio comune quando si parla di professionisti dell'ICT, che possono così aggiungere

valore alla propria carriera professionale.



Definizioni

Gli ambiti della sicurezza

Security

Safety & HSE Management

IT & Cyber Security

Privacy

Intelligence

8

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



Le attività del Professionista della **SECURITY** possono intrecciarsi con quelle di professionisti specializzati in altri ambiti relativi alla sicurezza (sicurezza delle informazioni, protezione dei dati personali, salute e sicurezza sul lavoro, antifrode, tutela di marchi e brevetti, continuità operativa o gestione delle crisi), operando di concerto per la tutela dalle minacce di natura DOLOSA, COLPOSA o ACCIDENTALE cui un'organizzazione è esposta e che possono incidere sfavorevolmente su un'efficace gestione delle variabili competitive tradizionali e sulla conservazione del patrimonio tangibile e intangibile.

Mentre il professionista della SECURITY deve prevenire e fronteggiare eventi negativi di natura dolosa o colposa intenzionalmente diretti a danneggiare le risorse aziendali, il professionista della **SAFETY** deve confrontarsi con eventi dannosi di origine accidentale, igienico-sanitario, naturale-casuale o derivanti da errori umani. Per quanto la sicurezza anticrimine non vada nettamente disgiunta da quella antinfortunistica, i due responsabili della sicurezza devono mantenere competenze complementari ma differenziate.

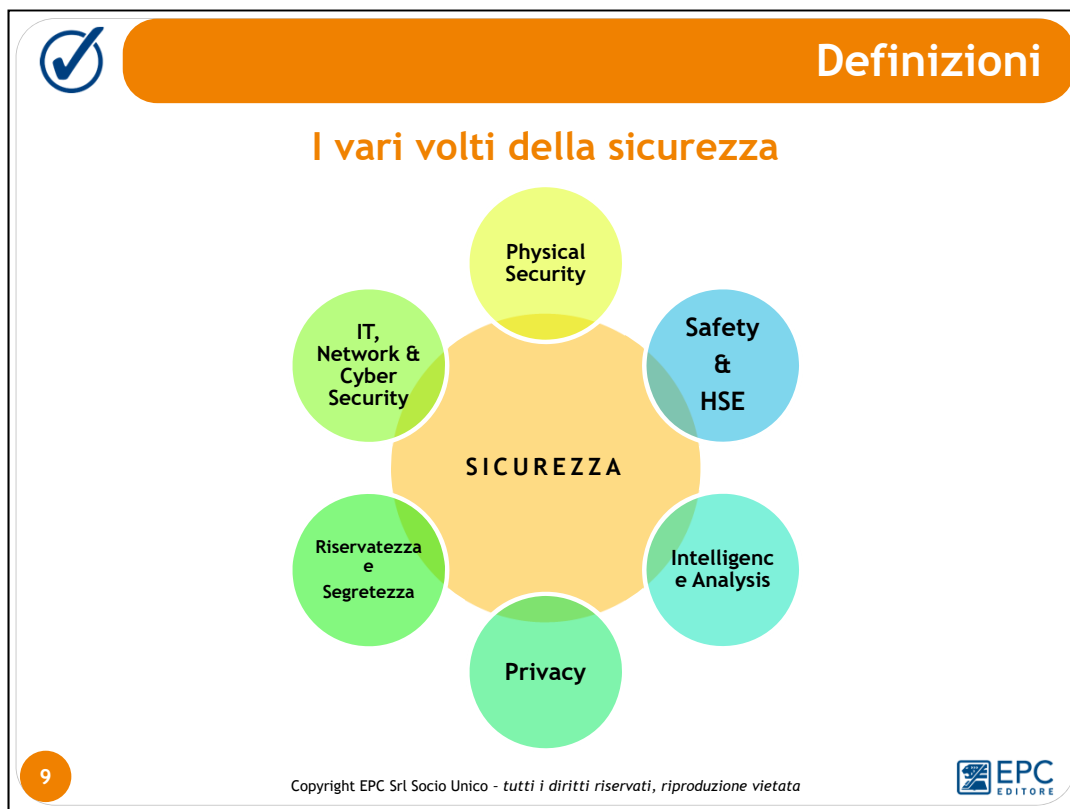
Il **Manager HSE** (HEALTH, SAFETY & ENVIRONMENT) supporta l'organizzazione nel conseguire gli obiettivi in ambito HSE sulla base delle proprie specifiche conoscenze, abilità e competenze, coerentemente con le normative vigenti.

Il professionista dei processi di **SICUREZZA LOGICA** (la c.d. Information & Communication Technology Security, normata dalla serie UNI 11621-1/4:2017) dovrà essere valorizzato per le sue conoscenze di natura tecnica e informatica. Al professionista della Security potrà essere richiesta la generica comprensione delle problematiche tecniche che attengono a tale settore, al fine di individuare tempestivamente eventuali pericoli provenienti dal fronte

tecnologico-informatico e concordare mirati interventi di difesa, nell'ottica di una politica di sicurezza aziendale globale e integrata.

La **PRIVACY** può essere compromessa a causa di un errore nella sicurezza. La privacy si riferisce all'utilizzo improprio delle informazioni da parte di utenti non autorizzati: l'obiettivo non è tanto la protezione del dato in sé quanto della persona fisica, che dal trattamento di quel dato potrebbe subire danno o pregiudizio ai suoi diritti e alle sue libertà fondamentali.

L'attività di **INTELLIGENCE** consiste nella raccolta e la successiva analisi di notizie e dati dalla cui elaborazione vengono ricavate informazioni utili al processo decisionale e alla prevenzione di attività destabilizzanti di qualsiasi natura. In senso più ampio si intendono tutte le attività legate allo spionaggio e al controspionaggio.




La sicurezza è una sfida che si basa sul gioco di squadra e non sulla competizione, che richiede comunione di intenti e travaso virtuoso di competenze e professionalità. In ogni moderna organizzazione, azienda o impresa, non necessariamente complessa, è inevitabile e indispensabile l’apporto professionale congiunto e coerente di tutti gli **“ESPERTI COMPETENTI”** che a vario titolo concorrono alla costruzione di un efficace sistema di sicurezza di qualità: RSPP, Security Manager, IT Security Manager, Data Protection Officer e, nelle realtà più complesse, Uffici Legali e Auditor 231/01 e di compliance concorrono a costruire ambienti di lavoro sempre più sicuri. Figure complementari e solidali ma non assimilabili, in quanto ciascuna di esse è portatrice di esperienze, conoscenze e competenze uniche e specifiche delle proprie aree di intervento sebbene accomunate da un medesimo obiettivo: rendere più sicuri i luoghi di lavoro attraverso processi di risk assessment e soluzioni operative basati su un’identica metodologia prevenzionale nella gestione e mitigazione delle minacce. Quando si parla di sicurezza, la convergenza di competenze e professionalità è anche un sistema di collaborazione strategica più efficace e meno costoso, visto che molto spesso viene richiesto di ridurre i costi della sicurezza mantenendo inalterata l’ampiezza del perimetro da proteggere.

Quanto maggiore risulterà l’esaustività dei rischi individuati, analizzati e mitigati secondo un **approccio di tipo “all hazard”**, tanto più semplice sarà per il Datore di Lavoro promuovere non una semplice cultura ma addirittura un’etica della prevenzione e della sicurezza aziendale, così come suggerisce nella tradizione anglosassone il concetto di **“duty of care”**. Un clima di benessere organizzativo e un ambiente lavorativo percepito come sicuro


stimoleranno il coinvolgimento proattivo dell'intera comunità aziendale, accrescendone il senso di appartenenza e favorendo il miglioramento delle prestazioni e del grado di soddisfazione dei lavoratori.

È indispensabile promuovere e progettare politiche e interventi di SICUREZZA INTEGRATA. La sicurezza necessita di un approccio integrato che permetta di correlare i problemi in una visione complessiva e governance tra tutti gli attori coinvolti: infatti, solo affrontando la complessità che il tema porta con sé è possibile individuare gli strumenti più idonei per rispondere a problemi che, per loro natura, hanno difficoltà a essere soddisfatti attraverso il ricorso a politiche e interventi settoriali e, quindi, inevitabilmente parziali.




Schema generale del corso

1. Il contesto giuridico-normativo



10

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



Ogni realtà imprenditoriale è esposta a rischi di security di varia natura e intensità, in grado di minacciare e rendere vulnerabili gli asset aziendali; ciò nonostante, a differenza del più noto e tradizionale settore della Safety, ampiamente normato, la Security ancora difetta di una specifica e precisa disciplina prevenzionistica integrata e sistematica: l'adozione di adeguate misure e standard di sicurezza anticrimine in ambito aziendale è pur tuttavia disciplinata da precise disposizioni normative che tutelano la salute e la sicurezza nei luoghi di lavoro.

In questa prima parte del corso, si richiameranno i principali riferimenti di legge che implicano l'adozione di specifiche e adeguate misure di protezione in grado di prevenire il verificarsi di eventi delittuosi e tutelare l'incolumità psicofisica dei lavoratori e dei soggetti terzi, muovendosi entro confini delimitati non soltanto dal buon senso ma anche da precisi obblighi di carattere giuridico. Verranno parimenti illustrate le norme che giustificano l'esigenza di erogare ai lavoratori una specifica formazione in materia di prevenzione e protezione dagli eventi di origine criminosa, a tutela della sicurezza, della salute e del benessere dei lavoratori stessi. In altri termini, si faranno emergere le connessioni - non sempre evidenti - tra la Security e i doveri in capo all'imprenditore di approntare idonee ed efficienti difese nei confronti dei rischi di natura delittuosa (rapine, truffe, frodi, furti, aggressioni, e simili fattispecie di origine antropica).



Il contesto giuridico-normativo

Il contesto legislativo di riferimento: le **NORME PREVENZIONISTICHE**

- Decreto Legislativo 9 aprile 2008, n. 81
- Codice Civile
- Costituzione della Repubblica Italiana
- Legge 20 maggio 1970, n. 300
- Decreto Legislativo 8 giugno 2001, n. 231
- Codice Penale

11

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



Di solito, la parte della normativa è quella considerata più noiosa: senza dilungarsi troppo, occorre trasmettere i concetti fondamentali che aiutano a inquadrare correttamente i contenuti della seconda parte di questo modulo formativo.

Nelle due slide che seguono, vengono riassunti i principali riferimenti normativi che impattano sulle tematiche della Security. Essi rappresentano un indispensabile strumento di supporto operativo nella predisposizione delle politiche di prevenzione e riduzione dei rischi e di contenimento dei danni a cose e persone.

Nella prima slide, vengono citate le **norme di carattere prevenzionistico**: in quanto norme di diritto pubblico, non possono essere derogate da determinazioni pattizie. Esse comprendono, innanzitutto, il testo unico in materia di salute e sicurezza del lavoro, la Carta Costituzionale, lo Statuto dei Lavoratori, il decreto che disciplina la responsabilità degli enti per gli illeciti amministrativi dipendenti da reati, la norma polivalente del Codice Civile che definisce le misure antinfortunistiche a tutela dell'integrità fisica del lavoratore e le disposizioni di legge sulla responsabilità penale personale.

Ciò che conta, non è l'approfondimento o il commento puntuale delle normative citate, ma la chiara evidenza di precisi obblighi di legge nel predisporre idonee misure di sicurezza anticrimine nei luoghi di lavoro.



Il contesto giuridico-normativo

Il contesto legislativo di riferimento:
le **NORME di SETTORE**

- Contratti Collettivi Nazionali di Lavoro
- TULPS e Decreti integrativi del Ministero dell'Interno
- Normativa ADR sulla sicurezza dei trasporti di merci pericolose
- Codice ISPS per la sicurezza marittima
- Programma Nazionale per la Sicurezza dell'Aviazione
- Infrastrutture Critiche

12

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



In questa seconda slide, vengono invece richiamate alcune norme di settore che hanno stretta attinenza con le problematiche di Security. Si tratta di esempi concreti e specifici di applicazione dei principi di Security ai processi di valutazione dei rischi di natura criminosa che possono manifestarsi con maggiore frequenza in alcune professioni (Guardie Particolari Giurate, cassieri di banche e supermercati, incaricati di maneggio valori, addetti ai trasporti di merci pericolose, marittimi, operatori presso infrastrutture critiche, ...).

Il tempo da dedicare ai singoli punti indicati nella slide varierà in base al taglio più o meno di settore che si vorrà dare al corso di formazione e all'approfondimento richiesto dai suoi fruitori.



Il contesto giuridico-normativo

Il D.Lgs. 81/2008

- Analisi di TUTTI i rischi, compresi quelli di origine criminosa, sia esogeni che endogeni (art. 3, primo comma)
- Valutazione dei rischi per la salute del lavoratore (artt. 17, 28 e 29)
- Soluzioni difensive attive e passive (art. 28, c. 2 lett. B - art. 29, c. 3)
- Redazione di procedure di sicurezza semplici, comprensibili e complete alle quali i lavoratori devono attenersi (art. 20, c. 2 lett. b - art. 18, primo comma lett. f)
- Informazione, formazione e addestramento dei lavoratori (artt. 36 e 37)
- Controlli sull'osservanza delle procedure (art. 28, c. 2 lett. d - art. 30) e sanzioni per gli inadempienti

13

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata




Nelle diapositive che seguono, verranno innanzitutto presentati gli articoli del **DECRETO LEGISLATIVO 9 APRILE 2008, N. 81** che hanno attinenza con gli aspetti di sicurezza anticrimine trattati nel presente modulo formativo.

La natura e la tipologia dei rischi di origine criminosa si sono modificate nel tempo, ma è sempre applicabile una elementare regola di prudenza: benché sia impossibile eliminare del tutto le causali di rischio, è indispensabile attuare un livello minimo di sicurezza al di sotto del quale non è possibile scendere, pena l'annullamento degli effetti benefici di qualsivoglia attività di prevenzione e pianificazione dei rischi. **Il D.Lgs. 81/2008 rappresenta senza dubbio un'eccellente base sulla quale costruire un sistema integrato e complementare di prevenzione anticrimine aziendale, in quanto racchiude importanti capisaldi della tutela della sicurezza dei lavoratori, quali ad esempio:**

- la valutazione di TUTTI i possibili rischi cui sono esposti i lavoratori;
- la centralità delle misure di prevenzione per ridurre i rischi alla fonte;
- il coinvolgimento dei lavoratori nelle tematiche della prevenzione e della sicurezza, secondo il principio innovativo della "protezione soggettiva e proattiva" (non più semplici comandi e divieti, ma coinvolgimento responsabile e consapevole dei destinatari delle politiche di sicurezza).

Una buona policy di sicurezza anticrimine aziendale dovrebbe - quanto meno - comprendere e sviluppare adeguatamente tutti i punti citati nella slide.



Il contesto giuridico-normativo


Art. 3, primo comma, D.Lgs. 81/2008

Il Decreto si applica:

- a tutti i settori di attività (privati e pubblici)
- a tutte le tipologie di rischio

OBIETTIVO

Promuovere un sistema di prevenzione aziendale efficace, che tuteli la salute e la sicurezza nei luoghi di lavoro

14
Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata


La diapositiva illustra l'ambito di applicazione oggettivo della normativa di prevenzione antinfortunistica di riferimento nel panorama italiano e ne sintetizza la vera essenza: la tutela della salute e della sicurezza nei luoghi di lavoro riguarda tutti i settori di attività privati e pubblici (fatte salve alcune eccezioni per alcune realtà caratterizzate da particolari esigenze di servizio e peculiarità organizzative) e tutte le tipologie di rischio.

Il docente richiamerà qui brevemente la differenza tra **PERICOLO** (proprietà o qualità intrinseca di un determinato evento o fattore di causare potenzialmente danni o lesioni a cose e/o persone) e **RISCHIO** (probabilità che sia raggiunto un livello potenziale di danno), per poi sottolineare l'importanza dell'attività di **valutazione globale e dinamica dei rischi per la salute e la sicurezza** (**RISCHIO = PROBABILE GRAVITÀ DEL DANNO X PROBABILITÀ DEL SUO ACCADIMENTO**) nella predisposizione di efficaci politiche di **prevenzione**. Attraverso l'individuazione, l'analisi e la valutazione dei rischi si possono, infatti, determinare gli interventi necessari per:

- eliminare il pericolo alla fonte,
- modificare le circostanze e le cause che determinano le situazioni di pericolo ineliminabili, al fine di prevenire il potenziale di rischio,
- eliminare il danno o sua ridurne la gravità.

Si tratta di un passaggio fondamentale per affrontare nella giusta ottica questo modulo formativo e per coglierne la vera essenza: il concetto di prevenzione deve costituire il leitmotiv di ogni efficace politica di sicurezza anticrimine.



Oltre alle definizioni riportate nell'art. 2, primo comma, lettere r) e s) del D.Lgs. 81/2008, può essere utile ricordare che le nozioni di **RISCHIO** e **PERICOLO**, in quanto fondamentali nella pianificazione di efficaci ed efficienti processi di risk management globale, ricorrono frequentemente nella terminologia delle specifiche tecniche rilasciate dagli Organismi Internazionali di Normazione.

La **Norma UNI 11230 del 2007** ("Gestione del rischio - Vocabolario"), ad esempio, è frutto di un'attenta analisi metodologica e definisce la terminologia fondamentale pertinente alla gestione del rischio (inteso come l'insieme delle attività coordinate per dirigere e presidiare un'organizzazione con riguardo al rischio) e rappresenta un riferimento generale in materia; essa è applicabile a tutte le organizzazioni, a prescindere dalla loro dimensione e tipologia di business, in qualunque momento della loro vita organizzativa, consentendo di promuovere un approccio coerente e organico nella gestione del rischio, in modo che i decision maker aziendali possano disporre di informazioni e strumenti manageriali davvero utili per prendere decisioni corrette nell'attività gestionale.

Applicabile a qualunque tipo di rischio, la **Norma UNI ISO 31000 del 2018** ("Gestione del rischio - Linee guida") afferma che qualunque tipo di organizzazione deve affrontare fattori e influenze interni ed esterni che rendono incerto il raggiungimento dei propri obiettivi: **il rischio costituisce l'effetto che questa incertezza ha sugli obiettivi dell'organizzazione**. Per una gestione efficace del rischio, un'organizzazione deve attenersi a precisi principi e dotarsi di un apposito **framework gestionale** incaricato di integrare,

progettare, implementare, valutare e monitorare/migliorare iterativamente i processi di gestione del rischio. Una corretta e attiva gestione del rischio, oltre ad accrescere le prestazioni in ambito salute e sicurezza, aumenta la probabilità di raggiungere gli obiettivi e incoraggia la gestione proattiva. **Un approccio di tipo preventivo è valorizzato e consigliato.**



Il contesto giuridico-normativo

Art. 17, primo comma, lett. a), D.Lgs. 81/08

Obbligo NON delegabile
del datore di lavoro
di valutare tutti i rischi
e di elaborare un documento specifico (DVR)

16

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



Il datore di lavoro è il primo e principale destinatario dell'obbligo di garantire le misure di prevenzione antinfortunistica a tutela dell'incolumità e del benessere dei lavoratori e di coloro che, a qualunque titolo, sono presenti nei luoghi di lavoro: egli deve valutare tutti i **rischi** per la sicurezza e la salute, sia quelli di **NATURA ENDOGENA** (propri, cioè, delle caratteristiche intrinseche di un processo o di un'attività, di una particolare attrezzatura o di un ambiente di lavoro) sia quelli di **NATURA ESOGENA** (correlati, cioè, alle caratteristiche e alle componenti del contesto sociale, politico, ambientale (comprese le cause naturali), oppure associati ad attività o sistemi con cui interagiscono, ovvero dipendenti da eventi e fenomeni originati dalla volontà dell'uomo). Partendo da questa distinzione, il docente introdurrà il concetto di **RISCHIO ESOGENO INTERFERENZIALE DI ORIGINE CRIMINOSA**.

La valutazione dei rischi deve tradursi in un documento contenente:

- una relazione dettagliata e ragionata sulla valutazione dei rischi per la sicurezza e la salute durante l'attività lavorativa;
- l'individuazione delle misure di prevenzione e protezione esistenti e delle relative procedure di attuazione;
- il piano di miglioramento nel tempo dei livelli di sicurezza;
- l'individuazione delle mansioni che espongono a rischi specifici.

Si utilizzi la slide per evidenziare le connessioni fra Safety e Security e le loro rispettive specificità, richiamando il contenuto delle slide di apertura. Cenni al DVR e alla valutazione dei rischi di Security (rapine, aggressioni e minacce,

estorsioni, truffe, rischi psicosociali, travel security, terrorismo (materiale o informatico), spionaggio, corruzione e infedeltà dei dipendenti, policy di *fraud management* e *loss prevention* per mitigare il rischio stress lavoro correlato, ...).



Il contesto giuridico-normativo

Capo III - Gestione della prevenzione nei luoghi di lavoro

Sezione II - VALUTAZIONE DEI RISCHI

Art. 28 - Oggetto della valutazione dei rischi

Art. 29 - Modalità di effettuazione della valutazione dei rischi

Art. 30 - Modelli di organizzazione e di gestione

(esimenti della responsabilità amministrativa delle persone giuridiche)

17

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



Nel commentare le diapositive che seguono dovrà emergere la spesso trascurata ma indiscutibile connessione fra il D.Lgs. 81/2008 e i rischi di origine criminosa, ambito di applicazione della Security. La giurisprudenza civile e penale è ormai concorde nel ritenere correlati all'attività lavorativa non solo i tipici rischi di origine antinfortunistica, ma anche i **RISCHI ATIPICI** (o "particolari", come li definisce l'art. 28) **derivanti da attività criminali di varia natura** (comprese quelle terroristiche), tenendo conto del contesto ambientale in cui viene svolta l'attività lavorativa. Il datore di lavoro, in quanto garante della sicurezza dei luoghi di lavoro, è responsabile (civilmente e penalmente) anche per i danni subiti dal lavoratore in conseguenza di azioni delittuose commesse da terzi (aggressioni, minacce, violenze, ...), teoricamente al di fuori della sua sfera di controllo.

Gli articoli 28 e 29 prescrivono al datore di lavoro di svolgere un'approfondita valutazione di tutti i rischi che incombono sul lavoratore, non limitandosi, quindi, ad adottare generiche misure di sicurezza che non tengano nella dovuta considerazione i rischi connessi alle specifiche tipologie contrattuali attraverso le quali viene resa la prestazione di lavoro. La *ratio* dei "**PROCESSI DI RISK ANALYSIS & ASSESSMENT**" dovrà essere ben evidente nel Documento di Valutazione dei Rischi.

Nel richiamare l'art. 30, si introdurrà il **D.Lgs. 231/2001** in materia di responsabilità amministrativa delle società e degli enti, in base al quale questi possono essere ritenuti responsabili e, conseguentemente, sanzionati in relazione ad alcuni reati commessi o tentati nell'interesse o a vantaggio della società dagli amministratori o dai dipendenti. La responsabilità delle citate

persone giuridiche viene esclusa se vengono adottati ed efficacemente attuati modelli di organizzazione, gestione e controllo in grado di prevenire i reati stessi.



Il contesto giuridico-normativo

Obiettivi della valutazione dei rischi

Identificare idonee
misure di prevenzione e protezione
e mantenerle efficienti

18

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



Le situazioni di crisi si manifestano sovente avvengono all'improvviso e possono riguardare qualsiasi circostanza. Non è umanamente possibile essere preparati a tutto, ma è indispensabile sviluppare un'adeguata mentalità difensiva, per non farsi trovare impreparati di fronte ai pericoli che possono interferire con l'attività lavorativa. L'**attività di prevenzione** comprende tutte le azioni e le cautele capaci di contrastare l'accadimento di eventi criminosi. Nell'ambito delle politiche di security, essa consiste nell'adozione delle opportune strategie in grado di:

- potenziare le resistenze opposte agli eventi criminosi, attraverso l'attuazione di particolari difese che mirano sempre più ad uno "scoraggiamento" per il criminale di raggiungere lo scopo dei tentativi di assalto (c.d. "**prevenzione primaria**", di tipo prevalentemente tecnico-impiantistico o strutturale);
- stimolare la diffusione, la condivisione e l'interiorizzazione di una mentalità della sicurezza, un risultato che comprende formazione, pensiero e azione (c.d. "**prevenzione secondaria**", di natura organizzativa e partecipativa).

Integrando fra loro adeguate procedure dispositive, idonee misure di sicurezza tecnico-difensive e comportamenti cautelativi adeguati e consapevoli, si possono ottenere risultati soddisfacenti nel campo della prevenzione anticrimine. **"Fare sicurezza" significa prevenire situazioni a rischio, programmare interventi, educare alla legalità, informare il personale, definire chiare e semplici regole comportamentali.** La sicurezza deve essere intesa come insieme di misure atte ad assicurare tranquillità e protezione all'impresa e alle persone. L'obiettivo è quello di favorire presso la compagine

aziendale l'interiorizzazione di procedure e comportamenti cautelativi ispirati dalla convinzione che sia realisticamente possibile prevenire gli eventi criminosi e difendersi da essi (questo passaggio è determinante nella **fase del “controllo del rischio”**).




La prevenzione e la protezione sono attività indispensabili per contrastare il verificarsi degli eventi dannosi o ridurre le conseguenze, per tutelare le persone che lavorano o si muovono all'interno di un'organizzazione e per proteggere le risorse (materiali e immateriali) che assicurano l'esistenza dell'organizzazione stessa. Rimandando l'approfondimento del concetto di prevenzione alla seconda parte del corso, può essere utile rimarcare l'importanza di alcune **MISURE GENERALI DI TUTELA** (sia strutturali che organizzative), ai sensi dell'art. 15 del D.Lgs. 81/2008:

- l'eliminazione o la riduzione al minimo dei rischi, in relazione alle conoscenze acquisite in base al progresso tecnico;
- il rispetto dei principi ergonomici fin dalla fase di progettazione dei luoghi di lavoro e nell'organizzazione del lavoro stesso;
- l'informazione, la formazione e l'addestramento di tutti i lavoratori;
- la programmazione della prevenzione intesa come integrazione fra fattori ambientali, condizioni tecniche produttive e organizzazione del lavoro;
- l'adozione di comportamenti e procedure operative idonei e adeguati;
- la regolare manutenzione di impianti, attrezzature e ambienti;
- un piano di miglioramento continuo e dinamico dei livelli di sicurezza (continua rielaborazione della valutazione dei rischi).

Si faccia riflettere l'aula sulle correlazioni esistenti fra i punti sopra esposti e le attività di security (ad esempio: l'uso di adeguati mezzi di custodia del denaro riduce l'incidenza delle rapine; l'efficienza degli impianti di allarme contrasta i

reati predatori; un atteggiamento responsabile e proattivo dei lavoratori previene molte tipologie di reato). Sottolineare l'importanza del **MIGLIORAMENTO CONTINUO DEI PROCESSI DI PREVENZIONE E SICUREZZA DEI LUOGHI DI LAVORO**, in ottica security.




Il contesto giuridico-normativo

Obiettivi della valutazione dei rischi

Individuare le **azioni** e le **procedure** per l'attuazione delle misure di prevenzione e protezione da realizzare

20

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



Il docente dovrà, in particolare, richiamare gli articoli del D.Lgs. 81/2008 che disciplinano:


- la redazione da parte del datore di lavoro e l'osservanza da parte del lavoratore di procedure e disposizioni aziendali di sicurezza che siano semplici, comprensibili e complete (art. 20, c. 2 lett. b - art. 18, primo comma lett. f);
- i controlli sull'osservanza delle procedure (art. 28, c. 2 lett. d - art. 30 primo comma lett. h) e le sanzioni per gli inadempienti.

Anche in questa fase di valutazione del rischio, il principio ispiratore è quello del miglioramento continuo: **la sicurezza è un percorso virtuoso che non conosce traguardi definitivi ma persegue una costante ascesa verso l'eccellenza.**

Riguardo al contenuto delle procedure, a titolo esemplificativo e non esaustivo, esse devono indicare:

- la chiara definizione e individuazione delle misure da adottare per ridurre i rischi di security;
- la valutazione delle modalità operative contingenti e dei rischi di security connessi;
- le procedure efficaci e idonee per fronteggiare le minacce;
- le procedure di verifica e valutazione delle politiche di security;
- le misure per assicurare la tutela fisica dei lavoratori;

- la precisa attribuzione di responsabilità ai vari livelli aziendali;
- le informazioni operative sufficienti e idonee a soddisfare il principio della "necessità di conoscere".




Il contesto giuridico-normativo

Obiettivi della valutazione dei rischi

Individuare le mansioni a rischio specifico

21

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



In fase di analisi del rischio e messa a punto delle idonee contromisure di prevenzione e protezione, è indispensabile considerare la sicurezza anticrimine (e, in generale, i “**RISCHI ESOGENI**” direttamente connessi all’azione, all’operato e alla volontà dell’uomo) tra gli aspetti che possono incidere negativamente e direttamente sull’integrità psicofisica dei lavoratori. Tra i rischi connessi all’attività di lavoro, il datore di lavoro ha l’obbligo di valutare anche quelli che sia pure indirettamente o in modo anomalo possono esporre il lavoratore a un potenziale danno, purché tali rischi siano oggettivamente e concretamente prevedibili (art. 73 D.Lgs. 81/2008). In quest’ottica, ad esempio, si ritiene che il “*rischio rapina*” debba formare, per le aziende bancarie, oggetto di valutazione ai sensi dell’art. 28 del D.Lgs. 81/2008, con specifico riferimento a quei lavoratori che svolgono mansioni comportanti la gestione di valori o che operano in luoghi ove tale gestione si verifichi, con conseguente esposizione a tale rischio. Il rischio rapina è particolarmente sentito in quanto va a incidere sull’incolumità fisica e psicologica dei dipendenti e dei clienti. Anche le aziende operanti in zone caratterizzate da intensa attività terroristica o di guerriglia (cc.dd. Paesi “Hot Spot”) o di criminalità diffusa devono valutare attentamente i rischi endemici di atti criminosi di terzi (come il reato di sequestro di persona), predisponendo le opportune cautele per la tutela della salute e sicurezza dei propri lavoratori. L’esposizione dei lavoratori ad atti di criminalità con finalità di turbamento dell’ordine socio-politico rappresenta un problema molto diffuso in quei settori produttivi come l’energia, i trasporti, le comunicazioni e le infrastrutture critiche, in cui i rischi di security aziendale costituiscono parte integrante dei

processi produttivi e devono essere affrontati con idonee misure di prevenzione. Pur essendo esterni all'attività produttiva, detti rischi sono prevedibili e devono essere ricompresi fra i rischi "ambientali" inscindibilmente connessi allo svolgimento dell'attività lavorativa e, quindi, assoggettati alla disciplina di cui all'art. 2087 c.c. e alle altre norme di tutela della salute e sicurezza sul lavoro sin qui osservate (Cass., n. 4012 del 20 aprile 1998; Cass., n. 5048 del 6 settembre 1988.; Cass. n. 7768 del 17 luglio 1999; Cass., n. 8486 dell'8 aprile 2013).



Il contesto giuridico-normativo

Artt. 36 e 37, D.Lgs. 81/2008

Formazione, informazione e addestramento dei lavoratori

22

Copyright EPC Srl Socio Unico - tutti i diritti riservati, riproduzione vietata



Il D.Lgs. 81/2008 pone l'obbligo per il datore di lavoro di informare e formare i propri dipendenti in ordine ai rischi specifici cui sono esposti riguardo l'attività svolta. Non sono, ovviamente, esclusi i RISCHI DI ORIGINE CRIMINOSA: le imprese sono tenute a formare il proprio personale sulla natura dei rischi di security, insegnando a riconoscerli e a fronteggiarli adeguatamente.

Il contributo di ogni dipendente alla politica di sicurezza aziendale è importante in fase di rilevazione dei rischi, in quanto molte possibili evenienze possono meglio essere intuite da chi tutti i giorni lavora nel luogo in cui si manifestano. Il "bisogno di sicurezza" dei dipendenti deve essere soddisfatto per vie assolutamente condivise, mediante risposte soddisfacenti e credibili.

La formazione del personale in materia di sicurezza deve favorire la diffusione e il mantenimento in ambito lavorativo di un **MODELLO DI "SICUREZZA AZIENDALE PARTECIPATA"** che si collochi tra la conoscenza (informazione) e la consapevolezza (formazione), che favorisca l'interiorizzazione di appropriate dinamiche comportamentali da attuare nelle situazioni di crisi e di emergenza, sensibilizzando il personale sull'importanza del proprio ruolo di soggetto attivo nell'ambito della sicurezza.

Favorendo adeguati e corretti processi formativi in materia di sicurezza, si rendono più efficaci le strategie e le misure atte a garantirla, oltre a trasmettere una generale e rassicurante sensazione di tranquillità. È indubbio che siamo più preoccupati dei rischi legati a temi che non conosciamo o non comprendiamo: la "familiarità" con le situazioni di rischio cui possiamo essere esposti induce a vedere detti rischi in modo differente, migliorando la

nostra percezione della sicurezza. La sicurezza è anche un modo di sentire che si basa sulle nostre reazioni psicologiche ai rischi e alle misure di protezione.