Ordine dei Dottori Commercialisti e degli Esperti Contabili di Roma

Commissione Informatica e Qualità

FONDAZIONE TELOS
CENTRO STUDI DELL'ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI DI ROMA

La gestione del rischio secondo le Norme Volontarie ISO. Conoscerlo per applicarlo alle PMI

Lunedì 1 febbraio 2021

(15:00 – 17:30)

PROGRAMMA

I Sistemi di Gestione secondo le norme ISO basati sul rischio

- Principi di Gestione, Modalità di applicazione e contesto Italiano delle Aziende Certificate

Relatore Ottorino Pomilio Presidente della Commissione INFORMATICA E QUALITÀ ODCEC di Roma

Le norme Volontarie ISO ed i rapporti con la Responsabilità Sociale di Impresa

Relatore Domenico Antonelli : membro della Commissione INFORMATICA E QUALITÀ ODCEC di Roma

Cosa è il rischio per un giocatore ?

Obiettivo : vincere la posta

Incertezza : le carte degli avversari

Rischio : perdere il denaro giocato

Cosa è il rischio per un lavoratore in raffineria ?

Obiettivo : lavorare in sicurezza

Incertezza: le procedure da applicare basteranno?

Rischio : subire un infortunio

Cosa è il rischio per un surfista?

Obiettivo : far durare più a lungo possibile la surfata

Incertezza: un evento che mi fa perdere l'equilibrio

Rischio : finire presto

Cosa è il rischio per noi professionisti?

Obiettivo : lavorare nelle regole, assicurare la continuità della professione

Incertezza : ho tutte le informazioni necessarie?

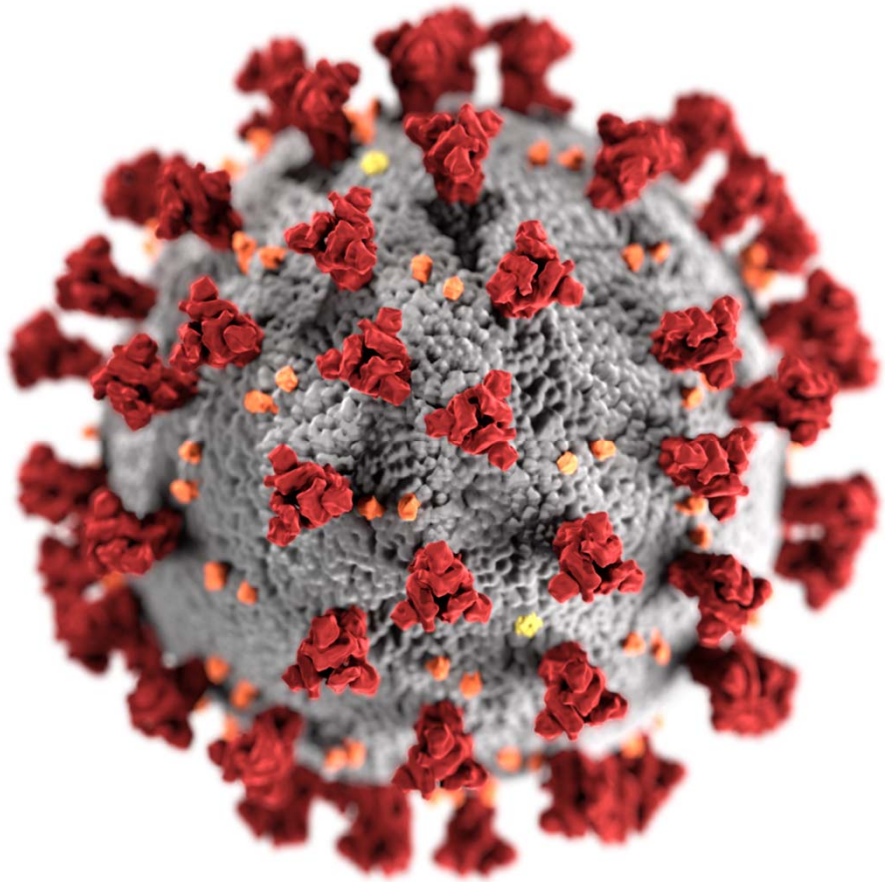
Rischio : sanzioni, mancati incassi, blocco dello Studio

Cosa è il rischio per Tutti Noi Oggi?

Obiettivo : Non contrarre il Virus

Incertezza : non si vede

Rischio : contrarre il virus



Definizione di Rischio secondo la Norma ISO 31000:10

RISCHIO: Effetto dell'incertezza sugli obiettivi

- Un **effetto** è uno scostamento da quanto atteso – positivo e/o negativo
- **L'incertezza** è lo stato, anche parziale, di assenza di informazioni relative alla comprensione o conoscenza di un evento, delle sue conseguenze o della loro verosimiglianza.
- **Gli obiettivi** possono presentare aspetti differenti (come scopi finanziari, di salute e sicurezza, ambientali) e possono intervenire a livelli differenti (come progetti, prodotti e processi strategici, riguardanti l'intera organizzazione)
- Il rischio è spesso caratterizzato dal riferimento a eventi potenziali e conseguenze, o una combinazione di questi
- Il rischio è spesso espresso in termini di combinazione delle conseguenze di un evento (compresi cambiamenti nelle circostanze) e della verosimiglianza del suo verificarsi

Il rischio è insito nel raggiungimento di un obiettivo

> *Chi non rischia nulla non fa nulla, non ha nulla e non è nulla.*

LEO BUSCAGLIA

Cit. da Vivere, amare, capirsi

Il Futuro è sempre Incerto, quindi generatore di rischi

> *Correremo questo rischio. E quello dopo.*

JIN ERSO

Dal film: Rogue One

Gli elementi che caratterizzano un rischio

Fonte di rischio: Elemento che da solo o in combinazione con altri possiede il potenziale intrinseco di originare il **rischio**

Una fonte di rischio può essere tangibile o intangibile.

Evento: Il verificarsi o il modificarsi di un particolare insieme di circostanze.

- Un evento può consistere in uno o più episodi e può avere diverse cause.
- Un evento può consistere nel non verificarsi di qualcosa.

Conseguenza: Esito di un evento che influenza gli **obiettivi**.

- Un evento può portare ad una gamma di conseguenze che possono essere certe o incerte e possono avere effetti positivi o negativi sugli obiettivi.
- Le conseguenze iniziali possono aggravarsi attraverso effetti indiretti (per esempio "effetto domino").

I rischi possono e devono essere gestiti se vogliamo raggiungere un obiettivo

La gestione del rischio è finalizzata a :

ridurre al minimo l'impatto di eventi potenziali negativi

ed, eventualmente,

trarre pieno vantaggio dalle opportunità.

Wēijī

Per quanto non universalmente riconosciuto l'ideogramma è composto da 2 elementi :

Pericolo ed Opportunità

L'incertezza è strettamente legata al Contesto

Il contesto Esterno : OPPORTUNITÀ / MINACCE

Ambiente esterno nel quale l'organizzazione cerca di conseguire i propri obiettivi, quali ad esempio l'ambiente culturale, sociale, politico, cogente, finanziario, tecnologico, economico, naturale e competitivo, sia internazionale, nazionale, regionale o locale inclusi gli elementi determinanti e tendenze fondamentali che hanno un impatto sugli obiettivi dell'organizzazione e sulle relazioni con i portatori di interesse esterni, loro percezioni e valori

Il contesto Interno : PUNTI DI FORZA / PUNTI DI DEBOLEZZA

Ambiente interno nel quale l'organizzazione cerca di conseguire i propri obiettivi ed è caratterizzato da :

- Governance, struttura organizzativa, ruoli e responsabilità, e processi decisionali (formali / informali) portatori d'interesse interni, loro percezioni e valori
- Politiche, obbiettivi e strategie che sono in atto per conseguirli
- Risorse e competenze disponibili, inclusi i Sistemi informativi, flusso di informazioni
- La cultura dell'organizzazione
- Norme, linee guida e modelli adottati dall'organizzazione
- Forma ed estensione delle relazioni contrattuali e dei rapporti con i portatori d'interesse esterni

Il Sistema Aziendale per la Gestione dei Rischi secondo ISO 31000

Ogni organizzazione ha come ragion d'essere il raggiungimento di obiettivi, che sono sempre incerti, essendo futuri.

È quindi necessario che la gestione tenga in dovuta considerazione tutti i rischi esistenti **con lo scopo di Creare e Proteggere il Valore** .

La Creazione e la Protezione del Valore è il pilastro di un Efficace Sistema di Gestione dei Rischi Aziendali ed è alla base dei principi di funzionamento del Sistema stesso.

Questi principi forniscono la guida per l'adozione e la gestione di un Sistema di Gestione dei rischi efficace ed efficiente

I principi del Sistema di Gestione del Rischio

Gestione Integrata	Parte integrante di tutte le attività organizzative.
Strutturata e completa	Un approccio strutturato e completo alla gestione del rischio contribuisce a risultati coerenti e comparabili.
Personalizzata	Strumenti personalizzati e proporzionati al contesto esterno e interno dell'organizzazione in relazione ai suoi obiettivi.
Inclusiva	Basata sul coinvolgimento delle parti interessate, allo scopo di considerare le loro conoscenze, opinioni e percezioni.

Dinamica	Si adatta ai cambiamenti del contesto
Le migliori informazioni disponibili	Le informazioni dovrebbero essere tempestive, chiare e disponibili per le parti interessate
Fattori umani e culturali	Il comportamento e la cultura umana influenzano in modo significativo tutti gli aspetti della gestione del rischio
Miglioramento continuo	La gestione del rischio è continuamente migliorata attraverso l'apprendimento e l'esperienza.

La struttura per la Gestione del Rischio

Figure 3 — Framework

Descrive il percorso per lo sviluppo e la gestione del Sistema di Gestione dei Rischi dell'Organizzazione (ERMS Enterprise Risk Management System)
Gli elementi caratterizzanti , descritti nel capitolo 5 della Linea guida, sono :

PLAN

Leadership ed Impegno (5.2)
Integrazione (5.3)
Progettazione (5.4)

DO Attuazione (5.5)

CHECK Valutazione (5.6)

ACT Miglioramento (5.7)

Progettazione dell'ERMS

Progettazione Step 1 : **Comprendere l'organizzazione ed il suo Contesto**

Progettazione Step 2 : Dare evidenza dell'Impegno sull'ERMS

Progettazione Step 3 : Assegnazione delle responsabilità ed autorità per l'ERMS

Progettazione Step 4 : Messa a disposizione delle risorse per l' ERMS

Progettazione Step 5 : Sistema di Comunicazione e Consultazione in materia di Rischi

Il Processo di Gestione del Rischio

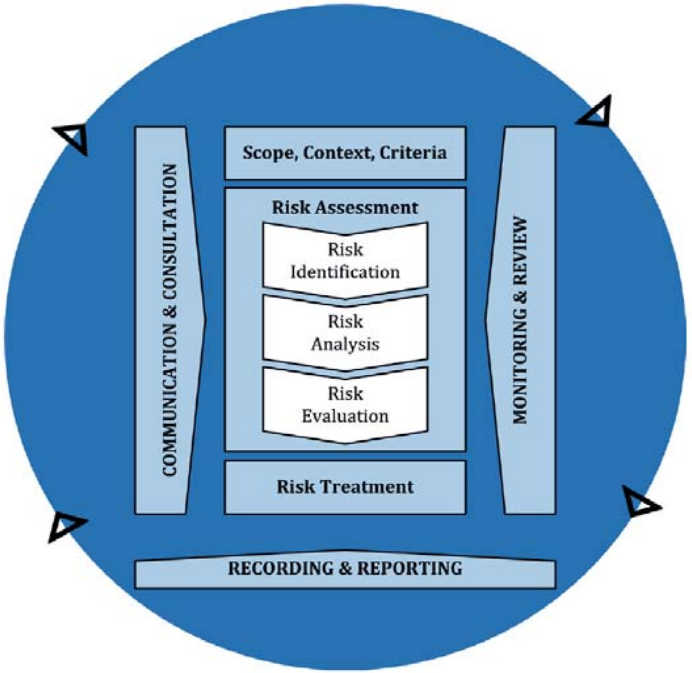


Figure 4 — Process

Fasi del processo di gestione del rischio

1. Comunicazione and consultazione
2. Campo di Applicazione , Contesto e Criteri
3. Valutazione del Rischio
4. Trattamento del Rischio
5. Monitoraggio e Riesame del rischio
6. Registrazioni e Reportistica sui rischi

Il modello della ISO 31000 alla base delle Norma sui Sistemi di Gestione

Un sistema di gestione aziendale ha l'obiettivo di soddisfare tutte le parti interessate, però non è sicuro che accada

Rischi

- Insoddisfazione del Cliente
- Mancato controllo dei costi
- Violazione di Norme relative a
  - Normativa Ambientale
  - Salute e Sicurezza Lavoratori
  - Dati ed Informazioni
  - Etiche
  - Altre violazioni

Incident

Conseguenze

- Perdite di Fatturato e/o aumento di Costi = (- Utile)
- Sanzioni
- Danni di immagine
- Danni Ambientali
- Incidenti Salute dei lavoratori
- Indisponibilità del sistema Informativo

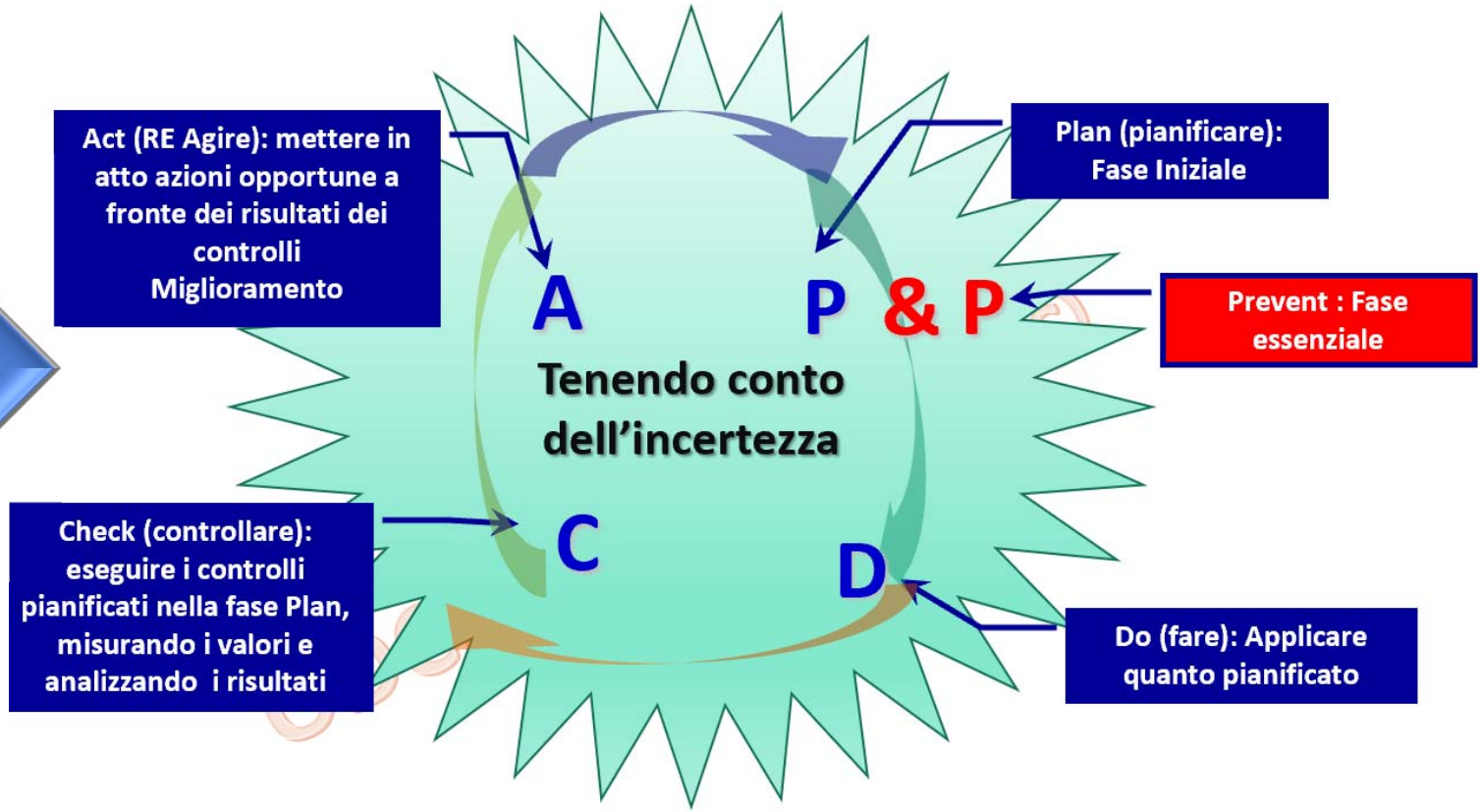
I modelli ISO per i Sistemi di Gestione Aziendali Certificabili.

Sono costruiti con questi obiettivi

- **Facilitare gli scambi commerciali**
- **Rilevanza per il Mercato**
- **Compatibilità tra i sistemi di Gestione**
- **Massima Copertura dei requisiti**
- **Flessibilità**
- **Certificabile (inclusi audit Combinati)**
- **Scollegato dai prodotti/servizi**
- **Di facile uso**

I modelli ISO per la Gestione Aziendali Certificabili.

Basati su questo approccio



I modelli ISO per la Gestione Aziendali Certificabili.

Prevedendo la gestione questi requisiti:

4. Contesto della Organizzazione
5. Leadership
6. Pianificazione
7. Processi di Supporto
8. Controlli Operativi
9. Valutazione delle Prestazioni
10. Miglioramento

Le principali Norme Iso sui sistemi di Gestione

ISO 9001 (Qualità)

ISO 14001 (Ambiente)

ISO 50001 (Gestione Energia)

ISO 45001 (Salute e Sicurezza sul lavoro)

ISO 37001 (Prevenzione della Corruzione)

ISO 22301 (Business Continuity)

ISO 27001 (Sicurezza delle Informazioni)

ISO 20001-1 (Servizi ICT)

Iso 9001: 2015 Sistemi di Gestione per la Qualità

Scopo della Norma : La norma specifica i requisiti di un sistema di gestione per la qualità quando un'organizzazione:

a) Ha l'esigenza di dimostrare la propria capacità di fornire con regolarità prodotti o servizi che soddisfano i requisiti del cliente e i requisiti cogenti applicabili; e

b) mira ad accrescere la soddisfazione del cliente tramite l'applicazione efficace del sistema, compresi i processi per migliorare il sistema stesso e assicurare la conformità ai requisiti del cliente e ai requisiti cogenti applicabili.

Tutti i requisiti sono di carattere generale e previsti per essere applicabili a tutte le organizzazioni, indipendentemente da tipo o dimensione, o dai prodotti forniti e servizi erogati.

Iso 14001: 2015 Sistemi di Gestione Ambientale

Scopo della Norma : La norma specifica i requisiti di un sistema di gestione ambientale che un'organizzazione può utilizzare per sviluppare le proprie prestazioni ambientali.

La norma è destinata ad un'organizzazione che desidera gestire le proprie responsabilità ambientali in un modo sistematico che contribuisce al pilastro ambientale della sostenibilità.

La norma aiuta un'organizzazione a raggiungere gli esiti attesi dal proprio sistema di gestione ambientale, che forniscono valore aggiunto per l'ambiente, per l'organizzazione stessa e per le parti interessate.

Iso 50001: 2015 Sistemi di Gestione dell'energia

Scopo della Norma : La norma definisce i requisiti per creare, attuare, mantenere e migliorare un sistema di gestione dell'energia (SGE).

L'obiettivo della norma è quello di consentire che un'organizzazione persegua, con un approccio sistematico, il miglioramento continuo della propria prestazione energetica e dello stesso SGE.

Iso 45001: 2018 Sistemi di Gestione per la salute e sicurezza sul lavoro

Scopo della Norma : La norma internazionale specifica i requisiti per un sistema di gestione per la salute e sicurezza sul lavoro (SSL) e fornisce una guida per il suo utilizzo, al fine di consentire alle organizzazioni di predisporre luoghi di lavoro sicuri e salubri, prevenendo lesioni e malattie correlate al lavoro, nonché migliorando proattivamente le proprie prestazioni relative alla SSL.

La presente norma internazionale è applicabile a qualsiasi organizzazione, indipendentemente dalle dimensioni, tipo e attività, che desideri istituire, attuare e mantenere un sistema di gestione per migliorare la salute e la sicurezza sul lavoro, eliminare i pericoli e minimizzare i rischi per la SSL (incluse carenze del sistema), cogliere le opportunità per la SSL e prendere in carico le non conformità del sistema di gestione per la SSL associate alle proprie attività.

Iso 37001: 2016 Sistemi di Gestione per la Prevenzione della Corruzione

Scopo della Norma : La UNI ISO 37001 specifica requisiti e fornisce una guida per stabilire, mettere in atto, mantenere, aggiornare e migliorare un sistema di gestione per la prevenzione della corruzione. Il sistema può essere a se stante o integrato in un sistema di gestione complessivo. La norma fornisce questi indirizzi in relazione alle attività dell'organizzazione:

· corruzione nei settori pubblico, privato e no-profit;
· corruzione da parte dell'organizzazione;
· corruzione da parte del personale dell'organizzazione che opera per conto dell'organizzazione o a beneficio di essa;
· corruzione da parte dei soci in affari dell'organizzazione che operano per conto dell'organizzazione o a beneficio di essa;
· corruzione dell'organizzazione;
· corruzione del personale dell'organizzazione in relazione alle attività dell'organizzazione;
· corruzione dei soci in affari dell'organizzazione in relazione alle attività dell'organizzazione;
· corruzione diretta e indiretta (per esempio una tangente offerta o accettata tramite o da una parte terza).

La norma è applicabile soltanto alla corruzione. Definisce requisiti e fornisce una guida per un sistema di gestione progettato per aiutare un'organizzazione a prevenire, rintracciare e affrontare la corruzione e a rispettare le leggi sulla prevenzione e lotta alla corruzione e gli impegni volontari applicabili alla propria attività.
La norma non affronta in modo specifico condotte fraudolente, cartelli e altri reati relativi ad anti-trust/concorrenza, riciclaggio di denaro sporco o altre attività legate a pratiche di malcostume e disoneste, sebbene un'organizzazione possa scegliere di estendere lo scopo del sistema di gestione per comprendere queste attività.

Iso 27001: 2013 Sistemi di Gestione della Sicurezza delle Informazioni

Scopo della Norma : La norma specifica i requisiti per stabilire, attuare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni nel contesto dell'organizzazione.

Inoltre essa include i requisiti per la valutazione e il trattamento dei rischi per la sicurezza dell'informazione adatti alle esigenze dell'organizzazione.

I requisiti presenti nella norma sono generici e destinati ad essere applicati a tutte le organizzazioni, indipendentemente dal tipo, dalla dimensione o dalla loro natura.

Iso 22301: 2019 Sistemi di Gestione per la continuità operativa

Scopo della Norma : La norma specifica i requisiti per attuare, mantenere e migliorare un sistema di gestione per proteggere l'organizzazione, ridurre la probabilità che si verifichino, prepararsi, rispondere e riprendersi dalle interruzioni quando si verificano, cioè un efficace sistema di gestione per la continuità operativa BCMS (Business Continuity Management System).

I requisiti specificati nella norma sono generici e sono destinati ad essere applicabili a tutte le organizzazioni, o a parti di esse, indipendentemente dal tipo, dalle dimensioni e dalla natura dell'organizzazione. La portata dell'applicazione di questi requisiti dipende dall'ambiente operativo e dalla complessità dell'organizzazione.

I numeri Accredia

fonte
https://www.accredia.it/

Dati al 30/09/2020

Aziende Certificate	
1 Norma	67.964
2 Norme	9140
3 Norme	3738
4 Norme	838
5 Norme	156
6 Norme	36
7 norme	3
8 norme	1
Tot. Aziende	81.876

Norma	N° Siti	Sistema
UNI EN ISO 9001	120.546	Qualità
ISO 39001	565	Sicurezza del traffico
ISO 22301	93	Business Continuity
ISO 55001	11	Asset Management
UNI ISO 37001	2.592	Antibribery
UNI EN ISO 14001	24.411	Ambiente
UNI CEI EN ISO 50001	2.926	
BS OHSAS 18001	10.472	Safety
UNI ISO 45001	12.484	
UNI CEI ISO/IEC 27001	2.482	ICT Security
ISO/IEC 27017:2015	92	
ISO/IEC 27018:2019	102	
UNI CEI EN ISO/IEC 20000-1	262	
UNI EN ISO 22000	1.577	Food

Norme NON ISO : SA8000

SA8000® è uno standard volontario che dimostra l'impegno delle organizzazioni per un ambiente di lavoro sicuro e che garantisca un approccio socialmente responsabile.

L'adozione dello standard contribuisce a gestire i rischi, la reputazione aziendale, soddisfare le esigenze dei clienti in termini di approccio etico, migliorare le relazioni con i fornitori, creare migliori condizioni di lavoro e un ambiente di lavoro più sicuro.

NB: lo standard non è ISO pertanto tutto il percorso di certificazione avviene con regole stabilite direttamente dal SAAS, Social Accountability Accreditation Services. In Italia risultano certificati al 2020 3.906 siti Fonte http://www.saasaccreditation.org/certfacilitieslist

Conclusioni

Per un Professionista al passo con i Tempi, che sicuramente tra i propri clienti ha aziende certificate è importante sapere che esistono questi strumenti gestionali.

Una volta i Sistemi di Gestione Normati erano materia da Ingeneri dato che si focalizzavano sui processi produttivi.

Oggi non più: l'evoluzione del modello su cui sono basate le norme richiede la disponibilità di competenze che siano in grado di leggere l'azienda nel suo complesso.

Queste è, o dovrebbe essere, nelle corde dii un Dottore Commercialista ed Esperto Contabile

Grazie per l'attenzione