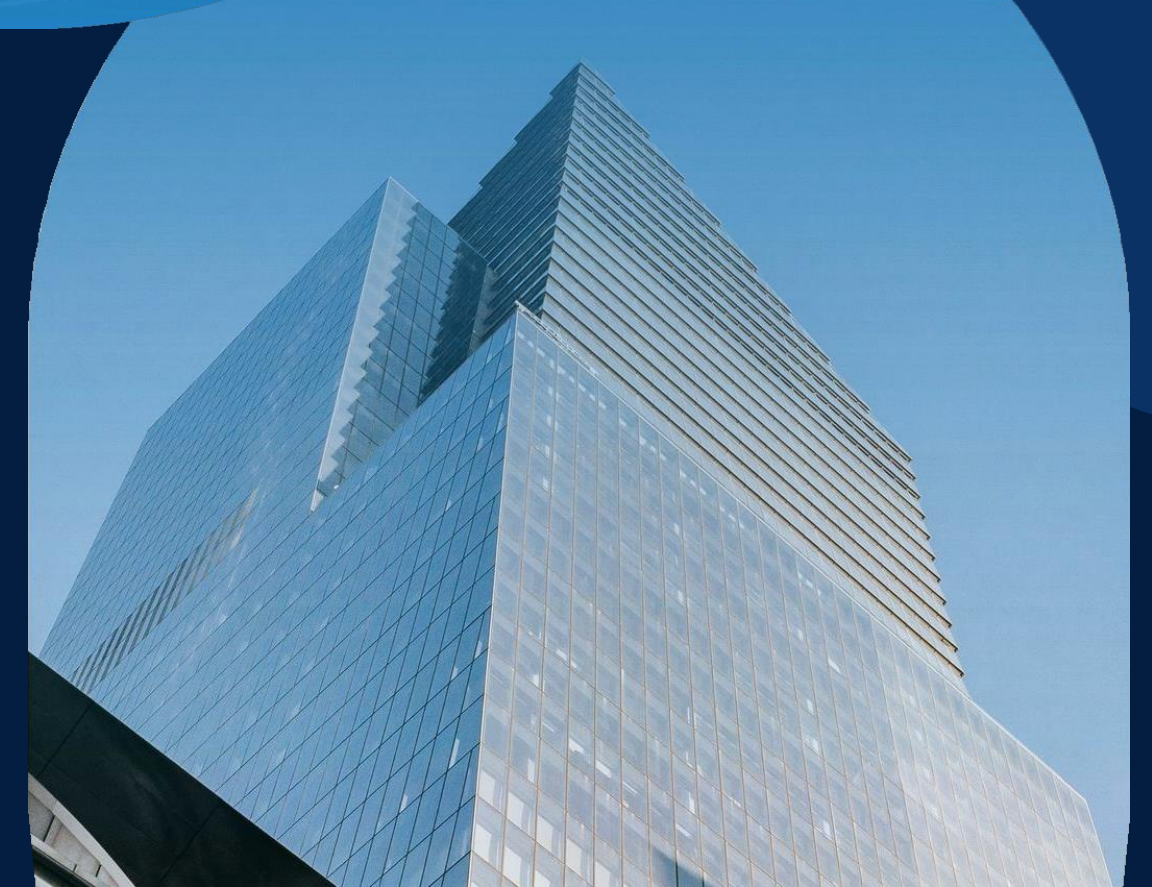




KNOW FIRST THEN ACT.
RISKsSECURITY CONSULTING

SECURITY & RISK Management



STRUMENTI E STRATEGIE PER UN'EFFICACE GOVERNANCE AZIENDALE



SVILUPPARE METRICHE E KPI

- Misure di conformità
- Gestione del rischio
- Soddisfazione degli stakeholders



MONITORAGGIO DELLE PRESTAZIONI

- Colmare eventuali lacune
- Individuare aree di miglioramento



RENDICONTAZIONE REGOLARE

- Report annuali
- Rapporti di sostenibilità
- Aggiornamenti periodici al CdA



BEST PRACTICES PER LA GOVERNANCE

- Formazione continua sui principi e sulle pratiche di governance
- Confronto con gli standard di settore
- Promozione di una comunicazione aperta

I RISCHI TRATTATI

E' necessario strutturare piani di azione e prevenzione certificati per evitare che le aziende subiscano danni a causa di analisi dei rischi non corrette o per negligenza e/o li provochino a terzi.

A RISCHI OPERATIVI

- Perdita fornitore strategico
- Perdita/furto merci durante il trasporto
- Blocco del flusso informativo di dati
- Furto di dati sensibili da Cyber-Attack

B RISCHI LEGALI

- Difesa e sconfinamento proprietà intellettuale
- Responsabilità Ambientale
- Responsabilità dell'impresa su terze parti coinvolte (Direttiva UE 2024/1760)

C RISCHI BUSINESS E FINANZIARI

- Insolvenza clienti

D RISCHI PURI O ASSICURATIVI

- NON TRATTATI

OVERVIEW

01

Are di
Intervento

02

Chi siamo

03

Reputational
Risk

04

Cyber
Security

05

Travel
Security

06

Phisical
Security

07

Our Team

01 AREE DI INTERVENTO

01 Security Management

Attività volta ad individuare, **valorizzare ed analizzare rischi** che possono provocare danni patrimoniali e non, come ad esempio furti, frodi, divulgazione di informazioni ecc. in un'azienda, ente o raggruppamento di beni e persone.

02 Risk Management

E' il processo mediante il quale si **misura** o si stima il **rischio** e successivamente si sviluppano delle **strategie** per **governarlo**.



01 AREE DI INTERVENTO

03 ESG & REPUTAZIONE AZIENDALE

Abbinare i criteri **ESG** (Environment, Social, Governance) alla **reputazione aziendale** è fondamentale, poiché le performance su queste tre dimensioni sono il fattore chiave per la percezione di un'azienda da parte di *stakeholder* (clienti, investitori, dipendenti, comunità locale). Un allineamento efficace trasforma la sostenibilità da un costo o un obbligo a un vero e proprio **vantaggio competitivo e reputazionale**.

Per costruire una reputazione solida, le politiche ESG non devono essere solo operazioni di facciata (*greenwashing*), ma devono essere integrate nel **modello di business** e nella **cultura aziendale**.

DI SEGUITO COME ASSISTIAMO I CLIENTI NELLE ATTIVITA' DI



01 AREE DI INTERVENTO

04 ESG & REPUTAZIONE AZIENDALE

La reputazione si basa sulla credibilità.

Le aziende devono dimostrare i risultati ESG in modo verificabile:

- **Reporting di Sostenibilità**: Pubblicare il **bilancio di sostenibilità** (o la Dichiarazione Non Finanziaria - DNF), utilizzando *standard* riconosciuti a livello internazionale (es. **GRI - Global Reporting Initiative**). Questo dimostra impegno e trasparenza.
- **KPI Chiari**: Utilizzare **indicatori di performance (KPI)** specifici (es. riduzione di CO2 per unità di prodotto, indice di *turnover* dei dipendenti, percentuale di donne nel CdA). L'assenza di dati misurabili lascia spazio al sospetto di *greenwashing*.
- **Certificazioni Esterne**: Ottenere certificazioni (es. ISO, B Corp) o farsi valutare da agenzie di rating ESG (es. MSCI, Sustainalytics) rafforza l'affidabilità esterna dei dati.

01 AREE DI INTERVENTO

05 ESG & REPUTAZIONE AZIENDALE

Un allineamento ESG efficace genera benefici diretti per la reputazione aziendale:

- **Attrazione di Talenti**: I giovani talenti scelgono sempre più spesso aziende con forti valori ESG, riducendo i costi di *recruitment* e aumentando l'engagement dei dipendenti.
- **Fidelizzazione del Cliente**: I consumatori sono disposti a pagare un *premium price* per prodotti di *brand* percepiti come sostenibili ed etici.
- **Gestione del Rischio**: Un'ottima *governance* e attenzione sociale riducono i rischi di scandali, multe, cause legali o boicottaggi, proteggendo il **valore del brand**.
- **Accesso al Capitale**: Una buona reputazione ESG è essenziale per accedere a fondi di investimento sostenibili (SRI) e ottenere finanziamenti a tassi più vantaggiosi (*green loans*).



LA STORIA

Teleinform nel settore dal 1970 ha sviluppato una nuova linea di business che nasce dall'esperienza diretta di chi ha osservato da vicino le difficoltà delle aziende nell'affrontare rischi e minacce.

L'obiettivo è quello di fornire alle aziende una "**LINEA GUIDA STANDARDIZZATA**" che delinei i requisiti minimi necessari per affrontare efficacemente i rischi, sia in termini di sicurezza fisica che informatica.

Teleinform, da la possibilità di adattare questi modelli a seconda delle esigenze specifiche di ogni azienda, con il supporto anche di un **Temporary Security Manager**.



LE ESPERIENZE

L'esperienza maturata nei **55** anni di attività, operando quale consulente nei settori della **SICUREZZA AZIENDALE** e nelle **INVESTIGAZIONI**, ha permesso di costruire modelli utili ad individuare i rischi nelle aziende e di attivare le contromisure utili alla mitigazione.

I nostri clienti hanno potuto ridurre i costi fissi legati alla presenza di un manager interno, rendendo la consulenza accessibile a piccole, medie e grandi imprese, e garantendo, allo stesso tempo, l'efficacia dei processi di sicurezza e tutela.

03 REPUTATIONAL RISK

Analisi terze parti

Attività finalizzata a classificare le aziende con cui si intrattengono rapporti d'affari – fornitori, partner, distributori, ecc. – attraverso un RATING ECONOMICO E REPUTAZIONALE, e a garantirne il monitoraggio continuo.”

Controllo persone

Attività volta a verificare tutti gli ospiti che accedono all'interno di uffici, stabilimenti e magazzini verificando che gli stessi non siano coinvolti in reati finanziari, siano sanzionati, o indagati in passato per riciclaggio, versamento di tangenti ecc.

Controllo supply chain & sostenibilità

Attività volta a verificare se i mezzi utilizzati per il trasporto della propria merce siano regolarmente assicurati, che abbiamo svolto le revisioni di legge e che le aziende di trasporto siano in possesso delle autorizzazioni e che siano in regola con gli adempimenti fiscali . Verifica CO2/Assicurazioni/revisioni dei camion.

Analisi terze parti

La Direttiva (UE) 2024/1760, nota come **Corporate Sustainability Due Diligence Directive (CSDDD)** o **CS3D**, introduce una forma di **responsabilità civile** che, sebbene non sia formalmente definita come "responsabilità solidale" in senso stretto tra l'impresa e i suoi partner commerciali, stabilisce un meccanismo di responsabilità per i danni causati da violazioni non prevenute lungo la catena di attività.

Ecco come la Direttiva disciplina la responsabilità e la catena di attività:

1. Responsabilità Civile dell'Impresa

La Direttiva impone alle imprese l'obbligo di esercitare la **Due Diligence (dovere di diligenza)** per identificare, prevenire, mitigare e porre fine agli impatti negativi sui **diritti umani** e sull'**ambiente** all'interno delle loro **catene di attività** (inclusi i fornitori).

03 REPUTATIONAL RISK

Analisi terze parti

L'**Articolo 29** della Direttiva (UE) 2024/1760 stabilisce un meccanismo di **responsabilità civile** nei confronti delle persone fisiche o giuridiche (ad esempio, comunità o associazioni) che hanno subito un danno a causa di una violazione degli obblighi di *due diligence* da parte dell'impresa, a condizione che:

- L'impresa non abbia adempiuto ai suoi obblighi di prevenzione, attenuazione o eliminazione degli impatti negativi, **intenzionalmente o per negligenza**.
- Sia stato causato un **danno** a seguito di tale inosservanza

2. Esclusione della Responsabilità Solidale con i Partner Commerciali

È fondamentale notare che la Direttiva ha esplicitamente **escluso** la previsione di una responsabilità solidale generalizzata tra l'impresa principale e i suoi partner commerciali nella catena di attività (fornitori, subappaltatori, ecc.).

Come indicato sulla Direttiva, **un'impresa non può essere ritenuta responsabile civilmente se il danno è stato causato esclusivamente dai suoi partner commerciali**, senza che vi sia stata una violazione dei propri obblighi di due diligence.

Analisi terze parti

Il Nesso Causale

L'impresa è responsabile **solo per i danni derivanti dalla propria inosservanza** del dovere di diligenza.

In altre parole, la responsabilità scatta se il danno si è verificato perché l'impresa:

- Non ha identificato un rischio grave.
- Ha identificato il rischio, ma non ha adottato le misure di prevenzione o mitigazione adeguate (come la richiesta di piani d'azione correttivi al fornitore).

3. Misure Indirette sulla Catena di Attività

Sebbene non ci sia responsabilità *solidale*, la Direttiva esercita una pressione enorme sulla catena di attività attraverso:

- **Obbligo di Misure Contrattuali:** Le imprese devono includere nelle loro clausole contrattuali con i partner commerciali (in particolare a monte) requisiti che impongano a questi ultimi di garantire il rispetto dei diritti umani e degli standard ambientali (Articolo 10).
- **Supporto alle PMI:** Per evitare che l'onere ricada esclusivamente sui fornitori più piccoli, la Direttiva richiede alle grandi imprese di fornire **supporto tecnico e finanziario** alle loro PMI partner, quando necessario, affinché possano adempiere ai requisiti contrattuali.

Analisi terze parti

Meccanismo di Cessazione: Se gli impatti negativi non possono essere prevenuti o mitigati, l'impresa è obbligata ad astenersi dal contrarre con il partner commerciale o a **cessare il rapporto** (come ultima risorsa)

La Direttiva CSDDD stabilisce che l'impresa principale è responsabile se non controlla o non gestisce correttamente la propria catena di attività, ma non crea un regime di responsabilità solidale automatica con i suoi fornitori per il danno da essi causato.

03

REPUTATIONAL RISK

CASE HISTORY

QUESTI CASI RAPPRESENTANO LE CRITICITA' NELLE QUALI LE AZIENDE POSSONO INCAPPARE PERCHE', NON AVENDO CONTROLLATO I PROPRI FORNITORI, VENGONO COMMISSARIATE OPPURE PERCHE', NON AVENDO CONTROLLATO IL FORNITORE CHE E' SANZIONATO PER AVER AGGIRATO LE RESTRIZIONI, QUESTA PROBLEMATICA RICADE ANCHE SULL'AZIENDA CLIENTE.

PROBLEMATICHE CAPORALATO DA PARTE DI FORNITORI

<https://www.milanotoday.it/cronaca/giorgio-armani-caporalato.html>

https://milano.corriere.it/notizie/cronaca/25_maggio_15/agevola-il-caporalato-degli-opifici-cinesi-il-tribunale-di-milano-mette-sotto-tutela-la-societa-di-valentino-che-fa-le-borse-69101cf7-a16e-4478-860e-f115e498cxlk.shtml

<https://www.ilsole24ore.com/art/alviero-martini-commissariata-il-tribunale-milano-sfruttava-lavoratori-cinesi-AF1KwFNC>

AZIENDE CHE AGGIRANO LE RESTRIZIONI CON CLIENTI O FORNITORI COMPIACENTI

<https://www.linkiesta.it/2025/10/italia-sanzioni-russia-europa/>

PERSONALE AZIENDALE SANZIONATO

<https://www.ilpost.it/2024/08/24/sanzioni-dirigenti-aziende-italiani-stati-uniti-affari-russia/>

04 CYBER SECURITY

Monitoraggio del Dark e Deep Web -Cyber Threat Intelligence

Il monitoraggio del Dark e Deep Web è un'attività cruciale nell'ambito della Cyber Threat Intelligence (CTI), poiché consente di identificare potenziali minacce e vulnerabilità che potrebbero compromettere la sicurezza di un'organizzazione. Servizio che monitora 24 ore su 24 e 7 giorni su 7.

Dark Web Research

Il Dark Web è un ambiente in cui cybercriminali e gruppi di hacker operano in modo anonimo, scambiando informazioni riservate, vendendo dati rubati e pianificando attacchi informatici. Il monitoraggio di questo spazio consente di individuare: Fughe di dati ed Account compromessi.

Monitoraggio del Deep Web

Il Deep Web comprende tutti quei contenuti non indicizzati dai motori di ricerca tradizionali, tra cui database interni, archivi riservati e pagine con accesso limitato. Qui è possibile rilevare: Informazioni sensibili esposte, File riservati e Discussioni su minacce emergenti.

04 CYBER SECURITY

Asset da Monitorare

- **Domini e indirizzi IP**
- **Indirizzi email aziendali**
- **Altri asset sensibili**
- **Elementi Monitorati Aggiuntivi**
 - Carte di credito
 - IBAN (International Bank Account Number)
 - Indirizzi MAC
 - Analisi e identificazione di data breach
 - Monitoraggio di eventuali fughe di dati che possano coinvolgere l'organizzazione

04 CYBER SECURITY

Bonifiche Ambientali/Device

Attraverso un protocollo ben predefinito, un team di tecnici specializzati e mediante apparecchiatura di ultima generazione, forniscono attività di bonifica ambientale in uffici, autovetture, appartamenti, aerei e in tutti i luoghi sensibili ove è possibile carpire informazioni. Attività volta a rintracciare apparecchiature che vengono utilizzate per intercettazioni ambientali. Una volta conclusa l'attività verranno predisposti dei sigilli per future attività di controllo.

Bonifica dei device quali telefonino, computer, stampanti ecc. per rintracciare la presenza di software che vengono installati per rubare informazioni su chat, mail e messaggi. Una volta conclusa l'attività verranno installati dei sistemi di alert utili a proteggere i device.

05 TRAVEL SECURITY

Le quotidiane attività commerciali ed i viaggi internazionali dei dipendenti delle aziende possono essere impegnativi e persino pericolosi nel volatile mondo di oggi.

Fa parte del dovere di diligenza delle organizzazioni proteggere la propria forza lavoro. Ogni azienda deve garantire una corretta gestione aziendale, rispondendo all'ampio obbligo del Duty of Care, dotandosi di un proprio Modello ex D. Lgs. 231/2001 e D.Lgs. 81/08 che menzioni, parallelamente al DVR, la prevenzione dei rischi di security con specifico riferimento alla realtà operativa dell'impresa ed alla sicurezza dei dipendenti anche all'estero.

Attraverso le attività di Travel Risk Analysis e di Travel Management, le aziende possono mitigare qualsiasi rischio correlato ai viaggi al fine di proteggere il personale, i beni, le informazioni, la reputazione e la capacità aziendale. Con partner attentamente selezionati, si riceve assistenza e servizi di sicurezza on ground in un gran numero di paesi, compresi quelli ostili e ad alto rischio.

Si tratta dell'insieme di misure volte a prevenire o scoraggiare l'accesso non autorizzato a locali, risorse o informazioni. I professionisti della security forniscono linee guida su come progettare strutture e procedure per aiutare le aziende a proteggersi da atti ostili.

Risk Assessment

E' l'attività che determina la valutazione quantitativa o qualitativa del rischio associato ad una situazione ben definita e ad una minaccia conosciuta (detta "pericolo"). Al termine di quest'attività vengono analizzati, e nel caso implementati, sistemi di:

- Security Policies
- Controllo accessi
- Video sorveglianza ed antintrusione ecc.

Vengono migliorati o predisposti anche protocolli operativi oltre a pianificare specifiche attività di security.

07 OUR TEAM

Classe 1970 ha maturato esperienza nell'azienda Telejform operante nel settore del Security Management da 55 anni.

Struttura consolidata con partner nei principali paesi del mondo.

CEO e consulente in ambito reputazionale, security, travel security, investigation e cyber di clienti che operano nei settori:

- **food&beverage:** Ferrero, Coca Cola, Lindt e Heineken
- **fashion:** Giorgio Armani
- **industrial:** Pirelli
- **automotive&bike:** Ferrari, Ducati e Iveco
- **finance:** BPM e BCC Brianza Laghi

Ha certificazioni/autorizzazioni di:

- Senior security manager di III livello
- Travel security expert
- Direttore Security Aeroportuale
- Licenza investigativa



**CARMINE
SPATOLISANO**

Founder

GRAZIE

CONTATTI

 +39 348 5855080

 carmine.spatolisano@teleinform.it

