O S I N T

# Tutela degli Asset Strategici Aziendali

## Mappatura, Audit, Risk Analisys, Policy di sedi, complessi produttivi, operativi e commerciali

***L'ANALISI DEL RISCHIO è lo strumento utilizzato dalle aziende per eliminare criticità di sistema in modo da evitare in futuro, incidenti ed inefficienze. Consiste nella valutazione sistematica e nel controllo dei rischi che gravano sulle strutture, l'organizzazione e le procedure a supporto delle decisioni aziendali.***

**RISK ASSESSMENT AZIENDALE** → **MAPPATURA ASSET** → **AUDIT DI SECURITY** → **RISK ANALISYS ASSET**

## FASE 1: ANALISI ASSETS

***Identificazione, catalogazione, analisi e valorizzazione dei beni aziendali (materiali e immateriali). Analisi dei processi aziendali e delle relazioni tra questi e gli utilizzatori.***

- *Inventario degli asset*
- *Esecuzione di sopralluoghi*
- *Pianificazione delle rilevazioni*
- *Analisi delle procedure e delle policy aziendali*
- *Redazione e stesura di Check List*
- *Redazione di Report con le proposte per il contenimento dei costi, l'eventuale correzione delle criticità, la revisione di policy e procedure*
- *Redazione informatizzata dei risultati ottenuti complessivamente e per singolo asset*


## FASE 2: IDENTIFICAZIONE CRITICITÀ

***Identificazione e classificazione delle potenziali cause che possono determinare danni e pericoli al patrimonio soprattutto nelle relazioni tra i soggetti componenti il sistema (persone, strumenti, informazioni, attività).***

### MINACCE ESTERNE

- *Furti*
- *Effrazioni*
- *Sabotaggi*
- *Atti vandalici*
- *Barbonaggio*
- *Attacchi hacker*
- *Attacchi media*
- *Eventi naturali*
- *Incendi*
- *Panico*
- *Calamità*
- *Spionaggio industriale*

### MINACCE INTERNE

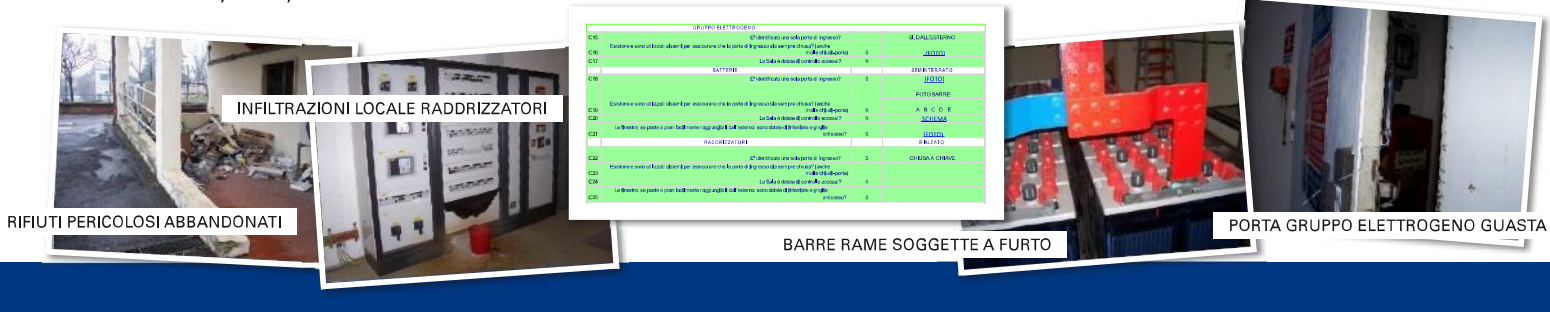
- *Assenteismo*
- *Furti know-how*
- *Furto documenti strategici*
- *Notizie*
- *Infedeltà aziendali*
- *Smaltimento rifiuti*
- *Errori umani*
- *Alimentazione elettrica*
- *Problemi hardware e software*
- *Riciclaggio*

### MINACCE STRUTTURALI

- *Difficoltà di controllo delle realtà locali e contestuale responsabilità dei vertici aziendali*
- *Disomogeneità degli standard di sicurezza*
- *Contenimento dei costi di esercizo*
- *Truffe*
- *Abuso di privilegi*
- *Furto di risorse*
- *Parcellizzazione delle competenze*

GLI ASSET VENGONO ANALIZZATI TRAMITE SCHEDE DI VALUTAZIONE COMPILATE DA NOSTRI PROFESSIONISTI REALIZZATE CON SOPRALLUOGHI E INTERVISTE AL PERSONALE COMPETENTE

LE SCHEDE OFFRONO SIA UNA SINTESI DEGLI ASSET NEL LORO COMPLESSO RIASSUMENDONE LE PRINCIPALI CRITICITA' E LE SPECIFICITA' DEI DIVERSI AMBITI (CONTESTO URBANO, PERIMETRO ESTERNO, SINGOLI EDIFICI, LOCALI PARTICOLARI, ETC.)



# FASE 3: GESTIONE VULNERABILITÀ

***Analisi e classificazione delle criticità e dei livelli di vulnerabilità di ogni asset in relazione alle cause che le hanno determinate. Individuazione delle minacce, del grado di rischio associabile e della loro frequenza di accadimento. Valutazione dei costi indotti dall'esposizione alle suddette minacce.***

**Approfondire l'esame dei fattori critici, delle vulnerabilità, dei possibili punti di forza, del contesto, dei case-history**

**Avere uno strumento di pianificazione e ottimizzare gli investimenti della security**

**Avere standard di sicurezza omogenei e nel contempo interventi mirati alle specifiche realtà**

**Economia di scala sui costi di esercizio della sicurezza**

*Le contromisure esistenti possono non essere adeguate al rischio e quindi essere causa di perdite significative quali la Riservatezza in caso di spionaggio, la Perdita degli Asset in caso di distruzione, la Fiducia in caso di inaffidabilità degli Asset, la Indisponabilità in caso di rifiuto del Servizio.*

- *Analisi della completezza degli ordini generali e delle istruzioni date agli addetti alla sicurezza*
- *Valutazione vulnerabilità, valutazione minaccia, valutazione economica del rischio*
- *aggiornamento e adeguamento delle procedure*
- *Verifica del sistema e delle procedure di controllo accessi*
- *Valutazione vulnerabilità dei Sistemi hardware, software e di comunicazione*
- *Review e assessment dei dispositivi di sicurezza*
- *Procedure di emergenza e simulazioni first aid e antincendio*
- *Livelli di competenza del personale*
- *Sicurezza informatica e dei dati*
- *Antiterrorismo*


DEPOSITI LASCIATI APERTI


BADGE FUORI USO


FINESTRE NON PROTETTE


PERIMETRO SCOPERTO

# FASE 4: GESTIONE DEL RISCHIO

***Valutazione degli impatti e conseguenze che le minacce riscontrate possono avere su sicurezza personale, riservatezza, obblighi di legge e contrattuali, interessi economici e finanziari, produttività, perdita di immagine. Calcolo delle perdite stimate.***

### RISK ASSESSMENT

- *Valutazione adeguatezza delle procedure vigenti rispetto ai contenuti, alle norme Asset*
- *Verifica del rispetto dei processi*
- *Verifica della qualità del servizio atteso, erogato e percepito*
- *Verifica della congruità costi/ efficacia della security*

### MAPPATURE ASSET

- *Valutare lo stato della sicurezza delle infrastrutture*
- *Miglioramento della conoscenza sullo stato della rete infrastrutturale*
- *Acquisire uno strumento di pianificazione per ottimizzare gli investimenti della security*
- *Uniformare gli standard di sicurezza con interventi mirati alle specifiche realtà*

### AUDIT ASSET

- *Individuare fattori di criticità specifici o contestualizzati*
- *Aderenza delle policy e dei protocolli alle normative, ai processi, al contesto e alle tipologie infrastrutturali*
- *Verifica dell'applicazione delle policy e dei protocolli di sicurezza*
- *Proposte di interventi migliorativi*

- *Redazione e/o adeguamento delle procedure per la sicurezza e la gestione del rischio.*
- *Attuazione misure di prevenzione.*
- *Formazione del personale.*
- *Conformità agli standard*


TORNELLI SENZA ANTI-PASSBACK


PORTA SEMPRE APERTA


FURTI ALLE AUTO NEL PARCHEGGIO

# FASE 5: AZIONI CORRETTIVE

***Progettazione delle contromisure alle minacce individuate finalizzate alla riduzione dei rischi, confronto con quelle esistenti, stesura linee guida nelle scelta delle soluzioni da adottare. Determinazione dei costi.***

**Particolare Locale Batterie**
**Criticità:** Il rame presente nei locali batterie è soggetto al fenomeno dei furti con danni incalcolabili all'azienda e forti disagi e disservizi all'utenza.
**Soluzione:** Installazione di videocamere che guardano direttamente i bulloni, la cui posizione viene registrata e controllata da remoto, attraverso un sistema di videosorveglianza attiva e analisi immagine che si attiva istantaneamente, nel momento in cui avviene la violazione.

**Quadro Chiavi**
**Criticità:** La gestione delle chiavi risulta confusa e discrezionale, priva di qualsiasi tipo di marcatura e di controllo, accessibili a chiunque e facili da duplicare.
**Soluzione:** Installazione su ogni porta sensibile degli edifici del Gruppo, di un unico tipo di serratura elettronica con accesso tramite chiave digitale. Si evita in questo modo la loro sostituzione in caso di smarrimento delle chiavi oltre ad attivare un efficace controllo accessi.

**Ingresso Gruppo Elettrogeno**
**Criticità:** La porta del Gruppo Elettrogeno interna all'edifico è guasta, accessibile ad estranei non autorizzati quali le ditte esterne e priva delle procedure di controllo e manutenzione.
**Soluzione:** Riparazione della porta attraverso l'installazione di serratura elettronica antintrusione con accesso controllato tramite chiave digitale, a supporto della videocamera presente nel locale da riparare e riattivare, essendo il sistema di videosorveglianza completamente fuori uso.

**Perimetro Lato Raddrizzatori**
**Criticità:** La telecamera che guarda alla porta dei raddrizzatori utilizza un sistema di videosorveglianza passiva non in grado di rilevare l'evento in tempo reale e quindi di intervenire in modo adeguato.
**Soluzione:** Installazione di un sistema perimetrale di Videosorveglianza Attiva e Analisi Immagine in grado di remotizzare immediatamente le immagini dell'effrazione ad una Centrale Operativa. Questa soluzione riduce drasticamente i costi della vigilanza privata ed elimina la sensoristica antintrusione.

**Sicurezza Informatica**
**Criticità:** Accertata vulnerabilità dei sistemi informatici sottoposti ai pericoli della rete sia sulla riservatezza dati, sul controllo degli accessi logici e fisici e sulla centralizzazione analisi e sicurezza log.
**Soluzione:** Adozione di prodotti in grado di garantire la Riservatezza dei Dati, una serie di dispositivi di riconoscimento ed una piattaforma software che consentono di gestire il Controllo degli Accessi Logici e Fisici, un sistema di Centralizzazione Analisi e Sicurizzazione dei file di Log generati da qualsiasi sistema informatico.

**Smaltimento Rifiuti e Sostanze Pericolose**
**Criticità:** Il retro dell'edificio è adibito a deposito di detriti di ogni genere, privo di controlli circa le eventuali sostanze pericolose e inquinanti presenti, e di procedure per il loro corretto smaltimento.
**Soluzione:** Verifica delle Conformità degli Asset alle normative vigenti in campo ambientale. Procedure informatizzate per la Classificazione e la Gestione dei Rifiuti Industriali. Controllo dei processi di smaltimento dalla raccolta alla consegna dei rifiuti, attraverso l'impiego di sistemi di Indirizzamento e Tracciabilità applicati ai materiali e ai mezzi di trasporto.

# FASE 6: REPORT FINALI

***Supporto alle decisioni. Controllo dei risultati attraverso la verifica del rispetto dei programmi e la verifica della riduzione dei rischi. Determinazione dei ritorni economici e dei risparmi nel breve e lungo termine.***

***Le relazioni si concludono con indicazioni e suggerimenti utili ad affrontare eventuali criticità o per sfruttare al meglio i punti di forza***

***A consuntivo dei lavori si produrranno relazioni, supportate da foto, grafici e tabelle che focalizzeranno la situazione rilevata sia nelle specifiche attività che nel complesso***

***Tutte le relazioni, le schede di audit, le tabelle, i grafici, etc. saranno consegnate sia in forma cartacea che su supporto informatico***

O S I N T

**OSINT centre ltd.**
*HEADQUARTERS*
20-22 Bedford Row - LONDON - UNITED KINDOM - WC1R 4JS
*ITALIAN COMPANY BRANCH*
Via Brunelleschi n. 1 - 50132 Firenze (Italy)
www.osint-ltd.com - info@osint-ltd.com