UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

CORSO DI PERFEZIONAMENTO IN «SECURITY MANAGER»

CORSO DI FORMAZIONE IN «PROFESSIONISTA DELLA SECURITY»

dott. ing. Gianni Andrei

Consulente Professionista in Sicurezza Integrata - Editorialista

Presidente Onorario dell'Associazione Italiana Professionisti della Sicurezza (www.aipros.it)

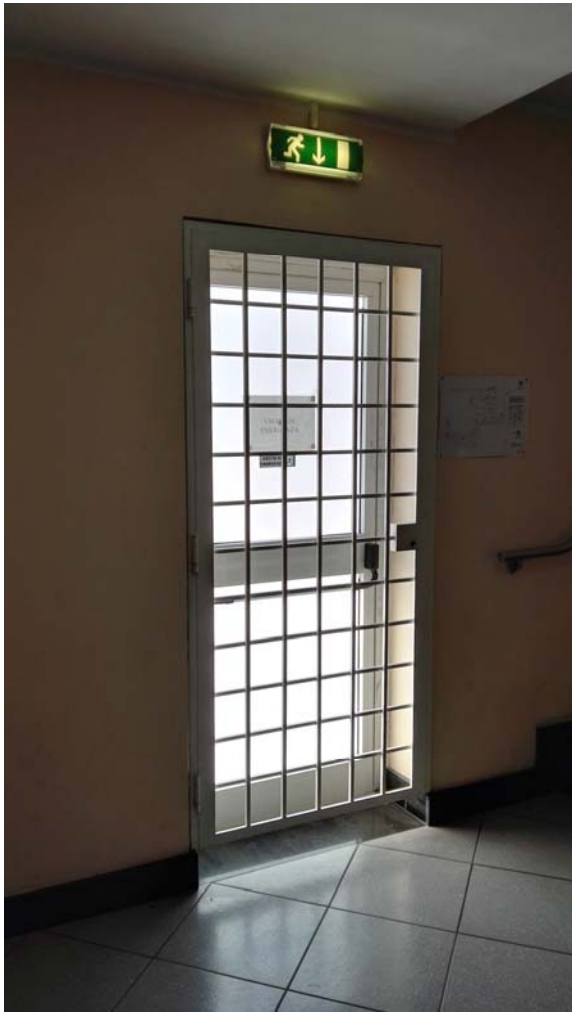
UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

Docente: Gianni Andrei

Modulo: **GOVERNO DELLA SECURITY:**
LA RISPOSTA ORGANIZZATIVA AI RISCHI DI SECURITY

L'analisi delle vulnerabilità

21 gennaio 2022 ***(ore 14.00 – 16.00)***



Uscita di emergenza dalle toilettes di un autogrill della A1

Compartimentazioni antincendio e uscite di emergenza in un supermarket

MADRID

Bombe
alla Stazione Atocha
sui treni
dei pendolari

11 marzo 2004

192 morti

1427 feriti

LONDRA

Attentati terroristici
a trasporti pubblici

7 luglio 2005

52 morti

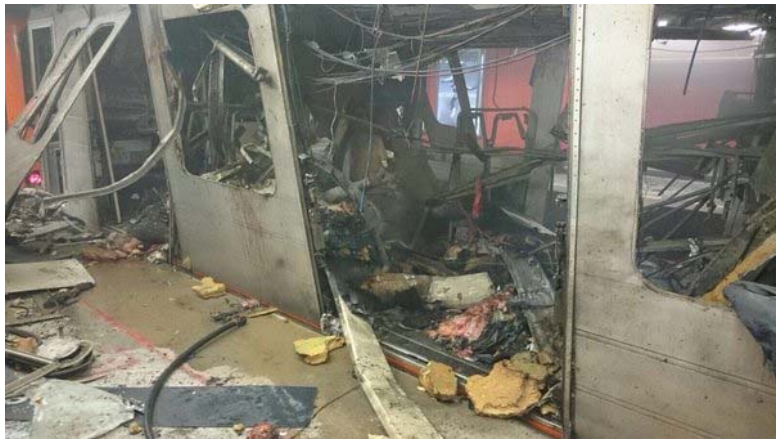
700 feriti

PARIGI: attacchi a luoghi di svago
13-14.11.2015

130 morti - 360 feriti

BRUXELLES: attacchi ad aeroporto e metro
22.03.2016

32 morti - 250 feriti



Indice di rischio: R = F x M

VALUTAZIONE

ACCETTABILITÀ

A prescindere dalla metodologia utilizzata, esistono molti elementi e passaggi del processo di analisi dei rischi comuni a tutte le metodologie:

1. **individuare, classificare e valorizzare i beni da proteggere**
2. **individuare e valutare gli agenti ostili, minacce, vulnerabilità e il rischio**
3. **definire quali minacce vanno fronteggiate e con quali contromisure (tecniche e non)**
4. **calcolare il rischio residuo, valutarne i livelli accettabili e definire le contromisure che permettono di mantenere il rischio entro questi livelli.**

Risk analysis

La risk analysis è dedicata all'identificazione di:

- ✓ beni
- ✓ minacce
- ✓ vulnerabilità
- ✓ impatto
- ✓ controlli in atto.

Un bene (asset) è una qualunque cosa che abbia valore per l'organizzazione e che quindi richieda protezione (non solo beni tangibili).

Risk analysis: Elementi essenziali

Gli elementi essenziali relativi ai beni sono:

- le **attività e processi aziendali**

- le **informazioni**.

Ad esempio, le informazioni sono funzioni la cui perdita o degrado impediscono o compromettono il raggiungimento degli obiettivi, funzioni che contengono segreti industriali, informazioni coperte dal segreto di Stato, informazioni vitali per il raggiungimento degli obiettivi, informazioni sensibili (ad es. dati personali), informazioni strategiche, informazioni "costose".

Risk analysis: Elementi di supporto

Sono costituiti da:

- hardware (computer fissi e portatili, server, stampanti, supporti rimuovibili)
- software (sistemi operativi, applicativi generici, applicativi business standard o specifici)
- reti (supporti, dispositivi, interfacce)
- personale (managers, utenti, operatori, sviluppatori)
- sede (edifici dell'azienda o di terzi, linee telefoniche, impianti, forniture di servizi).

Il rischio è più specificatamente espresso nell'equazione

$$R = P \times V \times E$$

dove:

P = ***Pericolosità***: è la probabilità che un fenomeno di determinata intensità si verifichi in un certo intervallo di tempo e in una data area;

V = ***Vulnerabilità***: è la propensione di un elemento (persone, edifici, infrastrutture, attività economiche) a subire danni in conseguenza di sollecitazioni indotte da un evento di una certa intensità;

E = ***Esposizione o Valore esposto***: è il numero di unità, o "valore", di ognuno degli elementi a rischio, come vite umane o case, presenti in una data area.

Identificazione delle vulnerabilità

Una vulnerabilità è una debolezza
che può essere sfruttata da una minaccia
per compromettere o danneggiare un bene.

Una vulnerabilità costituisce un rischio
solo se al sistema si applica
una minaccia in grado di sfruttarla.

La RESILIENZA

E' la forza delle persone che, nonostante siano state ferite, si considerano non vittime ma utilizzatori delle proprie risorse e si preparano a recuperare le risorse necessarie per affrontare il futuro con speranza progettuale.

Resilienza (dal latino "**resilire**", rimbalzare) è l'abilità di superare le avversità, di affrontare i fattori di rischio, di rialzarsi dopo più forti e più ingegnosi di prima: è l'abilità di superare le ingiustizie della vita senza soccombere.

La RESILIENZA

In *ingegneria*, la resilienza è la capacità di un materiale di assorbire energia di deformazione elastica

Nel *risk management*, la resilienza è la capacità intrinseca di un sistema di modificare il proprio funzionamento prima, durante e in seguito ad un cambiamento o ad una perturbazione, in modo da poter continuare le operazioni necessarie sia in condizioni previste che in condizioni impreviste.

La RESILIENZA

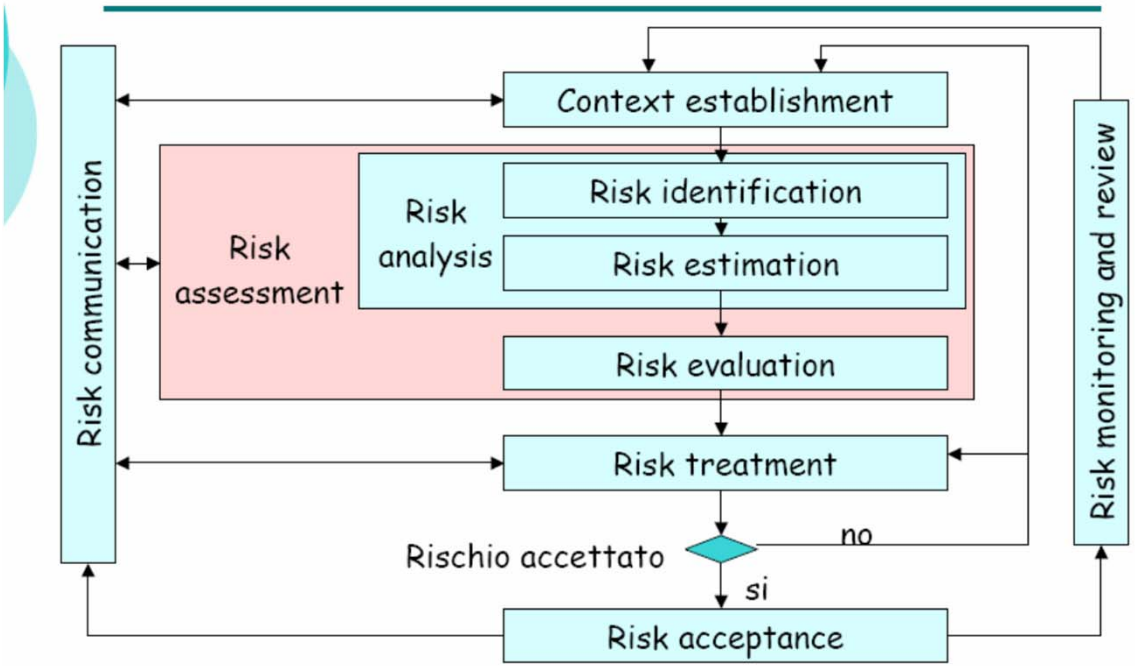
Secondo me … la resilienza è:

vedere e vivere i cambiamenti o esperienze negative come sfida e opportunità per migliorare sé stessi, per migliorare l'ambiente dove si vive, dove si condividono lavoro, attività sociale e svago, per migliorare il sistema circostante (sodalizio, comunità, ecc.) …

… applicando il Ciclo di Deming

Risk assessment :

identificazione, quantificazione, graduazione dei rischi secondo criteri e obiettivi stabiliti dall'organizzazione.



Passiamo ora ad esaminare e ad individuare le
potenziali minacce.

Una minaccia è una potenziale causa di incidente che potrebbe danneggiare un sistema o un'organizzazione.

Una minaccia può essere di origine naturale o umana, e può essere accidentale o intenzionale.

Alla luce delle caratteristiche del sito
da studiare e da proteggere, è necessario

analizzare e quantificare

le seguenti variabili:

1. possibili accadimenti naturali o accidentali
2. possibili azioni eversive e/o terroristiche
3. tipologie di sabotaggio o attacco esterno ipotizzabili
4. identificazione dei possibili bersagli
5. valutazione della probabilità di successo dell'attacco
6. conseguenze ed effetti

Possibili accadimenti naturali o accidentali

- ✓ Incendi - Esplosioni
- ✓ Terremoto – frane
- ✓ Allagamenti
- ✓ Interruzione alimentazione elettrica / termica
- ✓ Interruzione funzionamento delle reti
- ✓ Guasti tecnici
- ✓ ……

Possibili azioni eversive e/o terroristiche

- Incendi - Esplosioni
- Manomissioni - Sabotaggi
- Furti – Rapine (di beni e documenti)
- Atti vandalici
- Atti dimostrativi
- Atti terroristici

Tipologie di sabotaggio o attacco esterno ipotizzabili

- Manomissione impianti
- Sabotaggio impianti
- Blackout elettrico-termico-informatico
- Incendio / allagamento
- Attacco informatico (specialmente da esterno)
- Inquinamento aria/acqua
- Lancio di oggetti incendiari o esplosivi
- Posizionamento di oggetti incendiari o esplosivi
- Accesso non autorizzato (anche in aree riservate)
- Intrusione (da varco carraio o con effrazione perimetrale)
- .....

MOTIVAZIONI

di azioni eversive e/o terroristiche

- sfida di un hacker
- spionaggio industriale
- vendetta di ex-dipendente
- infedeltà di un dipendente
- azione di criminalità comune
- terrorismo
- ……

Identificazione dei possibili bersagli

- Laboratori di ricerca o produzione
- Magazzini materie grezze o prodotti finiti
- Sala operativa tecnologica
- Sala operativa di sicurezza e di emergenza
- C.E.D. e/o Disaster Recovery (dati info)
- Centrali termica, idrica / sottostazione elettrica
- Centrale telefonica
- Ufficio e archivi del Personale
- Uffici Management
- ……..

Valutazione
della probabilità di successo dell'attacco

- ❑ Altissima (9-10)
- ❑ Alta (7-8)
- ❑ Media (5-6)
- ❑ Bassa (3-4)
- ❑ Bassissima (1-2)

Conseguenze ed effetti dell'attacco
(relativamente all'azienda)

- distruzione totale
- distruzione parziale
- blocco totale delle attività
- blocco parziale delle attività
- rallentamento dell'attività
- perdita di dati e/o di know-how
- danno all'immagine aziendale
- ……

Elementi da considerare per la valutazione delle conseguenze di un attacco

a) aspetti di riservatezza, integrità, disponibilità

b) eventuali dipendenze tra i beni

c) impatto di un incidente di sicurezza su ognuno dei beni

(*diretto*: costo economico della sostituzione del bene e dell'interruzione del servizio – *indiretto*: con un potenziale uso malevolo delle informazioni, con violazioni di leggi o obblighi e con violazioni di codici di condotta)

d) la probabilità che ogni minaccia venga attuata sulla base di:

- frequenza della minaccia
- motivazione, capacità, risorse necessarie
- fattori geografici o ambientali.

Una metodologia applicativa
di analisi e valutazione delle variabili
per atti dolosi su un impianto industriale

a) **EVENTO**: manomissione, sabotaggio, intrusione, scoppio di ordigno, attacco armato.

b) **TIPOLOGIA DELL'EVENTO**: intrusione con dolo o con effrazione, posizionamento o lancio di ordigni esplosivi; attacco con armi convenzionali da parte di una o più persone (è qui da valutare l'eventualità che queste azioni possano essere messe in atto o semplicemente favorite da persone "interne" al luogo lavorativo)

c) **SCOPI E FINALITA'**: atto dimostrativo; danneggiamento; furto, anche di materiale pericoloso (ad es. chimico o radioattivo); ricatto; distruzione parziale o totale di impianti.

d) **MOVENTE:** vandalismo; delinquenza comune o organizzata; ideologia politica e terrorismo.

Una metodologia applicativa
di analisi e valutazione delle variabili
per atti dolosi su un impianto industriale

e) MEZZI IMPIEGATI: palesi (ad es. effrazione, anche con armi o bombe); occulti (per es. sabotaggio o manomissione, anche da parte di persone autorizzate ad accedere in zone sensibili dell'azienda o dell'impianto).

f) NUMERO DEGLI ASSALITORI: è da prendere in considerazione relativamente al numero degli uomini da impiegare nella difesa ed al livello di risposta che si vuole opporre.

g) TIPOLOGIA DELL'ASSALITORE O ATTENTATORE: delinquente comune; terrorista (e qui è da distinguere se si tratti di un ideologo fanatico, magari votato alla morte, o di un mercenario, forse meno determinato al sacrificio ma senz'altro dotato di maggior professionalità).

h) TRAGITTO PER RAGGIUNGERE L'OBIETTIVO: è questo un parametro ipotizzabile e quindi definibile e gestibile dal progettista e dal coordinatore dell'organizzazione di security.

Un metodo di calcolo dell'integrazione "uomo – sistema"

- **OBIETTIVO del metodo**: ricavare la percentuale di intercettazione di un intrusore prima che giunga sull'obiettivo, difeso dai sistemi di protezione fisica e dall'organizzazione di sicurezza esistente
- T_v = tempo del personale di Vigilanza per intervenire e bloccare l'intrusore (da valutare come *termine noto*; è, quindi un DATO DI PARTENZA)
- T_i = tempo occorrente all'intrusore per arrivare all'obiettivo

Condizione fondamentale: $T_v \leq T_i$

Un metodo di calcolo dell'integrazione "uomo – sistema"

Condizionamenti di T_v :

- Affidabilità dei sistemi antiintrusione (ostacoli passivi e segnalazioni di allarme)
- Prontezza delle reazioni (dei sistemi e della Vigilanza)
- Efficienza dei mezzi a disposizione per intervenire
- Efficacia e professionalità nell'intervento

Conseguenza dell'applicazione del metodo:

valutazione dei costi e dei benefici dell'intera organizzazione di security (sistemi di P.F. e servizio di vigilanza)

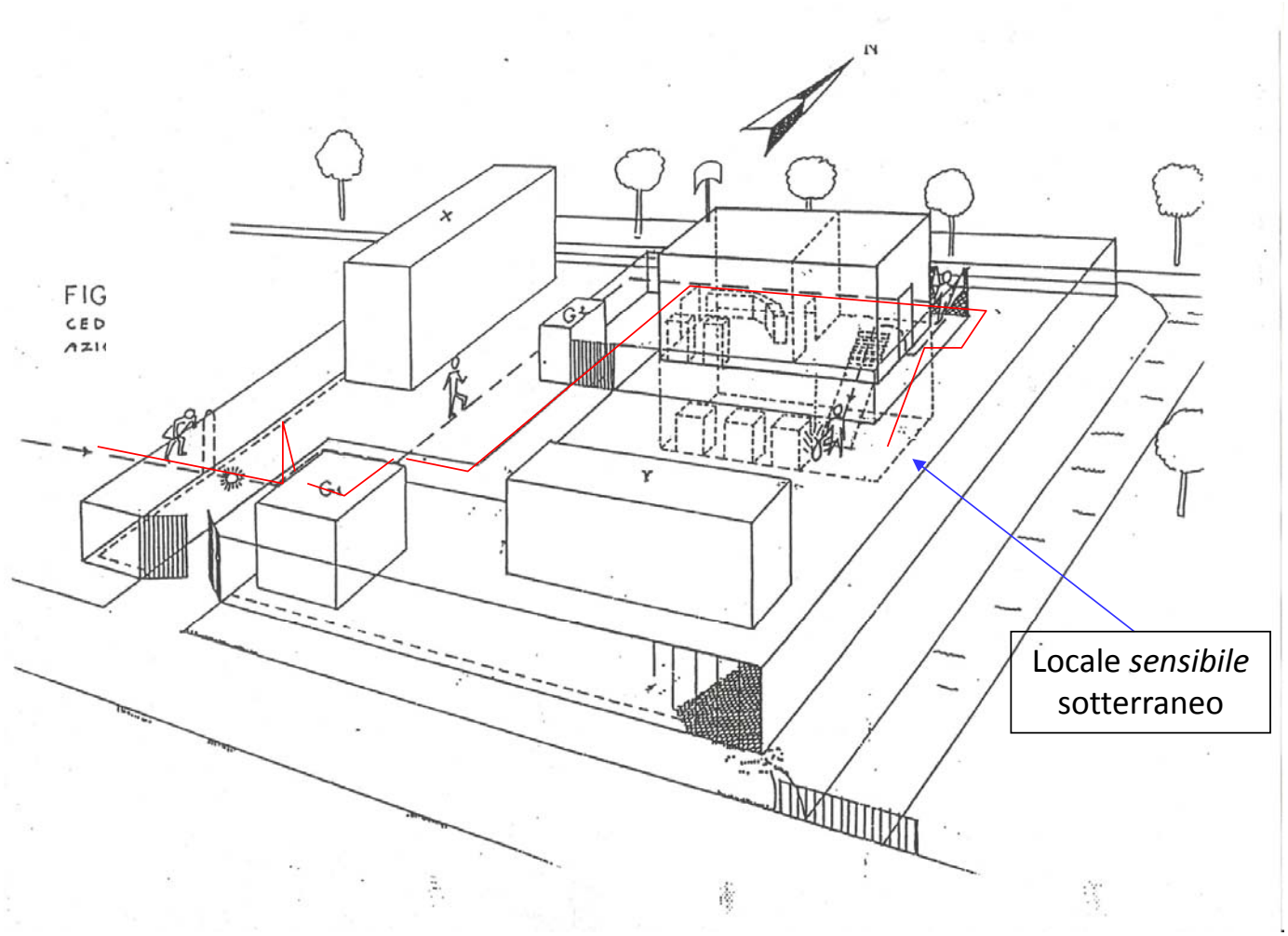


FIG
CED
AZI
X
Y
G
G
Locale *sensibile* sotterraneo

Organizzazione di sicurezza aziendale

- sistemi tecnici di protezione e prevenzione

- personale addetto alla vigilanza e all'intervento

- procedure operative e piano di emergenza

MISURE disponibili o da incrementare

- di carattere tecnico:
  - sistemi di rilevamento e segnalazione allarmi
  - sistemi di protezione fisica e antincendio
  - sistemi di TVCC e controllo accessi
  - sala operativa e di emergenza
  - sistemi di comunicazione audio
  - compartimentazioni e luoghi sicuri
  - porte e vetrature di sicurezza
  - vie di fuga – scale, porte ed uscite di emergenza
  - alimentazione elettrica e illuminazione di sicurezza.

MISURE disponibili o da incrementare

- di carattere organizzativo:

  - piano e procedure di intervento e di emergenza
  - organizzazione di primo soccorso e di intervento
  - sala operativa
  - procedure di comunicazione dello stato di emergenza
  - gestione dello stato di emergenza
  - coinvolgimento delle Forze esterne
  - gestione dello sfollamento e dell'evacuazione
  - gestione della continuità operativa.

MISURE disponibili o da incrementare

- **di carattere formativo:**
  - corsi di informazione e formazione
  - addestramento
  - esercitazioni

CASE STUDY

Azienda farmaceutica,

con 500 addetti, ubicata in zona industriale, periferica a centro abitato e vicina a ferrovia e autostrada, con reparti e laboratori di

- ricerca e sviluppo
- detenzione e manipolazione sostanze chimiche
- produzione e confezionamento
- immagazzinamento e spedizione prodotti finiti

Azienda farmaceutica, con 500 addetti,

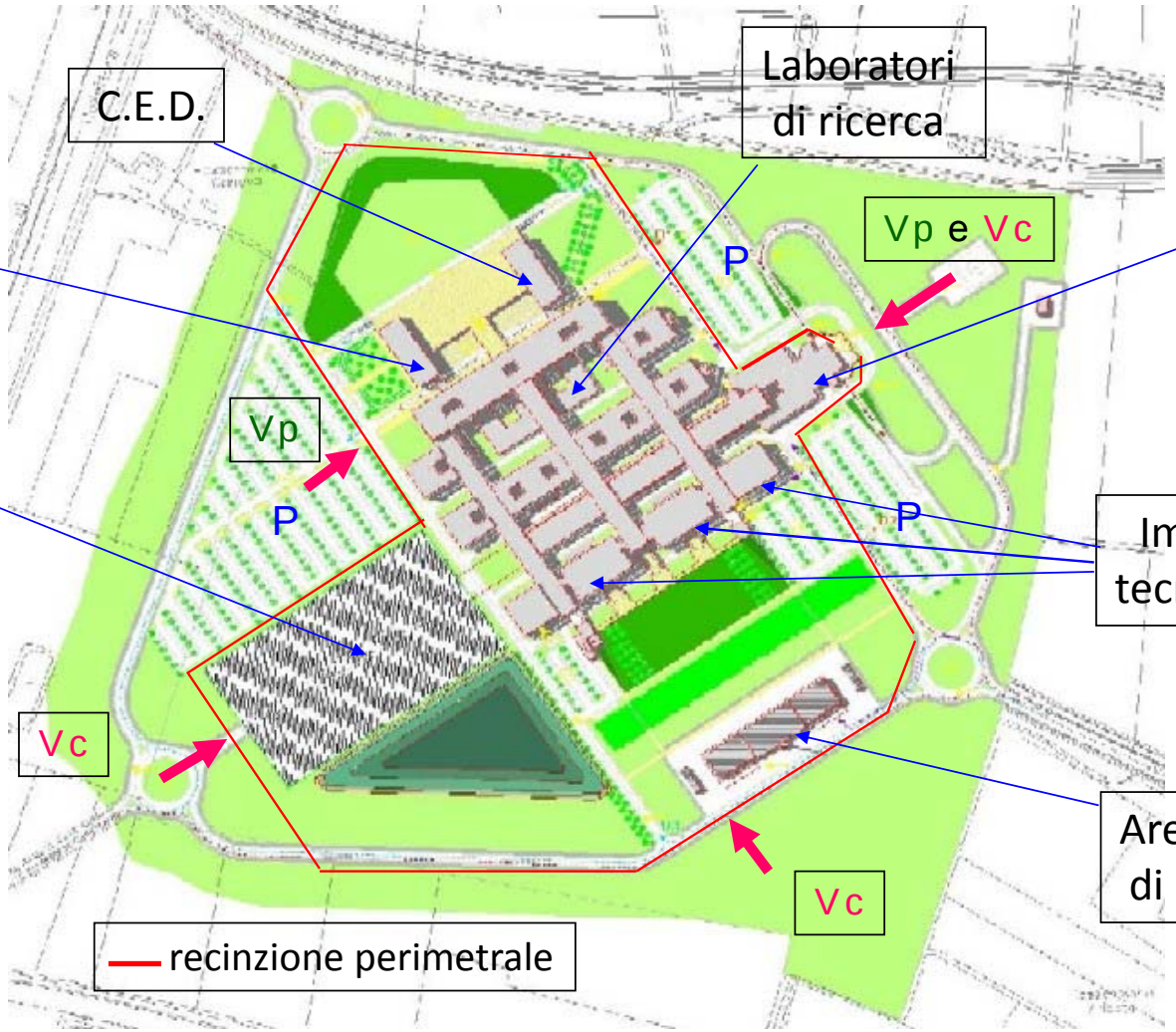
ubicata in zona industriale, periferica a centro abitato e vicina

a ferrovia e autostrada, con reparti e laboratori, difesa da:

- recinzione perimetrale con sistema di videosorveglianza
- Servizio Vigilanza 24h24 (c/o portineria, varco principale, sala operativa)
- sala operativa con unità di acquisizione allarmi e consolle TVCC
- sistema di controllo accessi all'azienda (non ad aree interne)
- impianti volumetrici e antincendio in laboratori, magazzini e archivi
- piano di intervento e di emergenza

Effettuare analisi e studio di sistemi e tecnologie, risorse umane disponibili e/o necessarie, percorsi di formazione e addestramento degli addetti, postazioni tecniche-operative, procedure, volti alla pianificazione dell'organizzazione aziendale di Security.

Individuare e valutare la vulnerabilità del sito produttivo e proporre qualitativamente le eventuali integrazioni alle soluzioni organizzative, tecniche e procedurali già in atto.



Vp: varco pedonale

Vc: varco carraio

P: parcheggi

UNIVERSITA DEGLI STUDI DI ROMA «TOR VERGATA»
CORSI SECURITY MANAGEMENT

dott. ing. Gianni Andrei

Consulente Professionista in Sicurezza Integrata - Editorialista

Presidente Onorario

dell'Associazione Italiana Professionisti della Sicurezza

(www.aipros.it)

ing.gandrei@gmail.com