Laboratorio 4.1 – Creazione di un registro dei rischi

1. Panoramica del laboratorio

1.1 Descrizione del laboratorio

In questo laboratorio imparerai come creare e mantenere un **registro dei rischi**, uno strumento fondamentale nella governance della sicurezza informatica e nella gestione dei rischi. A differenza dei laboratori tecnici incentrati sugli strumenti di sistema o di rete, questo esercizio pone l'accento **sull'analisi, sulla documentazione strutturata e sul pensiero strategico**.

Catturerai i rischi in un formato strutturato, ne valuterai la probabilità e l'impatto, assegnerai la responsabilità e li renderai **visibili e gestibili**. Alla fine, avrai il tuo registro dei rischi funzionante, un documento che le organizzazioni utilizzano quotidianamente per guidare le decisioni e rafforzare le difese.

1.2 Obiettivi di apprendimento

Dopo aver completato questo laboratorio, sarete in grado di:

- Definire cos'è un registro dei rischi e spiegarne lo scopo.
- Identificare i **componenti chiave** di un registro dei rischi (descrizione del rischio, probabilità, impatto, punteggio, proprietario, stato).
- Tradurre una minaccia reale in una voce di rischio strutturata.
- Applicare un **modello di punteggio di rischio** (impatto × probabilità).
- Creare voci di rischio sia tecniche che umane/politiche.
- Comprendere in che modo i registri dei rischi supportano **le decisioni strategiche in materia di sicurezza**.

1.3 Prerequisiti

Prima di iniziare questo laboratorio, è necessario:

- Una conoscenza di base delle **minacce, delle vulnerabilità e dei rischi** (acquisita nei moduli precedenti).
- Familiarità con **le scale di impatto e probabilità del rischio** (Basso, Medio, Alto).

- Un foglio di calcolo (Excel, Google Sheets o LibreOffice Calc) o una semplice tabella in Word/Docs.
- Un quaderno (digitale o cartaceo) per le domande di riflessione.

1.4 Tempo stimato per il completamento

Attività	**Tempo stimato**
Introduzione C contesto	30 minuti
Revisione delle componenti chiave del registro dei rischi	45 minuti
Esempio dettagliato (rischio di phishing)	30 minuti
Sfida: creare 2 voci di esempio	60 minuti
Uso strategico Discussione C	30 minuti
Riflessione C - Conclusione	15 minuti
Tempo totale stimato	**~3,5–4 ore**

Punto di controllo
Prima di proseguire, assicurati di:

- Hai a disposizione un foglio di calcolo.
- Comprendere le nozioni di base relative a rischi, minacce e vulnerabilità.
- Sappiate che creerete **almeno due voci di rischio** (tecnico + umano/politico).
- È possibile dedicare circa **3,5-4 ore** a questo laboratorio.

2. Per iniziare

2.1 Che cos'è un registro dei rischi?

Un **registro dei rischi** è un documento strutturato (spesso un foglio di calcolo o un database) che registra, tiene traccia e gestisce i rischi per la sicurezza.

Ogni voce del registro rappresenta un rischio specifico e contiene informazioni quali:

- Qual è il rischio (descrizione)
- Cosa lo causa (minacce + vulnerabilità)
- Quanto è probabile che si verifichi (probabilità)
- Quanto sarebbe dannoso se accadesse (impatto)
- Come viene gestito (mitigazione, stato, responsabile)

Considerate il registro dei rischi come la vostra **"torre di controllo"** per il monitoraggio dei rischi: vi offre un quadro completo del panorama dei rischi della vostra organizzazione.

2.2 Perché i registri dei rischi sono importanti nella sicurezza informatica

I registri dei rischi sono più che semplici documenti: sono **strumenti strategici**. Un registro ben tenuto aiuta le organizzazioni a:

- **Dare priorità alle azioni** → I problemi ad alto rischio vengono risolti per primi.
- **Supportare il processo decisionale** → La leadership vede quali rischi sono critici.
- **Monitorare i cambiamenti nel tempo** → Controllare se i rischi stanno aumentando, diminuendo o sono stati mitigati.
- **Fornire prove per gli audit e la conformità** → Dimostrare un approccio strutturato alla gestione dei rischi.

2.3 Lista di controllo per la configurazione del laboratorio

Prima di iniziare, assicurati di avere:

Un foglio di calcolo (Excel, Google Sheets o LibreOffice Calc).
Un modello di registro dei rischi vuoto (oppure crea una tabella con le colonne necessarie).

Esempi di rischi che desideri documentare (tecnici, umani o politici).
Note di riferimento dai moduli precedenti (minacce, vulnerabilità, valutazione dei rischi).

Facoltativo: se si lavora in gruppo o in classe, prepararsi a **confrontare le voci relative ai rischi**: spesso questo rivela prospettive diverse sullo stesso rischio.

Punto di controllo
Prima di proseguire:

- Capisci cos'è un registro dei rischi e perché è importante?
- Hai un foglio di calcolo o una tabella pronti per registrare i rischi?
- Hai rivisto i tuoi appunti su minacce, vulnerabilità e valutazione dei rischi?

3. Componenti chiave di un registro dei rischi

3.1 Colonne principali

Un registro dei rischi di base può variare in termini di complessità, ma la maggior parte include le seguenti colonne:

1. **Descrizione del rischio** → Una chiara descrizione del rischio (ad esempio, "Il sistema operativo non aggiornato potrebbe essere vulnerabile").
2. **Risorsa interessata** → Il sistema, i dati o il processo a rischio (ad esempio, "Server finanziario").
3. **Fonte della minaccia** → Chi o cosa potrebbe causare il rischio (ad esempio, "Attaccante esterno", "Uso improprio da parte di personale interno").
4. **Vulnerabilità** → La debolezza che rende possibile la minaccia (ad esempio, "Software non aggiornato").
5. **Probabilità** → Quanto è probabile che il rischio si verifichi (ad esempio, bassa, media, alta).
6. **Impatto** → Le potenziali conseguenze se il rischio si verifica (ad esempio, basso, medio, alto).
7. **Punteggio di rischio** → Un punteggio numerico o qualitativo (spesso calcolato come **Impatto × Probabilità**).
8. **Strategia di mitigazione** → Cosa fare per ridurre il rischio (ad esempio, "Applicare patch al sistema mensilmente").
9. **Responsabile del rischio** → La persona/il team responsabile della gestione del rischio.
10. **Stato** → Lo stato attuale (ad esempio, Aperto, In corso, Mitigato, Accettato).

3.2 Come funziona il punteggio di rischio

Il punteggio di rischio aiuta a stabilire la priorità dei rischi da affrontare per primi.

- **Modello qualitativo** (comune nei registri più piccoli):
    - Probabilità e impatto classificati come **Basso, Medio, Alto**.
    - Combinare i due modelli per classificare il rischio (ad esempio, "Critico", "Moderato", "Basso").
- **Modello quantitativo** (più avanzato):

- Assegnare valori numerici (ad esempio, Basso = 1, Medio = 2, Alto = 3).
- Calcolare il punteggio di rischio = Probabilità × Impatto.
- Esempio: Probabilità = 3 (Alta), Impatto = 2 (Medio) → Punteggio = 6.

Anche un metodo di punteggio semplice è utile, perché costringe a **confrontare i rischi in modo sistematico** piuttosto che soggettivo.

3.3 Riepilogo: trasformare i dati di rischio in campi utilizzabili

Colonna	**Scopo**
Descrizione del rischio	Definisce chiaramente il rischio
Risorse interessate	Mostra cosa potrebbe essere danneggiato
Fonte della minaccia	Identifica l'attore/la causa
Vulnerabilità	Spiega la debolezza sfruttata
Probabilità	Valuta la probabilità che l'evento si verifichi
Impatto	Valuta la gravità delle conseguenze
Punteggio di rischio	Assegna una priorità oggettiva ai rischi
Strategia di mitigazione	Definisce le difese pianificate
Responsabile del rischio	Assegna la responsabilità.
Stato	Tiene traccia dei progressi

Punto di controllo
Prima di proseguire:

- Comprendi il significato di ciascuna colonna nel registro dei rischi?
- Sai spiegare come la probabilità e l'impatto si combinano per formare un punteggio di rischio?
- Ti senti pronto a provare a compilare la tua prima voce?

4. Esempio di voce – Rischio di phishing

4.1 Procedura dettagliata: rischio di attacchi di phishing

Creiamo un esempio di voce relativa a un rischio comune per le organizzazioni: **i dipendenti che cadono vittime delle e-mail di phishing**.

Colonna	**Esempio**
Descrizione del rischio	I dipendenti potrebbero cliccare su link dannosi contenuti nelle e-mail di phishing.
Risorse interessate	Credenziali aziendali e account e-mail.
Fonte della minaccia	Attaccanti esterni che inviano campagne di phishing.
Vulnerabilità	Mancanza di consapevolezza da parte degli utenti e filtraggio delle e-mail insufficiente.
Probabilità	Elevata
Impatto	Elevato
Punteggio di rischio	Critico (alto × alto)
Strategia di mitigazione	Condurre corsi di formazione sulla sicurezza + implementare test di phishing simulati.
Responsabile del rischio	Team di sensibilizzazione alla sicurezza
Stato	In corso

4.2 Perché questo esempio è importante

- **Rischio comune** → Il phishing rimane uno dei principali metodi utilizzati dagli hacker per compromettere le organizzazioni.
- **Fattore umano** → Dimostra come le persone possano essere sia la difesa più forte che l'anello più debole.
- **Mitigazione attuabile** → La formazione e le simulazioni sono misure pratiche che riducono questo rischio.

- **Responsabilità assegnata** → I rischi vengono monitorati fino a quando qualcuno si assume la responsabilità di risolverli.

4.3 Riepilogo: come strutturare la propria voce

Quando si creano le proprie voci di rischio:

1. Inizia con una **descrizione chiara** (evita termini vaghi come "scarsa sicurezza").
2. Collegate il rischio a una **risorsa, una minaccia e una vulnerabilità**.
3. Valuta **la probabilità e l'impatto** in modo coerente (usa Basso/Medio/Alto o numeri).
4. Calcolare un **punteggio di rischio** per stabilire le priorità.
5. Definire una **strategia di mitigazione reale**, non limitarsi a "risolvere il problema in un secondo momento".
6. Assegnare un **responsabile del rischio** per chiarire le responsabilità.

Punto di controllo

Prima di proseguire:

- Siete in grado di spiegare perché il phishing è classificato come "Alta probabilità, Alto impatto"?
- Capisci come la mitigazione affronti direttamente la vulnerabilità?
- Sei pronto a creare le tue voci nel registro dei rischi?

5. Sfida di laboratorio: crea le tue voci

5.1 Crea una voce relativa al rischio tecnico

Il tuo primo compito è identificare e registrare un **rischio tecnico**. Alcuni esempi:

- Un **sistema non aggiornato** vulnerabile a exploit noti.
- **Una porta di rete aperta** accessibile da Internet.
- **Una regola firewall configurata in modo errato** che

espone i servizi. Per il rischio scelto, compilare tutti i campi:

Colonna	**La tua voce**
Descrizione del rischio	…
Risorsa interessata	…
Fonte della minaccia	…
Vulnerabilità	…
Probabilità	…
Impatto	…
Punteggio di rischio	…
Strategia di mitigazione	…
Responsabile del rischio	…
Stato	…

5.2 Creare una voce relativa al rischio umano o politico

Successivamente, crea un **rischio non tecnico** relativo a persone, processi o politiche. Alcuni esempi includono:

- **Uso di password deboli** da parte dei dipendenti.

- **Accesso condiviso** tra più membri del personale.
- **Mancanza di un processo di onboarding/offboarding** per la gestione degli

account. Utilizza la stessa struttura:

Colonna	**La tua voce**
Descrizione del rischio	…
Risorsa interessata	…
Fonte della minaccia	…
Vulnerabilità	…
Probabilità	…
Impatto	…
Punteggio di rischio	…
Strategia di mitigazione	…
Responsabile del rischio	…
Stato	…

5.3 Domande di riflessione

Dopo aver completato le voci, rifletti su quanto segue:

1. Quale rischio hai valutato come più critico: quello tecnico o quello umano/politico? Perché?
2. Hai trovato più facile descrivere **l'aspetto tecnico** (vulnerabilità, risorse) o **quello umano/politico** (processi, comportamenti)?
3. Se dovessi **presentare i tuoi risultati alla dirigenza**, come spiegheresti perché questi rischi meritano attenzione?
4. Quali azioni potresti intraprendere nei prossimi 30 giorni per ridurre uno di questi rischi?

Punto di controllo
Prima di proseguire:

- Hai creato almeno **due voci di rischio complete**?
- Hai assegnato valori **di probabilità e impatto** in modo coerente?
- Hai incluso una **chiara strategia di mitigazione** per ciascun rischio?
- Hai identificato un **responsabile del rischio** (anche se ipotetico)?

6. Utilizzo dei registri dei rischi per le decisioni strategiche

6.1 Dare priorità ai rischi elevati rispetto a quelli bassi

Un registro dei rischi non serve solo a elencare i rischi, ma anche a **stabilire le priorità d'azione**.

- **Gli elementi ad alto rischio** (alta probabilità + alto impatto) devono essere affrontati per primi.
- **Gli elementi a medio rischio** potrebbero richiedere un monitoraggio o una mitigazione parziale.
- **Gli elementi a basso rischio** potrebbero essere accettabili e documentati come "rischi accettati".

Ciò impedisce ai team di "inseguire ogni problema" e consente invece di concentrare gli sforzi dove è più importante.

6.2 Monitoraggio del rischio nel tempo

I rischi non sono statici. Nuove vulnerabilità compaiono, le minacce si evolvono e le misure di mitigazione riducono i livelli di rischio. Un registro dei rischi ti aiuta a:

- Aggiornare **lo stato** (Aperto → In corso → Mitigato/Accettato).
- Registrare quando i rischi sono stati registrati per la prima volta e quando sono stati aggiornati.
- Individuare le tendenze, ad esempio se il phishing sta diminuendo dopo la formazione o se i sistemi senza patch rimangono persistenti.

6.3 Segnalazione dei rischi alla dirigenza

I dirigenti e i manager raramente vogliono vedere i dettagli tecnici grezzi, ma sono molto interessati **alle sintesi dei rischi**.
Un registro dei rischi consente di:

- Mostra i **5 rischi critici principali** in un linguaggio semplice.
- Dimostrare i progressi compiuti indicando i rischi che sono passati da "critici" a "medi".
- Fornire prove che i rischi sono **stati identificati e sono oggetto di gestione**.

6.4 Supporto alla conformità e all'audit

I registri dei rischi sono fondamentali anche per i quadri normativi quali:

- **ISO 27001** (Sistemi di gestione della sicurezza delle informazioni)
- **Quadro di riferimento per la sicurezza informatica del NIST**
- **GDPR** (per i rischi relativi alla protezione dei dati)

Gli auditor spesso richiedono di visionare un registro dei rischi perché:

- Dimostra che i rischi sono **documentati** e **monitorati attivamente**.
- Dimostra che l'organizzazione non sta ignorando le minacce note.
- Collega i rischi alla mitigazione e alla responsabilità.

Punto di controllo

Prima di proseguire:

- Siete in grado di spiegare in che modo un registro dei rischi aiuta a stabilire le priorità delle azioni di sicurezza?
- Capisci come i registri dei rischi supportano la rendicontazione e la conformità?
- Hai aggiornato le tue voci con **lo stato** e **la titolarità** in modo che riflettano i progressi reali?

7. Conclusione

7.1 Punti chiave

In questo laboratorio hai:
Imparato cos'è un **registro dei rischi** e perché è importante.
Esplorato i **componenti principali** (descrizione, risorsa, minaccia, vulnerabilità, probabilità, impatto, punteggio, proprietario, stato).
Abbiamo esaminato un **esempio di phishing** per capire come sono strutturati i rischi. Abbiamo creato **le vostre voci di rischio** (tecniche + umane/politiche).
Comprensione di come i registri dei rischi supportano **la definizione delle priorità, il monitoraggio, la rendicontazione e la conformità**.

7.2 Competenze acquisite

Completando questo laboratorio, ora hai acquisito esperienza pratica in:

- Traduzione di minacce e vulnerabilità in voci di rischio strutturate.
- Applicazione **del punteggio di probabilità × impatto** per assegnare priorità ai rischi.
- Assegnazione della responsabilità e monitoraggio dello stato dei rischi.
- Utilizzo dei registri dei rischi come **strumenti strategici**, non solo come documentazione.

7.3 Prossimo passo: Quiz finale del Modulo 4

Sei giunto alla fine del **Modulo 4: Gestione dei rischi e politiche di sicurezza**. Ora dovrai sostenere il **quiz finale del Modulo 4**, che verificherà le tue conoscenze su:

- Concetti di rischio (minacce, vulnerabilità, risorse, controlli).
- Il ruolo della governance e delle politiche nella sicurezza informatica.
- L'uso pratico di un **registro dei rischi**.

Verifica finale
Prima di iniziare il quiz:

- Hai salvato almeno due voci complete relative ai rischi nel tuo registro?
- Sai spiegare come si calcola un punteggio di rischio?
- Sai descrivere in che modo un registro dei rischi supporta la strategia di

sicurezza? Se sì, sei pronto per il quiz!

8. Appendice

8.1 Modello di registro dei rischi (layout foglio di calcolo)

ID rischio	Descrizione del rischio	Risorsa Interessata	Fonte della minaccia	Probabilità di vulnerabilità	Impatto	Rischi Punteggio	Strategia di mitigazione	Responsabile	Stato
R-01	I dipendenti potrebbero cliccare link di phishing	Credenziali e-mail	Attaccante esterno	Mancanza di consapevolezza	Elevato	Elevato Critico	Consapevolezza formazione + simulazioni di phishing	Sicurezza Team di sensibilizzazione	In corso
R-02	Server non aggiornato vulnerabile a CVE	Server finanziario	Exploit malware	Aggiornamenti di sicurezza mancanti	Medio	Alta Alto	Ciclo mensile di gestione delle patch	IT Team infrastruttura	Aperto
R-03	Password deboli riutilizzate dal personale	Account interni	Abuso da parte di personale interno	Politica delle password inadeguata	Alto	Medio Alto	Applicazione di politiche di password complesse, MFA	IAM (Team Identità)	In corso

8.2 Esempi di categorie di rischio

Quando si riflette sui rischi, considerare le seguenti categorie:

- **Rischi tecnici**: sistemi senza patch, porte aperte, configurazioni non sicure.
- **Rischi umani**: phishing, password deboli, uso improprio da parte di personale interno.
- **Rischi legati alle politiche/ai processi**: politiche mancanti, mancanza di formazione, procedure di assunzione/dimissioni inadeguate.
- **Rischi legati a terzi**: violazioni da parte dei fornitori, attacchi alla catena di approvvigionamento, servizi in outsourcing.

Suggerimento: cercate di individuare **almeno un rischio per ogni categoria** per ottenere un registro più equilibrato.

8.3 Errori comuni da evitare

Quando gli studenti creano per la prima volta i registri dei rischi, spesso:

- **Scrivono descrizioni vaghe dei rischi** (ad esempio, "problema di sicurezza" invece di "vulnerabilità del sistema operativo non corretta").

- **Saltano l'assegnazione di un responsabile** → nessuno che si assuma la responsabilità significa nessun progresso.
- **Sopravvalutare tutto come rischio elevato** → rende insignificante la definizione delle priorità.
- **Dimenticare di aggiornare** → i registri devono evolversi con le nuove minacce.
- **Confondere minacce e vulnerabilità** → ricordare:
    - Minaccia = pericolo potenziale (ad es. aggressore).
    - Vulnerabilità = debolezza sfruttata (ad es. porta aperta).

8.4 Ulteriori risorse

- **NIST Cybersecurity Framework (CSF)** – Linee guida sulla gestione dei rischi: https://www.nist.gov/cyberframework
- **ISO/IEC 27005** – Norma internazionale sulla gestione dei rischi per la sicurezza delle informazioni.
- **Linee guida ENISA sulla gestione dei rischi** – Guide pratiche dell'Agenzia dell'Unione europea per la sicurezza informatica.
- **Metodologia di valutazione dei rischi OWASP** – Per la valutazione dei rischi nella sicurezza di siti web e app: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Lettura consigliata: *Managing Risk in Information Systems* (Darril Gibson) — un'introduzione accessibile alla creazione e alla gestione dei registri dei rischi.