TEMPLATE DI PROJECT WORK = 3 CFU **min 12 pagine - max 20 pagine**	
Cognome e Nome:	Bona Giacomo Angelo
Numero di Matricola:	0312200350
Corso di Studio: ◊ L-5 Filosofia ed Etica ◊ L-22 Scienze Motorie ● L-31 Informatica per le Aziende Digitali	● L-31 Informatica per le Aziende Digitali
Tema n: **Titolo del tema:**	Tema n. 2 Privacy e sicurezza aziendale
Traccia del PW n: **Titolo della traccia:**	Traccia 2.2 Sviluppo di un software per la sicurezza aziendale
Titolo dell'elaborato:	Approccio Sistematico al Risk Assessment
PARTE PRIMA – DESCRIZIONE DEL PROCESSO	
Utilizzo delle conoscenze e abilità derivate dal percorso di studio: Descrivere quali conoscenze e abilità apprese durante il percorso di studio sono state utilizzate per la redazione dell'elaborato, facendo eventualmente riferimento agli insegnamenti che hanno contribuito a maturarle.	Gli insegnamenti di **Calcolo delle Probabilità e Statistica** sono stati essenziali per comprendere i modelli matematici utilizzati nella valutazione del rischio, mentre i corsi di **Programmazione 1 e 2** hanno fornito le competenze **per sviluppare software** sicuri ed efficienti. Le conoscenze acquisite in **Reti di Calcolatori e Cybersecurity** e in **Criminologia** hanno permesso di **analizzare minacce e vulnerabilità** nel **contesto aziendale**. Il corso di **Diritto per le Aziende Digitali** ha aiutato a integrare **aspetti normativi** legati alla protezione dei dati, mentre i contributi di **Strategia, Organizzazione e Marketing** hanno supportato la **contestualizzazione** del progetto in un **ambiente aziendale reale**.
Fasi di lavoro e relativi tempi di implementazione per la predisposizione dell'elaborato: Descrivere le attività svolte in corrispondenza di ciascuna fase di redazione dell'elaborato. Indicare il tempo dedicato alla realizzazione di ciascuna fase, le difficoltà incontrate e come sono state superate	La redazione dell'elaborato è stata pianificata seguendo diverse fasi. Durante la prima settimana, ho partecipato a un incontro didattico per comprendere meglio la struttura del project work. Successivamente, ho dedicato la seconda settimana all'analisi del template fornito e alla revisione degli obiettivi e delle linee guida del regolamento finale. Nella terza settimana, ho effettuato ricerche approfondite su bibliografia e strumenti utili alla stesura del progetto. La quarta settimana è stata dedicata allo studio di stili e soluzioni per la creazione di una landing page che ospitasse il download del documento esplicativo, il cui contenuto è stato elaborato nella quinta settimana. Nella sesta settimana, ho realizzato la pagina web e nella settima settimana ho eseguito la finalizzazione del lavoro, includendo il controllo qualità per garantire la coerenza con gli obiettivi definiti.
Week 1	Project Work L-31 5 novembre - Ricevimento didattica interattiva per spiegazione compilazione project work Valentina Popolo (valentina.popolo@gmail.com)

Week 2	Analisi Template Project Work, Allegato Traccia 2.2, obiettivi, valutazioni e regolamento prova finale
Week 3	Ricerca / Lettura / Studio / Analisi Bibliografia, Banche dati e possibili strumenti utili
Week 4	Ricerca Stili e Website per Landing Page con Download
Week 5	Creazione documento esplicativo sul calcolo del rischio
Week 6	Creazione pagina web per il download del documento
Week 7	Finalizzazione documenti, WebPage e Quality check di aderenza agli obiettivi presenti nell'allegato

Risorse e strumenti impiegati:

Descrivere quali risorse (bibliografia, banche dati, ecc.) e strumenti (software, modelli teorici, ecc.) sono stati individuati ed utilizzati per la redazione dell'elaborato.

Si descrivano inoltre:

- i motivi che hanno orientato la scelta delle risorse e degli strumenti;

- la modalità di individuazione e reperimento delle risorse e degli strumenti;

- le eventuali difficoltà affrontate ed il modo in cui sono state superate

Libri e Manuali

1. "Risk Analysis and Security Countermeasure Selection" ThomasL.Norman
   Approfondisce i metodi per identificare e mitigare i rischi legati alla sicurezza.

2. "Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework" - Dr. Gary Hinson, Brian Honan
   Una guida pratica basata sul framework NIST.

3. "ISO 27001 Handbook: A Practical Guide to Implementing and Auditing ISO 27001" - Alan Calder
   Utile per comprendere la gestione del rischio in contesti aziendali.

4. "Introduction to Cybersecurity" - Charles P. Pfleeger, Shari Lawrence Pfleeger
   Fornisce una base per capire i concetti fondamentali di sicurezza informatica.

5. "The Art of Risk Management: Lessons from the Field" - David Hulett
   Copre strategie e approcci alla gestione dei rischi in vari settori, incluso l'IT.

6. "Security Risk Assessment: Managing Physical and Operational Security Risks" - John M. White
   Include metodologie per la valutazione e gestione del rischio in contesti IT.

Articoli Accademici

1. **"Risk Assessment in IT Security Projects"** - T. Sommestad et al.
   (Disponibile su IEEE Xplore)

2. **"A Cybersecurity Framework for Organizations"** - A. Campbell et al.
   Pubblicato su SpringerLink, tratta di framework di gestione del rischio.

3. **"Quantitative Risk Assessment for Cybersecurity in Organizations"** - D. Geer et al.
   (Disponibile su ACM Digital Library)

4. **"Mitigating IT Security Risks Through Effective Risk Management"** - M. Siponen et al.
   (Disponibile su Elsevier)

Framework e Standard

1. **NIST SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments**
2. **ISO/IEC 27005: Information security risk management**

3. **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**
   Una metodologia per la gestione dei rischi sviluppata dal SEI (Software Engineering Institute).

Risorse Online

1. **OWASP Risk Assessment Framework**
   Linee guida sulla gestione dei rischi nel contesto di applicazioni web.
2. **National Institute of Standards and Technology (NIST)**
   NIST Cybersecurity Framework
3. **ISACA (Information Systems Audit and Control Association)**
   Pubblicazioni sulla gestione del rischio IT e cybersecurity.
4. **ENISA (European Union Agency for Cybersecurity)**
   Report periodici sul panorama delle minacce e gestione del rischio.

Risorse Online

1. **Github**
2. **VSCode**

PARTE SECONDA – PREDISPOSIZIONE DELL'ELABORATO

DESCRIZIONE SITUAZIONE - PROBLEMA

Nell'ambito della gestione della sicurezza sul lavoro, è fondamentale comprendere e calcolare correttamente il fattore di rischio per valutare e mitigare i potenziali pericoli.

Tuttavia, il calcolo del fattore di rischio può essere complesso e richiede una conoscenza approfondita delle normative afferenti ed applicabili, così come delle procedure di valutazione del rischio.

Il problema principale che questo progetto si propone di affrontare è quello di fornire una guida, chiara e dettagliata, circa il calcolo del fattore di rischio in conformità alle normative vigenti e di creare un'interfaccia web per il download del documento.

Obiettivi dell'elaborato/progetto/artefatto:

Specificare gli obiettivi raggiunti dall'elaborato, indicando in che modo esso risponde a quanto richiesto dalla traccia del Project Work.

Obiettivi Linea Guida Project Work	**Aderenza progetto alle linee guida**
Analizzare le normative e le procedure di valutazione del rischio per comprendere i requisiti e le metodologie necessarie per il calcolo del fattore di rischio.	La tesi si basa su un approfondito studio delle normative internazionali quali la serie delle norme ISO/IEC ed il framework NIST per definire i requisiti necessari alla valutazione del rischio. Tali fonti normative sono state adottate in alcuni casi pratici per identificare le operazioni comportate dall'adattamento delle metodologie generali a ciascun contesto aziendale esaminato.
Progettare e redigere un documento esplicativo che spieghi in modo chiaro e dettagliato come calcolare il fattore di rischio, facendo riferimento alle	È stato progettato e redatto un documento che guida, passo dopo passo, il calcolo del fattore di rischio.

	normative ed alle migliori pratiche del settore.	La descrizione è stata integrata da esempi illustrativi e da tabelle di riferimento. La struttura segue un approccio user-friendly nell'intento di facilitare l'adozione anche da parte di utenti non esperti.
	Creare una pagina HTML che includa un link per il download del documento esplicativo, assicurandosi che l'interfaccia sia intuitiva e accessibile per gli utenti.	È stata sviluppata una pagina HTML che consente agli utenti di ottenere agevolmente il documento esplicativo. L'interfaccia è stata progettata con particolare attenzione all'accessibilità ed all'usabilità, garantendo un'esperienza ottimale sui principali dispositivi.
Contestualizzazione Elaborare una breve descrizione del contesto teorico-applicativo nell'ambito del quale è stato sviluppato l'elaborato	Il presente lavoro si inserisce in un contesto in cui le organizzazioni, soprattutto nel settore ICT, si trovano ad affrontare un panorama di rischi sempre più complesso ed interconnesso. La rapida evoluzione delle minacce informatiche e le crescenti prescrizioni normative a tutela dei dati richiedono un approccio integrato alla gestione del rischio. In questo scenario, la valutazione del rischio, fondata su modelli probabilistici e deterministici, è cruciale per identificare i pericoli e mitigarne gli effetti, salvaguardando le risorse aziendali in genere garantendo nel contempo il rispetto di disposizioni legislative come il Regolamento Europeo sulla Protezione dei Dati e la compliance con gli standard normativi internazionali come l'ISO/IEC 27001. Gli esempi pratici illustrano due tipiche problematiche affrontate dalle aziende ICT italiane: gli attacchi ransomware, che minacciano l'integrità operativa ed economica, e le violazioni del GDPR, che impattano sulla reputazione aziendale e sul rispetto di severi obblighi legali. La corretta applicazione delle tecniche di valutazione e gestione del rischio è essenziale per garantire la resilienza organizzativa e prevenire danni reputazionali e, in ultima istanza, economici.	
Descrizione dei principali aspetti progettuali Sviluppare l'elaborato richiesto dalla traccia prescelta. (qui va tutto: codice, testo e ….) 1. **Documento esplicativo sul calcolo del fattore di rischio**: Un documento redatto in formato PDF che fornisce una guida completa sul calcolo del fattore di rischio, includendo spiegazioni dettagliate, formule, esempi pratici e riferimenti alle normative di riferimento. 2. **Pagina HTML per il download del documento**: Una pagina web sviluppata utilizzando linguaggi HTML e CSS, che include un link per il download del documento esplicativo sul calcolo del fattore di rischio. L'interfaccia sarà progettata per essere intuitiva e accessibile agli utenti. 3. **Rapporto di Valutazione e Test:** Un rapporto che valuta l'efficacia del documento esplicativo e dell'interfaccia web, raccogliendo feedback dagli utenti e identificando eventuali aree di miglioramento. **SSSSSSS**	**"La valutazione dei rischi è lo strumento che consente di rendere stimabile ciò che non può essere deterministicamente calcolato"** **1. Calcolo del fattore di rischio** Il rischio è definito come l'indicatore del grado di allontanamento da una condizione ideale di sicurezza totale. Nel contesto informatico, il rischio rappresenta la probabilità che un evento imprevisto e indesiderato, capace di causare danni, si verifichi effettivamente. Il calcolo del rischio si basa su una formula consolidata, di applicazione generale: $$R_i\left[\frac{danno}{anno}\right] = f_i\left[\frac{eventi}{anno}\right] * D_i\left[\frac{danno}{evento}\right]$$ La valutazione del rischio si basa su un'analisi combinata che include una componente probabilistica (frequenza di accadimento degli eventi) ed una deterministica (stima dell'entità del danno) applicate ai diversi scenari presi in esame. Nel settore IT, la complessità delle infrastrutture, la presenza di sistemi interconnessi e la crescente sofisticazione delle	

minacce possono generare una vasta gamma di scenari critici; ciascuno di essi può presentare conseguenze anche sensibilmente diverse tra loro. A seconda del target interessato, i rischi informatici possono essere classificati nelle seguenti tipologie principali:

- **Rischio operativo**: riguarda l'impatto sulle funzionalità aziendali, espresso in termini di interruzioni dei servizi o di perdita di dati critici.
- **Rischio di conformità**: legato al mancato rispetto delle leggi vigenti, delle normative o degli standard di sicurezza, con conseguenti sanzioni legali, amministrative o penali.
- **Rischio economico**: si riferisce alle perdite finanziarie derivanti da violazioni della sicurezza, come il costo per il ripristino dei sistemi o le conseguenze di frodi informatiche.
- **Rischio reputazionale**: concerne il danno d'immagine subito dall'organizzazione a causa della diffusione di notizie relative a violazioni, attacchi o carenze/mancanze nella protezione dei dati.

I rischi operativi e di conformità, avendo un impatto diretto sul contesto normativo e sulla fiducia dei clienti, sono spesso soggetti a regolamentazioni e linee guida specifiche.
Al contrario, i rischi economici e reputazionali tendono a essere affrontati internamente dalle aziende, che utilizzano metodologie avanzate di analisi del rischio non solo per rispettare gli obblighi di legge, ma anche per preservare i propri interessi strategici.

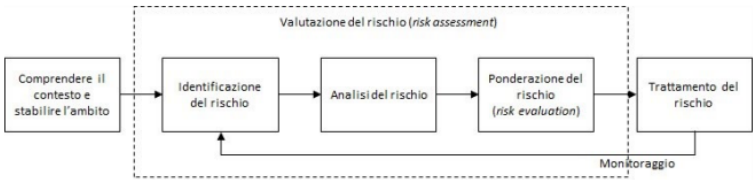
Tra gli strumenti disponibili per la gestione dei rischi, la mappatura dei rischi risulta essere l'approccio iniziale ineludibile.
Essa consente di identificare aree e processi critici, fornendo informazioni utili per interventi mirati. Nel contesto IT in particolare, l'adozione di metodologie come il Threat Modeling e la valutazione quantitativa del rischio (ad esempio utilizzando analisi basate su framework come FAIR) permette di ottimizzare le strategie di mitigazione, integrando opportune misure di sicurezza sin dalle prime fasi della progettazione dei sistemi.

È importante notare come l'efficacia nella gestione del rischio informatico dipenda anche dal bilanciamento tra i costi di implementazione delle soluzioni di sicurezza ed il livello di protezione desiderato. In questo equilibrio, la pianificazione strategica gioca un ruolo cruciale, consentendo alle organizzazioni, una volta stabilite le priorità e le risorse, di valutare la fattibilità degli interventi e di monitorare con continuità l'efficacia delle contromisure adottate.

Infine, una riduzione dei rischi operativi ed economici attraverso misure preventive e reattive adeguate, contribuisce indirettamente anche alla diminuzione dei rischi reputazionali e di mancata/carente conformità, rafforzando la resilienza complessiva dell'organizzazione. Per affrontare tali sfide, è fondamentale adottare un approccio basato sull'analisi

strutturata del rischio e sull'utilizzo di strumenti specifici, in conformità con le normative internazionali specifiche per il settore informatico.

È inoltre importante tenere presente che l'obiettivo del processo di gestione del rischio, nel contesto di un quadro di riferimento così ampio, non può essere certo quello (puramente ipotetico) di eliminare completamente i rischi, ma di perseguire il contenimento dei rischi complessivi a livelli accettabili.
Quindi, i processi operativi interni devono tendere a contenere ciascun fattore di rischio entro i limiti prestabiliti affinché il rischio complessivo che concorrono a determinare risulti accettabilmente ridotto. I passi che seguono aiutano a determinare e ad applicare le azioni specifiche a tal fine.



Fonte: Clusit – Associazione Italiana per la Sicurezza Informatica

Il processo di gestione del rischio si articola in diverse fasi:

1. **Identificazione degli obiettivi e del Risk Appetite**

   La definizione degli obiettivi aziendali richiede un'analisi preliminare dei rischi connessi al loro raggiungimento, valutando fino a che punto sia accettabile spingere le contromisure, ovvero il proprio **Risk Appetite**. Una pianificazione priva di questa analisi espone l'organizzazione all'eventualità di fissare obiettivi irrealistici e conduce all'uso inefficiente delle risorse disponibili.
   Nel settore finanziario, caratterizzato da alta volatilità, la crisi dei subprime del 2008-2009 ha evidenziato l'importanza di integrare la gestione del rischio nelle decisioni strategiche.
   Per affrontare questa criticità, il Comitato di Basilea e il Financial Stability Board hanno introdotto l'obbligo di formalizzare il **Risk Appetite Statement**, che deve sempre rimanere entro i limiti della **Risk Capacity**.
   Questo approccio consente una gestione sostenibile, bilanciando obiettivi ambiziosi e capacità, efficiente ed efficace, di sopportazione del rischio, prevenendo l'instabilità del sistema e, in ultima analisi, salvaguardando le risorse aziendali in senso lato.

2. **Individuazione dei rischi**

   La seconda fase della valutazione dei rischi consiste nella mappatura degli eventi avversi, confrontando obiettivi aziendali e risorse disponibili.
   Si utilizza un approccio combinato **top-down** e **bottom-up.**
   Il primo identifica i programmi critici da preservare e le condizioni che possono ostacolarli, mentre il secondo analizza le minacce conosciute (ad es. ransomware, terremoti …) ed il loro impatto sull'attività aziendale nel suo complesso.
   Un rischio è significativo solo se ha un impatto tangibile, quantificabile.
   Secondo il rapporto *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)*, un rischio dannoso richiede la prsenza dei seguenti fattori:
   1. un bene di valore colpito,

2. una fonte di minaccia,
3. una vulnerabilità preesistente,
4. un impatto dannoso.

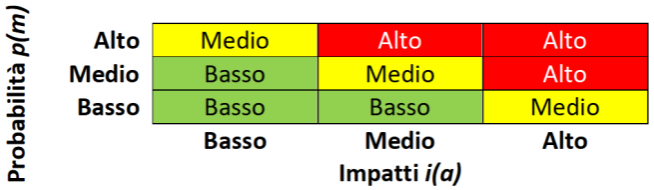
Descrivere il rischio come scenario facilita l'analisi della probabilità di accadimento e la quantificazione dell'impatto. Inoltre, pone le basi per la successiva definizione delle contromisure, preventive o protettive che siano.
È utile categorizzare i rischi in quattro aree principali, suggerite dal *Committee of Sponsoring Organizations of the Treadway Commission*:

- **Strategico**: reputazione, innovazione, relazioni.
- **Finanziario e reporting**: volatilità, fiscalità, credito.
- **Compliance e governance**: privacy, regolamentazione, etica.
- **Operativo**: sicurezza, supply chain, disastri naturali.

Questa categorizzazione supporta il monitoraggio e l'adozione di strategie di mitigazione, consentendo un'analisi integrata e proattiva dei rischi aziendali.

3. **Analisi della probabilità e dell'impatto del rischio**

Un evento è considerato un fattore di rischio solo se ha un impatto misurabile.
È essenziale classificare i rischi per priorità, poiché le misure di mitigazione comportano costi proporzionali all'entità del danno stimato. Le analisi del rischio si basano su tecniche scientifiche per stimare probabilità e impatti, spesso con strumenti qualitativi come la **matrice probabilità-impatto**.
Questa matrice, tradizionalmente rappresentata con una griglia bidimensionale, calcola il rischio combinando direttamente i fattori di **probabilità** ed **impatto**.



Fonte: Clusit – Associazione Italiana per la Sicurezza Informatica

Ogni organizzazione deve definire il proprio grado di tolleranza al rischio per ridurre i possibili pregiudizi nella mappatura.
Si distinguono due tipi di rischio:

- **Rischio inerente**: rischio massimo in assenza di interventi mitigativi.

- **Rischio residuo**: rischio che persiste anche a valle dell'adozione di misure di mitigazione.
  Il processo si concentra inizialmente sul rischio inerente per poi passare al rischio residuo, garantendo risposte adeguate e proporzionate.

4. **Definizione dei piani di risposta al rischio**

Dopo aver individuato i rischi e definito le priorità d'intervento, è necessario valutare le opzioni per il loro controllo e la conseguente mitigazione. Le possibili strategie includono:

1. **Accettazione del rischio**: se il rischio rientra nel livello definito accettabile dal **Risk Appetite Statement**, non sono necessari ulteriori interventi.
2. **Trasferimento del rischio**: condividere parte dell'impatto con terze parti, come compagnie assicurative o fornitori di servizi.
3. **Eliminazione del rischio**: rimuovere attività o esposizioni che generano il rischio qualora non sia possibile mitigarne altrimenti gli effetti.

I piani di gestione del rischio devono essere sostenibili economicamente, garantendo un equilibrio tra il valore delle attività protette e le risorse impiegate per la loro sicurezza.

5. Monitoraggio dei risultati della gestione del rischio

Il processo di mappatura e classificazione dei rischi, insieme ai piani di mitigazione, deve essere monitorato costantemente per garantire l'allineamento con la policy aziendale.
Le condizioni di rischio, il valore degli asset e le preferenze degli stakeholder possono cambiare rapidamente, richiedendo aggiornamenti tempestivi.
Un monitoraggio efficace include:

- Flusso informativo in tempo reale: per mantenere il management aggiornato sui progressi e sulle modifiche dei piani di gestione del rischio.
- Iterazione continua: i risultati delle azioni intraprese dai team devono contribuire a migliorare gli strumenti di analisi e le risposte che il sistema può offrire nelle successive richieste d'intervento.

L'obiettivo è assicurare che la gestione del rischio rimanga dinamica e reattiva rispetto ai cambiamenti organizzativi e di contesto.

Esempi pratici per un'azienda ICT italiana

Caso 1: Rischio operativo – Attacco ransomware

Scenario: Un attacco ransomware potrebbe criptare i dati aziendali, causando l'interruzione dei servizi per i clienti.

Probabilità (P): 25% (stimato in base alle statistiche di attacchi nel settore ICT in Italia).

Impatto (I):

- Perdita di fatturato: €300.000.
- Costi di ripristino: €50.000.
- Danno reputazionale: €150.000. **Totale impatto stimato: €500.000.**

Rischio (R): R = 0,25 × 500.000 = €125.000.

Mitigazione:

- Implementare un piano di disaster recovery con backup giornalieri.
- Acquistare un'assicurazione contro i rischi informatici.
- Formare i dipendenti sulle pratiche di cybersecurity.

Caso 2: Rischio di conformità – Violazione GDPR

Scenario: Perdita di dati personali a causa di un attacco informatico.

Probabilità (P): 10% (bassa, grazie a misure preventive già in atto).

Impatto (I):

- Sanzione GDPR: €200.000.
- Costi legali e amministrativi: €50.000.
- Perdita di fiducia da parte dei clienti: €100.000. **Totale impatto stimato: €350.000.**

Rischio (R): R = 0,10 × 350.000 = €35.000.

Mitigazione:

- Implementare crittografia end-to-end per i dati sensibili.
- Condurre audit regolari sulla conformità GDPR.
- Introdurre controlli periodici sui sistemi di protezione dei dati.

Normative di riferimento

GDPR (Regolamento Generale sulla Protezione dei Dati)

Il GDPR richiede alle aziende di:

- Implementare misure di sicurezza adeguate ai rischi identificati (art. 32).
- Segnalare le violazioni dei dati entro 72 ore (art. 33).
- Condurre valutazioni d'impatto sulla protezione dei dati (art. 35).

Queste misure devono essere integrate nei processi aziendali per garantire la compliance continua e minimizzare i rischi di sanzioni.

ISO/IEC 27001

La norma ISO/IEC 27001 fornisce un framework per la gestione della sicurezza delle informazioni, includendo:

- Identificazione e valutazione dei rischi (clausola 6.1.2).
- Pianificazione delle azioni di mitigazione (clausola 6.1.3).
- Monitoraggio e miglioramento continuo (clausola 9).

L'adozione della norma permette di costruire un sistema di gestione della sicurezza delle informazioni che risponde alle esigenze specifiche del settore ICT.

2. Pagina HTML per il download del documento
(bonagiacomo.com/tesi)

HomePage – Desktop

HomePage – Mobile

Codice Formattato con https://carbon.now.sh/

Sezione HTML “Download documento”

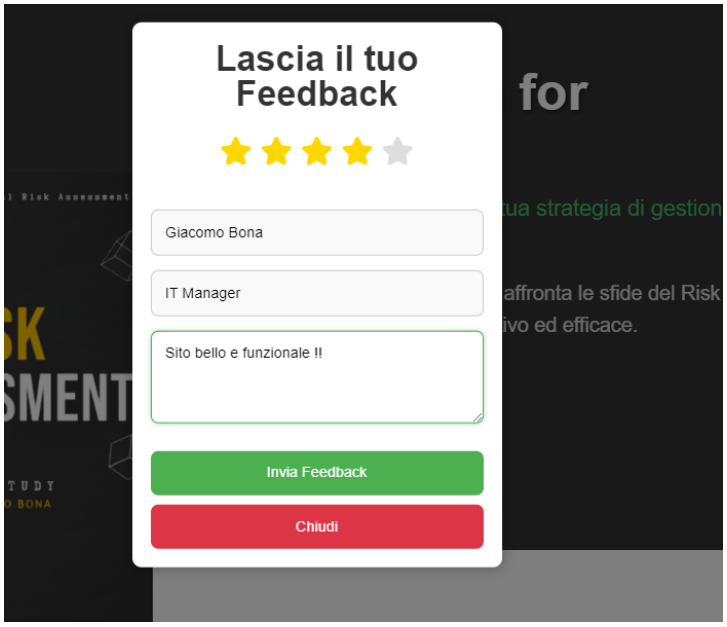
Codice RAW

```
<section class="hero hero-2 bg-dark" id="hero">
      <div class="hero-content bg-dark">
        <div class="container">
          <!-- Logo Section -->
          <div class="row">
            <div class="col-12 text-center">
              <div class="hero-logo mt-50">
                <img src="./testPage_files/logo-light.png" alt="logo hero" style="width: 300px; height: auto;">
              </div>
            </div>
          </div>
          <!-- Hero Content -->
          <div class="row row-content align-items-center mt-5">
            <!-- Image Section -->
            <div class="col-12 col-md-5 text-center">
              <div class="hero-holder" style="margin-top: -80px;">
                <!-- Spostato più in alto -->
                <img class="img-fluid" src="./testPage_files/book.png" alt="screens" style="max-width: 90%; height: auto;">
              </div>
            </div>
            <!-- Text Section -->
            <div class="col-12 col-md-6">
              <div class="hero-headline">Innovation for Security</div>
              <div class="hero-subheadline" style="color: #49b970; font-size: 24px; font-weight: 500; margin-bottom: 20px;"> Scopri come migliorare la tua strategia di gestione del rischio </div>
              <div class="hero-bio"> Con un approccio sistemico, affronta le sfide del Risk Assessment in modo innovativo ed efficace. </div>
              <div class="hero-action">
                <a class="btn btn--primary btn--rounded" href="javascript:void(0);" onclick="openPopup()"> DOWNLOAD </a>
              </div>
            </div>
            <…>

</section>
```

3. RACCOLTA FEEDBACK

Rapporto di valutazione e test



Sezione HTML

```
<!-- Popup e overlay -->
<div class="popup" id="popup">
  <h3>Lascia il tuo Feedback</h3>
  <div class="stars">
    <i class="fa fa-star" onclick="selectStar(this)"></i>
    <i class="fa fa-star" onclick="selectStar(this)"></i>
    <i class="fa fa-star" onclick="selectStar(this)"></i>
    <i class="fa fa-star" onclick="selectStar(this)"></i>
    <i class="fa fa-star" onclick="selectStar(this)"></i>
  </div>
  <br>
  <br>
  <input type="text" id="user-name" placeholder="Nome utente" />
  <input type="text" id="user-role" placeholder="Ruolo" />
  <textarea id="feedback-text" class="feedback-text" placeholder="Scrivi il tuo feedback..."></textarea>
  <button class="submit-btn" onclick="submitFeedback()">Invia Feedback</button>
  <button class="submit-btn" onclick="closePopup()">Chiudi</button>
</div>
<div class="popup-overlay" id="popup-overlay" onclick="closePopup()"></div>
</div>
```

Codice RAW

```
<!-- Popup e overlay -->
            <div class="popup" id="popup">
              <h3>Lascia il tuo Feedback</h3>
              <div class="stars">
                <i class="fa fa-star" onclick="selectStar(this)"></i>
                <i class="fa fa-star" onclick="selectStar(this)"></i>
                <i class="fa fa-star" onclick="selectStar(this)"></i>
                <i class="fa fa-star" onclick="selectStar(this)"></i>
                <i class="fa fa-star" onclick="selectStar(this)"></i>
              </div>
              <br>
              <br>
              <input type="text" id="user-name" placeholder="Nome utente" />
              <input type="text" id="user-role" placeholder="Ruolo" />
                            <textarea id="feedback-text" class="feedback-text" placeholder="Scrivi il tuo feedback..."></textarea>
                <button class="submit-btn" onclick="submitFeedback()">Invia Feedback</button>
                                                <button class="submit-btn" onclick="closePopup()">Chiudi</button>
            </div>
```

Sezione JS

```
<script>
  // Funzione per aprire il popup
  function openPopup() {
    document.getElementById("popup").style.display = "block";
    document.getElementById("popup-overlay").style.display = "block";
  }
  // Funzione per chiudere il popup
  function closePopup() {
    document.getElementById("popup").style.display = "none";
    document.getElementById("popup-overlay").style.display = "none";
  }
  // Funzione per gestire la selezione delle stelle
  function selectStar(star) {
    const stars = document.querySelectorAll(".stars i");
    let selected = false;
    // Controlla se la stella è già selezionata
    if (star.classList.contains("selected")) {
      selected = true;
      star.classList.remove("selected");
    } else {
      star.classList.add("selected");
    }
    // Se è stata deselezionata una stella, rimuovi la selezione dalle successive
    if (!selected) {
      for (let i = 0; i < stars.length; i++) {
        if (stars[i] === star) {
          break;
        }
        stars[i].classList.add("selected");
      }
    } else {
      for (let i = stars.length - 1; i >= 0; i--) {
        if (stars[i] === star) {
          break;
        }
        stars[i].classList.remove("selected");
      }
    }
  }
  // Funzione per inviare il feedback
  function submitFeedback() {
    // Ottieni i valori dal popup
    var name = document.getElementById("user-name").value;
    var role = document.getElementById("user-role").value;
    var feedbackText = document.getElementById("feedback-text").value;
    // Controllo di validità (puoi anche aggiungere altri controlli qui)
    if (!name || !role || !feedbackText) {
      alert("Tutti i campi sono obbligatori!");
      return;
    }
    // Crea il nuovo div della recensione
    var newReview = document.createElement("div");
    newReview.classList.add("owl-item");
    // Aggiungi il contenuto della recensione
    newReview.innerHTML = `


    <div class="testimonial-panel wow fadeInUp" data-wow-duration="1s" style="visibility: visible; animation-duration:
1s; animation-name: fadeInUp;">
        <div class="testimonial-body">
            <div class="testimonial--body">
                <p>"${feedbackText}"</p>
            </div>
            <div class="testimonial--meta">
                <div class="testimonial--author">
                    <img src="./testPage_files/1.png" alt="author">
                        <h5>${name}</h5>
                        <p>${role}</p>
                    </div>
                </div>
            </div>
        </div>
    `;
    // Aggiungi la recensione nel contenitore delle recensioni
    var reviewContainer = document.getElementById("reviews-container");
    reviewContainer.appendChild(newReview);
    // Pulisci i campi del popup
    document.getElementById("user-name").value = "";
    document.getElementById("user-role").value = "";
    document.getElementById("feedback-text").value = "";
    // Chiudi il popup
    closePopup();
  }
</script>
```

Codice RAW

```
<script>
  // Funzione per aprire il popup
  function openPopup() {
    document.getElementById("popup").style.display = "block";
    document.getElementById("popup-overlay").style.display = "block";
  }
  // Funzione per chiudere il popup
  function closePopup() {
    document.getElementById("popup").style.display = "none";
    document.getElementById("popup-overlay").style.display = "none";
  }
  // Funzione per gestire la selezione delle stelle
  function selectStar(star) {
    const stars = document.querySelectorAll(".stars i");
    let selected = false;
    // Controlla se la stella è già selezionata
    if (star.classList.contains("selected")) {
      selected = true;
      star.classList.remove("selected");
    } else {
```

```
      star.classList.add("selected");
    }
    // Se è stata deselezionata una stella, rimuovi la selezione dalle successive
    if (!selected) {
      for (let i = 0; i < stars.length; i++) {
        if (stars[i] === star) {
          break;
        }
        stars[i].classList.add("selected");
      }
    } else {
      for (let i = stars.length - 1; i >= 0; i--) {
        if (stars[i] === star) {
          break;
        }
        stars[i].classList.remove("selected");
      }
    }
  }
  // Funzione per inviare il feedback
  function submitFeedback() {
    // Ottieni i valori dal popup
    var name = document.getElementById("user-name").value;
    var role = document.getElementById("user-role").value;
    var feedbackText = document.getElementById("feedback-text").value;
    // Controllo di validità (puoi anche aggiungere altri controlli qui)
    if (!name || !role || !feedbackText) {
      alert("Tutti i campi sono obbligatori!");
      return;
    }
    // Crea il nuovo div della recensione
    var newReview = document.createElement("div");
    newReview.classList.add("owl-item");
    // Aggiungi il contenuto della recensione
    newReview.innerHTML = `
            <div class="testimonial-panel wow fadeInUp" data-wow-duration="1s" style="visibility: visible; animation-duration: 1s; animation-name: fadeInUp;">
                        <div class="testimonial-body">
                                <div class="testimonial--body">
                                        <p>“${feedbackText}”</p>
                                </div>
                                <div class="testimonial--meta">
                                        <div class="testimonial--author">
                                                <img src="./testPage_files/1.png" alt="author">
                                                        <h5>${name}</h5>
                                                        <p>${role}</p>
                                                </div>
                                        </div>
                                </div>
                        </div>
  `;
    // Aggiungi la recensione nel contenitore delle recensioni
    var reviewContainer = document.getElementById("reviews-container");
    reviewContainer.appendChild(newReview);
    // Pulisci i campi del popup
    document.getElementById("user-name").value = "";
    document.getElementById("user-role").value = "";
    document.getElementById("feedback-text").value = "";
    // Chiudi il popup
    closePopup();
  }
</script>
```

Campi di applicazione

Descrivere gli ambiti di applicazione dell’elaborato progettuale e i vantaggi derivanti della sua applicazione.

L'elaborato progettuale si applica principalmente nel contesto delle aziende ICT, ma i principi e le metodologie proposte possono essere adattati a qualsiasi organizzazione che desideri gestire e mitigare i rischi informatici in modo strutturato e proattivo. In particolare, le strategie di valutazione e gestione del rischio descritte nell'elaborato sono utili per affrontare i rischi operativi, di conformità, economici e reputazionali, che possono minacciare l'integrità delle infrastrutture IT, la protezione dei dati e la fiducia degli stakeholder.
Le metodologie di analisi del rischio, come la mappatura dei rischi e l'analisi della probabilità e dell'impatto, sono applicabili in vari scenari pratici, tra cui la protezione dalle minacce informatiche, la gestione delle vulnerabilità, e la prevenzione di attacchi come ransomware o violazioni delle normative come il GDPR. L'applicazione di queste metodologie consente alle aziende di migliorare la resilienza dei propri sistemi informatici, ridurre il rischio di danni economici e reputazionali, e garantire la conformità con le normative di sicurezza.

Inoltre, il modello di gestione del rischio proposto offre vantaggi concreti in termini di pianificazione e allocazione delle risorse. Implementando un approccio sistematico nella gestione del rischio, le aziende possono ottimizzare le loro risorse, massimizzare l'efficacia delle misure di sicurezza, e ridurre il tempo e i costi associati alla risposta agli incidenti.

L'adozione di strumenti come il Threat Modeling e l'analisi quantitativa del rischio fornisce un quadro chiaro per la priorizzazione degli interventi, migliorando la capacità dell'organizzazione di affrontare in modo tempestivo e adeguato le minacce emergenti.

Infine, la gestione del rischio informatico contribuisce in modo significativo al mantenimento di una buona reputazione aziendale e alla fiducia dei clienti, che è fondamentale per il successo a lungo termine, soprattutto in un contesto di crescente digitalizzazione e in un ambiente normativo sempre più complesso.

Valutazione dei risultati (potenzialità e criticità) Descrivere le criticità e i limiti ai quali i risultati dell'elaborato sono potenzialmente esposti.	I risultati dell'elaborato progettuale, pur essendo validi e utili in diversi ambiti, presentano alcune potenzialità e criticità che devono essere prese in considerazione per garantirne un'efficace applicazione. **Potenzialità** Un aspetto positivo del progetto è la sua adattabilità a contesti diversi, dalle piccole aziende alle grandi organizzazioni, rendendolo una soluzione scalabile e versatile. La gestione strutturata del rischio, infatti, consente alle aziende di rafforzare la propria postura di sicurezza, ridurre i danni derivanti da attacchi informatici e migliorare la resilienza operativa. Inoltre, l'approccio proposto fornisce un quadro teorico robusto per la valutazione delle minacce e la pianificazione delle contromisure, promuovendo una gestione del rischio più consapevole e mirata. Inoltre, l'utilizzo di tecniche avanzate di analisi del rischio, come il Threat Modeling e l'analisi quantitativa, permette di identificare e mitigare in modo tempestivo le vulnerabilità più critiche, ottimizzando l'allocazione delle risorse e aumentando l'efficacia delle misure di sicurezza adottate. Il miglioramento nella gestione delle vulnerabilità e dei rischi associati può tradursi in una significativa riduzione dei costi operativi e in un miglioramento della sicurezza informatica complessiva. **Criticità e limiti** Nonostante le potenzialità, ci sono alcuni limiti e criticità che potrebbero influenzare i risultati ottenuti. Innanzitutto, la completezza e l'efficacia della valutazione del rischio dipendono dalla qualità dei dati disponibili e dalla capacità dell'organizzazione di implementare correttamente gli strumenti di analisi. La mancanza di dati accurati e aggiornati potrebbe compromettere la precisione dell'analisi e ridurre l'affidabilità delle previsioni. Inoltre, l'approccio proposto richiede un elevato livello di competenza da parte dei professionisti coinvolti, e la formazione continua del personale è essenziale per mantenere l'efficacia nel tempo. Un altro limite riguarda la capacità di anticipare tutte le minacce emergenti, specialmente in un contesto in rapida evoluzione come quello della sicurezza informatica. Nuove vulnerabilità e attacchi zero-day potrebbero sfuggire all'analisi, rendendo necessario un continuo aggiornamento delle tecniche di valutazione e monitoraggio. Infine, la dipendenza dalla tecnologia e dalle risorse IT per implementare correttamente le soluzioni proposte potrebbe essere una sfida per le organizzazioni con risorse limitate. In questi casi, l'adozione di soluzioni efficaci potrebbe essere ostacolata dalla mancanza di infrastrutture adeguate o dalla difficoltà di integrazione con sistemi legacy.