PROJECT WORK	
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:	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:	La **redazione** dell'elaborato è stata **organizzata in diverse fasi**, ognuna delle quali ha contribuito al completamento del progetto finale. Durante la **prima settimana,** ho **partecipato a un incontro didattico** interattivo il 5 novembre, durante il quale sono state f**ornite spiegazioni sulla corretta compilazione del project work**. Questo **incontro**, **condotto** dalla **docente Valentina Popolo** (valentina.popolo@gmail.com), ha rappresentato il punto di partenza per comprendere meglio la struttura del lavoro da svolgere. Nella **seconda settimana**, ho dedicato il mio tempo all'**analisi del template fornito e alla revisione degli obiettivi**, delle valutazioni e delle linee guida stabilite nel regolamento per la prova finale. Questo passo è stato fondamentale per garantire che il progetto fosse conforme alle aspettative accademiche e ai requisiti stabiliti. La **terza settimana** è stata caratterizzata da un'intensa **attività di ricerca**. Ho esaminato la **bibliografia**, esplorato **banche dati** e **valutato possibili strumenti** utili per la stesura del progetto, al fine di acquisire tutte le conoscenze necessarie per la parte teorica.

	Nella **quarta settimana**, mi sono concentrato sulla **ricerca di stili e soluzioni per la creazione di una landing page** che avrebbe ospitato il download del documento esplicativo. Ho esplorato vari siti web e design per raccogliere idee utili a **rendere la pagina web funzionale e accattivante**. La **quinta settimana** è stata **dedicata** alla **creazione** del **documento esplicativo** sul **calcolo del rischio**, che è stato un elemento centrale del project work. Questo documento è stato sviluppato con attenzione, seguendo le linee guida teoriche e pratiche emerse nelle settimane precedenti. Durante la **sesta settimana**, mi sono concentrato sulla **realizzazione della pagina web** che avrebbe permesso agli utenti di scaricare il documento esplicativo. Ho lavorato sulla **struttura e sul layout della landing page**, assicurandomi che fosse **facilmente navigabile e funzionale**. Infine, nella **settima settimana,** ho proceduto con la **finalizzazione** dell'intero lavoro. Questa fase ha incluso un accurato controllo qualità per garantire che tutti gli elementi del progetto fossero in linea con gli obiettivi definiti, verificando l'aderenza alle specifiche del template e al regolamento fornito.
Risorse e strumenti impiegati:	**Tesi / Articoli di ricerca** 1. Sánchez-García, I.D.; Mejía, J.; San Feliu Gilabert, T. Cybersecurity Risk Assessment: A Systematic Mapping Review https://doi.org/10.3390/app13010395 2. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M. Cyber risk and cybersecurity: a systematic review of data availability. https://doi.org/10.1057/s41288-022-00266-6 3. El-Hajj, M.; Mirza, Z.A. ProtectingSmall and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool. https://doi.org/10.3390/electronics13193910 **Banche Dati** 4. Rapporto Clusit 2024: https://clusit.it/download/RapportoClusit2024.pdf **Normative** 5. ISO 27001: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en 6. GDPR: https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE **Strumenti Software** 7. Microsoft Visual Studio https://code.visualstudio.com/ 8. Cloudflare WAF https://www.cloudflare.com/it-it/application-services/ 9. GitHub Pages https://pages.github.com/

I motivi che hanno orientato la scelta delle risorse e degli strumenti

Le risorse selezionate sono state scelte per fornire una base completa e aggiornata sulle tematiche di cybersecurity e gestione del rischio. In particolare, gli articoli di ricerca offrono analisi approfondite su valutazioni e framework di sicurezza, nonché sul miglioramento della protezione per piccole e medie imprese (PMI).

Le banche dati come il **Rapporto Clusit 2024** forniscono dati specifici sulle minacce e le vulnerabilità, utili per comprendere l'evoluzione del rischio cibernetico.

Le normative come **ISO 27001** sono fondamentali per garantire che i processi di gestione della sicurezza delle informazioni siano standardizzati e certificabili.

Gli strumenti software come **Microsoft Visual Studio**, **Cloudflare WAF**, e **GitHub Pages** sono stati scelti per supportare lo sviluppo dell'applicazione web e la gestione dei contenuti online.

Modalità di individuazione e reperimento delle risorse e degli strumenti

Le risorse accademiche sono state selezionate attraverso una ricerca mirata in riviste scientifiche di settore e database accademici.

Il **Rapporto Clusit 2024** è stato reperito dal sito ufficiale del Clusit, che pubblica periodicamente report sui rischi cibernetici a livello globale. Le normative ISO, come la **ISO 27001**, sono state ottenute direttamente dal sito ufficiale ISO.

Gli strumenti software sono stati individuati in base alla loro reputazione nel settore e alla loro accessibilità: **Microsoft Visual Studio** è uno strumento di sviluppo popolare e largamente utilizzato, mentre **Cloudflare WAF** è una soluzione di protezione web molto apprezzata per le sue capacità di mitigazione degli attacchi / CDN, e **GitHub Pages** è una piattaforma gratuita per la gestione e il rilascio di contenuti web.

Difficoltà affrontate e soluzioni adottate

Una delle principali difficoltà incontrate durante il processo è stata la necessità di ottenere una visione integrata dei vari aspetti della cybersecurity, passando dalla teoria alla pratica. Sebbene gli articoli di ricerca fornissero una solida base teorica sulle metodologie e le tecniche di protezione, questi non offrivano indicazioni concrete su come implementare le soluzioni in scenari reali.

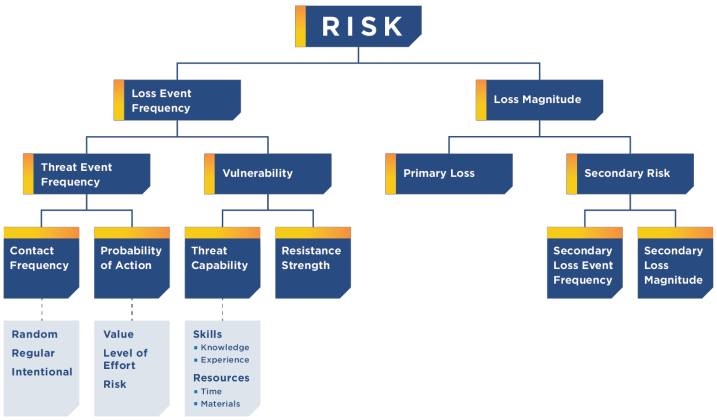
Per superare questa difficoltà, è stato necessario dedicare tempo alla comprensione delle specifiche tecniche e delle modalità di implementazione degli strumenti di sicurezza. Questo ha comportato la consultazione di manuali tecnici e risorse online, fondamentali per acquisire le competenze pratiche necessarie.

Inoltre, la selezione degli strumenti software si è rivelata una sfida, poiché richiedeva una valutazione delle funzionalità offerte e la loro adeguatezza rispetto alle esigenze specifiche di progetto.
In particolare, è stata presa in considerazione l'adozione di soluzioni gratuite o open-source, che hanno contribuito a ottimizzare i costi senza compromettere la sicurezza.

Infine, per affrontare queste difficoltà, è stato fondamentale un approccio pratico, che ha incluso test diretti delle soluzioni proposte. In questo modo, è stato possibile integrare le risorse teoriche con esperimentazioni concrete, permettendo di superare le difficoltà e garantire una comprensione completa e applicata delle soluzioni di cybersecurity.

PARTE SECONDA – PREDISPOSIZIONE DELL'ELABORATO	
Obiettivi dell'elaborato/progetto/artefatto:	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. La tesi è frutto dello studio di normative internazionali quali la serie delle norme ISO/IEC 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. È stato progettato e redatto un documento che introduce al calcolo del fattore di rischio. 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. 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:	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.

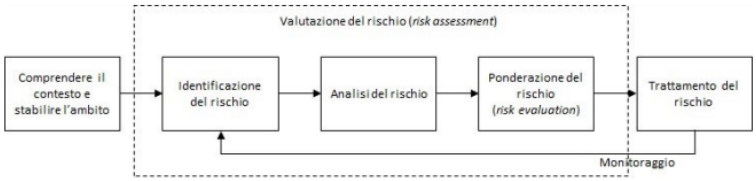
Descrizione dei principali aspetti progettuali:	**“La valutazione dei rischi è lo strumento che consente di rendere stimabile ciò che non può essere deterministicamente calcolato”** **Calcolo del fattore di rischio** Il rischio è definito come l'indicatore del grado di allontanamento da una condizione 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 presenza dei seguenti fattori:

1. un bene di valore colpito,
2. una fonte di minaccia,
3. una vulnerabilità preesistente,
4. un impatto dannoso.

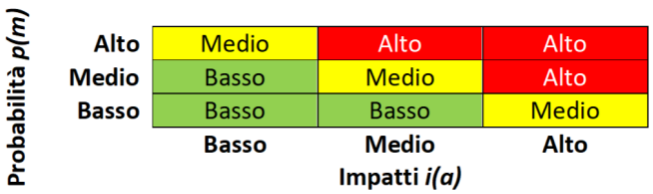
Descrivere il rischio come scenario facilita l'analisi della probabilità di accadimento e la quantificazione dell'impatto. Inoltre, pone le basi per la successiva definizione delle contromisure, preventive o protettive che siano.
È utile categorizzare i rischi in quattro aree principali, suggerite dal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

Elementi della Sicurezza delle Informazioni

La **sicurezza delle informazioni** si riferisce allo stato in cui le informazioni e le infrastrutture sono protette da rischi come il furto, la manomissione o l'interruzione dei servizi, mantenendo tali minacce a livelli tollerabili o minimi. Questa sicurezza si fonda su cinque principi fondamentali: riservatezza, integrità, disponibilità, autenticità e non ripudio.

Riservatezza
La riservatezza garantisce che solo gli utenti autorizzati possano accedere alle informazioni. Le violazioni di questa riservatezza possono derivare da pratiche di gestione inadeguate dei dati o da attacchi informatici. Le misure per proteggere la riservatezza comprendono la classificazione dei dati, l'uso della crittografia e la gestione sicura delle apparecchiature, come la distruzione di dispositivi di memorizzazione (DVD, USB, Blu-ray).

Integrità
L'integrità riguarda la protezione dei dati da alterazioni non autorizzate, assicurando che le informazioni rimangano precise e affidabili per il loro utilizzo. Per garantire l'integrità dei dati, si adottano strumenti come i checksum, che verificano la coerenza dei dati, e i controlli degli accessi, che limitano le operazioni di modifica, aggiunta o cancellazione a utenti autorizzati.

Disponibilità
La disponibilità implica che i sistemi che gestiscono, immagazzinano e elaborano le informazioni siano accessibili quando necessario dagli utenti legittimi. Per assicurare la disponibilità, vengono utilizzate soluzioni come sistemi di archiviazione ridondanti (array di dischi) e configurazioni clusterizzate per garantire la continuità del servizio in caso di guasti.

Autenticità
L'autenticità riguarda la caratteristica di comunicazioni, documenti o qualsiasi dato che garantisce la loro genuinità e integrità, evitando alterazioni. Il principale obiettivo dell'autenticazione è quello di verificare l'identità di un utente. Strumenti come le impronte biometriche, le carte intelligenti e i certificati digitali sono utilizzati per confermare l'autenticità di dati, transazioni, comunicazioni e documenti, assicurando che siano effettivamente originari e non manipolati.

Non Ripudio
Il non ripudio è un principio che garantisce che il mittente di un messaggio non possa successivamente negare di averlo inviato e che il destinatario non possa rifiutarsi di riconoscere di averlo ricevuto. Per garantire il non ripudio, si ricorre all'uso di firme digitali, che permettono di confermare l'autenticità e l'integrità del messaggio, evitando ogni possibile disconoscimento da parte delle persone coinvolte.

Strategia di Sicurezza Continua/Adattiva

La strategia di sicurezza adattiva prevede che vengano adottate azioni continue di previsione, prevenzione, rilevamento e risposta per garantire una difesa completa delle reti informatiche.

Protezione
Questa fase include una serie di misure preventive mirate a eliminare tutte le vulnerabilità potenziali presenti nella rete. Comprende misure di sicurezza come le politiche di sicurezza, la sicurezza fisica, la protezione degli host, i firewall e i sistemi di rilevamento delle intrusioni (IDS).

Rilevamento
Il rilevamento implica l'analisi della rete per individuare anomalie, come attacchi, danni, tentativi di accesso non autorizzato e modifiche, e per localizzarle all'interno della rete. Questo processo prevede il monitoraggio regolare del traffico di rete tramite strumenti di monitoraggio e analisi dei pacchetti.

Risposta
La risposta agli incidenti comprende azioni come l'identificazione degli eventi, l'individuazione delle loro cause principali e la pianificazione di un intervento per affrontarli. Questa fase include la risposta agli incidenti, l'investigazione, il contenimento, la mitigazione degli impatti e l'eradicazione dei problemi, nonché la determinazione se l'incidente rappresenta una vera minaccia o è un falso positivo.

Previsione
La previsione riguarda l'individuazione di potenziali attacchi, obiettivi e metodi prima che si concretizzino in un attacco effettivo. Include azioni come la valutazione del rischio e delle vulnerabilità, l'analisi della superficie di attacco e l'analisi delle informazioni relative alle minacce per prevedere i rischi futuri per l'organizzazione.

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)

E' una delle leggi più rigorose al mondo in materia di privacy e sicurezza. Pur essendo stato redatto e adottato dall'Unione Europea (UE), impone obblighi anche a organizzazioni al di fuori dell'UE, purché trattino dati relativi a persone residenti nell'UE. Il regolamento è entrato in vigore il 25 maggio 2018 e prevede sanzioni pesanti per coloro che violano i suoi standard di privacy e sicurezza, con multe che possono raggiungere decine di milioni di euro. Con il GDPR, l'Europa ha rafforzato la sua posizione sulla protezione dei dati personali in un contesto in cui sempre più persone affidano i propri dati a servizi cloud, e le violazioni della sicurezza sono all'ordine del giorno. Il regolamento stesso è ampio, di portata globale e relativamente vago nei dettagli, il che rende la conformità al GDPR una sfida impegnativa, soprattutto per le piccole e medie imprese (PMI).

Principi di Protezione dei Dati del GDPR
Il GDPR include sette principi di protezione e responsabilità, definiti nell'Articolo 5.1-2:

- **Liceità, equità e trasparenza**: Il trattamento deve essere lecito, equo e trasparente per l'interessato.
- **Limitazione delle finalità**: I dati devono essere trattati per scopi legittimi, esplicitamente comunicati all'interessato al momento della raccolta.
- **Minimizzazione dei dati**: I dati devono essere raccolti e trattati solo nella misura necessaria per gli scopi indicati.
- **Accuratezza**: I dati personali devono essere mantenuti accurati e aggiornati.

Il **GDPR** richiede inoltre 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), per garantire che i trattamenti di dati non comportino rischi per i diritti e le libertà degli individui.

Queste misure devono essere integrate nei processi aziendali quotidiani per garantire la conformità continua e minimizzare il rischio di sanzioni.

ISO/IEC 27001

Stabilisce i requisiti per la creazione, l'implementazione, il mantenimento e il miglioramento continuo di un sistema di gestione della sicurezza delle informazioni all'interno di un'organizzazione. La norma include requisiti per la valutazione e il trattamento dei rischi relativi alla sicurezza delle informazioni, personalizzati in base alle esigenze specifiche dell'organizzazione.

Tra gli obiettivi principali della norma vi sono:

- **Identificazione e valutazione dei rischi** (clausola 6.1.2), per rilevare minacce e vulnerabilità specifiche.
- **Pianificazione delle azioni di mitigazione** (clausola 6.1.3), per ridurre i rischi identificati e stabilire misure correttive.
- **Monitoraggio e miglioramento continuo** (clausola 9), per garantire che il sistema di gestione della sicurezza evolva costantemente e rimanga efficace.

Inoltre, la norma **ISO/IEC 27001** è progettata per essere utilizzata in vari contesti all'interno delle organizzazioni, come:

- Formulazione di requisiti e obiettivi di sicurezza.
- Gestione dei rischi di sicurezza in modo economico ed efficiente, ottimizzando risorse e costi.
- Garantire la conformità alle leggi e normative applicabili in materia di sicurezza delle informazioni.
- Definizione di nuovi processi di gestione della sicurezza delle informazioni e miglioramento di quelli esistenti.
- Determinazione dello stato delle attività di gestione della sicurezza da parte della direzione dell'organizzazione.
- Implementazione di una sicurezza delle informazioni che favorisca il business, supportando obiettivi strategici.
- Fornire informazioni rilevanti sulla sicurezza delle informazioni ai clienti, aumentando la trasparenza e la fiducia.

L'adozione di questa norma consente alle organizzazioni di costruire un sistema di gestione della sicurezza delle informazioni che risponde alle esigenze specifiche del settore ICT, migliorando la protezione delle informazioni aziendali e dei dati sensibili.

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”

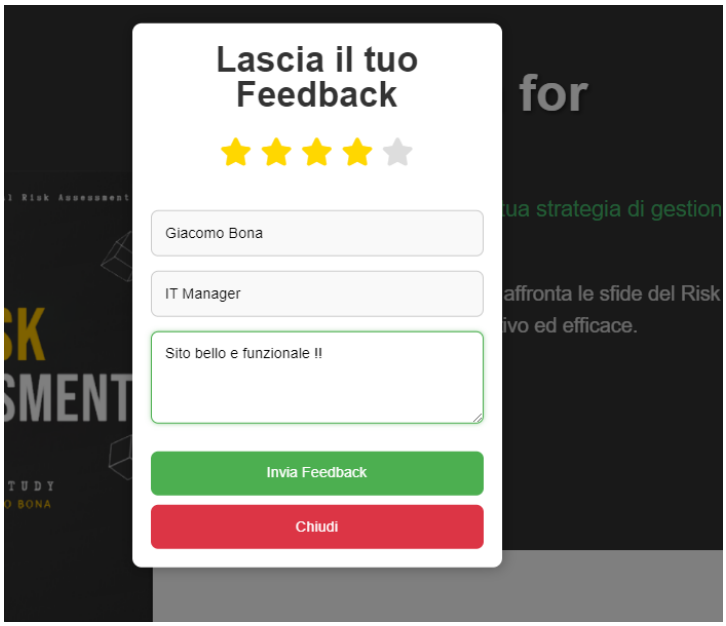
Codice RAW

```
<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>
```

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

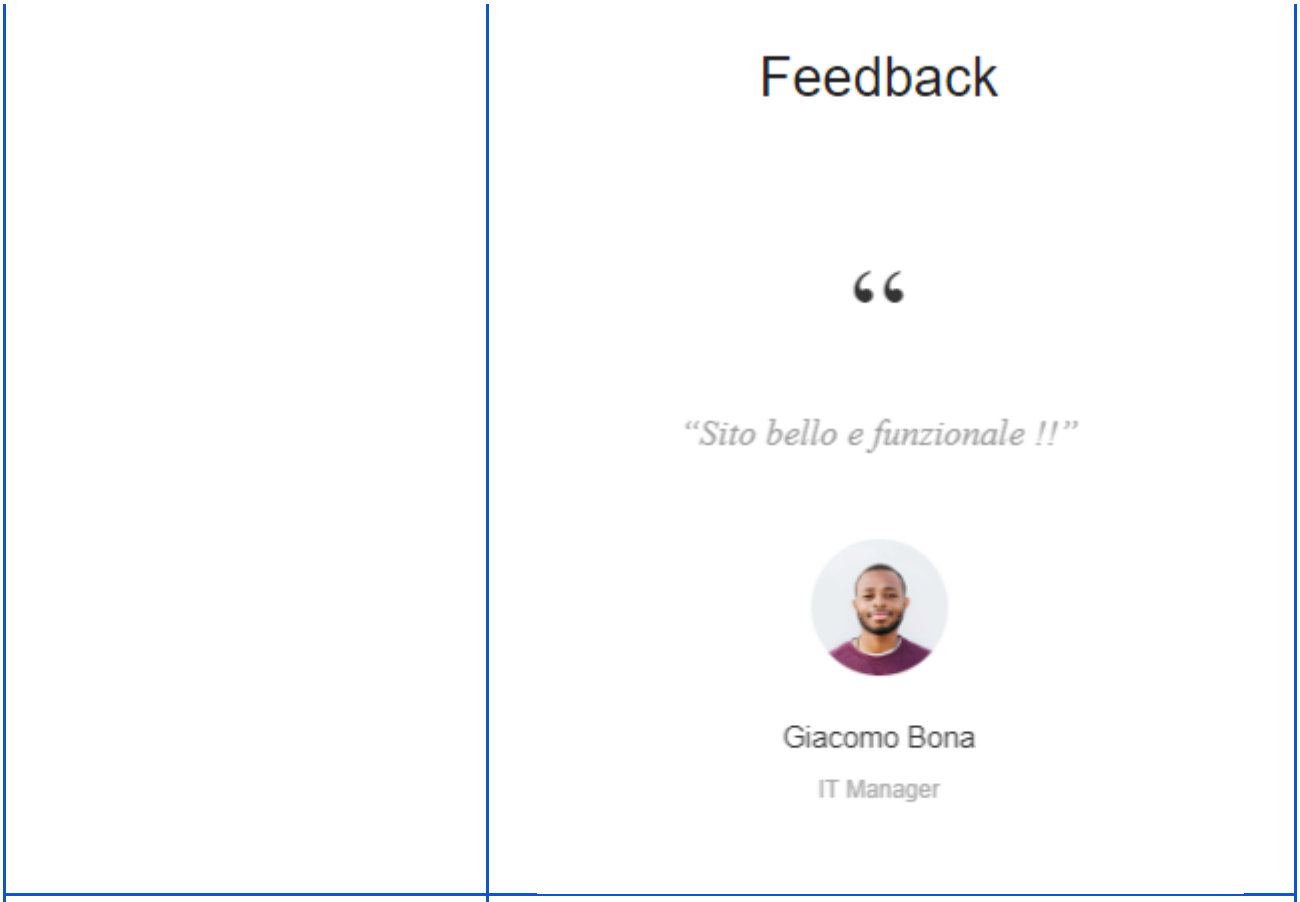
```
<script>
  // Funzione per aprire il popup
  function openPopup() {
    document.getElementById("popup").style.display = "block";
    document.getElementById("popup-overlay").style.display = "block";
  }
  // Funzione per chiudere il popup
  function closePopup() {
    document.getElementById("popup").style.display = "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:	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):	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.