

Corso di Studio	INFORMATICA PER LE AZIENDE DIGITALI (L-31)
Dimensione dell'elaborato	Minimo 6.000 – Massimo 10.000 parole (<i>pari a circa Minimo 12 – Massimo 20 pagine</i>)
Formato del file da caricare in piattaforma	PDF
Nome e Cognome	Vincenzo Maione
Numero di matricola	0312201095
Tema n. (Indicare il numero del tema scelto):	2
Titolo del tema (Indicare il titolo del tema scelto):	Privacy e sicurezza aziendale
Traccia del PW n. (Indicare il numero della traccia scelta):	3
Titolo della traccia (Indicare il titolo della traccia scelta):	Sviluppo di un software per la sicurezza aziendale.
Titolo dell'elaborato (Attribuire un titolo al proprio elaborato progettuale):	Sicurezza delle informazioni e valutazione del rischio: analisi normativa e sviluppo di un'interfaccia web.

PARTE PRIMA - DESCRIZIONE DEL PROCESSO

Utilizzo delle conoscenze e abilità derivate dal percorso di studio

il processo di trasformazione digitale che nel giro degli ultimi anni ha interessato anche le PMI ha causato un'accelerazione importante dell'adozione di procedure e processi di digitalizzazione anche nei contesti più tecnici ed operativi, che non erano ancora pronti a questo tipo di evoluzione.

Nelle moderne organizzazioni le applicazioni software sono aumentate a dismisura, anche per le operazioni ordinarie e, se da un lato comporta un vantaggio operativo, dall'altro inevitabilmente comporta un notevole aumento della mole di dati acquisiti e archiviati. Questi scenari rappresentano, purtroppo, un terreno fertile per l'intensificarsi delle minacce informatiche, sollevando non poche preoccupazioni sulla sicurezza e sulla protezione dei dati raccolti.

La stesura di questo progetto mi ha permesso di mettere alla prova gli insegnamenti acquisiti durante tutto il percorso universitario; in particolare evidenzio i corsi:

- **Diritto per le aziende digitali:** Un corso molto interessante, non solo per le normative inerenti al GDPR, ma per gli argomenti trattati in particolare per l'importanza data al **dato personale** sempre più spesso trascurato nella società in cui viviamo e in particolare nei trattamenti svolti; Oramai è diventato così semplice riempire dei moduli con dei dati che quasi non ci rendiamo conto di come verranno trattati e di chi li userà.
- **Reti di calcolatori e cyber security:** È stato un corso che ha suscitato in me un notevole interesse. L'esperienza lavorativa mi ha permesso di acquisire molti concetti a riguardo, ma solo tramite lo studio della materia ho trovato anche una solida base teorica sugli argomenti e sulle dinamiche trattate. Associare una visione didattica alla prospettiva quotidiana professionale è stato molto stimolante, mi ha permesso di ampliare le conoscenze con l'introduzione di nuovi concetti riguardo la sicurezza informatica e le infrastrutture delle reti. La materia è strettamente collegata alla valutazione dei rischi in ambito privacy e sicurezza, in quanto, conoscere le tecniche di intrusione permette di anticipare le possibili mosse degli attaccanti e implementare misure di difesa più pervasive.

La vera sicurezza si costruisce prima - *articolo 25 del GDPR - Privacy by Design e Privacy by Default.*

- **Tecnologie web:** Le competenze acquisite in questo corso mi hanno dato la possibilità di redigere la parte finale dell'elaborato. Lo studio e le esercitazioni mi hanno permesso di sviluppare una **pagina web dedicata**, utilizzando il linguaggio HTML e CSS. Un design responsive permette alla pagina di adattarsi in modo efficace a diversi dispositivi.

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):

Per la redazione completa del project work ho impiegato circa 180 ore complessive. Ho articolato il lavoro che ha portato alla stesura di questo progetto in più fasi:

1- Analisi preliminare: - Durata 3 giorni -

La scelta della traccia mi ha portato ad immedesimarmi in un titolare del trattamento che non ha molte conoscenze da un punto di vista sia tecnico che normativo riguardo la sicurezza dei dati. Ho preferito questo approccio perché è quello che rispecchia forse la gran parte delle aziende che per via dei cambiamenti di mercato si trovano ad affrontare, quasi travolte, sistemi di raccolta e condivisione dati, sia per l'organizzazione interna che per l'attività commerciale in generale. Le azioni intraprese, spesso, sono irrazionali e senza le dovute precauzioni.

2- Definizione del contesto e degli obiettivi: - Durata meno di 5 giorni -

L'idea era quella di riferirsi ad una PMI, ipotesi rafforzata dall'analisi preliminare svolta. L'obiettivo principale era chiaro: bisognava trovare un approccio semplice e preciso per introdurre gradualmente concetti chiave sulla sicurezza, fino a raggiungere il concetto della valutazione del rischio.

3- Analisi normative preliminare: - Durata 1 settimana -

L'analisi e lo studio del quadro normativo si è rivelato necessario: Nello specifico la valutazione del rischio non è solo una buona prassi, ma è un obbligo previsto dal Regolamento (UE) 2016/679; di conseguenza il richiamo al GDPR si è reso fondamentale. Ho ritenuto opportuno menzionare alcuni principi e articoli a mio avviso cardini per trattare e comprendere al meglio l'argomento scelto.

4- Raccolta della documentazione: - Durata 1 settimana -

In questa fase mi sono occupato di: ricerca e selezione di materiali utili a supportare la stesura del project work. Ho raccolto riferimenti giuridici necessari a tale scopo, non solo relativi al GDPR, ma anche articoli specialistici come i report pubblicati da ENISA, questo mi ha permesso di introdurre il contesto applicativo e evidenziare l'aumento del numero degli attacchi informatici e la loro complessità. Contemporaneamente, ho raccolto documentazioni ISO, approfondendo solo gli aspetti fondamentali riguardanti il progetto, in particolare ho estrapolato i termini chiave per introdurre ed affrontare con consapevolezza il tema sicurezza della protezione dei dati e della relativa matrice del rischio. Tutto questo materiale mi ha permesso di consolidare i concetti e raggiungere una padronanza di metodo e di terminologia fondamentale per l'acquisizione delle capacità teorico-pratiche.

5- Redazione del project work: - Durata 3 settimane -

Stesura vera e propria del PW: Il contenuto è stato suddiviso in sezioni, organizzate secondo un ordine logico. Ho introdotto termini nuovi solo dopo averli illustrati, cercando di utilizzare un linguaggio chiaro, ma allo stesso tempo tecnico.

6- Creazione di una pagina HTML: - Durata 1 settimana -

Fase conclusiva, la più pratica. La creazione di una pagina in linguaggio HTML e CSS che permetta il download di questo documento.

7- Revisione finale e riflessioni personali: - Durata 1 settimana -

In questa fase, ho corretto alcuni refusi e perfezionato la terminologia. È stata anche l'occasione per rileggere il progetto con un occhio più riflessivo e critico. Ho terminato l'attività a cui ho dato un forte valore non solo per ciò che rappresenta dal punto di vista accademico, ma anche per il suo significato umano e professionale.

Le normative spesso utilizzano una terminologia molto tecnica e inusuale. Per questo motivo si è ritenuto utile predisporre una sezione dedicata per chiarire termini e concetti, in ambito privacy e

sicurezza. Per non appesantire il testo, con spiegazioni molto teoriche, ho ritenuto utile portare solo i riferimenti più significativi.

Laddove necessario, sono stati esplicitati alcuni articoli chiave del GDPR e di alcune norme ISO internazionali relative alla sicurezza, con l'obiettivo di facilitare la comprensione dei contenuti sviluppati in questo contesto.

Un'ulteriore difficoltà ha riguardato l'approccio ENISA seguendo il modello semplificato. È un framework adatto per le PMI, ma non sempre si adatta a tutti gli scenari. Per superare questo limite ho portato un esempio di un caso reale attribuendo i valori di probabilità e di impatto quanto più realistici possibili nelle tabelle, in modo da rendere la valutazione più concreta.

Un altro aspetto che ho dovuto affrontare nella valutazione del rischio in ambito privacy e sicurezza riguarda la complessità dell'argomento. Le tecnologie di raccolta e trattamento dei dati si evolvono velocemente, e con esse anche i vari framework per la valutazione del rischio.

Da un lato, la molteplicità di approcci disponibili permette di selezionare quello più adatto al contesto operativo, da ciò ne deriva un vantaggio, in quanto i modelli esistenti si adattano alle realtà concrete.

Dall'altro lato, questa varietà può disorientare una persona meno esperta. Nel caso del seguente progetto, non è stato affatto semplice individuare il modello più adatto. Per superare questa difficoltà ho selezionato i concetti più rilevanti in materia di privacy e sicurezza, con lo scopo di portare alla luce una coerenza tra le normative e l'approccio proposto da ENISA, evidenziando come non esiste un modello predefinito valido per ogni azienda o per ogni trattamento dei dati.

Risorse e strumenti impiegati

Ho selezionato le risorse teoriche, le normative e i modelli necessari per trattare gli argomenti scelti e realizzare il seguente progetto

Purtroppo, in rete, non è facile orientarsi nel campo della sicurezza informatica e spesso la questione privacy e sicurezza è limitata esclusivamente ad aspetti interni o tecnici, tralasciando normative e conseguenze a discapito di tutti gli stakeholder. Il problema della sicurezza solo ultimamente sta ricevendo un interesse anche mediatico. Si menziona sempre il GDPR ma nello specifico mancano, a mio avviso, documentazioni chiare sulla sicurezza e la consapevolezza che la protezione dei dati passa per il fattore umano, il quale è il [punto critico di tutta la Cyber Security in generale. \[1\]](#)

Pertanto, la protezione dei dati non può limitarsi solo ed esclusivamente all'adozione di misure tecniche di prevenzione o al rispetto delle normative. Occorre implementare modelli di analisi dei rischi che monitorino costantemente il livello di esposizione dei dati e adottare misure, sia tecniche che, soprattutto formative, per limitare i danni.

La valutazione dei rischi è stata illustrata attraverso l'utilizzo del **modello ENISA**.

Si tratta di un modello specifico per le piccole e medie imprese.

NORME E REGOLAMENTI CONSIDERATI:

- [ISO/IEC 27005:2022 \[2\]](#): La norma è stata menzionata nel progetto per la definizione dello **scenario del rischio**. Essa è collegata alla **ISO/IEC 27001** e fornisce linee guida per identificare, analizzare e valutare i rischi legati alla sicurezza delle informazioni.
- [ISO/IEC 27001 – SGSI \[3\]](#) - SGSI è uno standard internazionale, supporta le organizzazioni nell'adottare un sistema di gestione della sicurezza delle informazioni (SGSI).

Lo standard evidenzia le tre colonne portanti della sicurezza delle informazioni:

- **Riservatezza** (Protezione dei dati dagli accessi non autorizzati)
- **Integrità** (Offrire la garanzia che i dati non vengano alterati o corrotti in tutte le fasi del trattamento, sia in modo accidentalmente, a seguito di una violazione dei dati, sia per azioni intenzionali).

- **Disponibilità** (Le informazioni devono essere sempre disponibili, su richiesta degli interessati).

- **ISO Guide 73:2009 [4]:** Utilizzata per la **definizione terminologica** del rischio.
- **Regolamento (UE) 2016/679 – GDPR [5]:** entrato in vigore nel 2018:

Il Regolamento, nato principalmente con l'obiettivo di tutelare i dati personali degli interessati, garantisce e protegge i loro diritti fondamentali. La normativa incoraggia responsabilità e trasparenza nel trattamento delle informazioni.

Il richiamo al GDPR, è stato necessario in quanto è il principale riferimento europeo; inoltre, si è rivelato utile per introdurre il concetto di **responsabilizzazione**. La valutazione dei rischi si basa su un concetto fondamentale: il titolare del trattamento, in piena libertà e autonomia decisionale e conoscendo la natura dei dati trattati, la modalità di raccolta e la loro conservazione, valuta il rischio del trattamento in piena accountability. (*articolo 5, paragrafo 2 del GDPR*)

La valutazione del rischio, infatti, oltre a rappresentare un obbligo per il titolare del trattamento, deve essere intesa come un punto d'inizio per definire strategie, organizzazione e procedure, e non come un semplice punto di arrivo.

- Alcuni **considerando del GDPR**, che aiutano a chiarire il significato di specifici articoli del Regolamento, risultano essenziali per comprendere il contesto normativo del progetto.

STRUMENTI UTILIZZATI:

Per la realizzazione della pagina web sono stati utilizzati i seguenti strumenti:

- **Visual Studio Code – VS Code [6] - rif. Wikipedia** : Editor di codice sorgente sviluppato da Microsoft, utilizzato per la creazione della pagina web. È stato utilizzato per la sincronizzazione con GitHub.
- **GitHub [7]:** Servizio di Hosting dedicato principalmente alla condivisione di codice sorgente. I file del progetto sono stati archiviati in un repository, offerto dal servizio. Il plugin GitHub è stato integrato direttamente in VS Code, questo ha permesso la sincronizzazione tra VS Code e la repo online, grazie alle funzioni *commit* e *push*.
- **Google Moduli:** Servizio offerto da Google Inc. utilizzato per la creazione e la gestione del questionario di valutazione ed integrato successivamente nella pagina HTML
- **Google Drive:** Usato per catalogare le risposte del questionario e generare i grafici.
- **Canva.com:** Strumento on line per progettare grafica, utilizzato per la realizzazione di immagini illustrative e tabelle per report ENISA.
- **Browser web** (Chrome – Edge) usati per testare e visualizzare le pagine web e l'usabilità.
- **Estensione “Mobile First” (Fig. 8)** utile a testare la pagina web su diversi dispositivi e dimensioni di schermo.



Fig. 8

RIFERIMENTI BIBLIOGRAFICI E LINK PUBBLICI:

- [1] **Il fattore umano nella protezione dei dati – il vero punto critico del cyber security:**
<https://www.cybersecurity360.it/cultura-cyber/la-vulnerabilita-invisibile-perche-il-fattore-umano-e-il-vero-punto-critico-della-cyber-security/>
- [2] **ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection - Guidance on managing information security risks.**
<https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en>
- [3] **ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection - Information security management systems**
<https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en>
- [4] **ISO/IEC Guide 73:2009 - For principles and guidelines on risk management – Risk management vocabulary**
<https://www.iso.org/standard/44651.html>
- [5] **GDPR - Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.**
<https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [6] **Visual Studio Code – Definizione Wikipedia**
<https://w.wiki/EbUt>
- [7] **GitHub**
<https://github.com/>
- [8] **WebMobileFirst (2024) - Responsive Design Testing Tool.**
<https://www.webmobilefirst.com/>
- [9] **ENISA – European Union Agency for Cybersecurity. –**
<https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape>
- [10] **ENISA – 2024 Report on the State of the Cybersecurity in the Union. -**
<https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>
- [11] **ISO 31000:2018 – Risk management – Guidelines -**
<https://www.iso.org/standard/65694.html>
- [12] **GOOGLE FORMS – Servizio gratuito offerto da Google per la creazione di sondaggi on line, con la possibilità di integrazione all'interno di pagine web.**

PARTE SECONDA – PREDISPOSIZIONE DELL'ELABORATO

Obiettivi del progetto

(Descrivere gli obiettivi raggiunti dall'elaborato, indicando in che modo esso risponde a quanto richiesto dalla traccia):

Il presente elaborato si propone come una guida pratica per la valutazione dei rischi in ambito privacy. Pur scegliendo volutamente un approccio molto semplificato al risk management, è stata data importanza all'aspetto delle normative. Un obiettivo del Project Work è far comprendere che la protezione dei dati non è solo una questione di principi morali, ma anche legale.

Frequentemente si fa uso del termine 'privacy' in modo molto generico, circoscrivendo la maggior parte degli aspetti rilevanti in un concetto di riservatezza. Ma nello specifico: perché si parla di privacy e di valutazione dei rischi quando si effettua un trattamento e perché è così importante? È da questo punto di domanda che si è scelto di partire, cercando di guidare il lettore in un percorso di consapevolezza sull'importanza della protezione del dato.

Un altro obiettivo prefissato è quello di andare a chiarire i concetti che fanno da base alle normative in materia di privacy e sicurezza: spesso si avviano dei trattamenti sui dati ignari delle conseguenze e si intraprendono delle procedure e dei processi al limite della sicurezza, talvolta per negligenza o per sottovalutazione del problema. Andare a determinare un fattore di rischio, per una piccola e media impresa, può essere un'operazione complessa pur essendo assolutamente necessario per garantire la conformità al GDPR; l'adozione di un approccio come quello proposto da ENISA semplifica di molto la valutazione del rischio: un metodo elementare, ma non per questo meno efficace.

Un ulteriore obiettivo riguarda la pubblicazione e la diffusione del presente documento. La guida alla valutazione del rischio sarà scaricabile, in formato pdf, da una pagina web, sviluppata utilizzando il linguaggio HTML5 e CSS3, strutturata con un design responsive, che si adatta alle diverse risoluzioni degli schermi dei diversi dispositivi. È stata prestata una maggiore attenzione al layout, rendendolo quanto più professionale e garantendo una buona leggibilità del documento. Nella pagina web, inoltre, è stato integrato un questionario per valutare il grado di soddisfazione del lettore e le possibili aree di miglioramento.

Contestualizzazione

(Descrivere il contesto teorico e quello applicativo dell'elaborato realizzato):

Prima di addentrarci nel percorso che ci porterà alla definizione e documentazione della valutazione dei rischi in ambito privacy e sicurezza, è importante conoscere il contesto attuale riguardo ai rischi reali cui le nostre aziende sono esposte. Per comprendere meglio questo aspetto i dati dei report di [ENISA \(European Union Agency for Cybersecurity\) \[9\]](#) che ricordiamo essere un organo ufficiale che periodicamente pubblica report sullo stato delle infezioni e sulle tecniche usate, ci aiutano a comprendere meglio la gravità della situazione.

ENISA ha pubblicato un report sullo stato delle minacce alla sicurezza informatica nei paesi UE: [2024 Report on the State of the Cybersecurity in the Union \[10\]](#).

Il report analizza un periodo compreso tra la fine del 2023 e la metà del 2024.

Vengono analizzati circa 11079 incidenti informatici.

L'aumento degli incidenti di sicurezza ha una forte correlazione con la situazione instabile tra Russia e Ucraina, il report ENISA 2024 sottolinea infatti questo legame. Gli attacchi, in forte aumento, sono principalmente di natura DDoS ((Distributed Denial of Service) [Fig. 2](#), essi sono pianificati da gruppi di attivisti, che mirano a rendere inaccessibili siti istituzionali o di grandi aziende.

Un simile attacco è stato sferrato da un noto gruppo hacker russo "NoName057" nei confronti di ministeri e forze dell'ordine, rif. <https://tg24.sky.it/tecnologia/2025/02/18/noname-attacco-hacker-italia>, sono attacchi informatici non semplici da individuare e contrastare in quanto i dispositivi che partecipano sono distribuiti su zone geografiche molto ampie.

In ordine, ma non per importanza, si registra un numero record di attacchi di tipo ransomware, una minaccia molto preoccupante per due motivi. Il primo obiettivo è sottrarre denaro alle imprese, obbligandole a pagare un riscatto per potersi riappropriare dei propri dati, in quanto vengono crittografati. Il secondo motivo, quello più allarmante e che più ci preoccupa, riguarda la diffusione sul dark web dei dati degli interessati, raccolti dalle aziende per fini leciti. La diffusione incontrollata genera trattative di scambio sul mercato nero per appropriarsi dei dati degli utenti per fini illeciti, compromettendo seriamente la loro privacy e sicurezza.

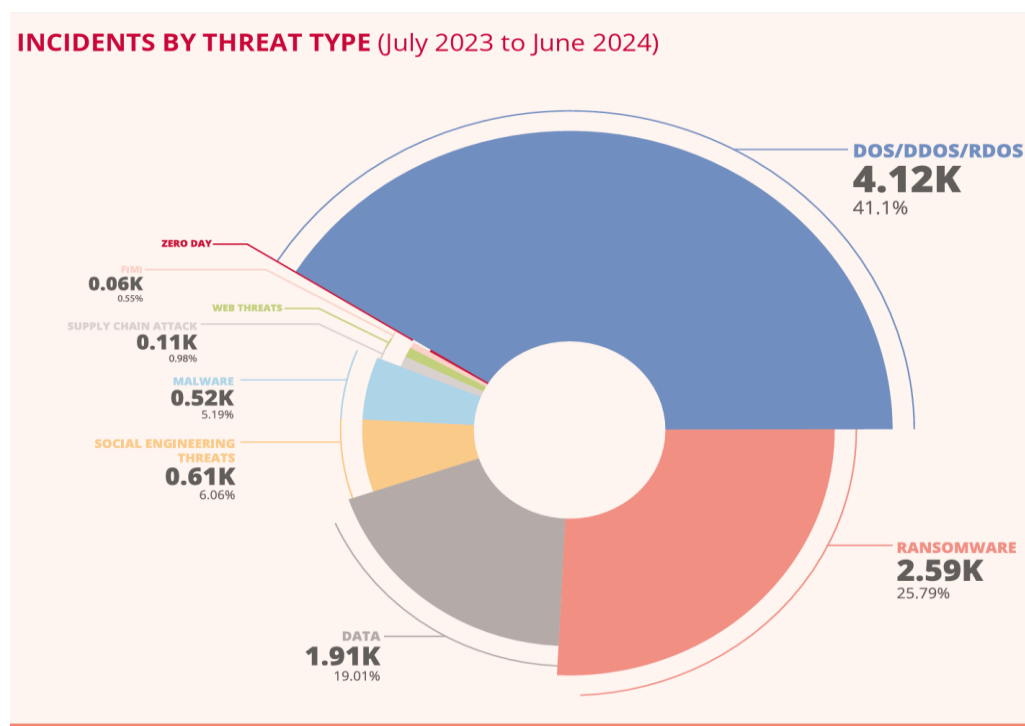


Fig.2

I continui attacchi informatici e la velocità con cui le tecniche cambiano e si aggiornano mettono a dura prova la protezione dei dati personali e aziendali, rendendola una sfida sempre più complessa. Le aziende affrontano il processo di digitalizzazione con un certo timore ed incertezza per aspetti riguardanti la sicurezza.

Sempre più dati vengono raccolti e inseriti in archivi informatici. L'interoperabilità dei sistemi sta raggiungendo ormai livelli significativi, complice anche la diffusione di soluzioni cloud e smart working.

Si tratta di dinamiche che creano un mix perfetto per vulnerabilità e accessi indesiderati da parte di potenziali hacker, la protezione dei dati personali si è trasformata, in sostanza, in una delle priorità nel mondo digitale e l'entrata in vigore del Regolamento (UE) 2016/679 (GDPR) che mira, tra i suoi obiettivi principali, a rendere più agevole e quindi favorire la diffusione di nuove tecnologie, mette in risalto la protezione dei dati e dei diritti fondamentali dei cittadini, in ambito privacy.

Con l'introduzione del GDPR la valutazione dei rischi ha assunto un ruolo determinante nella gestione del trattamento dei dati.

Il Regolamento ha introdotto un importante cambiamento nell'approccio alla protezione dei dati personali andando ad abbandonare del tutto il modello che si basava esclusivamente su adempimenti formali per poi andare ad adottare un modello fondato sul principio della **responsabilizzazione** (accountability).

Il Regolamento non soltanto obbliga il titolare o ove previsto, il responsabile del trattamento, a rispettare la normativa; gli addetti ai lavori devono anche essere in grado di dimostrare che i processi messi in atto siano ben documentati - *articolo 5, paragrafo 2 GDPR* -

Effettuare un'attenta valutazione dei rischi già durante la fase della progettazione di un sistema per trattamento dei dati (privacy by design) è importantissimo - *articolo 25 GDPR* - e permette di andare a valutare in modo adeguato le potenziali vulnerabilità adottando delle misure preventive volte a ridurre il rischio ed, eventualmente, ad attuare degli accorgimenti tecnici per la mitigazione ed il ridimensionamento.

Possiamo affermare, quindi, che la valutazione del rischio e il principio di accountability sono due facce della stessa medaglia. Per l'analisi e la valutazione del rischio, in questo elaborato, è stata presa in considerazione un'azienda operante nel settore IT, specializzata nel gestire assistenza ai sistemi informatici della Grande Distribuzione Organizzata (GDO).

Descrizione dei principali aspetti progettuali

(Sviluppare l'elaborato richiesto dalla traccia prescelta):

Per comprendere il calcolo del fattore di rischio, è necessario innanzitutto consolidare alcuni concetti chiave. Sono stati selezionati quelli ritenuti indispensabili per il metodo di analisi valutato:

- 1) **Minaccia** - è la potenziale causa di un incidente di sicurezza informatica, che può causare danni anche ingenti ad un'organizzazione e, quindi, determinare impatti negativi sugli asset aziendali e sui dati personali (si rimanda alla definizione dei termini "impatto" e "incidente" nelle sezioni successive). Le minacce più comuni possono riguardare diverse categorie: **Danni Fisici** (Vandalismo, furto, sabotaggi, incendi) - **Eventi Naturali** (terremoti, temporali, eventi che in generale possono provocare un blackout ed impedire l'accesso ai dati o distruggerli del tutto) - **Azioni non autorizzate** (Non si parla solo di malware, spam, attacchi DDOS ma anche di minacce causate da accessi di personale non autorizzato, es. assistenza tecnica in una sala server.)
- 2) **Vulnerabilità** - è la debolezza in un sistema, in una procedura o in un processo. Può essere sfruttata da una minaccia per causare un danno. Le vulnerabilità si suddividono in tre categorie principali:
 - ❖ **Organizzative**: scaturiscono da procedure inefficaci o non costantemente aggiornate.
 - ❖ **Tecniche**: causate da sistemi operativi obsoleti, errate configurazioni hardware e software di apparati di sicurezza, crittografia debole e in generale vulnerabilità non ancora conosciute.
 - ❖ **Umane**: una vulnerabilità spesso trascurata, quella umana, ma è quella più

determinante. Le minacce sfruttano l'errore umano per accedere a dati riservati, spesso inducono l'utente -inconsapevole- a visitare sito clone o rispondere ad email fraudolenti (phishing).

3) Evento - secondo la *ISO Guide 73:2009*, un evento è "il verificarsi o il modificarsi di un particolare insieme di circostanze". Un evento può avere diverse cause e con conseguenze di natura diverse. Un evento può produrre una conseguenza non grave o nulla se in presenza di un rischio "controllato". Ad esempio, **una minaccia** può consistere nell'intercettazione di traffico di rete tramite sniffing. **Il rischio** può essere formato dal furto di dati da un datacenter, e le **conseguenze** possono determinare violazioni della privacy, sanzioni legali o danni reputazionali. Ciò nonostante, se il rischio è controllato, ad esempio tramite l'utilizzo della crittografia, i dati in possesso dei malintenzionati saranno inutilizzabili e pertanto l'evento avrà conseguenze non gravi o addirittura nulle. Possiamo concludere che la crittografia non limita l'evento ma riduce l'impatto.

4) Impatto - generalmente, nell'ambito della valutazione dei rischi, si attribuisce all'impatto un valore negativo. La norma ISO/IEC 27005:2022 definisce l'impatto come "*il livello di danno causato all'organizzazione a seguito di un incidente di sicurezza delle informazioni*" (il termine incidente verrà definito a breve).

La minaccia sfrutta una vulnerabilità e compromette i dati personali.

L'impatto può causare danni all'organizzazione a livello **reputazionale, economico e legale**; può determinare:

- a) Una **sanzione amministrativa**, inflitta dall'organo di controllo (Garante per la Protezione dei Dati Personali);
- b) Un **impatto negativo sul mercato**. Un impatto sui dati dei clienti può far perdere fiducia all'azienda, innescando una reazione a catena che coinvolge tutti gli stakeholders (clienti, fornitori, investitori);
- c) Un **aumento dei costi**. Ripristinare le infrastrutture e l'operatività a seguito di un impatto può essere molto costoso, sia in termini economici che di tempo.
- d) Un **impatto per gli interessati**. Un impatto sui dati può riguardare un furto d'identità o un danno economico ed anche un furto di dati sensibili, che potrebbe sembrare meno importante, ma che può comunque compromettere una posizione sociale dovuta alla diffusione di informazioni strettamente personali andando ad arrecare ingenti danni sia morali che psicologici.

L'impatto compromette almeno 1 di 3 principi base della sicurezza informatica:

Riservatezza, Integrità e Disponibilità. I tre concetti sopra menzionati sono presenti nella norma ISO/IEC 27001 e sono talmente importanti per la salvaguardia della privacy da essere inclusi nell'articolo 32 del GDPR, paragrafo 1, lett. b.

- ❖ **Riservatezza:** L'accesso non autorizzato a dati sensibili implica necessariamente una violazione della riservatezza, infatti, il GDPR considera tale evento una violazione della sicurezza ed in assenza d'un giusto consenso da parte dell'interessato, questa inadempienza può arrecare un rischio enorme per i diritti ed anche per le libertà delle persone fisiche causando danni fisici, materiali e morali.
- ❖ **Integrità:** Il responsabile dei dati deve garantire che siano privi di errori, (sia intenzionali che accidentali). L'integrità è caratterizzata da due aspetti che sono: correttezza e completezza delle informazioni.
- ❖ **Disponibilità:** È un diritto dell'interessato richiedere, in ogni momento, i dati che lo riguardano. Secondo l'articolo 15 del GDPR - "Diritto di accesso dell'interessato" - Il titolare del trattamento, qualora riceva una richiesta di accesso, è tenuto a fornire le finalità del trattamento, la categoria e i dati effettivamente raccolti.

- 5) **Incidente** - lo Standard Internazionale ISO/IEC 27005:2022 lo considera come un evento singolo o una serie di eventi, non desiderati, che compromettono almeno uno se non tutti i tre principi sopra menzionati. Gestire in modo efficace un incidente è essenziale per tutelare la sicurezza delle informazioni oltre alla conformità normativa. La gestione di un incidente passa inevitabilmente per un'attenta valutazione del rischio già in fase di progettazione dei processi che trattano i dati personali.
- 6) **Rischio** - per comprendere meglio il termine "Rischio" sono stati presi in considerazione due prospettive:
- a) **Considerando 75 del Regolamento (UE) 2016/679 (GDPR)**. Lo definisce come un effetto negativo sulla libertà e sui diritti degli interessati. Il considerando evidenzia come valutare i rischi sia un elemento chiave per gestire la privacy.
 - b) **La Norma tecnica ISO Guide 73:2009 - Risk Management Vocabulary** - definisce il rischio come <<Effetto dell'incertezza sugli obiettivi>>. Questa definizione descrive in modo molto chiaro il contesto in cui ci troviamo e ci guida alla valutazione del rischio. Ogni decisione presa comporta un certo grado di incertezza, e questa può influenzare il raggiungimento di obiettivi. È in questo spazio variabile che entra in gioco il concetto di rischio.

In ambito privacy e sicurezza attorno al concetto di rischio ruotano **elementi chiave**.

Sono aspetti fondamentali per costruire una valutazione dei rischi coerente:

- **Scenario del rischio:** La norma ISO/IEC 27005:2022, par. 3.1.14, definisce lo scenario del rischio una sequenza o combinazione di eventi che portano dalla causa iniziale alla conseguenza indesiderata (il rischio). Uno scenario di rischio si concretizza quando una minaccia sfrutta una vulnerabilità. Lo scenario aiuta a comprendere il contesto in cui il rischio si materializza e analizzandolo si possono mettere in pratica contromisure efficaci.
- **Proprietario del rischio:** È la persona o entità con la responsabilità e l'autorità di gestire un rischio. (Fonte: ISO/IEC 27005:2022, par. 3.1.5). Il concetto di proprietario del rischio nella norma ISO/IEC ha un parallelismo con il principio di accountability, sancito dall'articolo 5, par. 2 GDPR.
- **Fonte del rischio:** Nel processo di valutazione dei rischi, la fonte del rischio, è strettamente legata alla vulnerabilità. La differenza tra le due nozioni è sottile ma determinante:
 - **La fonte del rischio** è un elemento che, da solo o in combinazione con altri, ha il potenziale di generare un rischio, può essere una minaccia o un'attività umana, intenzionale o non. (Fonte: ISO 31000:2018) [11]
 - **La vulnerabilità** è una debolezza o una lacuna di un sistema o procedura che può essere sfruttata.
- **Conseguenza:** <<L'esito di un evento che influenza gli obiettivi>> Rif. ISO 31000:2018. Una conseguenza può essere:
 - **Diretta**, misura l'impatto direttamente con il sopraggiungere dell'evento.
Esempio: una violazione dei dati personali provoca la perdita di informazioni sensibili.
 - **Indiretta:** L'effetto dell'impatto non è subito visibile ed è legato a ripercussioni future.
Esempio: la perdita di credibilità da parte degli stakeholder, può causare un danno reputazionale. Conoscere le conseguenze è fondamentale per comprendere e calcolare correttamente il **fattore di rischio**.

Al termine di questa introduzione su vari concetti e termini chiave, si può affermare che la valutazione del rischio deve seguire un processo predeterminato, oggettivo ed in linea con la tipologia dei dati trattati. La consapevolezza dei trattamenti svolti e il livello del rischio risultante che potrebbe compromettere la sicurezza delle informazioni e la libertà degli interessati, sono in linea con i principi fondamentali del **Regolamento (UE) 2016/679**.

Determinante è il processo di valutazione del rischio che un titolare deve adottare. In questo contesto verrà proposto il metodo ENISA:


Il processo scelto, ENISA, è basato su un modello a fasi cicliche:

- 1) **Identificazione degli asset e dei trattamenti** - In questo primo step bisogna identificare cosa deve essere protetto; è importante analizzare la finalità del trattamento al fine di poter comprendere le categorie dei dati trattati. Il risultato di questa fase preliminare delinea il contesto operativo dell'intero trattamento dei dati e costituisce la base su cui si poggia tutta la valutazione del rischio.
- 2) **Valutazione dell'impatto** - Il titolare del trattamento deve valutare il **potenziale impatto** che un incidente di sicurezza potrebbe avere sui dati personali e sui tre principi fondamentali della sicurezza: riservatezza, integrità e disponibilità, qualora una minaccia si concretizzasse

La valutazione dell'impatto può essere rappresentata in una **tabella a livelli (Tabella 1)**, La valutazione deve tener conto di aspetti importanti, quali:

- a) La tipologia dei dati trattati.
- b) Numero degli interessati potenzialmente coinvolti.
- c) L'eventuale possibilità che l'impatto possa essere annullato o rettificato in tempo, riducendo o eliminando le conseguenze dell'incidente.

A titolo esemplificativo si riporta di seguito una tabella che rappresenta i livelli di impatto in funzione degli scenari individuati:

 Tabella 1 VALUTAZIONE IMPATTO			
LIVELLO	DESCRIZIONE	SCENARIO	CRITERIO
1	Trascurabile	<ul style="list-style-type: none">• Violazione di dati personali già pubblici.• Violazione archivio di dati che non rendono possibile l'identificazione della persona, es. lista di soli nomi	<ul style="list-style-type: none">• L'impatto è trascurabile
2	Limitato	<ul style="list-style-type: none">• Violazione di dati che possono identificare una persona, es. numero di telefono, indirizzo email.• L'effetto della violazione può essere risolto ma richiede tempo e risorse	<ul style="list-style-type: none">• Impatto limitato sui diritti e libertà degli interessati.• La risoluzione non causa conseguenze gravi
3	Significativo	<ul style="list-style-type: none">• I dati della violazione rientrano nella categoria "particolari": Giudiziari e/o sanitari.<ul style="list-style-type: none">◦ Art. 4 GDPR, tali dati godono di una protezione rafforzata	<ul style="list-style-type: none">• L'impatto è grave e prolungato
4	Massimo	<ul style="list-style-type: none">• Le conseguenze della violazione sono gravi ed irreparabili, rimediare è quasi impossibile.• Violazione di dati biometrici• Furti d'identità	<ul style="list-style-type: none">• Impatto grave e irreversibile sui diritti e le libertà delle persone fisiche

3) **Identificazione delle possibili minacce e probabilità di accadimento:**

L'approccio ENISA prevede 4 livelli utili a valutare la probabilità di una minaccia.

I livelli sono determinati da una semplice checklist suddivisa in **quattro aree tematiche**:

- A - Rete e risorse tecniche (Hardware e software)**
- B - Processi e Procedure**
- C - Persone e soggetti coinvolti**
- D - Settore e scala del trattamento**

Per ogni area si risponde con “SI” o “NO” alle domande. La risposta “SI” sarà un indicatore della probabilità di accadimento del rischio collegato all’evento preso in considerazione. Saranno considerate solo le risposte con “SI”, per ciascun’area. **L’area che ottiene il punteggio più alto (Numero di risposte “SI”) è considerata la più critica**, e quel valore sarà utilizzato nella tabella della probabilità (Tabella 2).



Tabella 2

PROBABILITÀ

LIVELLO	NUMERO RISPOSTE “SI”	DESCRIZIONE DEL LIVELLO	CRITERIO
1	0 - 1	IMPROBABILE	L’episodio potrebbe verificarsi in avvenimenti rari (meno di una volta all’anno)
2	2	POCO PROBABILE	l’episodio potrebbe verificarsi in poche circostanze (una volta all’anno)
3	3	PROBABILE	L’episodio potrebbe verificarsi in poche circostanze (una volta al mese)
4+	4	MOLTO PROBABILE	L’episodio probabilmente si verificherà in moltissime circostanze (anche una volta a settimana)

DETERMINARE IL VALORE DELLA PROBABILITÀ - CASO PRATICO

Checklist ENISA, compilata per una PMI operante nel settore IT. si attribuisce per ogni area di probabilità un punteggio ed è stata aggiunta una colonna “NOTE” per giustificare la risposta.



Area tematica A :

RETE E RISORSE TECNICHE

DOMANDA	RISPOSTA	NOTE
Sistemi esposti su internet senza una protezione adeguata?	SI	Servizi Remote Desktop o FTP sono accessibili senza VPN o autenticazione a multi fattore
Software non aggiornati regolarmente?	SI	I sistemi vengono aggiornati ma non automaticamente e in modo discontinuo
Backup non cifrati o non testati?	SI	I backup vengono eseguiti ma non cifrati e non vengono eseguiti test per eventuali ripristini
Mancano sistemi di rilevamento intrusioni?	NO	Il sistema è provvisto di un firewall dotato di tecniche di rilevamento intrusione e filtraggio email, web e anti-spam



Area tematica B :

PROCESSI E PROCEDURE

DOMANDA	RISPOSTA	NOTE
Ruoli e responsabile non sono chiaramente definiti?	SI	Manca un organigramma valido e riconosciuto per la sicurezza IT.
Procedure di sicurezza non formalizzate?	SI	Le procedure sulla sicurezza mancano o non sono del tutto documentate
Accesso ai sistemi con dispositivi personali?	SI	I dipendenti possono usare notebook provati collegati alla rete aziendale
Operazioni sui dati non registrate in nessun log?	SI	Le operazioni sui dati non sono documentate nel registrate in appositi database



Area tematica C :

PERSONE E SOGGETTI COINVOLTI

DOMANDA	RISPOSTA	NOTE
Numero incaricati indefinito?	NO	L'elenco degli incaricati è presente.
Credenziali condivise tra utenti?	SI	Esistono account generici per effettuare login su più postazioni
Soggetti terzi accedono ai dati?	SI	Il servizio di assistenza al software contabile accede tramite controllo remoto non presidiato.
Archiviazione non sicura e cancellazione non definitiva dei dati personali?	SI	I dati non sono cifrati e nel caso di copie cartacee la distruzione non è sempre attuata con distruggi documenti



Area tematica D :

SETTORE E SCALA DEL TRATTAMENTO

DOMANDA	RISPOSTA	NOTE
Trattamento di dati sensibili o su larga scala?	NO	I dati trattati sono prevalentemente anagrafici e commerciali
Settore al alto rischio? Es. Sanità, finanza)	NO	L'impresa opera nel settore dei servizi
Attacco informatico o violazione negli ultimi 2 anni?	SI	Rilevato un attacco phishing compromettendo due caselle email.
Volume dei dati trattati molto elevato?	NO	Il database contiene circa 3.000 clienti, quantitativo considerato contenuto

Ecco il riepilogo dei valori per area (totale "SI")

- Rete e risorse tecniche: 3
- **Processi e procedure: 4 (Area Tematica B)**
- Persone e soggetti coinvolti: 3
- Settore e scala del trattamento: 1

Il valore massimo è 4, la probabilità finale è quindi "Molto Probabile":

- in base alla tabella 2 probabilità –

4) Valutazione del rischio con relativo calcolo:

Valutati impatto e probabilità di accadimento, si può procedere con la valutazione del rischio.

Il livello del rischio si ottiene moltiplicando il valore risultante della probabilità per il valore dell'impatto. (Fig.4)



Fig. 4

Il risultato di questo prodotto è un **valore compreso tra 1 e 16** (tabella 3):



Tabella 3

VALUTAZIONE DEL RISCHIO

VALORE DEL RISCHIO	COLORE ASSOCIATO NELLA GRIGLIA	LIVELLO DEL RISCHIO	DESCRIZIONE
1- 4	VERDE	BASSO	Il rischio è tollerabile, si consiglia solo il monitoraggio periodico.
5 - 8	GIALLO	MEDIO	Il rischio richiede attenzione e implementando misure di mitigazione , nel medio e lungo periodo, si può ridurre ad un livello accettabile.
9 - 12	ARANCIONE	ALTO	Il rischio è notevole e richiede misure urgenti nel breve termine
13 -16	ROSSO	CRITICO	Il rischio è inammissibile, richiede misure di mitigazione imediate

Per raffigurare i risultati del calcolo del rischio e per una semplice consultazione, ci serviamo della matrice del rischio (Fig. 5) composta da una griglia:

- Sull'asse orizzontale è raffigurato l'impatto del Rischio.
- Sull'asse verticale, la probabilità del Rischio.



LA MATRICE DEL RISCHIO

IMPATTO PROBABILITÀ	1 (Basso)	2 (Medio)	3 (Alto)	4 (Massimo)
1 (Improbabile)	1 (BASSO)	2 (BASSO)	3 (BASSO)	4 (MEDIO)
2 (Poco Probabile)	2 (BASSO)	4 (MEDIO)	6 (MEDIO)	8 (MEDIO)
3 (Probabile)	3 (BASSO)	6 (MEDIO)	9 (ALTO)	12 (ALTO)
4 (Molto Probabile)	4 (MEDIO)	8 (MEDIO)	12 (ALTO)	16 (CRITICO)

Vincenzo Maione

Fig.5

5) Mitigazione e calcolo del rischio residuo:

Accertato il livello di rischio è buona norma, oltre che necessario, dopo aver raggiunto una certa soglia, effettuare delle operazioni di **mitigazione**. Queste operazioni consistono nell'implementare strategie e decisioni per ridurre i valori di probabilità o di impatto, al fine di riportare il rischio a valori più accettabili.

Rifacendoci al nostro esempio del calcolo del rischio, ed ipotizzando una Valutazione d'impatto – Tab. 1" pari a 4 (Massimo), il rischio risultante è calcolato come:

(Impatto 4) x (Probabilità 4) → 16 Rischio Critico ([vedi figura 5](#))

Una misura di mitigazione potrebbe consistere nell'intervenire sull'area tematica B (quella che ha contribuito al maggior numero di risposte 4 "SI" - 4 in totale), e integrare delle strategie per ridurre il valore della probabilità, in modo da rientrare almeno nel livello "Alto" se non "Medio".

PUBBLICAZIONE PROJECT WORK

La guida alla valutazione del rischio sarà pubblicata on-line e scaricabile in pdf attraverso una landing page.

INFORMAZIONI DEL PROGETTO

TECNOLOGIE UTILIZZATE:

- **HTML5** supportato da tutti i browser moderni.
- **CSS3** per separare struttura (html) dalla presentazione.
- **FLEXBOX & GRID** tecnologie CSS che permettono di creare layout moderni senza troppe difficoltà e immaginando la pagina come un contenitore principale all'interno del quale si trovano varie "scatole" (box), quest'ultime possono essere disposte in varie direzioni e con vari allineamenti. Permettono un adattamento automatico alle dimensioni dello schermo.

STRUTTURA DEL PROGETTO:

```
project-work/  
index.html          # Pagina principale del progetto, punto di accesso  
css/style.css       # Foglio di stile per la personalizzazione grafica e usabilità  
assets/logo.png    # Logo del progetto  
assets/pw_maione.pdf # File PDF scaricabile contenete la guida alla valutazione dei rischi
```

DESCRIZIONE DEL CODICE:

Nella pagina html è stata inclusa una sezione "intro" per catturare l'attenzione del visitatore, una sezione <div> che contiene due colonne per un riepilogo informativo della pagina, e una sezione contenente un tasto per il download del project work, infine un questionario per la valutazione del progetto.

Di seguito, una breve analisi per presentare sinteticamente varie sezioni chiave del codice HTML e CSS.

Gli snippet di codice scelti verranno commentati per illustrare il ruolo che svolgono nella pagina.

Nel file **index.html** sono stati inseriti tag semantici, non obbligatori, come <main>, <section>, <header>, <footer>. Essi hanno il compito di descrivere meglio il contenuto e sono tag appetibili ai motori di ricerca, contribuendo al posizionamento della pagina in ottica SEO.

Il file index.html è il primo file che un browser carica appena si raggiunge un dominio o una cartella nel web.

➤ HEAD

- Setto la codifica UTF-8.
- Comunico al browser di adattare la larghezza della pagina a quella del dispositivo
- I tag meta Description e Author sono utili per i motori di ricerca: il primo descrive il contenuto della pagina, author invece indica l'autore del progetto.

```
<meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta name="description" content="Landing page del project work - Pagina responsive con HTML5 e CSS3">
  <meta name="author" content="Vincenzo Maione">
```

File index.html

Con questo snippet definisco il titolo della pagina:

- È visibile nella scheda del browser
- È utilizzato dai motori di ricerca.

```
<! -- Titolo della pagina -->
<title>Progetto Universitario - Landing Page</title>
```

File index.html

Collego un foglio di stile contenente le regole CSS, esterno alla pagina:

- href="css/style.css" indica il percorso relativo del file CSS:

```
<! -- Collegamento al file CSS esterno -->
<link rel="stylesheet" href="css/style.css">
```

File index.html

➤ BODY

In questo blocco di codice usato per header è stato utilizzando Flex-box:

```
<header>
  <div class="logo">
    
  </div>
  .....
</header>
```

File index.html

In particolare nel contenitore <header> troverà spazio il logo a sinistra e menù a destra, su un'unica riga:

```
header {
  display: flex;
  ...
}
```

File style.css

Il logo e il menù saranno distanziati tra loro grazie al codice CSS:

```
header {
  display: flex;
  justify-content: space-between;
  align-items: center;
  ...
}
```

File style.css

Il tag **<nav>** è semantico in HTML5 (specifica chiaramente il significato ai motori di ricerca e ai browser), permette di creare un menu di navigazione dove ogni list item **** corrisponde ad una voce di menu.

La riga `Download` contiene il riferimento all'id="download all'interno della stessa pagina; quando l'utente clicca su "Download", nel menu, la pagina scorre e si posiziona nei pressi della sezione

```
<div class="container" id="download">
```

```
<nav class="menu">
  <ul>
    <li><a href="#">Home</a></li>
    <li><a href="#informazioni">Informazioni</a></li>
    <li><a href="#download">Download</a></li>
    <li><a href="#valutazione">Valutazione</a></li>
  </ul>
</nav>
```

File index.html

➤ MAIN

Nel tag semantico **<main>** troviamo una sezione **<div>** con classe container. La classe è definita nel file CSS richiamato:

```
<div class="container" id="informazioni">
```

File index.html

Display: grid; imposta il contenitore **<div>** in una griglia CSS, dove ogni colonna è larga almeno 300px e con il parametro **auto-fit** consente alle colonne di auto adattarsi alla larghezza dello schermo:

```
/* Layout a 2 colonne con Grid */
.container {
  display: grid;
  grid-template-columns: repeat(auto-fit, minmax(300px, 1fr));
  gap: 2.5rem;
  padding: 0 2rem;
  max-width: 1200px;
  margin: 0 auto 4rem;
}
```

File style.css

Definisco le due colonne richiamando la classe “**container**”, inoltre la classe “**colonna**” dona ombra ed un effetto ad angoli morbidi:

```
<div class="container" id="informazioni">
    <!-- Primo box informativo -->
    <section class="colonna">
    <h2>Tecnologie Utilizzate</h2>
    <!-- Secondo box informativo -->
    <section class="colonna">
        <h2>Elementi di Design</h2>
        <p>Composizione dell'interfaccia:</p>
    </section>
</div>
```

File index.html

La classe colonna inoltre, al passaggio del mouse (:**hover**), dona un effetto ancor più accattivante: Tutto si sposta verso l'alto (**asse y**) e con un'ombra più marcata:

```
.colonna: hover {
    transform: translateY(-5px);
    box-shadow: 0 8px 25px rgba (0, 0, 0, 0.1);
}
```

File style.css

Infine per rendere le pagine responsive, adattabile a schermi di diverse risoluzioni, ho utilizzato due Media Queries:

- **@media (max-width: 768px)** – si attivano le regole CSS quando lo schermo dei dispositivi è al massimo 768px, parliamo di schermi di tablet o piccoli portatili.
- **@media (max-width: 480px)** – si attivano le regole CSS quando lo schermo dei dispositivi è al massimo 480px (smartphone e piccoli dispositivi).
-

CONDIVISIONE DEL CODICE:

Di seguito è riportato il link per la condivisione del progetto su GitHub. È inoltre possibile visualizzare il sito web pubblicato tramite GitHub Pages all'indirizzo indicato.

Repository personale del progetto (Contenete tutto il codice html, CSS, il logo ed il file pdf - pw_maione.pdf)

- <https://github.com/Mai1Lab/Project-work>

Pubblicazione pagina:

- <https://mai1lab.github.io/Project-work/>

SCREENSHOT DELLA PAGINA WEB:

Benvenuto nel mio progetto

Privacy e sicurezza aziendale: Sviluppo di un software per la sicurezza aziendale

Il documento propone un approccio sul calcolo del fattore del rischio. Le normative e gli standard ISO selezionati vengono evidenziati per affrontare una valutazione oggettiva e consapevole dei rischi in ambito privacy e sicurezza.

Proteggere i dati non significa solo salvaguardare gli asset aziendali, ma equivale soprattutto ad una responsabilità fondata su principi morali e legali.

Tecnologie Utilizzate

Questo progetto è stato sviluppato utilizzando:

- **HTML5:** Struttura semantica
- **CSS3:** Styling avanzato con layout moderni
- **Flexbox:** Allineamento e distribuzione degli elementi
- **Media Queries:** Adattamento mobile
- **Font di sistema:** Arial/sans-serif (nessun font esterno)

Elementi di Design

Composizione dell'interfaccia:

- **Container principale:** Due box informativi affiancati (CSS Grid)
- **Pulsante di download:** Utilizzato per il file pdf (Flexbox centrato)
- **Layout fluido:** Si adatta a tutte le risoluzioni
- **Mobile:** Layout verticale
- **Allineamenti:** Grazie a Flexbox

Download Documento

Scarica il documento completo in formato PDF:

Scarica PDF

Valuta il Progetto

Valutazione del Project Work

Grazie per dedicare 3-5 minuti a compilare questo questionario.
Clicca il tasto in basso "Avanti" per iniziare. **I dati saranno trattati in forma anonima.**

Non condiviso

Avanti

Pagina 1 di 7

Cancello modulo

Non inviare mai le password tramite Moduli Google.

ModuliGoogle

Questi contenuti non sono creati né analizzati da Google.

© 2025 Il mio progetto. Realizzato con HTML5, CSS3 e un po' di creatività! 🎨 🌱

Contattami: vincenzo.maione_4194@studenti.unipegaso.it

Campi di applicazione

(Descrivere gli ambiti di applicazione dell'elaborato progettuale e i vantaggi derivanti della sua applicazione):

Per la valutazione dei rischi in ambito privacy e sicurezza è stato scelto il modello ENISA.

Perché l'approccio ENISA?

È un modello caratterizzato da fasi iterative e presenta una struttura semplice e pratica.

Questo approccio è tra i più indicati per supportare l'utente, anche meno esperto, nell'identificare e riconoscere il livello di rischio associato al proprio trattamento e le relative di miglioramento.

L'utilizzo di tabelle e matrici rende il modello di facile consultazione, soprattutto in contesti aziendali di piccole dimensioni; inoltre, permette di avere un quadro completo e coerente della situazione attuale. Ciò risulta utile per predisporre il trattamento dei dati a misure di mitigazione, nell'intento di ridurre il valore del rischio qualora risulti elevato a seguito della valutazione, e portarlo quindi a livelli più accettabili e/o attesi.

È un modello particolarmente utile nella protezione dei dati personali, in quanto valuta il rischio di un trattamento, incrociando:

l'impatto che una violazione dei dati può avere sugli interessati con la probabilità della violazione.

Il modello ENISA è inoltre corrispondente con i principi del GDPR. Un esempio significativo è l'**art. 32 - Sicurezza del trattamento Regolamento UE** - stabilisce che il titolare del trattamento e il responsabile hanno l'obbligo di attuare misure tecniche e organizzative adeguate a garantire un elevato livello di sicurezza adeguato al rischio. Tale misure devono inoltre essere verificate e valutate regolarmente.

Rilevante è anche l'**articolo 42** del GDPR – Meccanismi di certificazione – Anche se il modello ENISA non è una certificazione, la sua adozione può costituire un elemento di prova in fase di audit o certificazione.

L'elaborato trova applicazione in quei contesti dove è necessario una valutazione dei rischi, in conformità con il Regolamento Europeo 2016/79 (GDPR). Il modello può essere adottato da:

Piccole e medie imprese che gestiscono dati di dipendenti, fornitori e clienti.

Titolari del trattamento per integrare la valutazione dei rischi all'interno dei processi aziendali, anche in assenza di competenze tecniche.

Organizzazioni private che trattano dati sensibili e che hanno bisogno di un elevato livello di sicurezza.

Valutazione dei risultati

(Descrivere le potenzialità e i limiti ai quali i risultati dell'elaborato sono potenzialmente esposti):

Il modello ENISA mostra i suoi punti di forza nei contesti a basso impatto di rischio; nei trattamenti sanitari, biometrici o giudiziari, i cosiddetti dati "sensibili", le tabelle e matrici semplificate non sono sufficienti. In questi contesti il modello è da affiancare ad altri strumenti simili ma più avanzati, come:

- **DPIA - Data Protection Impact Assessment o Valutazione d'Impatto sulla Protezione dei Dati.** Il titolare o il responsabile del trattamento, in base alla natura dei dati, valuta se una violazione degli stessi genera un rischio elevato per la libertà e i diritti degli interessati. L'articolo 35 del GDPR prevede, in questi casi, l'obbligo di una DPIA. Integrare la DPIA in una valutazione del rischio non è solo un obbligo normativo: essa garantisce trasparenza sull'utilizzo dei dati e, attraverso un'attenta valutazione dei rischi, consente di determinare misure tecniche e organizzative efficaci per intraprendere operazioni di mitigazione. La DPIA è inoltre un valido strumento per riconoscere il livello del rischio raggiunto per interpellare l'autorità garante per la protezione dei dati qualora, a seguito della valutazione, emergano rischi elevati che non possono essere mitigati.

MODELLO BASATO SU SCENARI – Riguarda l'attivazione di modelli basati su simulazioni e scenari che potrebbero verificarsi a seguito di un incidente informatico. È possibile analizzare con precisione impatto e probabilità di ogni evento al fine di rendere lo scenario quanto più realistico. Questo approccio mette in risalto le conseguenze di eventuali casi di violazione, guasti o attacchi informatici, testando i sistemi di sicurezza e le procedure attuate, inoltre cosa non da sottovalutare, è possibile analizzare il comportamento del personale coinvolto.

Un ulteriore limite del modello ENISA riguarda la staticità della valutazione del rischio. Nello specifico, la valutazione viene effettuata in un momento preciso, come abbiamo potuto verificare anche dagli esempi, tramite l'utilizzo di tabelle e matrici. Il modello non prevede, purtroppo, un aggiornamento o un monitoraggio continuo, né tantomeno sistemi di alert qualora i trattamenti subiscano variazioni che implicherebbe un ricalcolo del rischio. Il modello, quindi, non è sempre allineato ai cambiamenti tecnologici e normativi; pertanto per superare questo limite, è possibile integrare il modello con sistemi dinamici che monitorano continuamente le modifiche ai trattamenti e, quindi, sono solerti nel proporre nuove valutazioni.

QUESTIONARIO DI SODDISFAZIONE:

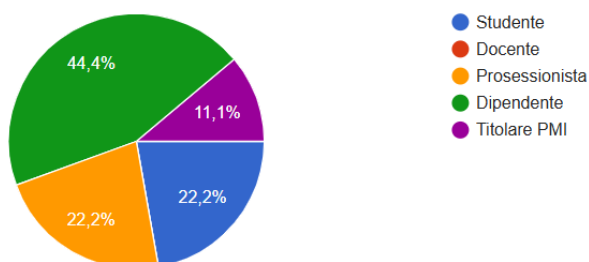
Per completare la valutazione dei risultati in modo partecipativo e accogliendo da parte dei lettori i suggerimenti per migliorare il lavoro svolto, è stato predisposto un **questionario di feedback**.

Lo strumento utilizzato è [Google Forms \[12\]](#). Il questionario è stato compilato da 9 partecipanti. Il sistema, oltre a salvare i dati in un foglio di Google Workspace, produce per ogni domanda dei grafici che aiutano la visualizzazione immediata e sintetica dei risultati:

Informazioni generali

Qual è il tuo ruolo?

9 risposte

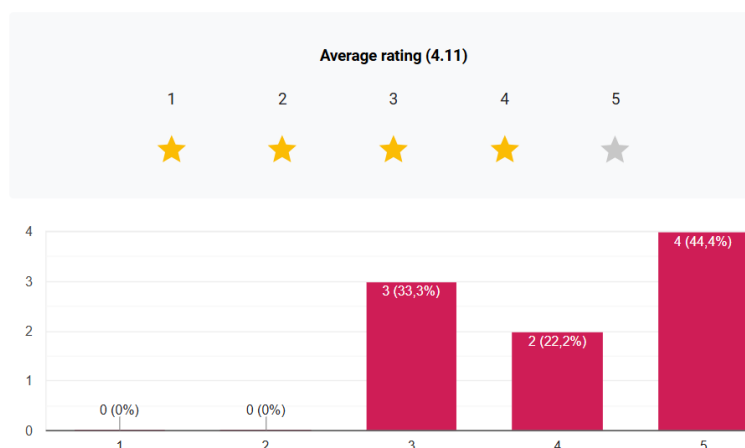


Quanto hai trovato chiari i contenuti del documento?

Tipo: Scala da 1 (poco) a 5 (molto)

9 risposte

Copia graficc



RIFLESSIONE FINALE:

Il progetto è organizzato in due componenti principali:

- Un **documento in formato PDF**, che illustra la terminologia e i concetti chiave per familiarizzare con gli argomenti trattati. Le normative e gli standard ISO selezionati vengono evidenziati e presi in considerazione per affrontare una valutazione oggettiva e consapevole dei rischi in ambito privacy e sicurezza.
- Una **pagina web**, strutturata per dare la possibilità di scaricare il documento e di effettuare una valutazione da parte del lettore.

La compilazione del documento ha trattato molteplici argomenti; pertanto, alcune sezioni risultano cariche di informazioni e andrebbero sintetizzate, dando spazio a dei casi specifici di valutazione del rischio. L'ausilio di infografiche potrebbe, inoltre, migliorare la visibilità e sintetizzare i concetti chiave.

Riguardo alla pagina web, l'interfaccia è semplice e intuitiva, adatta anche a utenti meno esperti. Il layout è pulito e responsive, aspetti determinanti soprattutto per la velocità di caricamento.

Integrare un menù a scomparsa per smartphone potrebbe migliorare l'user experience; la creazione di un modulo "Contattaci" o l'integrazione di un servizio di chatbot aumenterebbe il grado di partecipazione dell'utente, nell'ottica di migliorare il servizio offerto.