

UNIVERSITÀ DEGLI STUDI DI NAPOLI
PARTHENOPE

DIPARTIMENTO DI INGEGNERIA



**CORSO DI LAUREA IN INGEGNERIA E SCIENZE INFORMATICHE
PER LA CYBERSECURITY**

PROJECT WORK

Tema selezionato

SMART SHIELD

DOCENTE

PROF. ROBERTO CERCHIONE

GRUPPO

ANNO ACCADEMICO 2023/2024

Project Work

Smart Shield S.r.l. - CIS di Nola, isola 8 - smartshieldenterprise@gmail.com -
<https://smartshieldenterpr.wixsite.com/smart-shield>

a.a. 2023/2024

Prof. Roberto Cerchione

SCHEDA PROGETTO

Tema:

Nome del progetto: SMART SHIELD STARTUP, il software che cambierà la sicurezza digitale

Ambito/i di applicazione prevalente: settore software, mercati B2B E B2C

Composizione del team (indicare un unico proponente in caso di progetto individuale):

Nome e Cognome	Matricola	E-mail istituzionale	E-mail privata	Recapito telefonico
Andrea di Palo	0334000176	andrea.dipalo001@studenti.uniparthenope.it	Andreadipalo17@gmail.com	+39 3347225715
Francesco Petillo	0334000195	francesco.petillo001@studenti.uniparthenope.it	Fpetillo2001@gmail.com	+39 3338173270
Raffaele Murolo	0334000164	raffaele.murolo001@studenti.uniparthenope.it	Amon1988@hotmail.it	+39 3467479165
Ziadul Islam	0334000144	ziadul.islam001@studenti.uniparthenope.it	Ziadulsm969@gmail.com	+39 3512986697

**RESPONSABILI DELLE VARIE SEZIONI (DA COMPILEARE SOLO IN CASO DI
PROGETTO DI GRUPPO INDICANDO. OGNI COMPONENTE RICOPRIRE IL RUOLO
DI RESPONSABILE DI STESURA E RESPONSABILE DI REVISIONE DI ALMENO DUE
PIANI DIFFERENTI)**

Piano	Responsabile/i stesura	Responsabile/i revisione
Piano Strategico	Andrea di Palo	Raffaele Murolo
Piano Marketing	Raffaele Murolo	Francesco Petillo
Piano Operativo	Francesco Petillo	Ziadul Islam
Piano Economico- Finanziario	Ziadul Islam	Andrea di Palo

Indice

1.	Executive Summary	5
2.	Descrizione dell'azienda	10
2.1	I soggetti proponenti.....	12
2.2	Descrizione del prodotto/servizio	19
2.3	Partnership o altri rapporti di collaborazione da attivare.....	25
	Identificazione di Possibili Alleanze Future.....	25
2.4	Possesso di brevetti o certificazioni	27
3.	Piano strategico.....	30
4.	Piano marketing	40
4.1	Definizione e segmentazione del mercato	42
4.2	Strategia di marketing.....	46
4.3	Stima della domanda	48
5.	Piano organizzativo.....	51
6.	Piano operativo	53
7.	Piano economico-finanziario	101
7.1	STRUTTURA FINANZIARIA.....	105
7.2	PROIEZIONI FUTURE.....	106
7.	Bibliografia.....	107
8.	Sitografia	108

1. Executive Summary

SmartShield è una startup innovativa fondata da quattro studenti della Facoltà di Ingegneria e Scienze Informatiche per la Cybersecurity dell'Università degli Studi di Napoli Parthenope. Il progetto prevede la creazione di un software di sicurezza informatica, disponibile tramite abbonamento, il quale offre una protezione completa contro le minacce digitali. Il prodotto creato non è solo un semplice antivirus, ma un vero e proprio companion digitale in grado di monitorare costantemente il traffico dati sui dispositivi degli utenti, proteggendoli dalle minacce in tempo reale e garantendo la privacy secondo il GDPR (Regolamento generale sulla protezione dei dati).

Funzionalità del Software

Per comprendere al meglio il software e l'idea di prodotto creato abbiamo optato per dividere il prodotto in macroaree, ovvero:

Daisy, l'Intelligenza Artificiale: Daisy monitora costantemente il sistema per rilevare malware, tentativi di phishing, email spam e altre minacce. Avvisa sempre l'utente prima di prendere qualsiasi azione, garantendo il controllo totale.

Il centro di gestione richieste: In caso di minacce gravi, il call center di SmartShield viene avvisato automaticamente, e un operatore contatta il cliente per fornire assistenza immediata.

La gestione flessibile delle minacce: Gli utenti possono gestire le minacce come preferiscono, con Daisy che notifica sempre l'utente prima di prendere qualsiasi azione. In caso di minacce meno gravi, l'utente può decidere autonomamente come procedere.

La Protezione della Privacy: Il software rispetta rigorosamente la privacy degli utenti secondo il GDPR, assicurando che i dati personali siano trattati con la massima riservatezza.

Unique Selling Proposition

SmartShield si distingue per:

Protezione Olistica: Non solo antivirus, ma un sistema di sicurezza completo che copre tutte le possibili minacce digitali.

Intelligenza Artificiale Avanzata: Daisy, l'AI di SmartShield, è in grado di rilevare e gestire le minacce in modo autonomo e tempestivo.

Supporto Personalizzato: Assistenza immediata tramite call center in caso di minacce gravi.

Flessibilità e Controllo: Gli utenti hanno sempre il controllo sulle azioni intraprese dal software, garantendo una gestione personalizzata delle minacce.

Soluzioni su Misura per le Imprese: Pacchetti personalizzati per le esigenze specifiche delle piccole e medie imprese, e soluzioni ad hoc per le grandi aziende.

Opportunità di Mercato, Dimensioni del Mercato

Il mercato della cybersecurity è in rapida espansione, con un valore stimato di 2,15 miliardi di euro. Questa crescita è alimentata dall'aumento delle minacce informatiche e dalla crescente consapevolezza dell'importanza della sicurezza digitale tra gli utenti privati e le imprese.

Opportunità Specifiche

Utenti Privati: Protezione per giovani, bambini, anziani e utenti meno esperti, che sono spesso le vittime principali di truffe online. Secondo recenti statistiche, migliaia di persone cadono vittima di truffe online ogni anno, con un aumento significativo dei casi di phishing e altre forme di cybercrime.

Piccole e Medie Imprese (PMI): Molte PMI italiane stanno attraversando una fase di digitalizzazione e necessitano di soluzioni di sicurezza affidabili per proteggere i loro dati. La sicurezza informatica è essenziale per queste aziende, che spesso non dispongono di risorse interne sufficienti per gestire le minacce in modo efficace.

Crescita Prevista

Puntiamo a catturare una quota di mercato significativa nei prossimi anni:

Primo Anno: 5% del mercato.

Secondo Anno: 12% del mercato.

Terzo Anno: 25% del mercato in uno scenario ottimistico.

La nostra Mission

La mission di SmartShield è di ridurre significativamente i reati informatici nei prossimi 20 anni. L'obiettivo è eliminare quasi totalmente le truffe rivolte alle fasce di età protette, e scoraggiare chi si approfitta delle persone più fragili. Attraverso un progetto europeo mirato alla sicurezza e strategie pubblicitarie mirate, aspiriamo a rendere il nostro software gratuito per tutti i cittadini.

Risultati Economico-Finanziari Previsti

Fatturato

Prevediamo una crescita sostenuta del fatturato, con un aumento progressivo della nostra quota di mercato grazie all'espansione dei nostri servizi e al consolidamento della nostra base di clienti.

Redditività

Grazie all'efficienza delle nostre operazioni e alla qualità del nostro servizio, prevediamo di raggiungere una redditività elevata. Il nostro modello di abbonamento garantisce entrate ricorrenti e una solida base finanziaria.

Capitale da Investire

Oltre al capitale sociale minimo, il progetto sarà finanziato tramite il bonus giovani. Siamo aperti anche agli investitori interessati a supportare la nostra visione e a contribuire alla crescita della nostra startup.

Previsione dei principali risultati economico-finanziari dopo i tre anni

N.B.: Le previsioni sono basate su una serie di ipotesi e sono soggette a un certo grado di incertezza. Tuttavia, si ritiene che siano raggiungibili. Se le previsioni sono giuste, la società sarà in grado di generare un significativo aumento del fatturato e della redditività nel corso degli anni, nonché di creare valore per gli azionisti.

Obiettivi per consolidare il margine economico della startup

Continuare a investire nella crescita:

La società dovrebbe continuare a investire nella crescita, attraverso l'espansione del mercato, l'introduzione di nuovi prodotti e l'aumento della quota di mercato.

Migliorare l'efficienza operativa:

La società dovrebbe continuare a migliorare l'efficienza operativa, al fine di ridurre i costi di produzione e aumentare la redditività.

Gestire il debito in modo efficiente:

La società dovrebbe gestire il debito in modo efficiente, al fine di ridurre gli oneri finanziari e migliorare la propria struttura finanziaria.

-La società si trova in una posizione finanziaria solida e ha buone possibilità di crescita nei prossimi anni. Se la società riuscirà a mettere in atto le giuste manovre nel mercato sarà grado di fatturare in modo proficuo.

FATTURATO

Si prevede che il fatturato aumenti significativamente. Questo incremento è dovuto a una serie di fattori, tra cui:

Aumento del volume delle vendite:

Si prevede che il volume delle vendite aumenti da 435.700 unità nel primo anno a 2.178.500 unità nel terzo anno. Questo è dovuto a una serie di fattori, tra cui l'espansione del mercato, l'introduzione di nuovi prodotti e l'aumento della quota di mercato.

Prezzo stabile:

Si prevede che il prezzo medio rimanga stabile a 18 euro per tutti e cinque gli anni. Questo è un presupposto, dato che il prezzo è determinato principalmente dalle leggi di mercato e l'inflazione futura nonché dai costi di produzione e dai prezzi dei concorrenti.

Redditività

Si prevede che la redditività aumenti significativamente nei prossimi tre anni. Il margine di profitto lordo dovrebbe passare dal 60% nel primo anno al 70% nel terzo anno. Questo è dovuto a una serie di fattori, tra cui:

Riduzione dei costi di produzione:

Si prevede che i costi di produzione diminuiscano come conseguenza dell'aumento dei volumi di produzione e dell'efficienza operativa.

Aumento dei prezzi di vendita:

Si prevede che i prezzi di vendita rimangano stabili, ma che l'aumento dei volumi di vendita compensi l'aumento dei costi di produzione.

Riduzione degli oneri finanziari:

Si prevede che gli oneri finanziari diminuiscano come conseguenza della riduzione del debito.

Ammontare del capitale da investire

Si prevede che l'ammontare del capitale da investire aumenti significativamente nei prossimi tre anni. L'investimento complessivo dovrebbe passare da 1.400.000 euro nel primo anno a 2.400.000 euro nel terzo anno.

Richiesta al Destinatario del Business Plan

Chiediamo al destinatario del business plan di credere fermamente nel nostro progetto e di supportarci nella nostra missione. Oltre al capitale necessario, che è minimo dato che la startup prevede di nascere e svilupparsi tramite il finanziamento statale Resta al Sud dedicato alle startup con alta componente tecnologica, quindi, cerchiamo partner strategici che possano aiutarci a espandere la nostra visione e a realizzare il nostro obiettivo di rendere internet un luogo più sicuro per tutti.

SmartShield rappresenta una soluzione innovativa e completa per la protezione contro le minacce informatiche. Con il nostro software avanzato e l'assistente AI Daisy, offriamo un livello di sicurezza superiore rispetto ai concorrenti. Invitiamo i potenziali investitori a unirsi a noi in questa missione, per costruire insieme un futuro digitale più sicuro e protetto. La nostra startup è pronta a fare la differenza nel campo della cybersecurity, proteggendo utenti privati e aziende dalle minacce digitali in continua evoluzione.

Analisi di Supporto

Statistiche sulle Truffe Online

Secondo il rapporto annuale della Polizia Postale, il numero di truffe online è aumentato del 25% negli ultimi cinque anni. Le fasce di età più colpite sono quelle dei giovani tra i 18 e i 30 anni e degli anziani oltre i 65 anni, che spesso mancano delle competenze digitali necessarie per riconoscere e difendersi dalle minacce informatiche.

Digitalizzazione delle PMI

Secondo un rapporto di Confcommercio, circa il 45% delle PMI italiane ha avviato un processo di digitalizzazione negli ultimi tre anni, ma solo il 20% ha implementato adeguate misure di sicurezza informatica. Questo rappresenta un'opportunità significativa per SmartShield, che può offrire soluzioni su misura per proteggere queste aziende durante la loro transizione digitale.

2. Descrizione dell'azienda

SmartShield S.r.l., ubicata nel CIS di Nola, Isola 8, CAP 80035, è una startup innovativa fondata da quattro neoimprenditori, studenti della Facoltà di Ingegneria e Scienze Informatiche per la Cybersecurity dell'Università degli Studi di Napoli Parthenope. I soci fondatori, grazie alla loro esperienza nello sviluppo software e alle loro spiccate capacità imprenditoriali, hanno dato vita a un'azienda all'avanguardia nel campo della sicurezza informatica.

I quattro soci fondatori di SmartShield S.r.l. sono esperti nel settore dello sviluppo software, con competenze approfondite nella cybersecurity. Oltre alle capacità tecniche, i fondatori possiedono una forte inclinazione imprenditoriale, che ha permesso loro di individuare un'importante nicchia di mercato e di sviluppare una soluzione innovativa per proteggere gli utenti dalle minacce digitali.

Ubicazione Strategica

La scelta di ubicare SmartShield S.r.l. nel CIS di Nola non è casuale. Questo complesso è una delle realtà commerciali più grandi d'Europa, offrendo un ambiente dinamico e ben collegato. La posizione è strategica, trovandosi a pochi metri dall'Asse Mediano che collega direttamente il CIS a Napoli. Questa vicinanza a una delle principali città italiane garantisce facilità di accesso e ottime opportunità di networking e collaborazione con altre imprese.

I vantaggi dell'ubicazione sono svariati, innanzitutto le Infrastrutture Avanzate: La zona è dotata di tutte le infrastrutture necessarie per supportare le attività aziendali, incluse connessioni internet ad alta velocità e un adeguato wattaggio e corrente per le apparecchiature informatiche.

Poi l'accessibilità: La vicinanza all'Asse Mediano assicura una facile accessibilità per dipendenti, partner e clienti, facilitando la logistica e le operazioni quotidiane.

Struttura dell'Ufficio

L'ufficio di SmartShield S.r.l. è stato progettato per supportare al meglio le diverse attività aziendali, combinando aree operative e direzionali in modo efficiente.

Area Direzionale

Uffici per i Call Center: Un'area dedicata al supporto clienti, con operatori pronti a fornire assistenza immediata e personalizzata in caso di minacce informatiche.

Sala Riunioni: Uno spazio per le riunioni aziendali, dotato delle tecnologie necessarie per videoconferenze e presentazioni, facilitando la collaborazione interna e con partner esterni.

Uffici per i Soci Fondatori: Uffici dedicati ai soci fondatori, dove possono concentrarsi sulla gestione aziendale e sulla strategia di sviluppo.

Per i burnout dovuti ai problemi di lavoro si è optato di creare, budget permettendo, una piccola panic room e zona relax.

Area Operativa

Uffici per gli Sviluppatori: Spazi dedicati ai due sviluppatori che lavorano a stretto contatto con i soci fondatori sul continuo miglioramento del software SmartShield.

Magazzino e Capannone: Un piccolo magazzino capannone che contiene le apparecchiature per la rete neurale dell'intelligenza artificiale, inclusi server e altre infrastrutture tecnologiche essenziali per il funzionamento del software.

Apparecchiature Tecnologiche

L'area operativa è dotata di apparecchiature avanzate, necessarie per supportare la rete neurale di Daisy, l'intelligenza artificiale di SmartShield. Queste includono server di ultima generazione e altre infrastrutture tecnologiche che garantiscono la sicurezza e l'efficienza del software.

SmartShield S.r.l. rappresenta un esempio di eccellenza nell'innovazione e nella protezione informatica. Grazie alla combinazione di competenze tecniche avanzate e capacità imprenditoriali dei suoi fondatori, l'azienda è posizionata strategicamente nel CIS di Nola per sfruttare al meglio le opportunità offerte dal mercato. La struttura dell'ufficio è stata pensata per supportare efficacemente tutte le attività aziendali, garantendo un ambiente di lavoro produttivo e tecnologicamente avanzato.

2.1 I soggetti proponenti



Il sottoscritto Francesco Petillo, nato ad Avellino il 18 Giugno 2001, residente in Roccarainola (NA) in Via Luigi D'Avanzo 21, ai sensi e per gli effetti degli art. 46 e 47 DPR 445/2000, consapevole delle sanzioni penali previste dall'art. 76 del DPR 445/2000 e successive modificazioni ed integrazioni per le ipotesi di falsità in atti e dichiarazioni mendaci, dichiara sotto la propria responsabilità:



ISTRUZIONE

Aa 2020/2021

TITOLO DI STUDIO:

Diploma di istruzione liceale, liceo classico statale "Giosuè Carducci", Nola, conseguito con punteggio 93/100 nell'anno 2020.

Nome

Francesco Petillo

Luogo e data di nascita

Avellino, 18 giugno 2001

Residenza

Roccarainola, Via Luigi D'Avanzo 21

Telefono cellulare

+ 39 3338173270

Email

fpetillo2001@gmail.com

CAPACITÀ E COMPETENZE

- ➡ Ottima conoscenza della lingua inglese di livello medio/avanzata, certificata B2 Cambridge.
- ➡ Conoscenza intermedia dello spagnolo, certificato B1 rilasciato dall'Università Degli Studi di Salerno
- ➡ Patente A1-A2-A3-B

Corretto utilizzo del computer:

- ➡ Sistemi operativi (Windows, Mac, Linux, Ubuntu);
- ➡ Programmi comuni: pacchetto Office, Adobe.
- ➡ Conoscenza dei fondamenti di programmazione, familiarità con l'utilizzo di linguaggi quali C, C++, Python, Java, Assembly, Sql, e dei correlati ambienti di sviluppo integrati.

ESPERIENZE LAVORATIVE

Nel periodo estivo del 2018 ho lavorato come fattorino presso Consegnam, Cimitile (NA).

Da giugno 2020 a luglio 2021 ho lavorato presso Fratelli Pizza S.r.l. Saviano (NA) come manovale per scarico attrezzature eventi e tecnico luci.

Da giugno 2020 a luglio 2021 ho lavorato come manutentore informatico presso Euclide S.r.l., Roccarainola (Na).

Da gennaio 2022, la domenica e nei giorni festivi, sono ufficiale di gara autorizzato ACI, quindi arbitro durante le competizioni a livello agonistico di motocross.

Da settembre 2022 a febbraio 2023, vincitore di bando Erasmus, ho vissuto a Gran Canaria (Spagna, isole canarie), frequentando la facoltà di "Ingeniería Informática" della Universidad de Las Palmas De Gran Canaria.

SU DI ME

Sono molto appassionato di informatica e del mondo tech in generale, qualsiasi cosa riguardi un elaboratore elettronico o il mondo di internet mi affascina, vedo la tecnologia come innovazione e senza **Innovazione** non c'è futuro.

Mi reputo una persona solare, dinamica e **molto onesta**. Amo mettermi in gioco e affrontare sempre nuove sfide, credo fortemente nel lavoro di squadra, **esperienze come la mia permanenza all'estero** mi hanno insegnato ad ascoltare il punto di vista altrui prima di esprimere il proprio, in modo da poter sempre arrivare ad un risultato che utilizzi le esperienze pregresse di tutte le menti coinvolte in un progetto; oltre ad avermi insegnato cosa vuol dire lavorare in gruppo in un contesto **culturalmente eterogeneo**.

Autorizzo il trattamento dei miei dati personali ai sensi del Dlgs 196 del 30 giugno 2003 e dell'art. 13 GDPR*

in fede *Francesco Petillo*

Andrea Di Palo

Studente

Profilo

Sono un giovane intraprendente e motivato, con una forte passione per le sfide e una propensione a mettermi in gioco in ogni situazione. Sono alla ricerca di opportunità che mi permettano di crescere professionalmente, contribuendo al successo dell'azienda.

Competenze chiave

- **Problem Solving:** Capacità di analizzare situazioni complesse e trovare soluzioni efficaci e innovative, anche sotto pressione.
- **Spirito di iniziativa:** Mi piace proporre nuove idee e miglioramenti..
- **Adattabilità:** Flessibilità nell'adattarmi rapidamente a nuovi ambienti e situazioni, mantenendo alti livelli di performance.

Contatti

 3347225715

 andreadipalo17@gmail.com

Formazione

- Diplomato in Liceo Linguistico presso "Liceo Statale Pasquale Villari"
- Studente al primo anno di Ingegneria e Scienze informatiche per la Cybersecurity presso L'Università degli Studi di Napoli Parthenope

Passioni

- **Tecnologia:** Interesse per le ultime innovazioni tecnologiche e il loro impatto sul mondo.
- **Sport:** Appassionato di sport che richiedono collaborazione e strategia; e sport che fanno della tecnologia e dell'ingegneria un punto fondamentale
- **Viaggi:** Esplorare nuove culture e affrontare le sfide di ambienti sconosciuti.

Altre info

- automunito
- lingua italiana , inglese e francese

Murolo Raffaele

📍 Via Vico III ponte N°13, 80145 Napoli (Italia)

📞 3467479165 📞 0813416357 📩 amon1988@hotmail.it 📩 raffaele1988@pec.it

Ho una buona dimestichezza dei sistemi operativi, autonomia nell'esecuzione di ciò che mi viene assegnato e ottemperanza negli impegni presi.

Desidero propormi a Voi come candidato idoneo a ricoprire mansioni operative in quest'ambito, ma anche in nuovi, che mi diano la possibilità di acquisire nuove conoscenze.

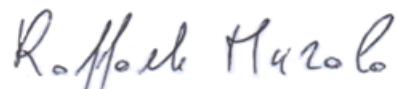
Sono capace di lavorare in gruppo e a colloquiare con il pubblico, doti che ho imparato ad acquisire grazie alle mie precedenti esperienze.

Non ho problemi a adattarmi alle mansioni per me nuove, che siano di manovalanza o di ufficio.

Ritengo di possedere l'interesse e la volontà necessaria per un positivo inserimento nella Vostra società. Sono disponibile alle diverse modalità di rapporto contrattuali esistenti a ricoprire anche altre posizioni che risultassero più funzionali alle vostre esigenze.

Confidando nella possibilità di esporvi personalmente il mio curriculum vitae, rimango a vostra disposizione per qualsiasi ulteriore chiarimento Vi fosse necessario e vi prego i più cordiali saluti.

FIRMA



Curriculum vitae



Raffaele Murolo Sesso Maschile | Data di nascita 07/10/1988 | Nazionalità Italiana

ESPERIENZA PROFESSIONALE

- Servizio civile anno 2007/08 presso la scuola elementare 58° circolo J.F. KENNEDY in Via Monte Rosa, 14
- Lavoro presso Dama demolizioni S.r.l. come manovale nel 2017 in Via R. Apicella, 15, Pollena Trocchia NA
- Cameriere ne ristorante "MADE IN FOOD" Piazza S. Luigi, 14 Napoli anno 2018
- Aiuto-Pizzaiolo ristorante "DE ROSA" Via Giuseppe Verdi Napoli anno 2019

CORSI DI FORMAZIONE

Corso di pizzaiolo, tramite garanzia giovani, durato dal 13/10/2017 al 12/12/ 2017
Praticità e capacità di manipolazione, staglio, stesura, condimento e cottura
Dell'impasto. Capacità di cottura in forni a legna, gas ed elettrici.
Conoscenza delle norme igieniche e sanitarie nonché conoscenza delle basi
Principali del sistema HACCP.
Tali competenze sopraindicate sono state accertate tramite le seguenti modalità
di valutazione: prova scritta, prova pratica e colloquio superato.

Corso di programmazione java (durata di 2 mesi) nel 2019 nella società ~~Begear srl~~,
Centro Direzionale Isola E7, 80143 Napoli NA.



DIPLOMA

Diploma di Tecnico chimico-biologico conseguito nel 2007 Istituto Istruzione Superiore Statale "Giovanni Caselli", con punteggio di 60/100.

DIPLOMA

Diploma di Tecnico informatico conseguito nel 2023 Istituto Tecnico Industriale Galileo Ferraris, con punteggio di 94/100.

Iscritto al corso di laurea triennale in ingegneria e scienze informatiche della ~~Cyber security~~ all'università PARTHENOPE DI NAPOLI.

Smart Shield S.r.l. - CIS di Nola, isola 8 - smartshieldenterprise@gmail.com -
<https://smartshieldenterprise.wixsite.com/smart-shield>

COMPRENSIONE		PARLATO		PRODUZIONE SCRITTA
Ascolto	Lettura	Interazione	Produzione orale	
A2	A2	A2	A2	A2

20/03/2008

ECDL

Napoli (Italia)

- 1 Fondamenti dell'informatica
- 2 Gestione funzioni base del sistema operativo
- 3 Foglio elettronico
- 4 Internet e Networking
- 5 Gestioni di dati strutturali
- 6 Utilizzo OS: Windows xp, vista, 7, 8, 10, 11
- 7 Utilizzo Office: word, Excel, PowerPoint
- 8 Formattazione, montaggio e installazione dispositivi e programmi

Lingua madre

Italiano [Altre lingue](#)

inglese Livello: C2 ESOL CERTIFICATE

[Livelli: A1 e A2: Utente base - B1 e B2: Utente autonomo - C1 e C2: Utente avanzato](#)

[Quadro Comune Europeo di Riferimento delle Lingue](#)

Competenze comunicative

Nel corso della mia esperienza lavorativa ho acquisito una capacità di relazionarmi con il prossimo.

D

© Unione europea, 2002-2016 | <http://europass.cedefop.europa.eu>



AUTOVALUTAZIONE				
Elaborazione delle informazioni	Comunicazione	Creazione di Contenuti	Sicurezza	Risoluzione di problemi
Utente autonomo	Utente autonomo	Utente base	Utente base	Utente autonomo
Competenze digitali - Scheda per l'autovalutazioni				

Curriculum vitae

Patente di guida

B

ULTERIORI INFORMAZIONI

Patente

-PATENTE CARRELLO ELEVATORE

Disponibilità

- Disponibile a trasferimento
- Disponibile a lavori stagionali in villaggi
- Automunito

© Unione europea, 2002-2016 | <http://europass.cedefop.europa.eu>

Smart Shield S.r.l. - CIS di Nola, isola 8 - smartshieldenterprise@gmail.com - <https://smartshieldenterpr.wixsite.com/smart-shield>



Ziadul Islam

STUDENTE UNIVERSITARIO

CONTATTO

+39 351 298 6697

ziadulsmm969@gmail.com
ziadul@icloud.com

—

CHI SONO

Sono uno studente universitario, persona molto seria e aperta a nuove esperienze. Sto sviluppando le mie conoscenze per quanto riguarda il mondo dell'informatica e aiuto le persone straniere in vece di mediatore culturale da volontario.

COMPETENZE

Competenze informatiche: Word, PowerPoint, HTML e un po' di CSS, utilizzo dei linguaggi di programmazione (Python, C e C++).

Soft skills: buone capacità comunicative, capacità di lavorare in team e mi adatto con facilità.

LINGUE

Bengalese - Madrelingua
Italiano - Molto avanzato - C2 (CEFR)
Inglese - Intermedio

REFERENZE

Disponibili su richiesta.

FORMAZIONE ACADEMICA

Diploma di Maturità Classica

Liceo Classico Quadriennale - curvatura in Biomedicina(LI21) "Liceo Classico A. Diaz", Ottaviano, anno di conseguimento 2023.

Università degli Studi di Napoli Parthenope

Corso di Laurea Triennale in Ingegneria e Scienze Informatiche per la Cybersecurity(interclasse L-8 e L-31), Nola, anno di inizio 2023 - presente.

ESPERIENZE LAVORATIVE

Volontariato

Dal 2019 in poi ho lavorato come volontario nell'ambito dell'interprete in luoghi come comuni o istituti in cui ho aiutato stranieri residenti nelle pratiche burocratiche e faccio anche da mediatore culturale.

Partecipazione ai PLS (2022 e 2023)

Ho partecipato ai vari incontri lanciati dal MIUR nell'ambito scientifico per stimolarne l'interesse. Al fine di questi incontri sono stati rilasciati degli attestati. [Disponibili su richiesta]

Utilizzo dei dati

Autorizzo il trattamento dei dati personali contenuti nel mio curriculum vitae in base al D. Lgs. 196/2003 e al Regolamento UE 2016/679.

2.2 Descrizione del prodotto/servizio

Il nostro servizio consiste in un software antivirus con intelligenza artificiale integrata, fruibile sia via mobile che da personal computer. Il prodotto è accessibile tramite sottoscrizione di un abbonamento acquistabile sulla nostra piattaforma e-commerce, che funge anche da sito web per l'assistenza clienti.

Nell'era dell'intelligenza artificiale, l'idea nasce con lo scopo di utilizzare l'IA come un assistente personale che ci protegga in ogni momento. Grazie alla sua potenza di calcolo e alla capacità di monitorare costantemente i nostri dispositivi, e-mail, spam e tentativi di accesso, il software può garantire la nostra sicurezza, in particolare quella delle persone più a rischio, quando noi non siamo presenti. Quante volte sentiamo al telegiornale di anziani truffati da criminali che simulavano la voce del figlio? O di finte mail di istituti di credito che causano la perdita dei risparmi di una vita? Quante volte abbiamo sentito di quell'amico a cui hanno rubato tutti i dati personali, di quella ragazza che non esce più di casa perché le sono state rubate foto intime dal cellulare, di quelle piccole imprese ricattate da hacker che chiedono un riscatto per accedere ai loro stessi computer, di quei professionisti mandati sul lastrico perché un competitor ha ingaggiato terzi per bucare il loro drive digitale... Potremmo continuare all'infinito.

Abbiamo deciso di porre fine a tutto questo.

Grazie a SmartShield, e in particolare a Daisy, il companion artificiale che ci proteggerà sempre e dovunque, tutte queste storie raccapriccianti saranno solo un lontano ricordo.

Come specificato nel piano operativo, il software è utilizzabile in cinque diverse tipologie di abbonamento:

1. **Piano LITE:** Gratuito, offre servizi come VPN, anti-tracker e ad-block per una navigazione sicura, ma non include l'assistente digitale con IA. Utile dal punto di vista aziendale per pubblicità e per far conoscere il marchio, occasionalmente vengono offerti periodi di prova gratuiti per fidelizzare gli utenti.
2. **Piano Classic:** Al prezzo di 9,99 euro, è il prodotto completo che intendiamo proporre, con una serie infinita di funzionalità, inclusi il companion Daisy, che è l'IA che ci protegge, e il servizio clienti disponibile 24/7.
3. **Piano Family:** A 12,90 euro, offre tutte le potenzialità del piano Classic, oltre a una copertura multidispositivo e particolari features dedicate esclusivamente alla famiglia.
4. **Piano For Business:** A 29,90 euro, è dedicato alle aziende e offre una protezione avanzata e funzioni specifiche per il mondo business.
5. **Piano Ad Hoc For Business:** Prezzo da concordare dopo consulenza, è personalizzabile in base alle esigenze specifiche delle aziende.

FUNZIONAMENTO DEL PRODOTTO

Una volta installato il prodotto sarà utilizzabile inizialmente in italiano, spagnolo ed inglese, in base al successo di vendite saranno poi incrementati gli idiomi in base ai paesi in cui ci saranno più vendite.

Essendo un software e non un videogame, ad esempio, l'utente non avrà molto "da fare" con l'app vera e propria, una volta sottoscritto l'abbonamento e installato il software dovrà solo procedere alla configurazione. Aperta l'app ci sarà un menù di benvenuto in cui loggarsi con le credenziali fornite al momento dell'iscrizione, sarà automaticamente riconosciuta la tipologia di abbonamento e in base a questo cambierà leggermente l'interfaccia grafica, ovviamente saranno diverse le funzionalità.

In linea di massima la configurazione sarà uguale per tutti, **Daisy** si presenterà, chiederà età, sesso (se lo si vuole specificare) e altre info utili a delineare la persona, cosa fa sul cellulare ad esempio, che lavoro fa, quali sono le minacce a cui si sente più esposta, se ne è stata vittima in passato.

Terminate la serie di domande l'app impiegherà qualche decina di secondi per configurarsi, nel caso si dovesse trattare di un account business, familiare o comunque da usare il gruppo, allora verrà richiesto di impostare tutti gli utenti, differenziandoli da genitore, figlio, dirigente, impiegato ecc... in questo modo ognuno avrà determinati privilegi in base al suo ruolo. Il padre potrà impostare il parental control sul dispositivo dei figli ad esempio.

Una volta configurata, l'app questa opererà sempre in back ground, in caso di minaccia rilevata Daisy ci mostrerà un popup, sarà in grado di risolvere quasi tutti problemi da sola, nel caso di problemi maggiori invierà un alert al centralino di controllo che verificherà immediatamente.

All'interno dell'app ci sarà poi un menù dove saranno elencate tutte le opzioni e le risorse a cui il software ha accesso, in qualsiasi momento potranno essere disattivate alcune o tutte le funzionalità, ovviamente dall'account manager.

Si rimanda al piano operativo, oppure al sito web <https://smartshieldenterpr.wixsite.com/smart-shield/shop> nella sezione prodotti, per maggiori info e per l'elenco dettagliato di funzionalità di ogni pacchetto.

ANALYSIS SWOT

Punti di forza

I punti di forza del nostro prodotto sono le innumerevoli funzionalità, l'IA allenata in maniera specifica per predire le minacce da parte di malware e tentativi di:

- Phishing Attacchi che avvengono via e-mail
- Vishing: Attacchi di phishing che avvengono tramite chiamate vocali
- Phishing media: Attacchi di phishing che vengono condotti sui social

Smart Shield S.r.l. - CIS di Nola, isola 8 - smartshieldenterprise@gmail.com -
<https://smartshieldenterpr.wixsite.com/smart-shield>

- Phishing web: Attacchi di phishing che vengono condotti su siti web

- Phishing app: Attacchi di phishing condotti su applicazioni mobili

Oltre ad un prezzo conveniente anche se la linea con la concorrenza ma con maggiori funzionalità come detto in precedenza

Punti di debolezza

Non aggiornato su tutti i malware esistenti (ancora in fase di aggiornamento) e limite nella potenza di calcolo computazionale dell'IA.

Opportunità

Il mercato italiano della cybersecurity sta vivendo una crescita significativa, con un aumento del 16% rispetto all'anno precedente. Nel 2023 ha raggiunto un record di 2,15 miliardi di euro.

Possibili minacce

a)Aumento della concorrenza

b)Nuove normative governative

c)Crisi economica

Prestazioni

Prestazioni di ottima qualità tanto da ottenere le seguenti certificazioni che hanno testato la bontà del nostro prodotto.

a)Certificazione Common Criteria (CC)

b)Certificazione ISO 27001

c)Certificazione di conformità GDPR

Prezzi

prezzo abbonamento mensile per singolo utente: €9.90

Prezzo abbonamento mensile per famiglia (fino a 5 dispositivi): €12,90

prezzo abbonamento mensile per aziende: €29.90

versione gratuita con presenza di banner pubblicitari

Ricavi

1°anno: €5.297.430 (5% del mercato)

2°anno: €13.158.360 (12% del mercato)

3°anno: €26.487.150 (25% del mercato)

Costi

I costi si riscontrano non tanto nello sviluppo del software antivirus in sé ma nei costi dei dispositivi e programmi necessari per tale mansione:

- Attrezzature/PC HW, CPU, GPU, RAM, SSD, NAS ecc....
- internet ad alta velocità (500mb/s)
- Implementazione delle soluzioni di archiviazione cloud (Microsoft Azure Blob Storage, Google Cloud Storage)
- Configurazione degli ambienti di sviluppo (Visual Studio, IntelliJ, ecc.)
- Acquisizione e configurazione del dominio per il sito web

Per un totale di €25.300

Composizione del portafoglio clienti

Per canale di vendita:

- Clienti online

Per tipologia di cliente:

- Clienti B2B (business to business)
- Clienti B2C (business to consumer)

Per dimensione del cliente:

- Piccole imprese
- Medie imprese

Per settore:

Smart Shield S.r.l. - CIS di Nola, isola 8 - smartshieldenterprise@gmail.com -
<https://smartshieldenterpr.wixsite.com/smart-shield>

- Servizi

Per geografia:

- Nazionale

Per valore del cliente:

- Clienti a valore medio

Per potenziale di crescita:

- Clienti ad alto potenziale

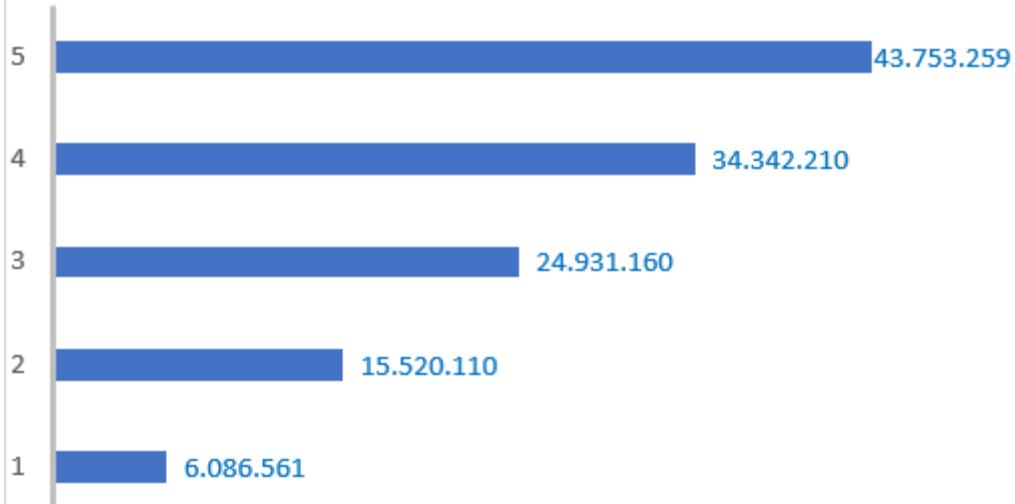
margine di ciascuna linea di prodotto

Conto Economico	Anno 1	Anno 2	Anno 3
+ Ricavi di vendita	7.668.320	19.120.640	38.341.600
- Costo materiali	766.832	1.912.064	3.834.160
- Provvigioni	766.832	1.912.064	3.834.160
= Margine di contribuzione	6.134.656	15.296.512	30.673.280
- Manodopera diretta	1.533.664	3.824.128	7.668.320
- Accantonamento TFR MDO diretta	85.204	212.452	426.018
= MDC - Costo MDO diretta	4.515.788	11.259.932	22.578.942
- Costi fissi di struttura	37.200	37.200	37.200
- Manodopera indiretta	120.000	120.000	120.000
- Accantonamento TFR MDO indiretta	6.667	6.667	6.667
- Costi di sviluppo	100.000	200.000	300.000
= EBITDA	4.251.922	10.896.066	22.115.076
- Ammortamenti (inserirlo prima nello SP)	45.000	67.500	89.000
= EBIT (Reddito Operativo)	4.206.922	10.828.566	22.026.076
- Oneri (Gestione finanziaria)	100.000	122.500	144.000
= Reddito ante imposte	4.106.922	10.706.066	21.882.076
- Imposte	1.642.769	4.282.426	8.752.830
= Reddito netto	2.464.153	6.423.639	13.129.245

Sulla tabella qui sopra sono riportate i ricavi del 1°, 2° e 3° anno con le relative spese, costi fissi, imposte e l'effettivo margine di profitto netto.

Evoluzione prevista di vendite nel tempo

cash flow



Sulla tabella qui sopra sono riportate i ricavi del 1°, 2° e 3° e i possibili ricavi futuri del 4° e 5° anno.

2.3 Partnership o altri rapporti di collaborazione da attivare

Come si crea valore?

Per una nuova azienda nel campo della Cybersecurity creare valore per i propri clienti deve avvenire attraverso la collaborazione con altri attori del settore. I partner chiave saranno:

- **Società di consulenza:** Aziende che offrono competenze specifiche e servizi di implementazione.
- **Provider di servizi cloud:** Piattaforme cloud sicure e affidabili per l'hosting delle soluzioni di cybersecurity.
- **Università e istituti di ricerca:** Collaborazioni per attività di ricerca e sviluppo. (Si Veda Piano Strategico).
- **Agenzie governative:** Partnership per il rispetto delle normative e la protezione delle infrastrutture critiche. (Si Veda Piano Strategico).

L'azienda e i suoi partner lavoreranno insieme per creare soluzioni integrate che rispondano alle esigenze specifiche dei clienti, migliorando la sicurezza complessiva e riducendo i rischi di cyberattacchi

Sintesi delle alleanze e degli accordi già raggiunti:

- **Accordo con un provider di servizi cloud:** Partnership con un leader del settore come AWS.
- **Partnership con società di consulenza IT:** Accordi con aziende per offrire servizi di implementazione e consulenza personalizzati ai clienti.
- **Accordo con università per la Ricerca e Sviluppo:** Collaborazioni con istituti accademici per sviluppare nuove tecnologie e migliorare quelle esistenti attraverso attività di ricerca avanzata.

Identificazione di Possibili Alleanze Future

- **Alleanze con altre aziende di cybersecurity:** Unirsi a consorzi o reti di aziende di cybersecurity per condividere conoscenze e risorse.
- **Partnership con aziende di telecomunicazioni:** Lavorare con provider di telecomunicazioni per migliorare la sicurezza delle reti di comunicazione.(Si veda Piano Strategico)
- **Accordi con piattaforme di e-commerce:** Fornire soluzioni di sicurezza per proteggere le transazioni online e i dati dei clienti
- **Partecipazione a fiere e conferenze del settore:** Le fiere e le conferenze sono un ottimo modo per incontrare potenziali partner e conoscere le ultime tendenze del settore.
- **Iscrizione a organizzazioni del settore:** Esistono diverse organizzazioni del settore della cybersecurity che offrono opportunità di networking e sviluppo professionale.
- **Stabilimento di relazioni con analisti e influencer del settore:** Gli analisti e gli influencer del settore possono aiutare le nuove aziende a farsi conoscere e a guadagnare credibilità.

MAKE OR BUY?

La strada che Smart Shield ha scelto; è quella di mantenere il controllo diretto su tecnologie critiche in modo da garantire innovazione continua e sicurezza; quindi, di creare internamente le soluzioni permettendo così di proteggere la proprietà intellettuale e differenziarsi dalla concorrenza. Inoltre, l’Azienda, così facendo, resterà più autonoma non essendo soggetta a contratti\richieste delle grandi aziende fornitrice di questi servizi che possono minare la propria stabilità

2.4 Possesso di brevetti o certificazioni

BREVETTI

Brevetti per algoritmi di rilevamento: Questi brevetti proteggono i metodi utilizzati dal software antivirus per identificare e classificare malware e altri tipi di minacce informatiche. Ad esempio, un brevetto potrebbe coprire un nuovo algoritmo di apprendimento automatico in grado di identificare malware sconosciuto in base al suo comportamento.

(proprietario)

Brevetti per tecniche di rimozione: Questi brevetti proteggono i metodi utilizzati dal software antivirus per rimuovere malware e altri tipi di minacce informatiche dai sistemi informatici. Ad esempio, un brevetto potrebbe coprire una nuova tecnica per rimuovere malware che si nasconde nel registro di sistema.

(proprietario)

Brevetti per interfacce utente: Questi brevetti proteggono il design dell'interfaccia utente del software antivirus. Ad esempio, un brevetto potrebbe coprire un nuovo design per la dashboard principale del software antivirus, che consente agli utenti di visualizzare e gestire facilmente lo stato della sicurezza del proprio sistema.

(in licenza)

Brevetti per funzionalità di sicurezza: Questi brevetti proteggono le funzionalità di sicurezza specifiche del software antivirus. Ad esempio, un brevetto potrebbe coprire una nuova funzionalità di firewall che protegge i sistemi informatici dagli attacchi informatici.

(in licenza)

Protezione del Marchio: I marchi proteggono i nomi e i loghi utilizzati da una startup per identificare i propri prodotti o servizi. Ad esempio, il marchio "Norton" è protetto da un marchio, che impedisce ad altre aziende di utilizzare quel nome per i propri prodotti antivirus.

(in licenza)

Segreti commerciali: I segreti commerciali proteggono le informazioni riservate che danno a un'azienda un vantaggio competitivo. Ad esempio, una startup di software antivirus potrebbe avere un segreto commerciale relativo al suo algoritmo di rilevamento del malware.

(in licenza)

CERTIFICAZIONI

Certificazione Common Criteria (CC): Common Criteria è uno standard internazionale per la valutazione della sicurezza dei prodotti IT. La certificazione CC può garantire che il tuo software antivirus soddisfi rigorosi requisiti di sicurezza.

Certificazione ISO 27001: ISO 27001 è uno standard internazionale per i sistemi di gestione della sicurezza delle informazioni. L'ottenimento della certificazione ISO 27001 dimostra che la tua azienda ha implementato un approccio globale alla gestione e alla protezione del proprio patrimonio informativo.

Certificazione di conformità GDPR: Il Regolamento generale sulla protezione dei dati (GDPR) è un regolamento dell'Unione Europea che stabilisce i requisiti per la protezione dei dati personali. La conformità al GDPR può essere essenziale per le società di software antivirus che gestiscono dati personali.

LICENZE

Licenza software: Licenza software per lo sviluppo e la distribuzione del software antivirus. Questa licenza garantisce il diritto di riprodurre, distribuire e vendere il software. Potrebbe essere necessario ottenere licenze per qualsiasi software di terze parti utilizzato nel prodotto.

(in licenza)

Licenze di brevetto: Il software antivirus include una tecnologia brevettata, quindi licenze dai titolari del brevetto. Include brevetti per algoritmi, tecniche o funzionalità specifiche del software.

(in licenza)

Licenze sui marchi: Si utilizzano marchi commerciali nel software, ottenimento di licenze dai titolari dei marchi. Include marchi commerciali per il nome della azienda, il logo o i nomi dei prodotti.

(in licenza)

Licenze sulla privacy dei dati: Il software antivirus raccoglie e elabora dati personali, quindi rispetta le leggi sulla privacy dei dati come il Regolamento generale sulla protezione dei dati (GDPR).

(in licenza)

Smart Shield S.r.l. - CIS di Nola, isola 8 - smartshieldenterprise@gmail.com -
<https://smartshieldenterpr.wixsite.com/smart-shield>

PER PROGETTI FUTURI

Licenze di esportazione: Se prevedi di esportare il software antivirus in altri paesi, quindi sarà necessario ottenere licenze di esportazione dal governo italiano.

NORMATIVE DA RISPETTARE

Regolamento generale sulla protezione dei dati (GDPR): questo regolamento europeo disciplina la raccolta e l'utilizzo dei dati personali. Le startup che sviluppano software antivirus devono assicurarsi che il loro software sia conforme al GDPR, in particolare per quanto riguarda la raccolta e l'utilizzo dei dati degli utenti.

CONFORMITA' ALLE NORMATIVE

Proteggere gli utenti: il software antivirus conforme alle normative è più sicuro e affidabile e offre una migliore protezione agli utenti contro le minacce malware.

Aumentare la fiducia degli utenti: gli utenti sono più propensi a utilizzare un software antivirus conforme alle normative perché sanno che è stato testato e certificato da organizzazioni indipendenti.

Accedere a nuovi mercati: la conformità alle normative può essere un requisito per vendere software antivirus in alcuni mercati.

3. Piano strategico

Visione:

Diventare il leader riconosciuto nel settore della sicurezza informatica offrendo soluzioni innovative e affidabili che proteggano le Famiglie, le Università, gli Ospedali e tutti gli enti pubblici dai rischi informatici in continua evoluzione.

Analisi del mercato e identificazione del target:

Il settore della sicurezza informatica è in costante evoluzione a causa della crescente minaccia di attacchi informatici e della sempre maggiore dipendenza dalle tecnologie digitali. La stessa cosa si può dire per il mercato in questione, che ha sì tanti competitor, ma allo stesso tempo offre opportunità senza precedenti, in quanto i principali concorrenti come: McAfee, Cisco Systems Inc. , BitDefender, detengono buona fetta del mercato per quel che concerne la sicurezza informatica di multinazionali, che spaziano dal settore bancario a quello alimentare; lasciando però un buco per tutti quegli enti pubblici e famiglie che al giorno d'oggi sono soggette ad innumerevoli truffe e furti di dati per via digitale.

Dalla Pandemia in poi, si è riscontrato un notevole aumento per i cosiddetti attacchi “Phishing”; leggendo il rapporto Cluist, (Associazione di Milano che promuove la sicurezza Informatica), a livello Globale il numero di attacchi hacker è aumentato del 21%. E l’Italia risulta tra i paesi più colpiti con un aumento del 169% rispetto all’anno 2022. Scendendo nel dettaglio, il settore Manifatturiero risulta essere quello più danneggiato con il 27% degli attacchi, subito dopo c’è quello Governativo con il 20%. Un altro dato significativo ci dice che il nostro Paese ha subito il 7,6% di tutti gli attacchi globali, contro il 3,4 del 2021.

In Italia, per ciò che riguarda la consapevolezza delle minacce informatiche, siamo messi molto male. Stando al Digital Economy and Society Index 2022 dell’UE, il nostro Paese è diciottesimo su 27 per livello di digitalizzazione e ,dato più allarmante, è al 23esimo posto su 27 per popolazione con competenze digitali di base, con solo il 46% della popolazione. Inoltre l’Italia è ultima in Europa per Laureati in ambito *ICT* (Information and Communication Technology) con il solo 1,4% della popolazione.

Dunque, è in questo contesto sociale in cui la nostra Azienda vuole inserirsi siccome gli investimenti dello Stato non sono sufficienti a competere con le altre Nazioni Europee e alle infinite minacce che la rete ha da offrire.

3.1.1 Analisi di attrattività del business

5. Potere contrattuale con i clienti

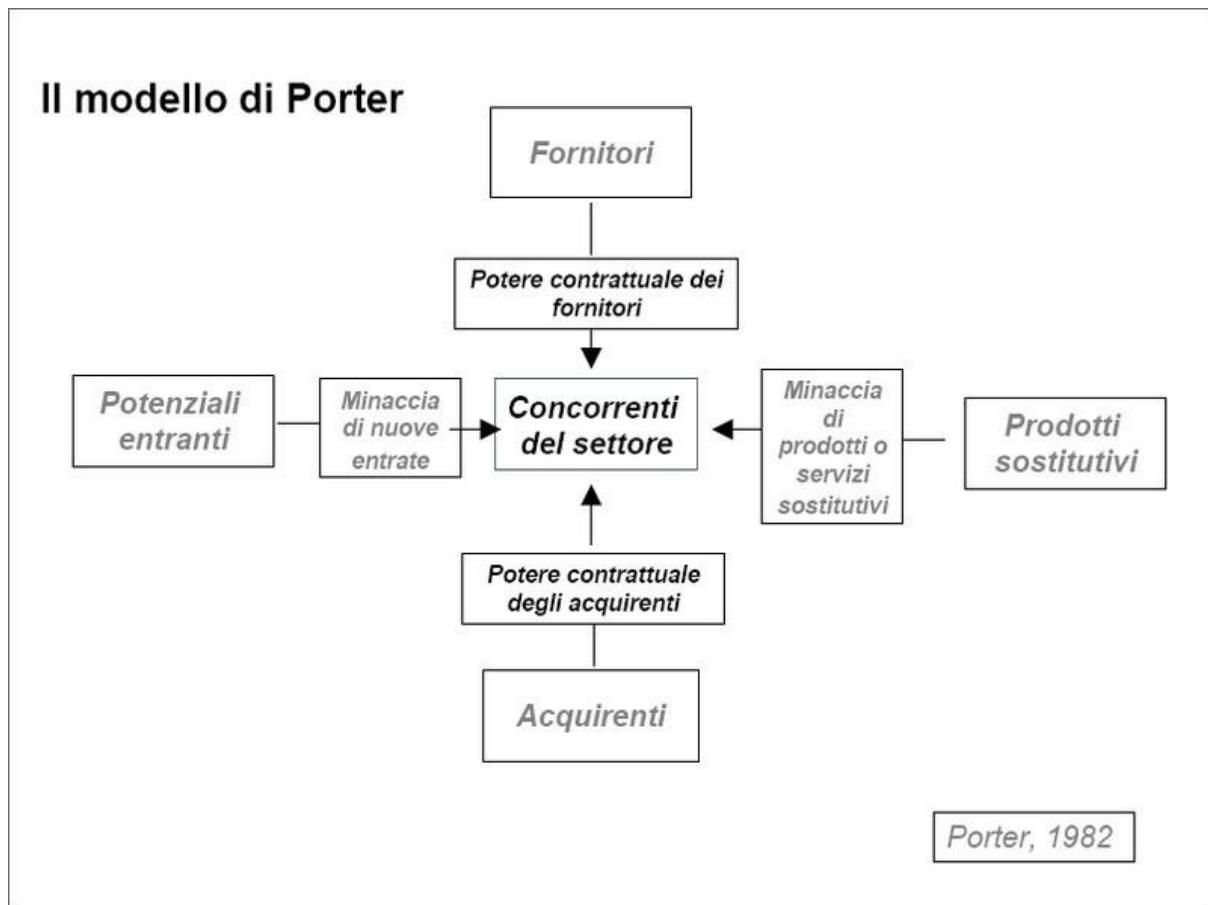


Figura 1. Il modello di Porter

Tabella 1. Concorrenti diretti

Presente: X Futuro: Y	Grado di attrattività (1: ass. non attrattivo; 2: scarsa attrattività; 3: neutrale; 4: attrattivo; 5: molto attrattivo)						
		1	2	3	4	5	
1. <u>Intensità della concorrenza</u>							
<i>Barriere all'uscita</i>							
Specializzazione degli investimenti	Elevata		X	Y			Bassa
Interrelazioni strategiche con altri business	Elevate		XY				Basse
Barriere emotive	Elevate		Y	X			Basse

Vincoli sociali e governativi	Elevati			XY			Bassi
	RISCONTRO PARZIALE						
<i>Rivalità fra i concorrenti</i>							
Crescita del settore	Bassa				XY		Alta
Costi fissi	Elevati		X		Y		Bassi
Grado di concentrazione	Elevato		Y	X			Basso
Differenziazione dei prodotti	Bassa				X	Y	Elevata
	TOTALE			X	Y		

Specializzazione degli investimenti: Nel presente 2 in quanto per poter partire la start up avrà bisogno di importanti investimenti nel settore tecnologico in modo da garantirne il corretto inserimento nel mercato;
 Nel futuro 3 in quanto una volta inseriti nel mercato si dovranno effettuare investimenti meno consistenti e specifici.

Interrelazioni strategiche con altri buisness: Sia nel presente che nel futuro 3 in quanto cercheremo di insturare rapporti di collaborazione con diversi Partner strategici

Barriere emotive: Nel presente 4 in quanto ci saranno notevoli sforzi per far nascere l'azienda, nel futuro 3

Vincoli sociale e governativi: Sia nel presente che nel futuro 3 in quanto essendo un settore strategico ci saranno vincoli Governativi

Crescita del Settore: Sia nel presente che nel futuro 5 in quanto il settore della sicurezza informatica sarà sempre in continua crescita in un mondo sempre più digitalizzato, interconnesso e dove i dati personali rappresentano un rischio per privati cittadini, Pubbliche Amministrazioni e aziende.

Costi fissi: Nel presente 2 in quanto, la mancanza di una clientela stabile e ampia, i costi fissi impatteranno maggiormente;
 Nel futuro 4 poiché è auspicabile un considerevole aumento di clienti già entro il primo anno di esercizio.

Grado di concentrazione: Sia nel presente che nel futuro 3 in quanto la grossa fetta di mercato è detenuto dalle grandi aziende conoscitrici del settore dunque, dovrebbe essere stabile nel tempo.

Differenziazione dei prodotti: Presente 4 poiché per riuscire ad abbracciare una quantità di clienti più ampia possibile e fornire servizi sempre più adeguati, la Start-Up dovrà garantire prodotti e soluzioni diversificate
Futuro 5 in quanto la strategia sarà quella di ampliare i prodotti offerti.

Tabella 2. Minaccia di potenziali entranti

Presente: X Futuro: Y		Grado di attrattività (1: ass. non attrattivo; 2: scarsa attrattività; 3: neutrale; 4: attrattivo; 5: molto attrattivo)					
		1	2	3	4	5	
1. Entrate potenziali							
Economie di scala	Basse		X	Y			Elevate
Differenziazione dei prodotti	Basse			X	Y		Elevate
Identità di marca	Bassa			X	Y		Elevata
Accesso ai canali di distribuzione	Semplice	Y	X				Complesso
Accesso alla tecnologia più avanzata	Semplice	Y		X			Complesso
Economie di esperienza	Basse				XY		Elevate
Provvedimenti governativi all'ingresso	Bassi	X		Y			Elevati
	TOTALE			X Y			

Economia di scala: Nel presente 3 in quanto l'azienda essendo nuova e avrà un bacino di clienti più stretto e di conseguenza un economia di scala più bassa, nel futuro, per precauzione, 4 ma potrebbe anche essere 5

Differenziazione dei prodotti: Similmente per quanto detto nella tabella precedente.

Identità di marca: 4 nel presente in quanto il marchio è conosciuto ma non abbastanza;

5 nel futuro grazie ad investimenti e nuove tecnologie.

Accesso ai canali di distribuzione: nel presente 4 siccome la conoscenza riguardo rischi informatici è ancora estremamente bassa;

Nel futuro 5 in quanta grazie all'affermazione dell'azienda sarà più facile entrare in nuovi mercati.

Accesso alla tecnologia più avanzata: Nel presente 4 dovuta alla limitata presenza di fondi, che però verrà soppiata dalle avanzate conoscenze del personale;
Nel futuro 2 in quanto all'elevate skill del personale si aggiungeranno dei fondi sempre più cospicui.

Economie di esperienze: Sia nel presente che nel futuro 5 siccome per avere successo è necessario avere esperienza in tutti i campi in cui l'azienda opererà.

Provvedimenti governativi all'ingresso: Nel presente 2 poiché in quanto è un settore in continua evoluzione le normative vigenti non sono stringenti;
Nel futuro 4 poiché il legislatore non tarderà a legiferare in materia, ma si presuppone che in quel momento l'azienda sarà già collocata in una fetta di mercato ampio; dunque, questo problema non sarà così importante.

Tabella 3. Minaccia di produttori di servizi o prodotti sostitutivi

Presente: X Futuro: Y	Grado di attrattività (1: ass. non attrattivo; 2: scarsa attrattività; 3: neutrale; 4: attrattivo; 5: molto attrattivo)						
		1	2	3	4	5	
1. Prodotti sostitutivi							
Disponibilità di prodotti sostitutivi	Elevata				X	Y	Bassa
Aggressività di chi produce prodotti sostitutivi	Elevata		X	Y			Bassa
Costi di riconversione cliente	Bassi			Y	X		Elevati
	TOTALE			X	Y		

Disponibilità di prodotti sostitutivi: Sia nel presente 4 , nel futuro 3; Siccome il nostro obiettivo, come già detto, è quello di offrire servizi differenti e personalizzabili; dunque, la disponibilità di prodotti sostitutivi non dovrebbe essere elevata.

Aggressività di chi produce prodotti sostitutivi: Come in ogni settore, anche in questo caso la concorrenza sarà aggressiva; dunque, spetta all'azienda saper districarsi e offrire prodotti sempre migliori rispetto alle altre aziende.

Costi di riconversione cliente: Nel presente 3 in quanto essendo una nuova azienda nel settore potrebbe capitare di perdere clienti;

Nel futuro 4 poiché di forniremo servizi di alta qualità auspiciamo una riconversione molto bassa

Tabella 4. Potere contrattuale con i fornitori

Presente: X Futuro: Y	Grado di attrattività (1: ass. non attrattivo; 2: scarsa attrattività; 3: neutrale; 4: attrattivo; 5: molto attrattivo)		1	2	3	4	5	
1. <u>Potere dei fornitori</u>								
Numero dei fornitori	Elevato				X	Y		Basso
Disponibilità di prodotti sostitutivi a quelli dei fornitori	Bassa					XY		Alta
Costi di sostituzione dei fornitori	Elevati			X	Y			Bassi
Minaccia di integrazione a valle dei fornitori	Elevata			X		Y		Bassa
Minaccia di integrazione a monte da parte del settore	Elevata			XY				Bassa
Contributo del fornitore alla qualità	Elevato					XY		Basso
Contributo del fornitore al costo industriale	Elevato			X		Y		Basso
	TOTALE				X	Y		

Numero dei fornitori: Nel presente 4 e nel futuro 5 poiché l'Azienda sarà quasi del tutto autonoma da aziende fornitrice;

Per le altre voci, si segue quanto detto.

Tabella 5. Potere contrattuale con i clienti

Presente: X Futuro: Y	Grado di attrattività (1: ass. non attrattivo; 2: scarsa attrattività; 3: neutrale; 4: attrattivo; 5: molto attrattivo)						
		1	2	3	4	5	
1. Potere degli acquirenti							
Numero degli acquirenti	Basso			X		Y	Elevato
Disponibilità di prodotti sostitutivi	Elevata			X	Y		Basse
Costi di sostituzione dell'acquirente	Elevati			Y	X		Bassi
Minaccia di integrazione a monte da parte degli acquirenti	Elevata				X	Y	Bassa
Contributo dell'acquirente alla qualità	Elevato		X	Y			Basso
Redditività dell'acquirente	Elevato			XY			Basso
	TOTALE			X	Y		

Numero degli acquirenti: Nel presente 3 visto che la Start-Up è di nuova costituzione;

Nel futuro 5, in quanto si stima una crescita di minacce informatiche è di conseguenza una protezione adeguata.

Disponibilità di prodotti sostitutivi: come già detto nella tabella precedente.

Costi di sostituzione dell'acquirente: Sia nel presente che nel futuro si prevede una consistenza simile in quanto i nostri servizi saranno proposti su larga scala.

Contributo dell'acquirente alla qualità: Nel presente 2, siccome, il cliente deve essere al centro dei nostri servizi avere dei riscontri da essi all'inizio della nostra attività non potranno fare altro che migliorare la qualità del servizio offerto; Nel futuro 3 poiché si presuppone che l'azienda sia rodata.

Redditività dell'Acquirente:

3.1.2 Scelta della strategia competitiva

Obiettivi Strategici:

1. Differenziazione dei prodotti e dei servizi offerti:

- Offrire soluzioni di sicurezza informatica altamente personalizzabili e adattabili alle esigenze specifiche dei clienti, superando così le offerte dei concorrenti che offrono soluzioni standardizzate.
- Sviluppare, lanciare nuove soluzioni e servizi innovativi per affrontare le minacce informatiche emergenti.

2. Investimento nella Ricerca e Sviluppo:

- Allocheremo risorse significative per la ricerca e lo sviluppo in tecnologie avanzate di sicurezza informatica e non solo.
- Cercheremo di instaurare rapporti di stretta collaborazione con istituti accademici e apparati dello Stato per rimanere all'avanguardia delle nuove scoperte e diffondere i rischi della rete alle nuove generazioni.

3. Fidelizzazione e soddisfazione dei clienti:

- Uno dei principali obiettivi strategici per avere un bacino clienti sufficiente in modo da garantire la corretta stabilità dell'azienda sarà quello di migliorare costantemente l'esperienza complessiva del cliente attraverso l'eccellenza del servizio e la risoluzione tempestiva delle problematiche.
- Ci saranno programmi di fidelizzazione, per garantire una piena soddisfazione ai quali sceglieranno Smart Shield; inoltre forniremo un vero e proprio servizio di formazione ai clienti di alto livello, in modo da massimizzare le soluzioni da noi offerte.
- Garantiremo un supporto tecnico rapido e mirato.

4. Collaborazioni e Partnership Strategiche:

- Instaureremo partnership con altre aziende tecnologiche e fornitori di servizi in modo da offrire soluzioni integrate e complete ai clienti cercando di soddisfare a pieno le loro esigenze personali.
- Cercheremo di creare rapporti di collaborazione con le autorità e le Istituzioni Governative per affrontare le minacce che il cyber spazio ci pone.
- Partnership con provider di Telecomunicazioni, in modo da garantire sicurezza a 360 gradi ai clienti.

5. Innovazione Tecnologica e Aggiornamenti Continui:

- Mantenere un'infrastruttura tecnologica all'avanguardia tramite investimenti costanti in componenti hardware e software.

6. Sviluppo di Talenti e Team:

- Uno dei tanti obiettivi che ci porremo sarà quello di collaborare con le Università in modo da: attrarre, sviluppare e trattenere i migliori talenti nel campo della sicurezza informatica attraverso programmi di formazione, incentivi competitivi e un ambiente di lavoro stimolante.
- Creeremo team multidisciplinari con competenze a 360 gradi per affrontare in modo efficace le sfide tecnologiche e commerciali.

3.2 Analisi interna

Nessuna fonte nel documento corrente.

Punti di forza:

1. **Competenza tecnica:** L'azienda disporrà di personale altamente qualificato e competente nel campo della sicurezza informatica, in modo da offrire soluzioni innovative ed efficaci ai clienti.
2. **Indipendenza di Tecnologie:** L'Azienda sarà in grado di sviluppare l'AI e tutti i software necessari al fine di garantire la sicurezza dei clienti. Così facendo saremo più riconoscibili sul mercato in quanto non dipenderemo da aziende terze.
3. **Flessibilità e adattabilità:** L'azienda essendo nuova avrà la capacità di adattarsi rapidamente alle mutevoli esigenze del mercato e ai nuovi sviluppi tecnologici, offrendo soluzioni più agili rispetto ai diretti concorrenti.
4. **Approccio innovativo:** Essendo un nuovi nel settore, l'Azienda potrebbe portare nuove idee e approcci innovativi alla sicurezza informatica, distinguendosi dai concorrenti.
5. **Focus su specifiche esigenze di settore:** Ci concentreremo su settori o segmenti di mercato specifici, diventando esperta nelle esigenze di sicurezza informatica di quei settori e fornendo soluzioni altamente specializzate.

Smart Shield S.r.l. - CIS di Nola, isola 8 - smartshieldenterprise@gmail.com -

<https://smartshieldenterprise.wixsite.com/smart-shield>

Debolezze:

1. **Mancanza di reputazione:** La nostra azienda dovrà “lottare” per guadagnare la fiducia dei clienti a causa di un iniziale mancanza di reputazione nel settore.
2. **Limitazioni finanziarie:** La mancanza di risorse finanziarie potrà limitarci nella capacità di investire in ricerca e sviluppo o di competere con le aziende più grandi.
3. **Mancanza di esperienza nel settore:** Anche se l'azienda avrà un elevato talento tecnico, potrebbe mancare di esperienza nel settore della sicurezza informatica, il che potrebbe influire sulla sua capacità di comprendere appieno le esigenze dei clienti e di sviluppare soluzioni efficaci.

Conclusioni:

IL piano strategico delineato offre una strategia chiara per il successo dell'Azienda, orientando gli sforzi verso l'innovazione, la soddisfazione del cliente e la leadership nel settore. Implementando le strategie e monitorando attentamente i KPI, saremo in grado di adattarci alle mutevoli sfide del panorama della sicurezza informatica e crescere in modo sostenibile nel tempo.

4. Piano marketing

situazione italiana

Il mercato degli antivirus è in continua espansione dovuto all'aumento esponenziali di attacchi di phishing ai privati ed attacchi di tipo ransomware alle aziende. Secondo un report pubblicato da SWASCAN, importante società di cyber security italiana, 80% delle aziende energetiche e aziende sanitarie hanno un basso livello di difesa contro gli attacchi informatici. Vittorio Colao, Ex Ministro per l'innovazione tecnologica e la transizione digitale, nel 2021 ha dichiarato che il 95% dei server della pubblica amministrazione italiana e PMI hanno un basso livello di difesa contro i crimini informatici.

SPECIFICHE DEL NOSTRO PRODOTTO

Punti di forza e debolezza di Smartshield

Virus e malware: L'IA dovrebbe essere in grado di rilevare la presenza di virus, malware, worm e altri software dannosi sui dispositivi degli utenti.

Phishing e truffe online: Deve essere in grado di identificare e avvisare gli utenti di tentativi di phishing tramite e-mail, messaggi di testo, social media o altri mezzi online.

Attacchi di ingegneria sociale: Dovrebbe essere in grado di rilevare tentativi di ingegneria sociale, come truffe telefoniche, richieste di informazioni personali o altre tattiche per ottenere accesso non autorizzato.

Attacchi di ransomware: Deve essere in grado di rilevare e prevenire attacchi di ransomware che criptano i file degli utenti e richiedono un riscatto per il ripristino.

Attacchi di tipo man-in-the-middle: Deve essere in grado di rilevare attacchi man-in-the-middle, dove un aggressore intercetta e manipola la comunicazione tra due parti.

Violazioni della privacy: Dovrebbe essere in grado di rilevare violazioni della privacy, come accessi non autorizzati alle informazioni personali degli utenti o tentativi di monitoraggio non autorizzato.

Attività sospette dell'account: Deve essere in grado di rilevare attività sospette sugli account degli utenti, come accessi da posizioni insolite o tentativi di accesso ripetuti.

Anomalie di rete: Dovrebbe essere in grado di rilevare anomalie di rete, come traffico anomalo o tentativi di scansione o attacchi da parte di terze parti.

Accessi non autorizzati al dispositivo: Deve essere in grado di rilevare tentativi di accesso non autorizzato ai dispositivi degli utenti, come tentativi di forzare la password o di bypassare i controlli di sicurezza.

Violazioni dei dati: Deve essere in grado di rilevare violazioni dei dati, come accessi non autorizzati ai database o alle informazioni sensibili degli utenti.

Abusi online e bullismo: Deve essere in grado di rilevare attività di abuso online, come cyberbullismo o molestie, e fornire supporto agli utenti interessati.

Copertura multi-dispositivo: Consente agli utenti del piano famiglia di proteggere un numero specificato di dispositivi per ciascun membro della famiglia, ad esempio computer, smartphone, tablet e dispositivi smart home.

Gestione centralizzata degli account: Fornisce un pannello di controllo centralizzato per la gestione degli account degli utenti, consentendo ai genitori di controllare e monitorare l'attività online dei loro figli e proteggere tutti i membri della famiglia da una singola piattaforma.

Controllo genitoriale avanzato: Offre funzionalità avanzate di controllo genitoriale per i genitori, inclusa la possibilità di impostare limiti di tempo per l'uso dei dispositivi, bloccare l'accesso a determinati siti web o applicazioni e monitorare l'attività online dei bambini.

Protezione per tutte le età: Assicura che il piano famiglia offra una protezione adatta a tutte le età, con funzionalità specifiche per proteggere sia i bambini che gli adulti dagli attacchi informatici e dalle minacce online.

Supporto dedicato per la famiglia: Fornisce un supporto clienti dedicato per le famiglie, con risorse educative e assistenza personalizzata per affrontare le sfide legate alla sicurezza informatica all'interno della famiglia.

Prezzo scontato: il piano famiglia offre un prezzo scontato rispetto all'acquisto di abbonamenti individuali per ciascun membro della famiglia, rendendo la protezione più accessibile per tutti.

Privacy e sicurezza dei dati familiari: Assicura che la tua intelligenza artificiale rispetti la privacy e la sicurezza dei dati della famiglia, proteggendo le informazioni personali e sensibili di tutti i membri della famiglia.

Backup familiare condiviso: Offre uno spazio di archiviazione condiviso per il backup dei dati per tutti i membri della famiglia, consentendo loro di proteggere e accedere facilmente ai propri file importanti da tutti i dispositivi.

Controllo dei dispositivi smart home: Integra funzionalità per proteggere i dispositivi smart home della famiglia, inclusi telecamere di sicurezza, termostati intelligenti e dispositivi di domotica, da accessi non autorizzati e vulnerabilità di sicurezza.

Filtri di navigazione familiare: Fornisce filtri di navigazione web personalizzati per i bambini, consentendo ai genitori di impostare regole specifiche per ciascun membro della famiglia e proteggere i più piccoli da contenuti inappropriati online.

Allerta di geolocalizzazione familiare: Introduce funzionalità di allerta di geolocalizzazione per avvisare i genitori quando i loro figli entrano o escono da determinate aree, contribuendo a garantire la sicurezza dei più piccoli quando sono fuori casa.

Monitoraggio dell'utilizzo del tempo familiare: Fornisce strumenti per monitorare l'utilizzo del tempo online e sui dispositivi per ogni membro della famiglia, aiutando a promuovere un equilibrio sano tra l'uso della tecnologia e le attività offline.

Sicurezza dei social media familiari: Integra funzionalità per proteggere i profili sui social media dei membri della famiglia da account falsi, phishing e altre minacce online comuni sui social network.

Formazione sulla sicurezza informatica familiare: Offriremo risorse educative sulla sicurezza informatica progettate appositamente per le famiglie, con consigli pratici su come proteggere sé stessi e i propri dati online.

Gestione delle password familiare: Fornisce un'opzione per la condivisione sicura delle password tra i membri della famiglia e un gestore di password integrato per semplificare la gestione delle credenziali online.

Difetti

Non aggiornato su tutti i malware esistenti, ancora in fase di aggiornamento e limite nella potenza computazionale dell'IA. Ma, ciò nonostante, non esiste un prodotto simile al nostro sul mercato italiano con tali caratteristiche.

4.1 Definizione e segmentazione del mercato

Segmenti target di mercato

Puntiamo sia al **B2B (Business to Business)** che al **B2C (Business to Consumer)** sul mercato nazionale italiano

Dimensioni del Mercato globale e nazionale

Il mercato globale dell'IA nella cybersecurity dovrebbe crescere da 22,4 miliardi di dollari nel 2023 a 60,6 miliardi di dollari entro il 2028. Si prevede che il mercato globale dei software antivirus crescerà da 4,40 miliardi di dollari nel 2023 a 7,54 miliardi di dollari entro il 2030. Anche il mercato italiano della cybersecurity sta vivendo una crescita significativa, con un aumento del 16% rispetto all'anno precedente. Nel 2023, ha raggiunto un record di 2,15 miliardi di euro.

Tuttavia, l'Italia si colloca ancora all'ultimo posto tra i Paesi del G7 per il rapporto tra spesa in cybersecurity e PIL, attestandosi allo 0,12%. Questo indica che, nonostante l'interesse crescente, c'è ancora spazio per migliorare gli investimenti nel settore.

Numero di Utenti e Domanda Potenziale

Come riportato sopra il mercato italiano della cybersecurity sta vivendo una crescita significativa, con un aumento del 16% rispetto all'anno precedente. Nel 2023, ha raggiunto un record di 2,15 miliardi di euro.

Numero di Imprese Presenti

35 aziende quotate in Italia operano nel settore dell'intelligenza artificiale e nelle sue possibili integrazioni, con un market Cap di 1,46 miliardi di dollari. In Europa, 24 dollari per abitante vengono investiti nelle imprese di IA nell'Eurozona invece 9 dollari, cioè un valore doppio rispetto alla Cina.

Domanda di Mercato

Le aziende stanno sempre più optando per soluzioni basate sull'IA piuttosto che per gli antivirus tradizionali, data la crescente complessità delle minacce informatiche. La fiducia nell'IA e la sua capacità di migliorare la produttività stanno spingendo la domanda di software antivirus con intelligenza artificiale. In sintesi, il mercato per i software antivirus con IA integrato è in crescita, con un numero crescente di utenti e un'ampia domanda da parte delle aziende che cercano soluzioni avanzate per proteggere i loro sistemi e i privati che vogliono proteggersi dai ormai comuni attacchi di fishing.

CONCORRENZA

- **Abbonamento mensile base:** Circa 7-10 €
- **Abbonamento mensile con funzionalità avanzate:** Circa 10-15 €
- **Abbonamento mensile per la protezione di più dispositivi:** Circa 15-25€

Ecco alcuni esempi di prezzi attuali di abbonamenti mensili popolari per antivirus in Italia:

Smart Shield S.r.l. - CIS di Nola, isola 8 - smartshieldenterprise@gmail.com -
<https://smartshieldenterprise.wixsite.com/smart-shield>

- **Norton360 Deluxe:** 9,99 €
- **Bitdefender Antivirus Plus:** 7,49 € **Avast Premium Security:** 6,99 € / **Avast Ultimate:** 9,99 €
- **AVG Internet Security:** 7,99 € / **AVG Ultimate:** 11,99 €

Le versioni aziendali della concorrenza hanno dei costi che variano tra i €50 e i €100.

Analisi del Mercato

Secondo gli ultimi dati di Statcounter: le quote di mercato dei 5 antivirus in Italia a maggio 2024 sono:

Bitdefender: 32.2%

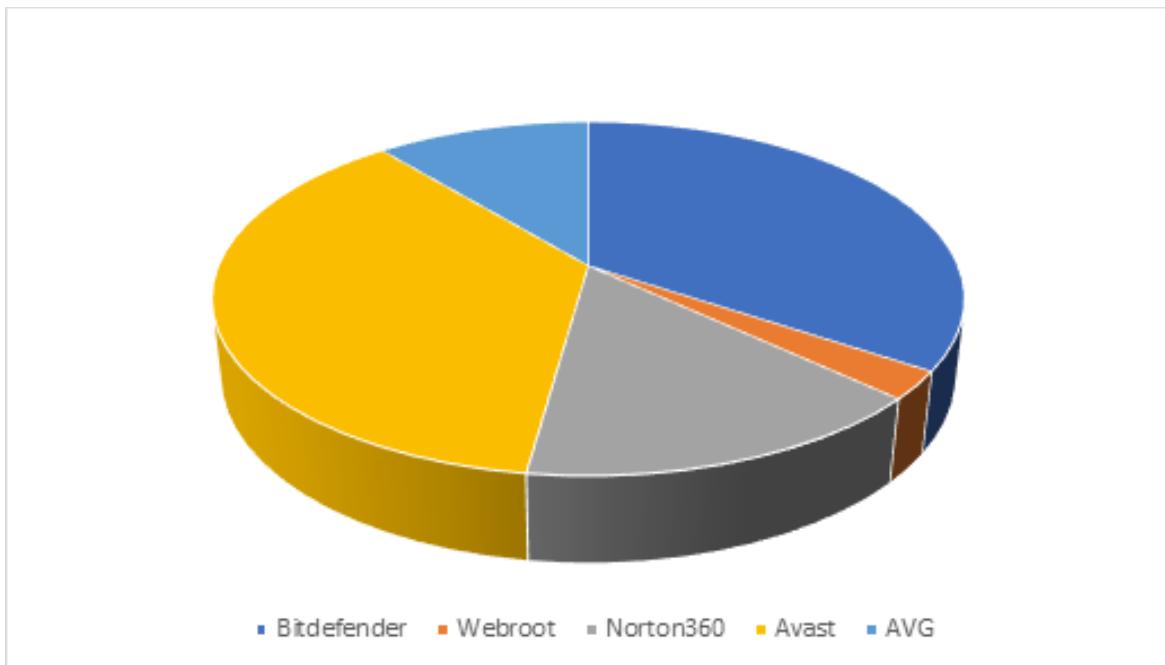
Webroot: 2.4%

Norton 360: 14.3%

Avast: 34.5%

AVG: 10.3%

In totale, questi 5 antivirus rappresentano il 93,7% del mercato italiano degli antivirus, il resto sono di poca rilevanza.



CONCLUSIONE

In sintesi, Bitdefender, Webroot, Norton 360 e Avast sono tra i principali concorrenti nel mercato degli antivirus con IA. Ognuno ha i suoi punti di forza e debolezza, ma tutti si concentrano sulla protezione avanzata e l'utilizzo dell'intelligenza artificiale per affrontare le minacce informatiche.

- Costo abbonamento mensile per singolo utente: **€9,90**
- Costo abbonamento mensile per famiglia (fino a 5 dispositivi): **€12,90** invece che **€19,90**
- Costo abbonamento mensile per aziende: **€29,90**

Esiste una versione gratuita con presenza di banner pubblicitari.

PUNTI DI FORZA E DEBOLEZZA DEI PRODOTTI DEI NOSTRI CONCORRENTI

Per valutare le quote di mercato e i punti di forza/debolezza dei principali software antivirus con intelligenza artificiale (IA), esaminiamo alcune soluzioni rilevanti.

Bitdefender

Bitdefender è uno dei leader nel settore della sicurezza informatica. La sua ampia base di utenti e la reputazione consolidata lo pongono in una posizione di forza.

Punti di Forza: Offre una protezione avanzata contro malware, ransomware e altre minacce.

È noto per essere uno dei programmi antivirus più leggeri e veloci.

Include funzionalità come Bitdefender VPN e Bitdefender Safepay.

Debolezzze: Alcuni utenti potrebbero considerare il prezzo di Bitdefender relativamente alto rispetto ad altre opzioni.

Webroot

Webroot è apprezzato per la sua leggerezza e l'approccio basato su cloud.

Punti di Forza: Esegue scansioni ad alta velocità utilizzando risorse minime del sistema.

Include il gestore di password LastPass.

Utilizza un'analisi euristica e una directory di malware basata su cloud.

Debolezzze: Alcuni utenti potrebbero desiderare funzionalità aggiuntive oltre alla protezione di base.

Norton 360

Norton è un nome noto nella sicurezza informatica.

Punti di Forza: Utilizza un motore di scansione basato su analisi euristica e apprendimento automatico.

Protezione da Virus e Malware: Offre una solida protezione.

Debolezzze: Potrebbe essere considerato costoso rispetto ad alcune alternative simili.

Avast

Punti di forza: Avast offre una vasta gamma di funzionalità, tra cui protezione in tempo reale, protezione della webcam, distruggi-dati e altro ancora.

Avast offre assistenza tecnica continua per gli utenti, supporto tecnico 24/7.

Debolezze: Anche se Avast ha una versione gratuita, alcune delle funzionalità avanzate richiedono un abbonamento a pagamento non economico.

Alcuni utenti segnalano che Avast potrebbe rallentare il sistema.

AVG

Punti di forza: AVG consente agli utenti di personalizzare le impostazioni di sicurezza in base alle proprie esigenze.

AVG offre funzionalità di protezione aggiuntive come il firewall e la protezione da phishing.

Debolezze: Rispetto ad Avast, AVG potrebbe mancare di alcune funzionalità avanzate come la protezione della webcam o il distruggi-dati.

Anche se AVG ha una versione gratuita, alcune funzionalità premium richiedono un abbonamento a pagamento non economiche.

4.2 Strategia di marketing

Politica di Prezzo

Alto (Nicchia): Se il software antivirus con intelligenza artificiale fosse altamente specializzato e offrisse funzionalità avanzate, potrebbe essere posizionato come un prodotto di nicchia. In tal caso, il prezzo dovrebbe riflettere questa esclusività.

Medio (Allineamento ai Principali Competitor): Se il prodotto si posiziona come una soluzione completa, allineata ai principali competitor, il prezzo dovrebbe essere competitivo rispetto a prodotti simili sul mercato.

(opzione scelta per privati e famiglie)

Basso (Politica di Prezzo Aggressiva): l'obiettivo sarebbe quello di acquisire una quota di mercato significativa, puntando su una politica di prezzo aggressiva che potrebbe essere appropriata. Questo potrebbe attirare clienti che vogliono una soluzione economica.

(opzione scelta per le aziende)

Prodotto

Cosa offre: software antivirus che offre una protezione efficace contro le minacce informatiche, utilizzando l'intelligenza artificiale per rilevare e prevenire attacchi. Le caratteristiche tangibili includono l'interfaccia utente, la facilità d'uso e la compatibilità con i sistemi operativi oltre ad un innumerevole funzionalità riportate in precedenza e sulla effettiva efficace dell'IA da noi generata.

Elementi Immateriali: Assistenza clienti, manutenzione del software e aggiornamenti regolari sono elementi immateriali importanti. Garantire un supporto tempestivo e di alta qualità può influenzare la percezione del prodotto nei confronti dei clienti.

Promozione

Pubblicità: Utilizzare campagne pubblicitarie online per aumentare la consapevolezza del prodotto. Ad esempio, annunci sui social media, banner pubblicitari e pubblicità porta a porta, oltre al nostro sito web sotto riportato.

Attività Promozionali: Offrire sconti temporanei o pacchetti promozionali per incentivare l'acquisto. Ad esempio, "Acquista un anno e ottieni tre mesi gratuiti" oppure software formato famiglia (protezione fino a cinque dispositivi).

Posto

Distribuzione Online: Vendere il software attraverso il proprio sito web:

www.smartshieldenterpr.wixsite.com

offrendo un accesso diretto ai clienti. Per gli iscritti al sito ci sono anche corsi di formazioni. Per quanto riguarda il budget di marketing, è importante considerare le risorse finanziarie disponibili e gli obiettivi di crescita. Questo è un esempio approssimativo di budget annuale per le spese di marketing nei prossimi tre anni:

TABELLA COSTI PER SPESE PUBBLICITARIE

Tipologia di costo	1° anno	2° anno	3° anno
Pubblicità online	€40.000	€50.000	€60.000
Attività promozionali	€20.000	€25.000	€25.000
Supporto clienti	€10.000	€15.000	€20.000
Altre spese	€15.000	€30.000	€35.000
totale	€85.000	€120.000	€140.000

Dalle ricerche svolte su internet, in media le aziende di software con un fatturato annuo di 5 milioni di euro spendono tra 250.000 e 500.000 euro annui in pubblicità.

4.3 Stima della domanda

Ricerca di mercato

Come detto in precedenza il mercato globale dell'IA nella cybersecurity dovrebbe crescere da 22,4 miliardi di dollari nel 2023 a 60,6 miliardi di dollari entro il 2028. Si prevede che il mercato globale dei software antivirus crescerà da 4,40 miliardi di dollari nel 2023 a 7,54 miliardi di dollari entro il 2030. Anche il mercato italiano della cybersecurity sta vivendo una crescita significativa, con un aumento del 16% rispetto all'anno precedente. Nel 2023, ha raggiunto un record di 2,15 miliardi di euro.

Tuttavia, l'Italia si colloca ancora all'ultimo posto tra i Paesi del G7 per il rapporto tra spesa in cybersecurity e PIL, attestandosi allo 0,12%.

Questo indica che, nonostante l'interesse crescente, c'è ancora spazio per migliorare gli investimenti nel settore ed è su questo margine che la nostra azienda punta.

Domanda attesa

Spazio nel mercato c'è ne grazie al numero di dispositivi (computer, smartphone e tablet) che richiedono protezione antivirus. La crescente digitalizzazione e la diffusione di dispositivi intelligenti aumentano la richiesta di soluzioni di sicurezza. Valutiamo anche la consapevolezza del pubblico (ad ogni fascia di età) riguardo alle minacce informatiche e l'importanza della protezione dei dati personali.

Scenari possibili

Worst case:

Situazione in cui la concorrenza è feroce, la domanda diminuisce e i costi di sviluppo e marketing aumentano. In questo scenario, l'azienda potrebbe lottare per sopravvivere dovendo abbassare i prezzi per sbaragliare la concorrenza.

Best case:

Se l'azienda riesce a posizionarsi come leader nel settore degli antivirus con IA. La domanda crescerebbe rapidamente, e i ricavi potrebbero anche superare le aspettative previste.

Scenario realistico:

Basato su dati di mercato e le relative analisi, si considera una crescita graduale. L'azienda si adatterà alle esigenze del mercato e investendo in innovazione, in particolar modo nell'IA.

Economicamente sostenibile

Valutare i costi di sviluppo, marketing, personale e operativi. Considerare anche i ricavi previsti e i margini di profitto. Assicurare che l'azienda abbia una solida strategia finanziaria per affrontare eventuali difficoltà. In sintesi, l'azienda che sviluppa un antivirus con IA condurrà ricerche approfondite, dovrà pianificare scenari realistici e adotterà una visione sostenibile per garantire il successo sia nel medio e lungo periodo cercando di diffondersi in futuro su un mercato più ampio, puntando anche al mercato globale.

	Mercato potenziale	Mercato raggiunto	Vendite previste (entrate)	Spese di Pubblicità/Promozione (risultati della sezione precedente)
1° Anno	7 milioni di utenti privati, 14,5 milioni di famiglie e 570.000 PMI	(2%) 140.000 utenti privati (2%) 290.000 famiglie (1%) 5.700 PMI	utenti privati €1.386.000 Famiglie €3.741.000 PMI €170.430	€85.000
2° Anno	7 milioni di utenti privati, 14,5 milioni di famiglie e 570.000 PMI	(5%) 350.000 utenti privati (5%) 725.000 famiglie (2%) 11.400 PMI	utenti privati €3.465.000 Famiglie €9.352.500 PMI €340.860	€120.000
3° Anno	7 milioni di utenti privati, 14,5 milioni di famiglie e 570.000 PMI	(10%) 700.000 utenti privati (10%) 1.450.000 famiglie (5%) 28.500 PMI	utenti privati €6.930.000 Famiglie €18.705.000 PMI €852.150	€140.000

Al terzo anno ci posizioniamo al terzo posto con il 25.0% del mercato potenziale nazionale (mercato italiano). Al primo posto troviamo Avast con il 34.5% e al secondo posto Bitdefender con il 32.2%.

Questa tabella è basata su questi dati ricavati da internet:

Ci sono 22 milioni di famiglie in Italia. Il 66% delle famiglie possiede almeno un computer, tablet o smartphone. Quindi 14,5 milioni è il numero che rappresenta le famiglie che possiedono almeno un pc, tablet o smartphone. Circa 8,5 milioni adulti (uomini e donne) vivono da sole in Italia e di questi l'83% (cioè circa 7 milioni) possiedono un PC, tablet o smartphone.

Piccole e Medie Imprese (PMI) sono presenti sul territorio italiano e costituiscono il 75% delle aziende totali, pari a circa 760 mila aziende. Il 75% delle PMI italiane con almeno 10 addetti utilizza internet e dispositivi informatici, cioè circa 570mila PMI su 760mila.

Le aziende sono più restie a cambiare prodotto o servizio quando è nuovo sul mercato a differenza di famiglie e singoli privati che puntano ad una miglior offerta di prezzo.

OBIETTIVI FUTURI: ampliare il mercato puntando a grandi aziende e amministrazioni pubbliche spingendoci fino al mercato globale.

ALTRI OBIETTIVI: L'obiettivo degli sviluppatori sarebbe quello di riuscire a stringere patti con l'Enisa, l'Agenzia della cybersicurezza europea e il governo italiano per rendere a basso costo l'IA e l'app a tutti gli utenti (a varie fasce di età) che utilizzano dispositivi elettronici connessi ad internet. Il sogno sarebbe quello di diminuire del 97% le frodi informatiche ai privati, e del 50% nelle aziende entro il 2045.

5. Piano organizzativo

Le figure professionali coinvolte nell'azienda sono innanzitutto i 4 soci fondatori della startup, a seguire 2 addetti vendita e 2 centralinisti call center.

Per il suo periodo iniziale di nascita la start-up si pone l'idea di essere un vero e proprio gruppo in cui non c'è una figura di un team leader con poteri sopra gli altri, ma i quattro soci hanno tutti pari privilegi e pari doveri per il corretto funzionamento dell'azienda, questo in modo da avere totale democrazia e libertà di espressione per ogni parte del progetto.

La filosofia adottata riprende un vecchio detto: "Se io ho un oggetto e un'altra persona ha un oggetto e ce li scambiamo a vicenda, entrambi avremo un solo oggetto dopo lo scambio. Se io ho un'idea e un'altra persona ha un'idea e ce le scambiamo a vicenda, alla fine dello scambio entrambi avremo due idee".

Secondo il nostro project work, le funzioni sono suddivise in:

PRODUZIONE E SVILUPPO: affidata principalmente a Francesco Petillo, in qualità di project manager e technology coofficer, a lui la supervisione generale del progetto di sviluppo software e coordinamento delle attività di sviluppo.

VENDITE e BILANCI: le prime affidate agli addetti vendita, coordinati da Ziadul Islam, planning manager e financial officer, in quanto responsabile del piano economico finanziario sarà poi suo onere occuparsi di tutta la parte economica della startup. Per quanto riguarda la parte di vendite sarà affiancato da Raffaele Murolo, in particolare si occuperà della parte di marketing intesa come pubblicità, sponsorizzazioni ecc... non strettamente legata alle vendite.

QUALITA' E PIANIFICAZIONE STRATEGICA: affidata ad Andrea di Palo, responsabile del Piano Strategico, a lui la responsabilità di monitorare gli standard di qualità, fornire analisi di mercato, strategie ecc... fanno poi a lui capo gli impiegati del servizio clienti.

All'organico dirigenziale si aggiungono 2 impiegati call center e 2 sviluppatori software, i primi due gestiranno il centralino del servizio clienti, i secondi due parteciperanno alla creazione, sviluppo e mantenimento software.

Progetto futuro

Come riportato nel piano operativo questo l'organigramma deciso dai 4 soci, con loro in prima persona che compiono più mansioni, sarà adottato per il periodo di inizio per almeno 4/5 anni confidando nel successo dell'azienda, a seguire se le vendite saranno quelle prospettate l'ampliamente del personale sarà graduale.

Si procederà all'assunzione di sviluppatori software che si occuperanno di gestire il software più grande e con più utenti, alla pari sarà necessario un centralino con più addetti per soddisfare la richiesta crescente di clienti e potenziali clienti.

Organizzazione attuale

Smart Shield S.r.l. - CIS di Nola, isola 8 - smartshieldenterprise@gmail.com -
<https://smartshieldenterprise.wixsite.com/smart-shield>

E' importante aggiungere che l'organico non si divide i compiti in maniera mai del tutto esclusiva, l'approccio del tutto innovativo che si è voluto utilizzare è proprio quello di avere un'azienda improntata come un gruppo di amici che si aiutano a vicenda per un esame, Ziadul Islam ad esempio si occupa dei bilanci, ma sorveglia anche la parte marketing in quanto responsabile delle vendite, Francesco Petillo sviluppa il software e resta continuamente in contatto con Raffaele Murolo per l'implementazione tecnologica dell'IA, il quale alla pari gestisce il piano Marketing, Andrea di palo si occupa della qualità e delle richieste dei clienti, pertanto collabora con Francesco e Raffaele sul software per presentare le richieste dei clienti... e così per gran parte di tutti gli aspetti della start-up, in un loop che unisce simbioticamente tutte le sezioni aziendali tra i dirigenti.

Si rimanda al piano operativo, in particolare alla matrice RACI e alla mappa OBS per ulteriori delucidazioni.

6. Piano operativo

La startup avrà sede nel C.I.S. di Nola, CAP 80035 isola 8, qui i soci avranno la sede; essendo un prodotto digitale si è optato per una zona commerciale e non una via rinomata nel centro di Napoli di grandi città italiane, in modo da abbattere i costi di locazione mantenendo requisiti industriali per una realtà software piuttosto energivora.

È necessario che l'ubicazione scelta rispecchi tutti i requisiti di una azienda software quali: connessione internet di almeno 500mb/s, limiti energetici molto alti in modo da garantire pieno funzionamento a tutti i pc ad alte prestazioni e alle componenti per l'IA, ovvero:

CPU essenziali per l'elaborazione generale e l'esecuzione degli algoritmi, necessarie per operazioni di calcolo che servono per i calcoli delle reti neurali.

GPU, adatte per elaborazione parallela, rendendole ideali per algoritmi di machine learning come le reti neurali profonde. Le loro architetture parallele possono accelerare significativamente il calcolo delle operazioni matematiche necessarie durante il processo di addestramento.

TPU specializzate per l'elaborazione di operazioni di tensori, che sono comuni nei modelli di machine learning. Sono progettate specificamente per il calcolo delle reti neurali e possono offrire prestazioni superiori rispetto alle CPU e alle GPU per determinati tipi di task di machine learning.

MEMORIA RAM, per elaborare i dati velocemente.

MEMORIA A LUNGO TERMINE, quella strettamente legata all'IA sarà tenuta su SSD o HDD, mentre il resto sarà tenuto in un vault online.

Personale impiegato

Per quanto riguarda il capitale umano della startup, essendo un'azienda piccola e neonata il personale sarà ridotto a membri strettamente necessari per il funzionamento dell'attività, ovviamente nella speranza di un ampliamento continuo e duraturo nel tempo, arrivando in un futuro non troppo remoto a quelli che sono i numeri di soci e dipendenti delle grandi holding europee e mondiali dell'ambito tech.

Il primo piano dell'apparato costituente la società include i soci fondatori del progetto come sviluppatori esperti, in modo da abbattere i costi, al contempo affianca personale da assumere per quanto riguarda il marketing e l'assistenza clienti. Confidando in una startup di successo i soci lasceranno lentamente i ruoli di sviluppatori agli impiegati che verranno, mantenendo le redini del progetto in ambito dirigenziale, ovviamente ascoltando sempre in primis gli sviluppatori.

L'organico è quindi composto da:

Sviluppatori esperti che si occuperanno del software, del sito web dedicato alla vendita e dell'intelligenza artificiale, 4 persone (i soci), che si alterneranno in turni, in modo da seguire tutto il personale a rotazione.

Esperti di marketing che si occupino delle strategie di vendita, della gestione (prettamente teorica) del sito web e che pubblicizzino il prodotto porta a porta e nei centri per anziani o categorie protette, nelle aziende, negli eventi pubblici, presso le dovute sedi per arrivare agli enti governativi,due persone.

Centralinisti call center, due tecnici informatici con consulenze basiche di cellulari e personal computer, dopo un'attenta formazione da parte dei soci, si occuperanno dell'assistenza h24 ai clienti.

Nel momento in cui lo scanner dell'IA rileverà malware, virus, soggetti con intenzioni malevoli o qualsiasi minaccia specificata nei dettagli del nostro pacchetto di protezione digitale, sarà loro cura mettersi in contatto tempestivamente con il diretto interessato al fine di fornirgli assistenza.

Il contatto avverrà quindi o da parte del cliente verso il servizio clienti, oppure sarà il servizio clienti ad avvertire l'utente nel caso in cui fosse stata rilevata una minaccia dall'intelligenza artificiale.

Sarà poi richiesto un feedback subito dopo il problema, con un report nel caso fossero state risolte nuove minacce, in modo da avere sempre un servizio clienti cordiale, efficiente.

Strategia tecnologica

Gli sviluppatori avranno necessità di un drive ad alta sicurezza dove archiviare i dati inerenti il progetto, gli utilizzatori, le minacce, dopo un'attenta analisi tra costi e sicurezza si è optato per:

1.Microsoft Azure Blob Storage: Simile a Amazon S3, offre uno spazio di archiviazione scalabile per i dati non strutturati.

2.Google Cloud Storage: Offre archiviazione altamente scalabile per oggetti e file, con opzioni per accesso frequente o meno frequente ai dati.

I due spazi di archiviazione fungeranno uno da backup dell'altro nel caso di falle, essendo due prodotti appartenenti a società totalmente diverse garantiranno sempre il massimo della sicurezza e del funzionamento del software.

Gli sviluppatori saranno forniti di ambienti di sviluppo sui cui operare (visual studio, intellij ecc).

Dominio per sito web, gli sviluppatori si occuperanno anche di un sito web dove ci saranno tutti i prodotti in vendita, uno sportello di assistenza clienti, contatti ecc...

PIANI DI ABBONAMENTO

LITE: piano di abbonamento con pubblicità integrate che offre un semplice ad Block e tracker, difende da tracciamenti non desiderati.

Classic:

Protezione della webcam: Implementa un sistema per monitorare e notificare agli utenti quando la loro webcam è attiva, proteggendoli da intrusioni non autorizzate.

Firewall personale: Integra un firewall personale per controllare il traffico di rete in entrata e in uscita e prevenire l'accesso non autorizzato al dispositivo.

Controllo genitoriale: Per i genitori che vogliono proteggere i propri figli online, fornisce strumenti di controllo genitoriale per limitare l'accesso a determinati siti web o applicazioni e monitorare l'attività online dei bambini.

Monitoraggio dell'identità: Implementa un sistema per monitorare l'identità degli utenti e avvisarli in caso di possibili violazioni dei dati personali o tentativi di furto di identità.

Protezione del Wi-Fi: Offre strumenti per proteggere la rete Wi-Fi domestica dagli attacchi esterni e per garantire che sia configurata in modo sicuro.

Crittografia dei dati: Abilita la crittografia dei dati sensibili memorizzati sui dispositivi degli utenti per proteggerli da accessi non autorizzati.

Backup automatico: Integra un sistema di backup automatico per consentire agli utenti di ripristinare i propri dati in caso di perdita o danneggiamento dei dispositivi.

Sicurezza delle transazioni online: Offre una protezione avanzata durante le transazioni online, inclusi acquisti, pagamenti e operazioni bancarie, per prevenire frodi finanziarie.

Protezione da ransomware: Implementa misure di protezione contro i ransomware per impedire il blocco o la crittografia dei dati da parte di malware dannoso.

Notifiche di sicurezza personalizzate: Forniscono notifiche personalizzate agli utenti in base alle loro abitudini e comportamenti online, per avvisarli di potenziali rischi di sicurezza.

Sicurezza delle reti Wi-Fi pubbliche: Forniscono strumenti per proteggere gli utenti quando si connettono a reti Wi-Fi pubbliche non sicure, inclusa la crittografia dei dati e la protezione da attacchi man-in-the-middle.

Blocco delle app malevoli: Integra un meccanismo per identificare e bloccare applicazioni malevoli o non sicure sul dispositivo degli utenti.

IN PARTICOLARE, L'IA SI OCCUPERA' DI:

Virus e malware: L'IA dovrebbe essere in grado di rilevare la presenza di virus, malware, worm e altri software dannosi sui dispositivi degli utenti.

Phishing e truffe online: Deve essere in grado di identificare e avvisare gli utenti di tentativi di phishing tramite e-mail, messaggi di testo, social media o altri mezzi online.

Attacchi di ingegneria sociale: Dovrebbe essere in grado di rilevare tentativi di ingegneria sociale, come truffe telefoniche, richieste di informazioni personali o altre tattiche per ottenere accesso non autorizzato.

Attacchi di ransomware: Deve essere in grado di rilevare e prevenire attacchi di ransomware che criptano i file degli utenti e richiedono un riscatto per il ripristino.

Attacchi di tipo man-in-the-middle: Deve essere in grado di rilevare attacchi man-in-the-middle, dove un aggressore intercetta e manipola la comunicazione tra due parti.

Violazioni della privacy: Dovrebbe essere in grado di rilevare violazioni della privacy, come accessi non autorizzati alle informazioni personali degli utenti o tentativi di monitoraggio non autorizzato.

Attività sospette dell'account: Deve essere in grado di rilevare attività sospette sugli account degli utenti, come accessi da posizioni insolite o tentativi di accesso ripetuti.

Anomalie di rete: Dovrebbe essere in grado di rilevare anomalie di rete, come traffico anomalo o tentativi di scansione o attacchi da parte di terze parti.

Accessi non autorizzati al dispositivo: Deve essere in grado di rilevare tentativi di accesso non autorizzato ai dispositivi degli utenti, come tentativi di forzare la password o di bypassare i controlli di sicurezza.

Violazioni dei dati: Deve essere in grado di rilevare violazioni dei dati, come accessi non autorizzati ai database o alle informazioni sensibili degli utenti.

Abusi online e bullismo: Deve essere in grado di rilevare attività di abuso online, come cyberbullismo o molestie, e fornire supporto agli utenti interessati.

FAMILY:

Copertura multi-dispositivo: Consente agli utenti del piano famiglia di proteggere un numero specificato di dispositivi per ciascun membro della famiglia, ad esempio computer, smartphone, tablet e dispositivi smart home.

Gestione centralizzata degli account: Fornisce un pannello di controllo centralizzato per la gestione degli account degli utenti, consentendo ai genitori di controllare e monitorare l'attività online dei loro figli e proteggere tutti i membri della famiglia da una singola piattaforma.

Controllo genitoriale avanzato: Offre funzionalità avanzate di controllo genitoriale per i genitori, inclusa la possibilità di impostare limiti di tempo per l'uso dei dispositivi, bloccare l'accesso a determinati siti web o applicazioni e monitorare l'attività online dei bambini.

Protezione per tutte le età: Assicura che il piano famiglia offra una protezione adatta a tutte le età, con funzionalità specifiche per proteggere sia i bambini che gli adulti dagli attacchi informatici e dalle minacce online.

Supporto dedicato per la famiglia: Fornisce un supporto clienti dedicato per le famiglie, con risorse educative e assistenza personalizzata per affrontare le sfide legate alla sicurezza informatica all'interno della famiglia.

Prezzo scontato: il piano famiglia offre un prezzo scontato rispetto all'acquisto di abbonamenti individuali per ciascun membro della famiglia, rendendo la protezione più accessibile per tutti.

Privacy e sicurezza dei dati familiari: Assicura che la tua intelligenza artificiale rispetti la privacy e la sicurezza dei dati della famiglia, proteggendo le informazioni personali e sensibili di tutti i membri della famiglia.

Backup familiare condiviso: Offre uno spazio di archiviazione condiviso per il backup dei dati per tutti i membri della famiglia, consentendo loro di proteggere e accedere facilmente ai propri file importanti da tutti i dispositivi.

Controllo dei dispositivi smart home: Integra funzionalità per proteggere i dispositivi smart home della famiglia, inclusi telecamere di sicurezza, termostati intelligenti e dispositivi di domotica, da accessi non autorizzati e vulnerabilità di sicurezza.

Filtri di navigazione familiare: Fornisce filtri di navigazione web personalizzati per i bambini, consentendo ai genitori di impostare regole specifiche per ciascun membro della famiglia e proteggere i più piccoli da contenuti inappropriati online.

Allerta di geolocalizzazione familiare: Introduce funzionalità di allerta di geolocalizzazione per avvisare i genitori quando i loro figli entrano o escono da determinate aree, contribuendo a garantire la sicurezza dei più piccoli quando sono fuori casa.

Monitoraggio dell'utilizzo del tempo familiare: Fornisce strumenti per monitorare l'utilizzo del tempo online e sui dispositivi per ogni membro della famiglia, aiutando a promuovere un equilibrio sano tra l'uso della tecnologia e le attività offline.

Sicurezza dei social media familiari: Integra funzionalità per proteggere i profili sui social media dei membri della famiglia da account falsi, phishing e altre minacce online comuni sui social network.

Formazione sulla sicurezza informatica familiare: Offriremo risorse educative sulla sicurezza informatica progettate appositamente per le famiglie, con consigli pratici su come proteggere se stessi e i propri dati online.

Gestione delle password familiari: Fornisce un'opzione per la condivisione sicura delle password tra i membri della famiglia e un gestore di password integrato per semplificare la gestione delle credenziali online.

Eventi di sicurezza familiari: Organizzeremo eventi o webinar sulla sicurezza informatica familiare per educare i genitori e i bambini su temi importanti come la protezione della privacy online

FOR BUSINESS

Sicurezza avanzata dei server: Protezione dedicata per server aziendali contro malware, virus e attacchi informatici sofisticati.

Protezione endpoint aziendale: Gestione centralizzata della sicurezza per tutti i dispositivi aziendali, inclusi desktop, laptop e dispositivi mobili.

Sicurezza del cloud e delle applicazioni: Protezione delle applicazioni aziendali e dei dati memorizzati nel cloud da accessi non autorizzati e attacchi.

Firewall avanzato: Firewall di livello aziendale per monitorare e controllare il traffico di rete in entrata e in uscita, migliorando la difesa contro intrusioni.

Protezione avanzata contro il ransomware: Misure specifiche per prevenire e rispondere agli attacchi di ransomware che mirano alle reti aziendali.

Formazione alla sicurezza per i dipendenti: Programmi di formazione regolari per i dipendenti su sicurezza informatica, phishing e migliori pratiche di sicurezza.

Audit di sicurezza e compliance: Servizi di audit per assicurare che l'infrastruttura IT aziendale sia conforme agli standard di sicurezza vigenti.

Supporto tecnico prioritario: Assistenza clienti prioritaria e supporto tecnico dedicato per rispondere rapidamente alle esigenze aziendali.

Analisi forense digitale: Servizi per investigare e analizzare violazioni di sicurezza o incidenti informatici.

Protezione dell'integrità dei dati: Soluzioni per garantire l'integrità e la non alterazione dei dati aziendali importanti.

Gestione delle vulnerabilità: Strumenti per rilevare e mitigare le vulnerabilità nella rete e nei software aziendali.

Assicurazione contro le frodi cyber: Polizze assicurative per mitigare le perdite finanziarie in caso di incidenti di sicurezza.

VPN aziendale: Rete privata virtuale dedicata per garantire connessioni sicure e criptate per i dipendenti, anche in remoto.

Controllo e monitoraggio dell'accesso: Soluzioni per gestire e monitorare gli accessi ai sistemi informativi aziendali, prevenendo l'accesso non autorizzato.

Sicurezza mobile enterprise: Protezione specifica per dispositivi mobili aziendali, inclusa la gestione dei dispositivi mobili e la protezione contro le minacce mobile.

Crittografia avanzata: Utilizzo di tecniche di crittografia avanzate per proteggere i dati aziendali sensibili durante la trasmissione e in archiviazione.

Protezione degli asset digitali: Soluzioni specifiche per la sicurezza di asset digitali critici come database di proprietà intellettuale e altri dati sensibili.

Gestione degli aggiornamenti di sicurezza: Automatizzazione della distribuzione degli aggiornamenti di sicurezza per software e sistemi operativi, garantendo che tutte le componenti siano aggiornate.

Backup e ripristino di emergenza: Implementazione di soluzioni robuste di backup e ripristino per garantire la continuità operativa in caso di disastri o incidenti.

Protezione della posta elettronica aziendale: Strumenti specifici per proteggere la comunicazione via email contro malware, spam e attacchi di phishing.

Controllo di conformità normativa: Supporto per assicurare che l'azienda rispetti le normative di settore relative alla protezione dei dati, come GDPR, HIPAA, etc.

Analisi del comportamento degli utenti: Monitoraggio e analisi del comportamento degli utenti per identificare azioni sospette che potrebbero indicare una violazione della sicurezza.

Isolamento di applicazioni: Tecnologie per eseguire applicazioni in ambienti isolati per prevenire la diffusione di malware nel caso una singola applicazione venga compromessa.

Accesso remoto sicuro: Implementazione di tecnologie come desktop virtuali e applicazioni remote per permettere un accesso sicuro alle risorse aziendali da remoto.

Gestione integrata delle minacce: Piattaforme che integrano la rilevazione di minacce, la prevenzione e la risposta per una gestione olistica delle minacce informatiche.

Segnalazione di incidenti di sicurezza: Strumenti per facilitare la segnalazione rapida e accurata di incidenti di sicurezza, migliorando la risposta agli incidenti.

Monitoraggio dell'infrastruttura critica: Soluzioni per il monitoraggio continuo dell'infrastruttura IT critica, come server di database e sistemi di rete.

Controllo accessi fisico: Integrazione di soluzioni di controllo degli accessi fisici per proteggere gli ambienti IT critici.

AD HOC FOR BUSINESS

È un Piano For Business creato appositamente per l'azienda richiedente, include tutte le caratteristiche del piano standard a cui si possono aggiungere strumenti, servizi e modalità. Il prezzo va definito dopo un'attenta consulenza con il cliente, in base alle richieste, al budget ed al numero di dipendenti

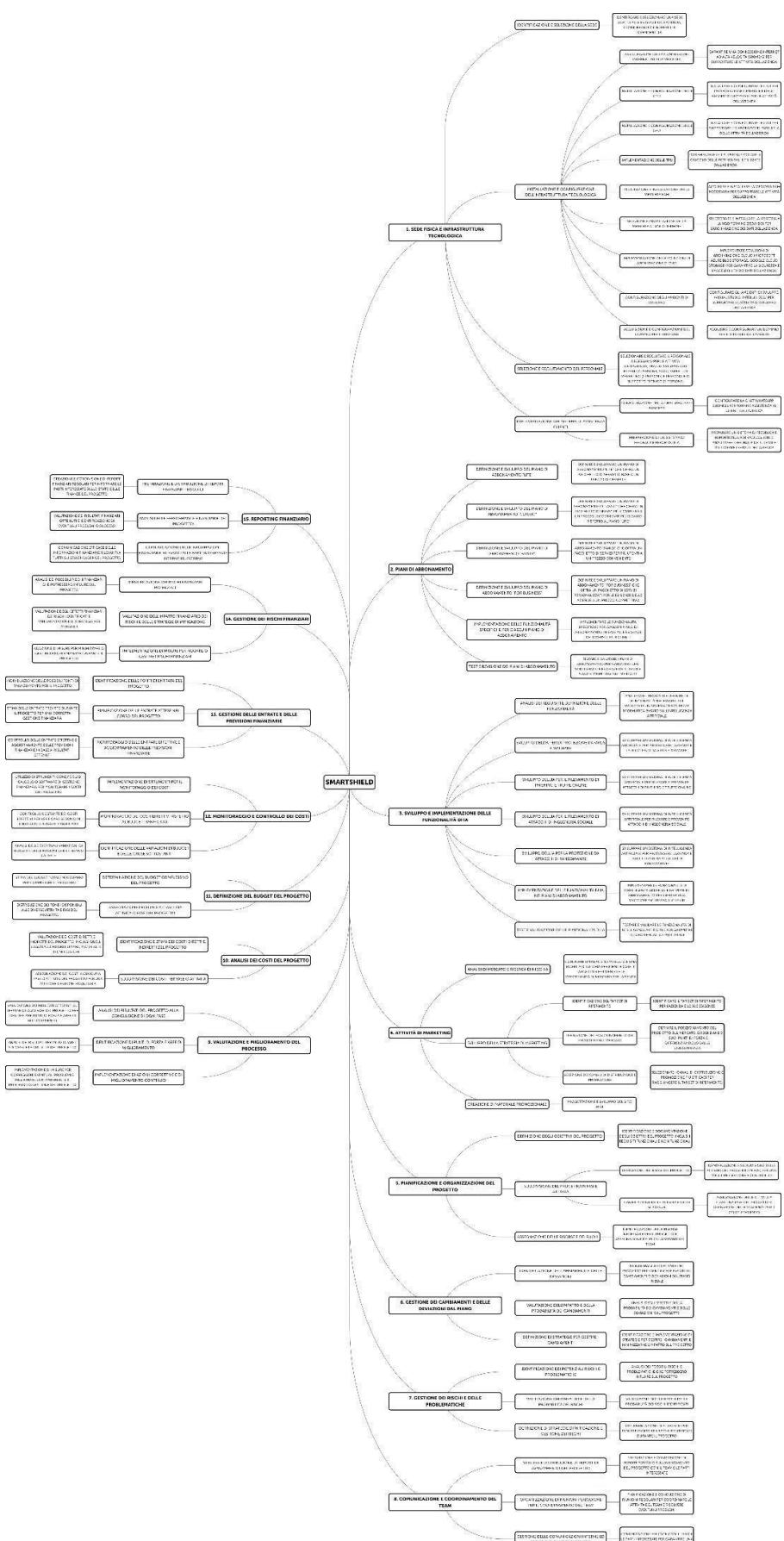
L'obiettivo degli sviluppatori sarebbe quello di riuscire a stringere patti con l'Enisa, l'Agenzia della cybersicurezza europea e il governo italiano per rendere gratuita l'ia e l'app a tutti gli utenti over 65 e i bambini under 15 che utilizzano dispositivi elettronici connessi ad internet, il sogno sarebbe quello di diminuire del 97% le frodi informatiche alle categorie indifese come anziani e bambini, e del 50% ai privati entro il 2045.

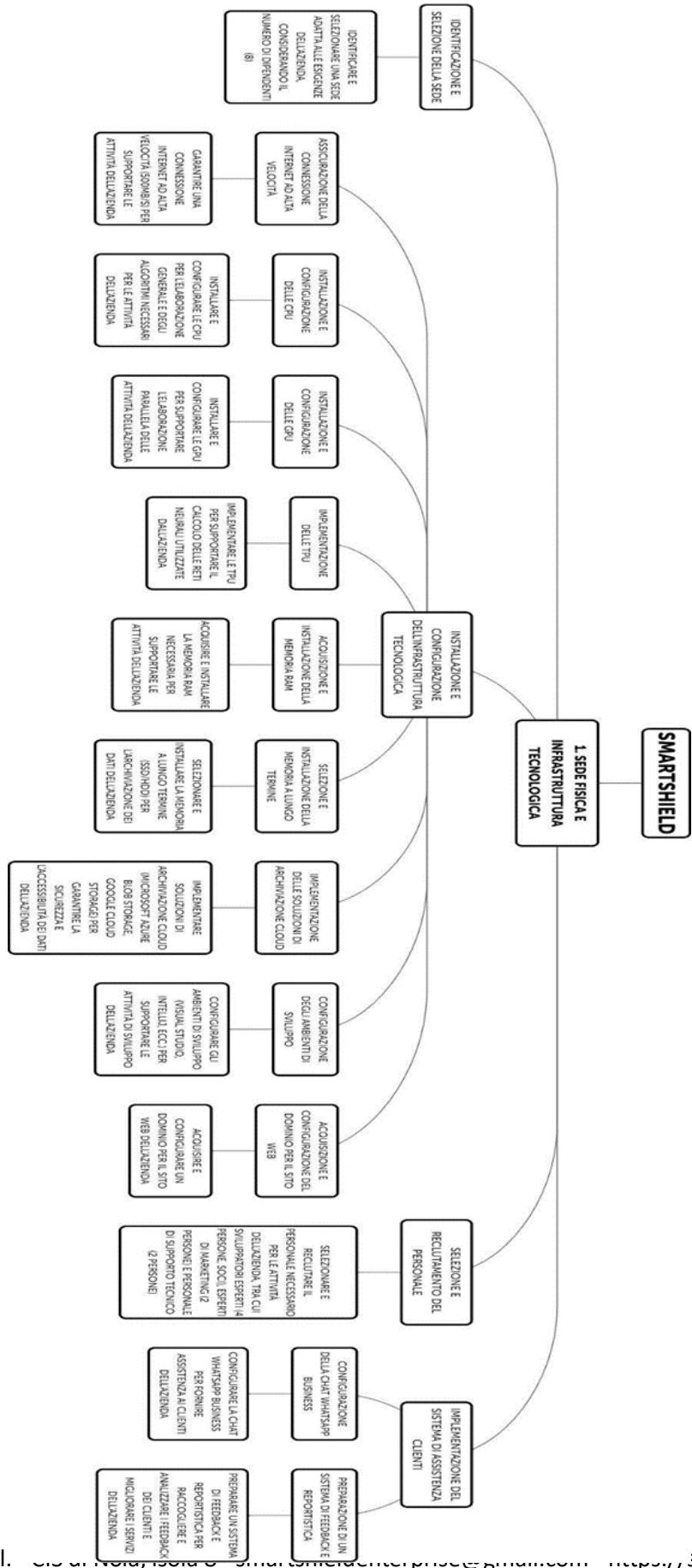
WBS

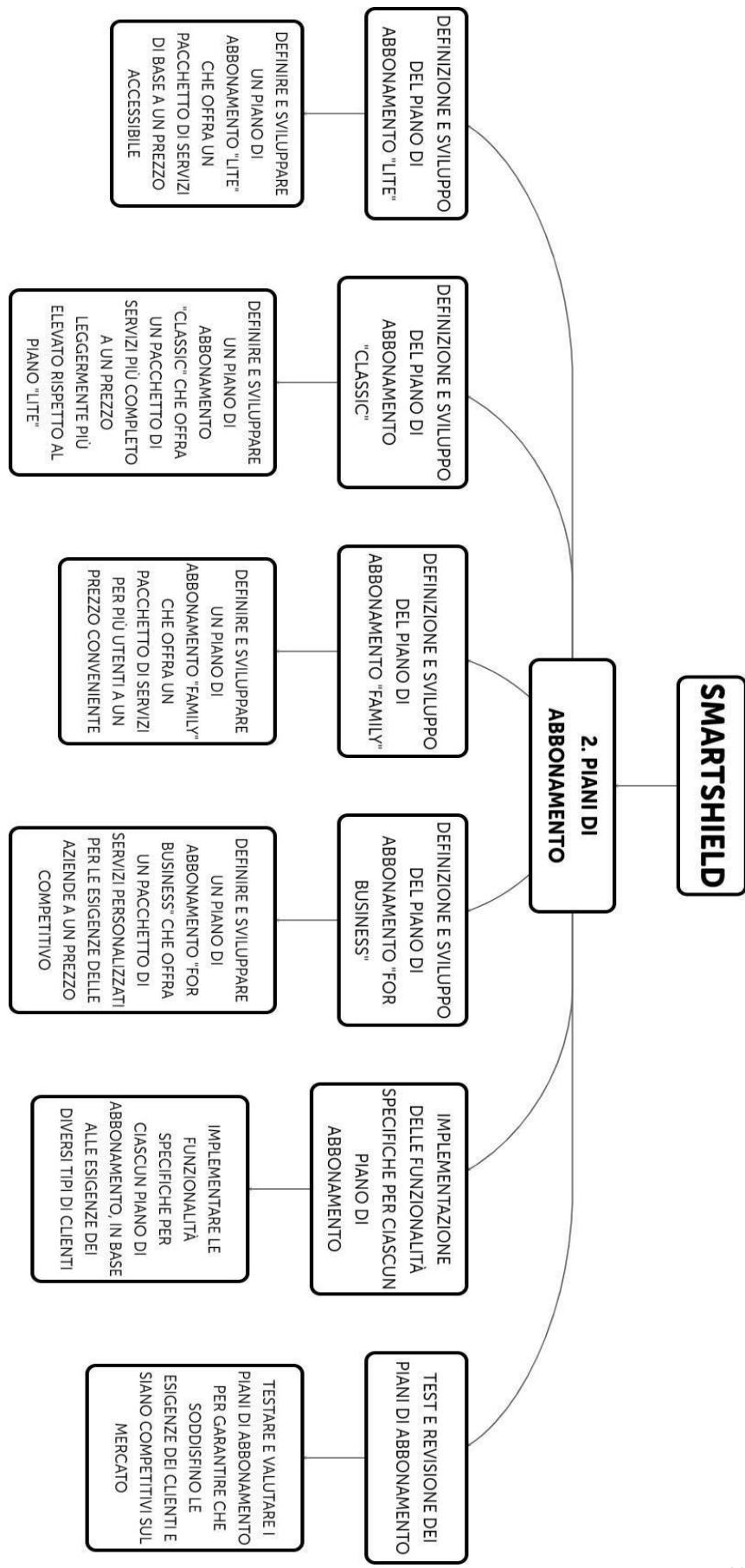
Al fine di una corretta comprensione del nostro piano operativo è qui illustrata la nostra WBS, anche definita come “scomposizione strutturata del progetto”.

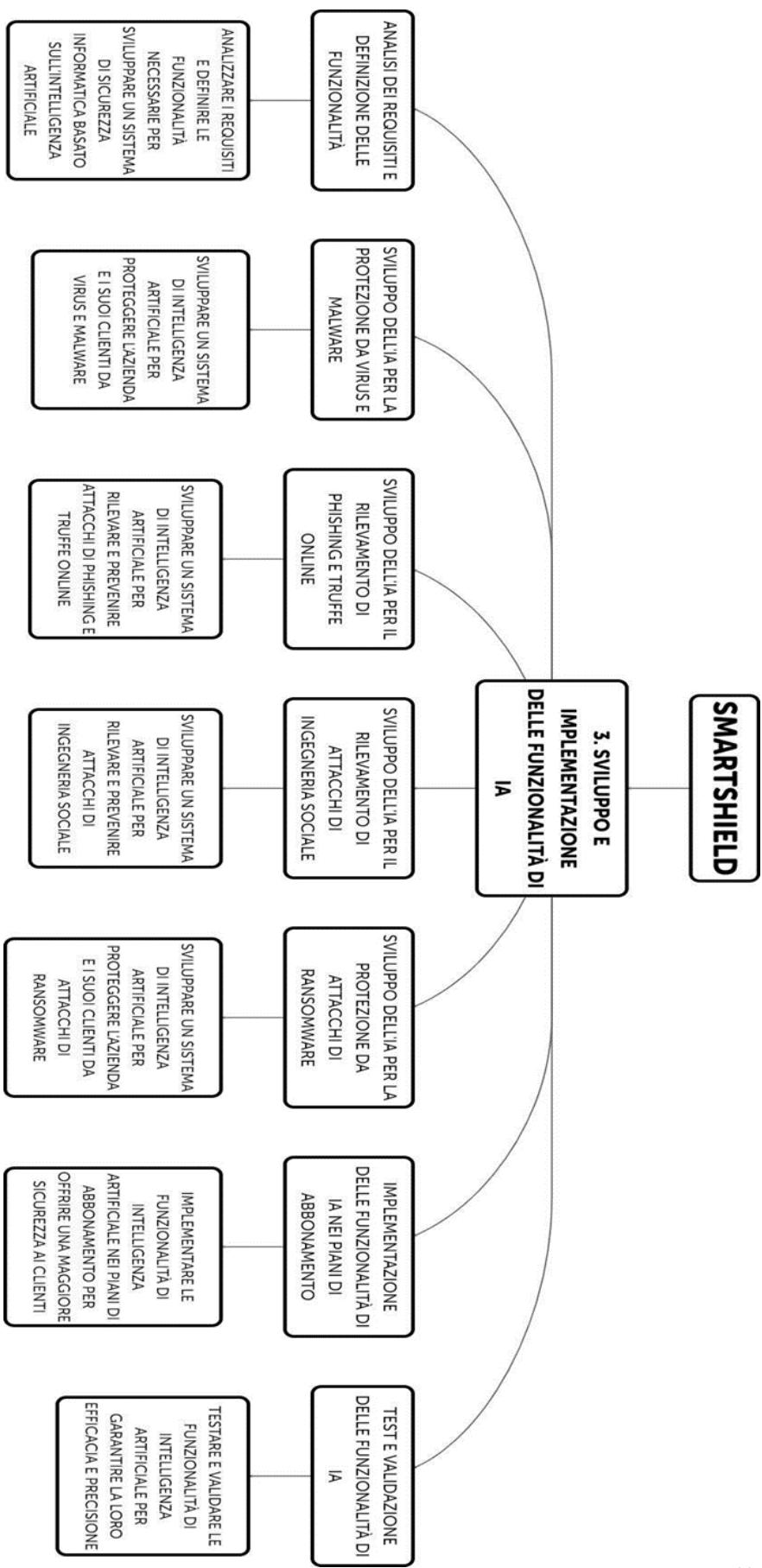
La WBS è una rappresentazione gerarchica e strutturata di un progetto. Essenzialmente, divide il lavoro necessario per completare un progetto in compiti più piccoli e gestibili. Grazie alla sua scomposizione analitica del progetto aiuta a organizzare e visualizzare tutte le attività necessarie per raggiungere gli obiettivi del progetto in modo chiaro e dettagliato.

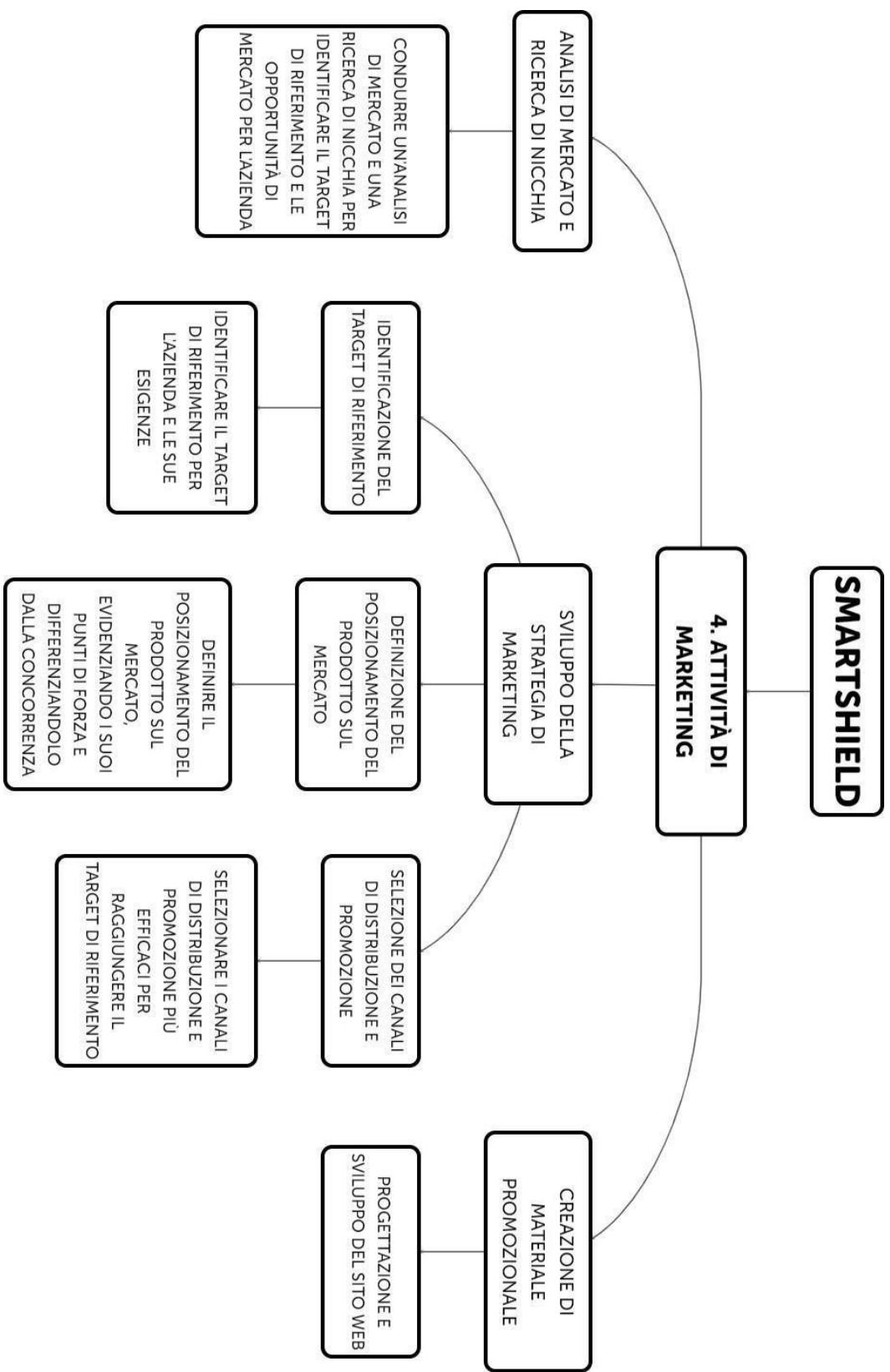
La nostra WBS è la seguente, essendo un progetto vasto e altamente tecnologico, tutte le mappe sono studiate ad hoc per una consultazione digitale; pertanto, alcune mappe nella seguente versione cartacea saranno presentate prima in formato unico (poco leggibile per l'occhio umano), poi scomposte in sezioni, per una facile consultazione della copia fisica.

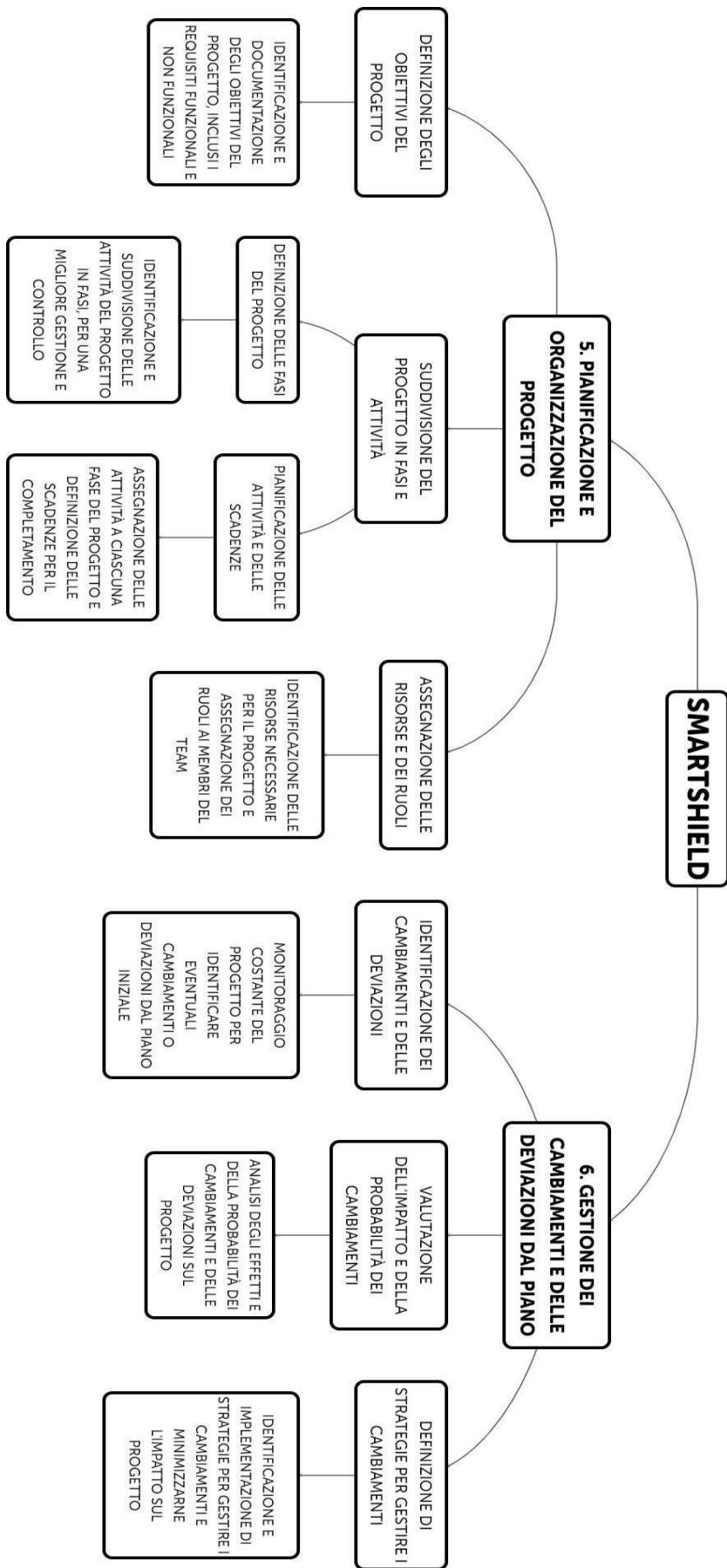


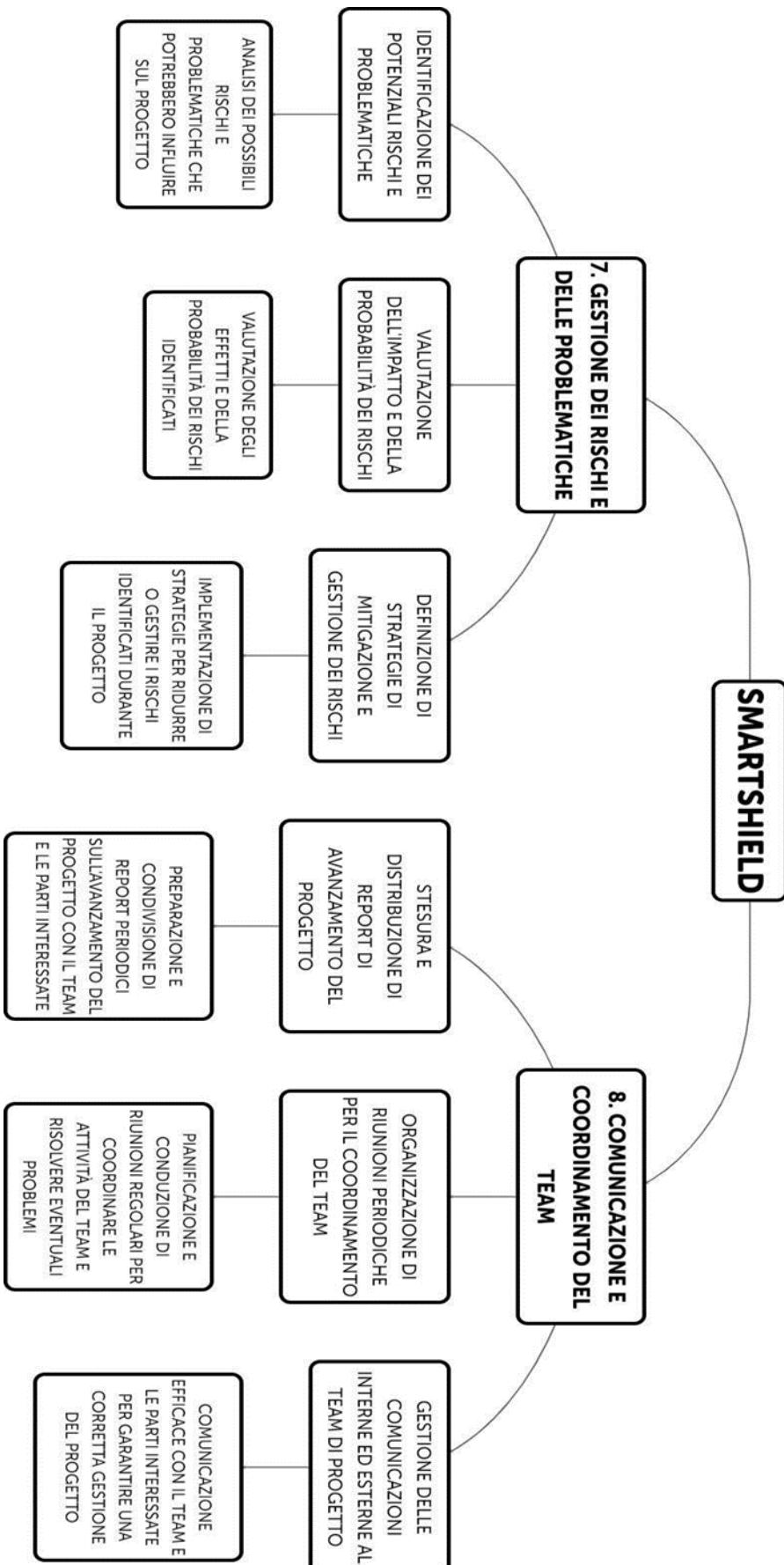


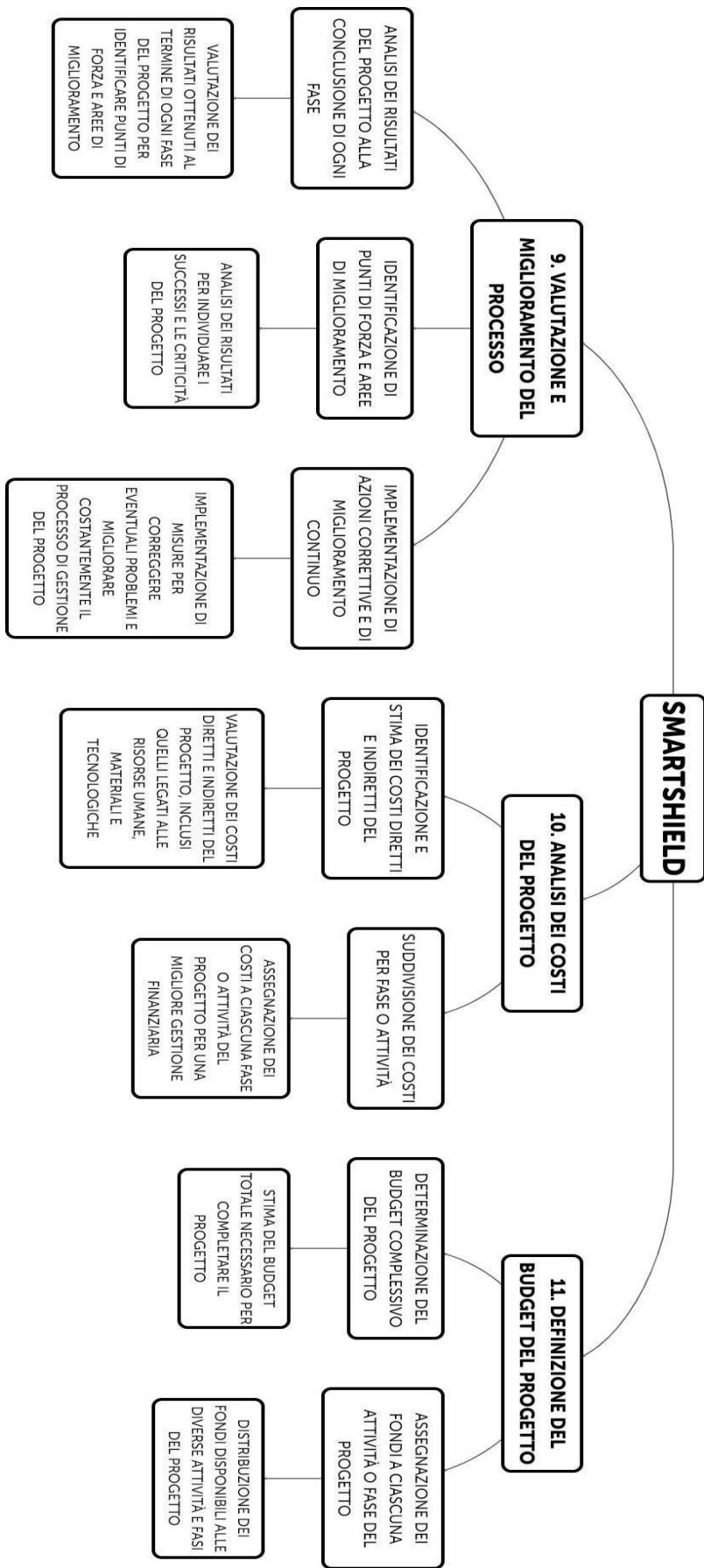


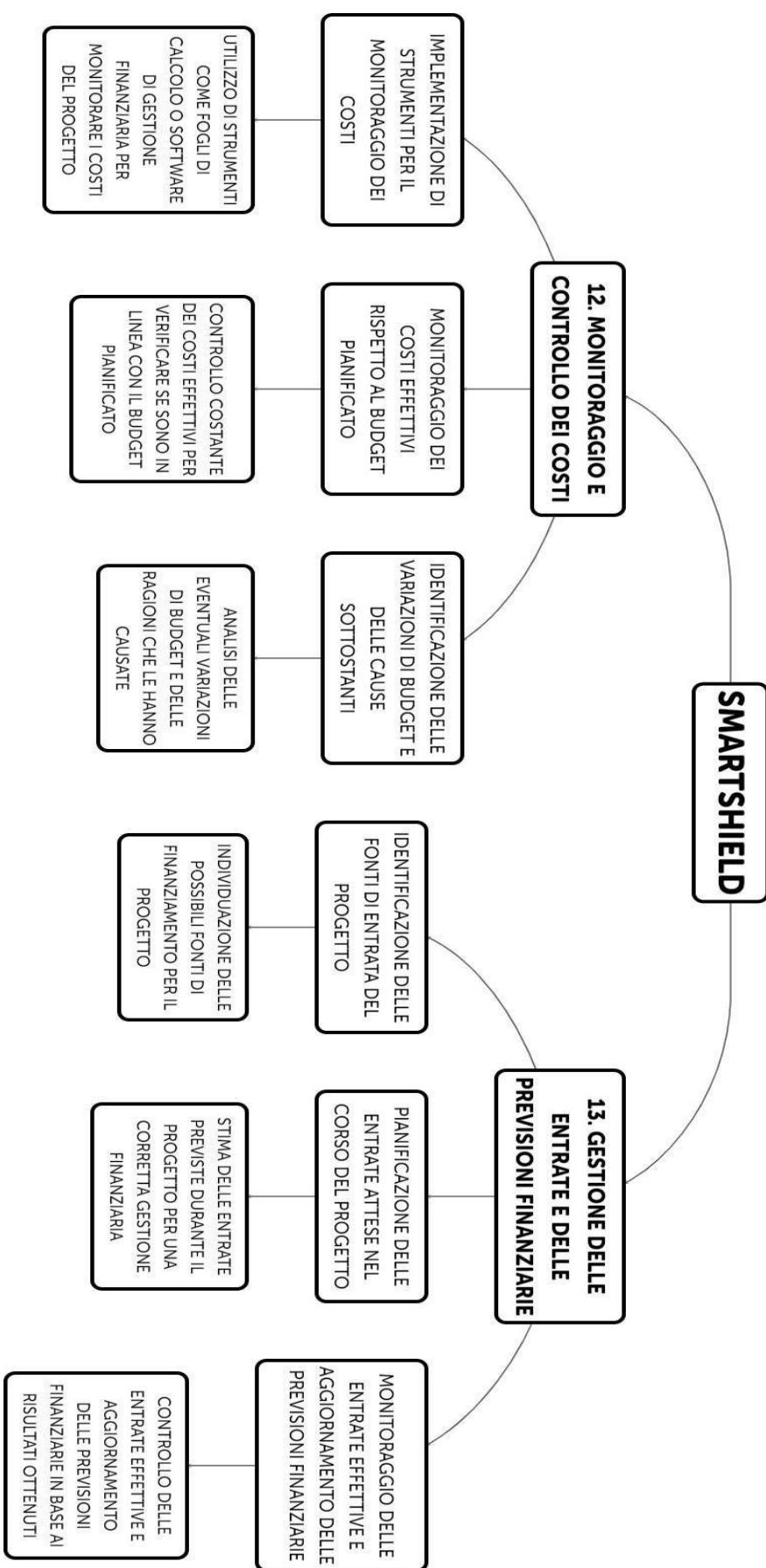


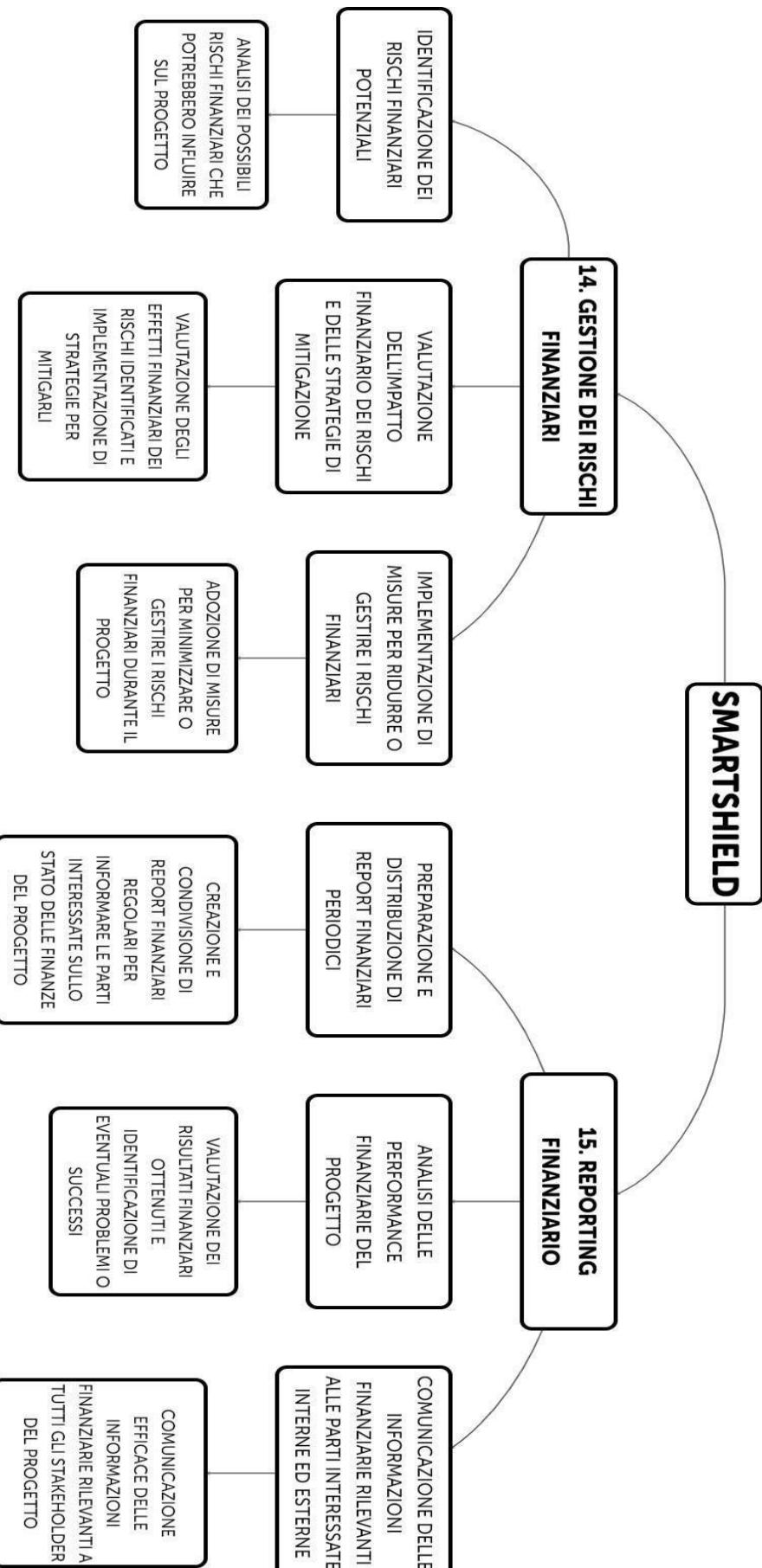










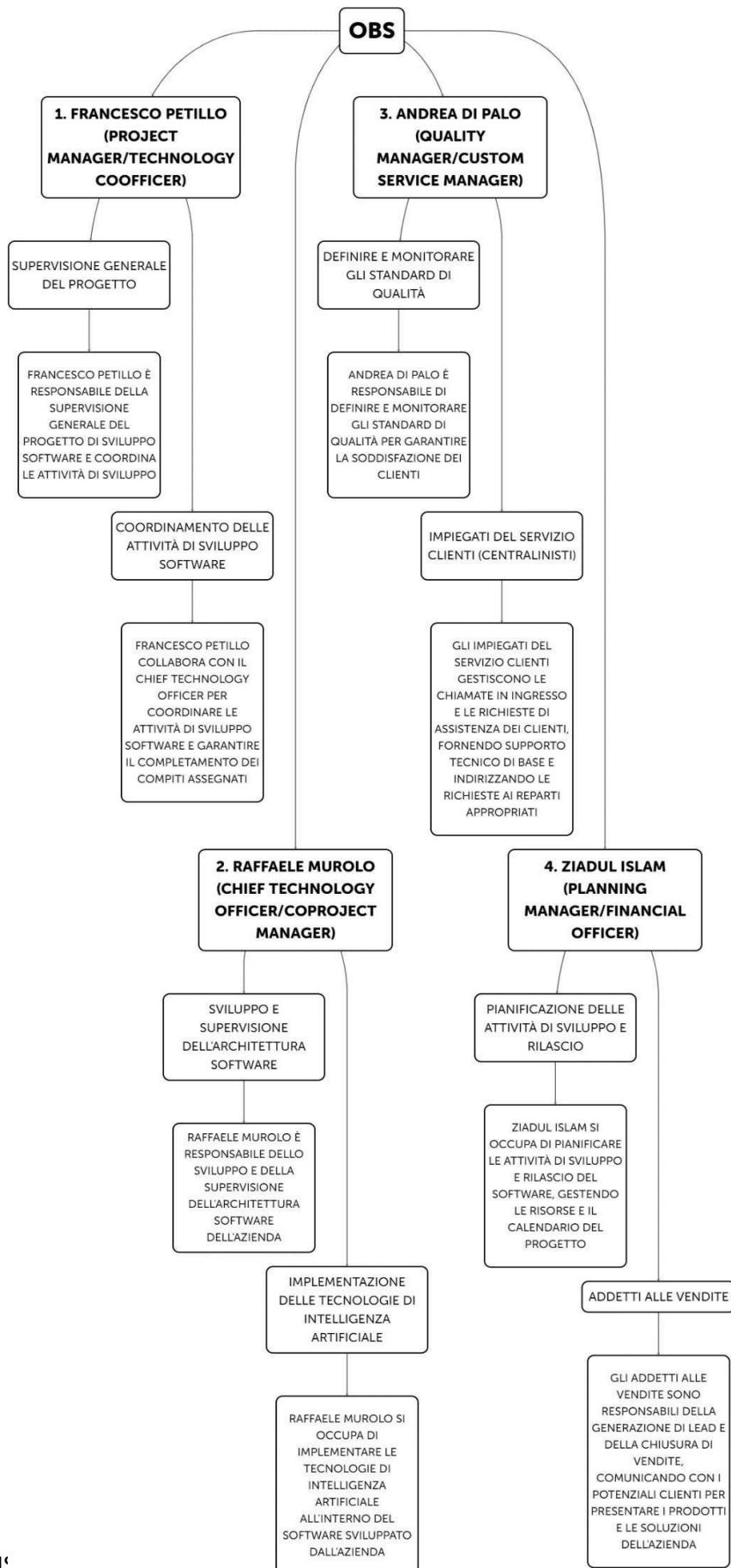


OBS

Una volta delineata la WBS, che ha scomposto le attività principali in sottoattività più gestibili e monitorabili, è necessario allocare le risorse umane della startup all'interno dell'organizzazione. In questo contesto, entriamo nella sfera **dell'Organization Breakdown Structure (OBS)**, che ci offre una visione dettagliata della struttura gerarchica dell'organizzazione coinvolta nel progetto.

Grazie a tale rappresentazione godiamo di un facile monitoraggio del progetto da parte dei project managers, oltre che del miglioramento delle prestazioni organizzative.

La mappa presenta pari privilegi tra i quattro soci fondatori, che gerarchicamente fanno capo agli impiegati, come gli addetti alle vendite, nella speranza di un organico sempre crescente in futuro.



Una volta definiti i ruoli all'interno dell'azienda di tutto l'organico, dai soci agli impiegati, è necessario stabilire quelle che sono le responsabilità in base ai ruoli prima definiti.

Per fare ciò utilizziamo una matrice **RACI**, ovvero uno strumento di gestione dei progetti utilizzato per assegnare e mostrare le responsabilità delle persone coinvolte in un compito o un processo all'interno di un'organizzazione.

Legenda delle responsabilità:

- **Responsible (R):** Chi esegue l'attività.
- **Accountable (A):** Chi è responsabile del completamento dell'attività e dell'approvazione finale.
- **Consulted (C):** Persone che forniscono informazioni, note e feedback durante il processo.
- **Informed (I):** Persone che devono essere informate del progresso o delle decisioni, ma a solo scopo informativo, non avendo un ruolo attivo nel compito.

Attività/ Role	Francesco Petillo	Raffaele Murolo	Andrea Di Palo	Ziadul Islam	Sviluppatori Software (da utilizzare in futuro)	Impiegati servizio Clienti	Addetti alle Vendite
Supervisione generale del progetto	A/R	C	C	C			
Coordinamento dello sviluppo software	R	C	I	I	R		
Progettazione software	A/R	C	I	I	R		
Sviluppo software	A	C	I	I	R		
Testing software	A	C			R		
Supervisione architettura software	C	A/R					
Implementazione intelligenza artificiale	C	R			R		
Definizione standard di qualità	C		A/R	C			
Monitoraggio standard di qualità			A/R				
Gestione chiamate di assistenza			C			R	
Supporto tecnico di base			C			R	
Pianificazione sviluppo e rilascio	C	C	C	A/R			
Gestione risorse e calendario	C	C	C	A/R			
Generazione lead				C			R
Chiusura vendite	I	I	I	C			R
Comunicazione con potenziali clienti				C			R

FLOWCHART

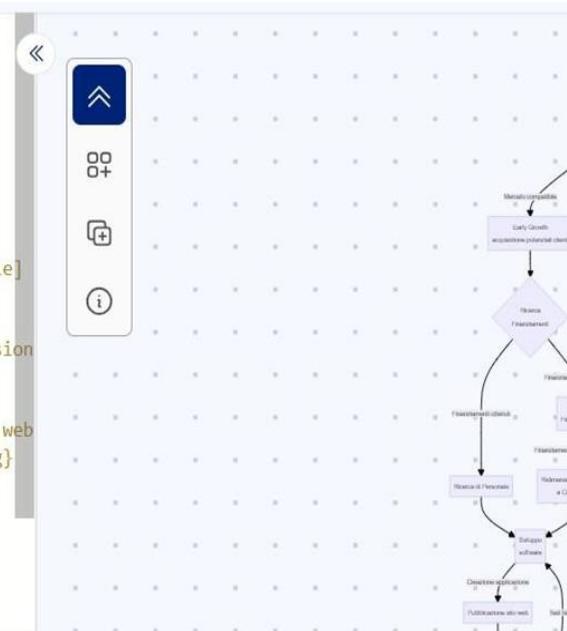
Delineati obiettivi e capitale umano dell'azienda andremo a schematizzare il percorso che la startup dovrà affrontare per passare dall'essere una semplice idea ad una azienda reale.

Per fare ciò andremo ad avvalerci di un Flowchart, ovvero una rappresentazione visuale del processo. Nel materiale aziendale è consultabile il codice con cui è stato scritto per modificarlo o visualizzarlo su <https://mermaid.js.org/>, di seguito è riportato uno screenshot del codice utilizzato per costruirlo.

```

1 flowchart TD
2 A([Inizio]) --> B{EARLY STAGE}
3 feedback del mercato
4 B -->|Mercato compatibile| C[Early Growth  
acquisizione potenziali clienti]
5 B -->|Mercato non compatibile| D[SEED  
affinamento business da business model]
6 C --> E{Ricerca  
Finanziamenti}
7 E -->|Finanziamenti ottenuti| F[Ricerca di Personale]
8 E -->|Finanziamenti non ottenuti| G[Ricerca  
Finanziamenti]
9 G -->|Finanziamenti ancora non ottenuti| H[Ridimensionamento]
10 F --> I[Sviluppo \n software]
11 H --> I
12 I -->|Creazione applicazione| J[Pubblicazione sito web]
13 J -->|Creazione intelligenza artificiale| K[Testing]
14 K -->|Test superato| L[Rilascio Prodotti]
15 K -->|Test fallito| I
16 L --> M[Attività Post-Commerciale]
17 M --> N([Fine])
18 D --> B
23

```

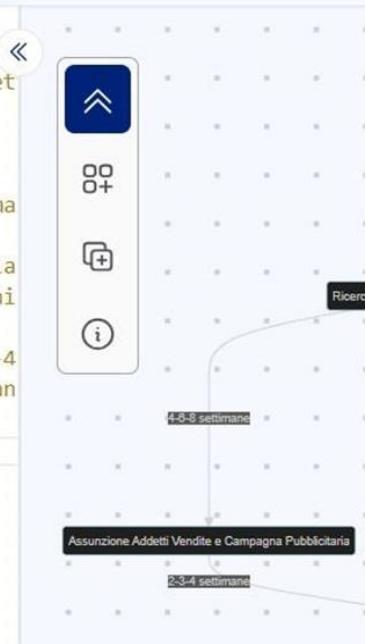


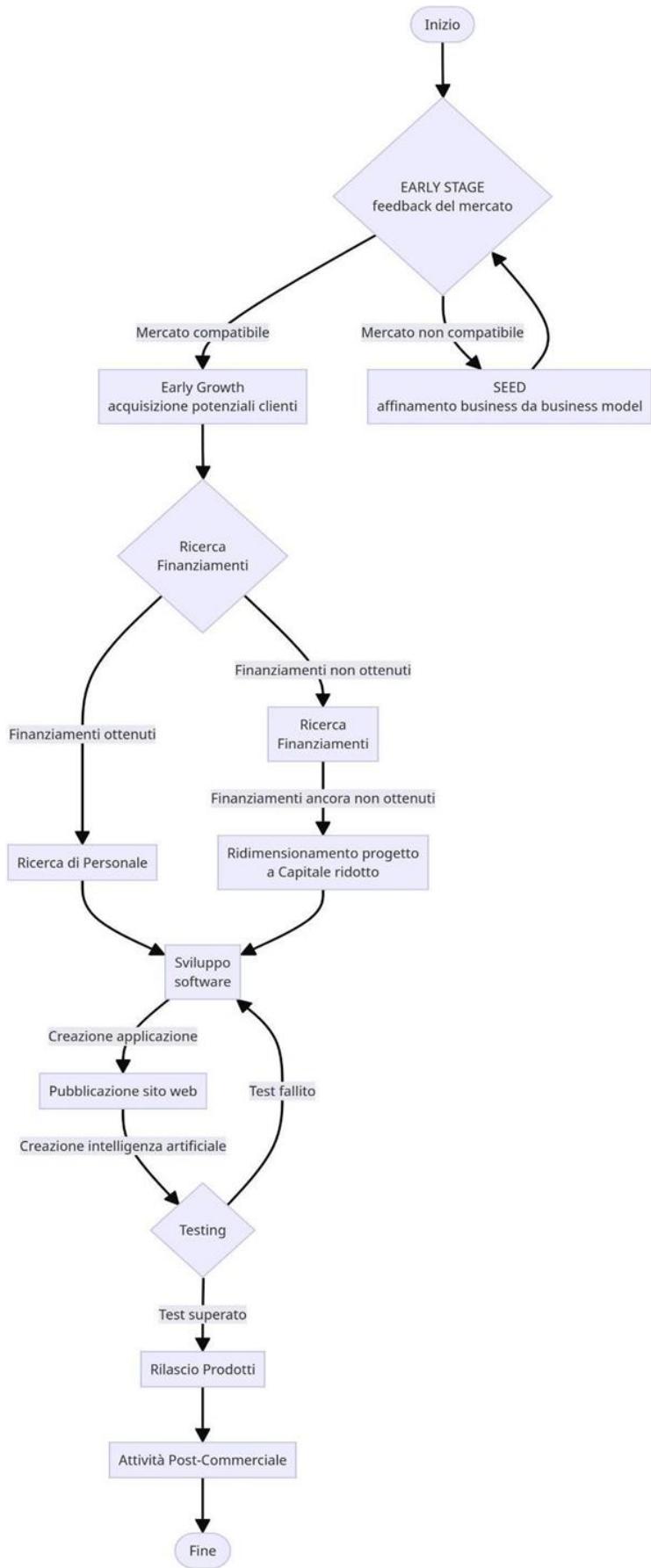
Similmente sarà utilizzato un codice per il diagramma Pert, visualizzabile sulla stessa piattaforma

```

1 graph TD
2 A2(Pianificazione e Ricerca di Risorse) -->|2-5-8 settimane| A1(Ricerca di Mercato)
3 A3(Ricerca e Assunzione di Sviluppatori) -->|4-6-8 settimane| A4(Aggiornamento del Sito Web)
4 A1 -->|3-6-9 settimane| A4
5 A2 -->|6-8-10 settimane| A6
6 A3 --> A6
7 A6(Creazione di Software, App e IA) -->|6-8-10 settimana| A7(Testing e Training)
8 A7 -->|3-5-7 settimane| A8
9 A5(Assunzione Addetti Vendite e Campagna Pubblicitaria)
10 A4 -->|2 giorni - 3 giorni| A7
11 A7 -->|3-5-7 settimane| A10
12 A8(Assunzione del Personale del Call Center) -->|2-3-4 settimane| A9
13 A9(Messa in Commercio dei Prodotti) -->|3-5-7 settimane| A10
14 A10(Miglioramento e Manutenzione della Piattaforma)
15

```





Arrivati alla fine del flowchart la startup sarà effettivamente nata; pertanto, vanno **individuati i processi da eseguire** ovvero:

Ricerca di mercato nel settore già delineato:

- Conduciamo un'analisi approfondita del settore della sicurezza informatica per identificare trend, opportunità e concorrenti.
- Raccogliamo dati demografici e comportamentali per comprendere meglio il nostro target di mercato e le loro esigenze.

Pianificazione e Ricerca di Risorse:

- Pianifichiamo attentamente le attività e le risorse necessarie per avviare e gestire la nostra startup nel settore della sicurezza informatica una volta inseriti sul mercato.
- Esploriamo i possibili incentivi governativi come il Bonus Giovani, cercando di tenere il Capitale Sociale come garanzia e non per finanziare le nostre attività iniziali.

Formazione del personale

- Provvediamo alla formazione degli addetti al centralino in modo da renderli quasi totalmente autonomi per la maggior parte delle problematiche rilevate, nel caso ci fossero problemi faranno capo al loro responsabile.
- Volendo ipotizzare poi tra diversi anni un ampliamento dell'organico, ci sarà la formazione dei nuovi sviluppatori assunti oltre a i 4 soci, informandoli sulla mission aziendale, sui processi produttivi e fornendoli degli strumenti necessari, dal software abbozzato nel flowchart, creato dai soli soci, si passa ad una versione definitiva.

Aggiornamento del Sito Web:

- Aggiorniamo regolarmente il nostro sito web con informazioni sui nostri prodotti in sviluppo e le date di uscita.
- Creiamo contenuti e materiali promozionali coinvolgenti per generare interesse tra potenziali clienti e partner commerciali.

Continuo contatto con gli Addetti Vendite

- Consultazione continua con gli addetti vendita per rendersi conto delle vendite e della campagna pubblicitaria.

Creazione definitiva del Software, App e Intelligenza Artificiale:

- Sviluppiamo software di sicurezza informatica innovativi, inclusi app e funzionalità di intelligenza artificiale, in collaborazione con esperti del settore.
- Garantiamo un rigoroso processo di testing e training per assicurare la qualità e l'efficacia dei nostri prodotti prima del lancio sul mercato.

Messa in Commercio dei Prodotti:

- Lanciamo i nostri prodotti sul mercato utilizzando piattaforme di vendita online e offline, nei casi di grandi enti provvederemo all'attività di rappresentanza fisica, fatta in maniera saltuaria da uno degli esperti di vendita.

Monitoraggio

- Monitoriamo costantemente le performance e il feedback dei clienti per apportare miglioramenti continui ai nostri prodotti e servizi.
- servizi.**

Miglioramento e Manutenzione della Piattaforma:

- Aggiorniamo regolarmente il nostro software e le funzionalità in base ai feedback degli utenti e alle nuove minacce informatiche.

Servizi post-vendita:

- Offriamo servizi post-vendita, come aggiornamenti di sicurezza e assistenza tecnica continua, per garantire la soddisfazione e la fidelizzazione dei clienti.

Sviluppo dei Partner e delle Collaborazioni:

- Identifichiamo potenziali partner strategici nel settore della sicurezza informatica per ampliare la portata e la distribuzione dei nostri prodotti.
- Negoziamo accordi di collaborazione che ci consentano di sfruttare al meglio le competenze e le risorse dei nostri partner per il beneficio reciproco e dei nostri clienti.

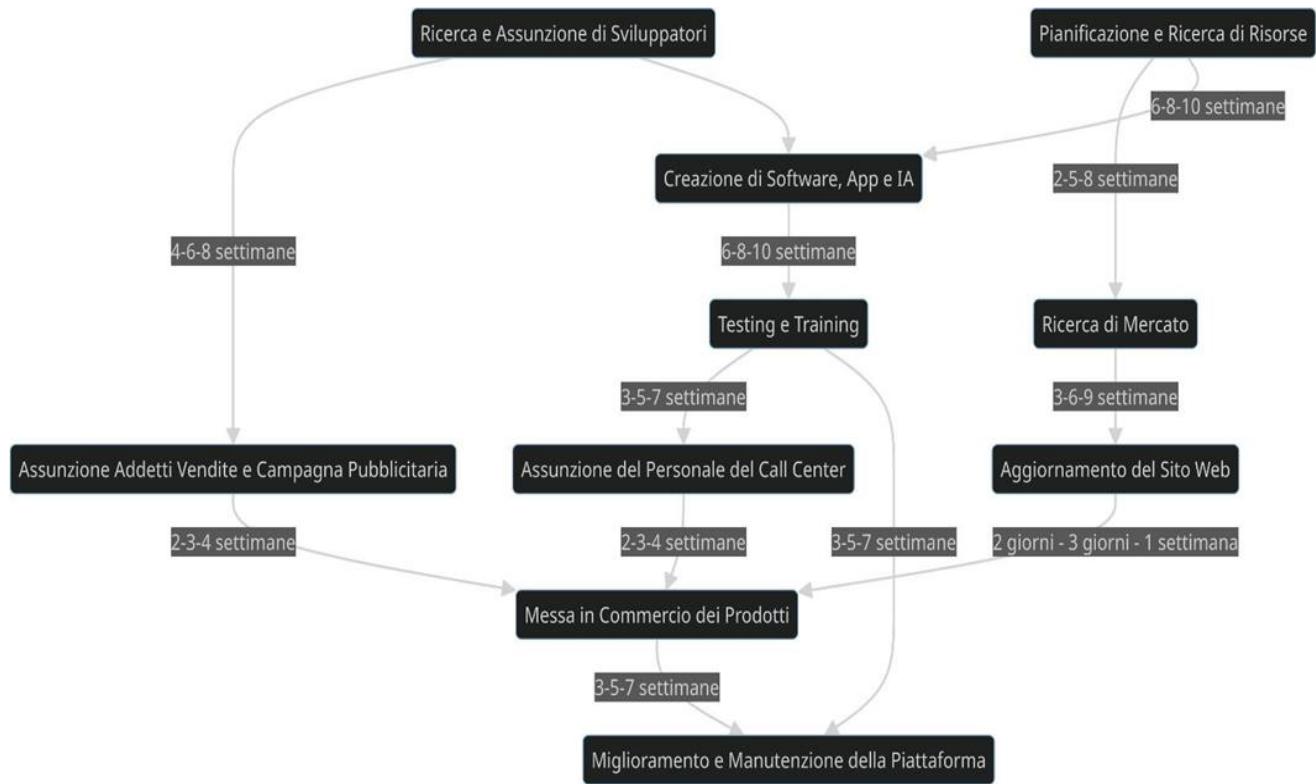
PERT

Tutte le fasi, dall'ideazione della startup, alla definitiva commercializzazione del prodotto, necessiteranno di tempistiche differenti e talvolta di un ordine preciso di svolgimento.

Ci avvaliamo pertanto del diagramma **PERT** ovvero **Project Evaluation Review Technique** che ci permette di schematizzare la programmazione delle attività, inserendone previsioni ottimistiche, probabili e pessimistiche. Le previsioni sono date in parte da un'attenta analisi online dei tempi richiesti mediamente per le varie fasi, in parte (primariamente) dalla diretta esperienza dei soci riguardanti testing, sviluppo ecc... oppure dalla creazione del sito web che è stato creato dallo stesso autore del diagramma Pert.

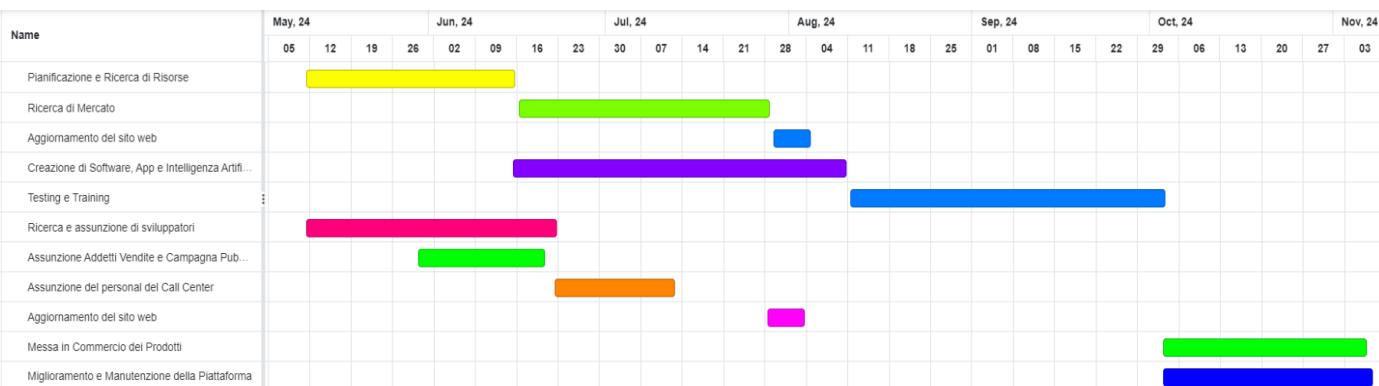
Le date sulle frecce sono scritte in 3 unità, ottimistiche, probabili, pessimistiche, la lettura è da sinistra verso destra.

Di seguito il diagramma Pert:



GANT

Proseguiamo con l'organizzazione temporale del progetto da inizio opera, considerando una media realistica-ottimistica e l'organico di 4 esperti software, tra soci e sviluppatori, occorrerebbero circa 7/8 mesi per mettere in piedi una startup. Le attività sono messe in ordine cronologico, consultando il file Gant.json allegato digitalmente è poi possibile visualizzare meglio le dipendenze tra le attività tramite le opzioni del grafico.



TUTORIAL CLIENTI

Presso la nostra azienda, ci impegniamo a fornire soluzioni di sicurezza informatica su misura per soddisfare le diverse esigenze dei nostri clienti, che comprendono privati, imprese e piccole aziende. Riconosciamo che ogni cliente ha necessità uniche e un budget specifico; pertanto, offriamo una gamma di pacchetti personalizzati tra cui scegliere. I nostri pacchetti standard sono progettati per offrire una protezione completa a prezzi accessibili, consentendo a privati e piccole aziende di godere di una sicurezza informatica di alta qualità senza compromettere la loro redditività.

Per le aziende che richiedono una protezione informatica più specializzata e specifica, offriamo anche un pacchetto ad hoc. Questo pacchetto è stato appositamente progettato per soddisfare le esigenze uniche delle aziende, offrendo una gamma di funzionalità personalizzate e un supporto dedicato.

Sebbene la maggior parte delle nostre transazioni avvenga online attraverso il nostro sito web, comprendiamo l'importanza di un approccio personalizzato per alcune aziende. I nostri addetti alle vendite sono disponibili per fornire consulenza e assistenza diretta, aiutando le aziende a identificare le soluzioni più adatte alle loro esigenze specifiche.

Il sito web è progettato per offrire una panoramica completa della nostra azienda e dei nostri prodotti. La sezione "Chi Siamo" fornisce informazioni dettagliate sulla nostra storia, la nostra missione e il nostro team, mentre la sezione "Prodotti" presenta in dettaglio le nostre soluzioni di sicurezza informatica. La sezione "Assistenza" è dedicata a fornire supporto e risposte alle domande frequenti dei clienti, garantendo un'esperienza utente completa e soddisfacente.

In conclusione, siamo qui per garantire che ogni cliente, indipendentemente dalle proprie esigenze, riceva il livello di protezione e assistenza di cui ha bisogno per navigare in modo sicuro nel mondo digitale in continua evoluzione. Siamo impegnati a creare relazioni durature con i nostri clienti, offrendo soluzioni innovative e un servizio clientieccenzionale.

HOME DEL SITO



AREA ASSISTENZA CLIENTI

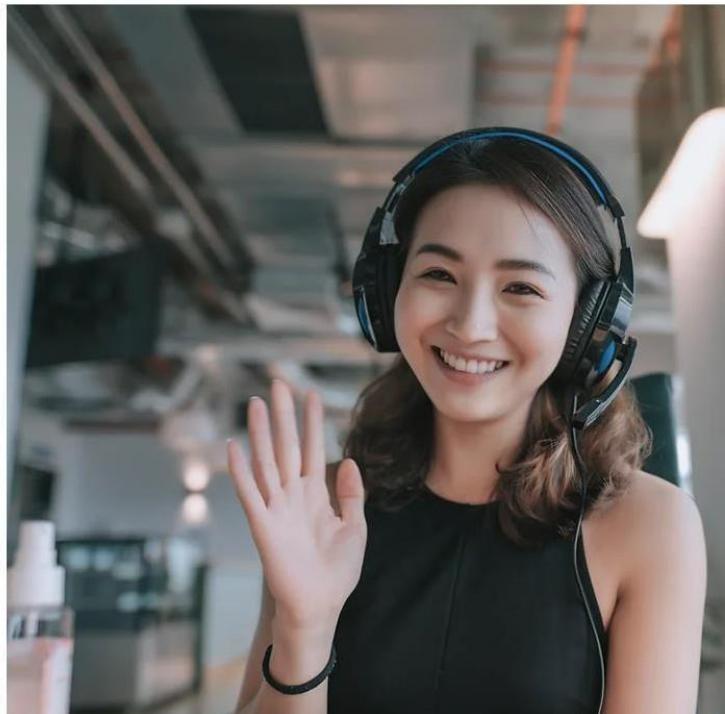
Selezionando la voce “Assistenza” dal menù si va nella pagina dedicata, qui è possibile chattare direttamente con gli addetti del call center, la chat è utilizzabile sia ai clienti per qualsiasi informazione o aiuto, che riguardino sia l'utilizzo del software che le minacce, altrettanto è fruibile ai non clienti desiderosi di info riguardo il software, le capacità e l'intelligenza artificiale.

The screenshot shows the SmartShield website's "Assistenza" (Assistance) page. At the top, there is a navigation bar with links for "Assistenza", "Chi siamo" (with a shopping cart icon showing '4'), "PRODOTTI", and "Iscriviti". The main headline reads "WE TAKE CARE OF YOUR FAMILY". Below the headline, a text block states: "Il nostro call center è attivo h24, 7 giorni su 7, nel momento in cui lo scanner dell'IA rileverà malware, virus, soggetti con intenzioni malevole o qualsiasi minaccia specificata nei dettagli del nostro pacchetto di protezione digitale, sarà loro cura mettersi in contatto tempestivamente con te." A smaller text below says: "Hai dubbi? Scrivi qui sotto, ti rispondiamo in tempo reale." The background features a dark, abstract graphic of glowing blue dots.

ASSISTENZA H24

La tua sicurezza è la nostra priorità. Con il nostro servizio di supporto H24, saremo al tuo fianco in ogni momento, pronti a contattarti al primo segnale di minaccia sui dispositivi dei tuoi cari o dei tuoi dipendenti. La tranquillità non ha orario: siamo qui per te 24 ore su 24.

[Leggi altro](#) →





MASSIMA SENSIBILITÀ

Incontra Daisy, la nostra intelligenza artificiale all'avanguardia progettata per rilevare e contrastare le minacce informatiche in tempo reale. Daisy è molto più di un semplice antivirus; è il guardiano digitale che protegge costantemente voi e il vostro mondo digitale.

Dotata di capacità avanzate di apprendimento automatico e analisi comportamentale, Daisy è in grado di identificare e neutralizzare le minacce prima che possano causare danni. Analizza costantemente il traffico web, le email, i file e altro ancora, individuando pattern e comportamenti sospetti per prevenire attacchi prima che possano infiltrarsi nei vostri sistemi.

Ma Daisy non si ferma qui. Grazie alla sua capacità di adattarsi e apprendere dalle esperienze passate, diventa sempre più efficace nel proteggervi dalle minacce più sofisticate e in continua evoluzione. Ogni nuova minaccia rilevata è un'opportunità per

INFORMAZIONI IN DIRETTA

Educare e proteggere i tuoi figli online non ha mai sonno: con le notifiche integrate, siamo presenti anche quando dormi, per garantire la loro sicurezza digitale 24/7.

[Leggi altro](#)



VISION

SmartShield apre la strada per un futuro in cui non esisteranno più minacce web

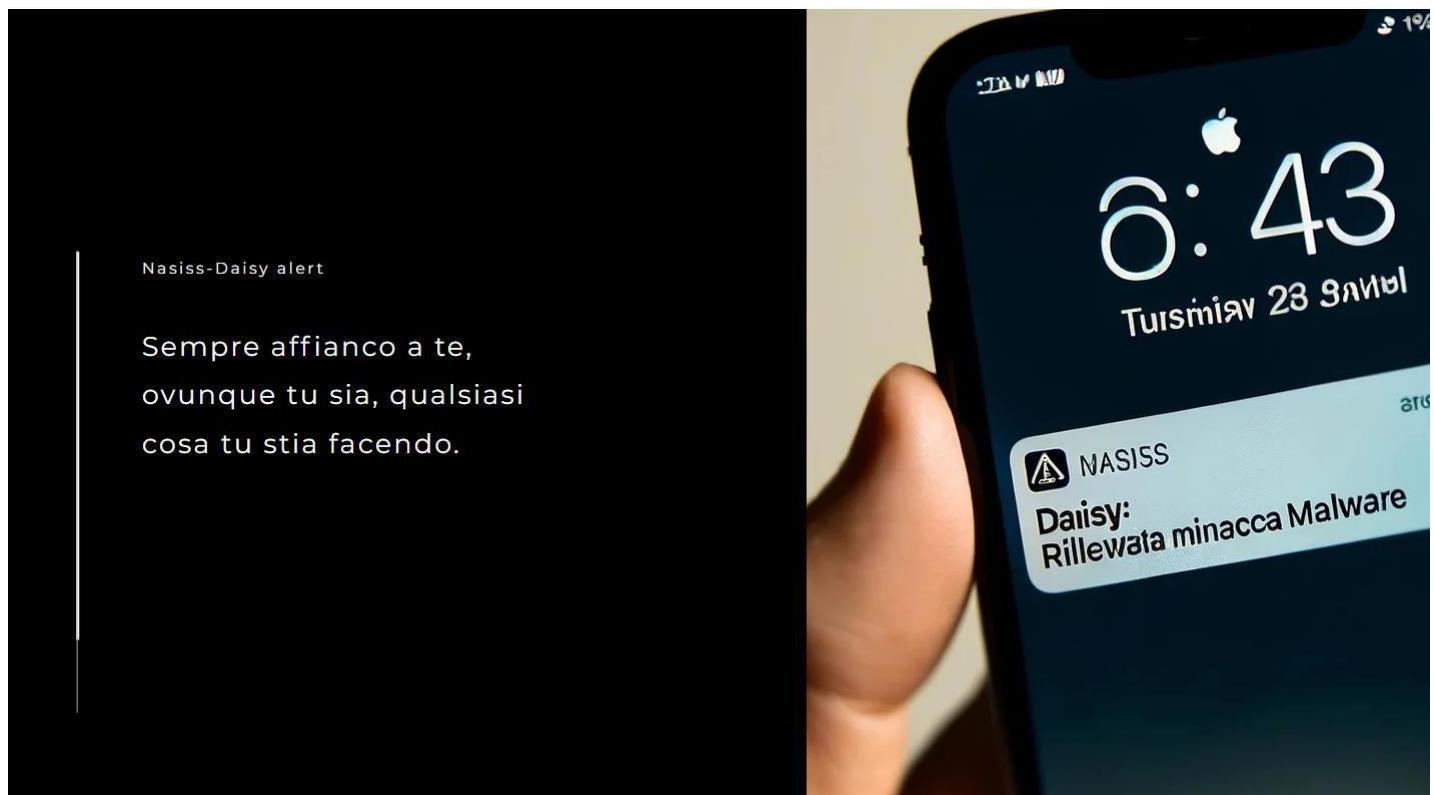


LA NOSTRA MISSION

Ridefinire il concetto di sicurezza

La nostra visione è audace: immaginiamo un futuro in cui le minacce informatiche non siano più una costante preoccupazione, ma un ricordo lontano. Con questo obiettivo in mente, abbiamo sviluppato Smart Shield, un antivirus all'avanguardia con intelligenza artificiale integrata.

Siamo consapevoli che la sicurezza informatica è un diritto fondamentale, non un privilegio. È per questo che ci impegniamo a rendere Smart Shield accessibile a tutti, senza compromettere mai la qualità o l'efficacia della nostra protezione.



Il nostro viaggio

2024

NASCE SMARTSHIELD

Francesco Petillo, Raffaele Murolo, Ziadul Islam e Andrea Di Palo danno vita alla loro startup, posando il primo mattone per il software antivirus.

2025

PRIMO UTILIZZO DI DAISY

PERCHÉ AUTONO

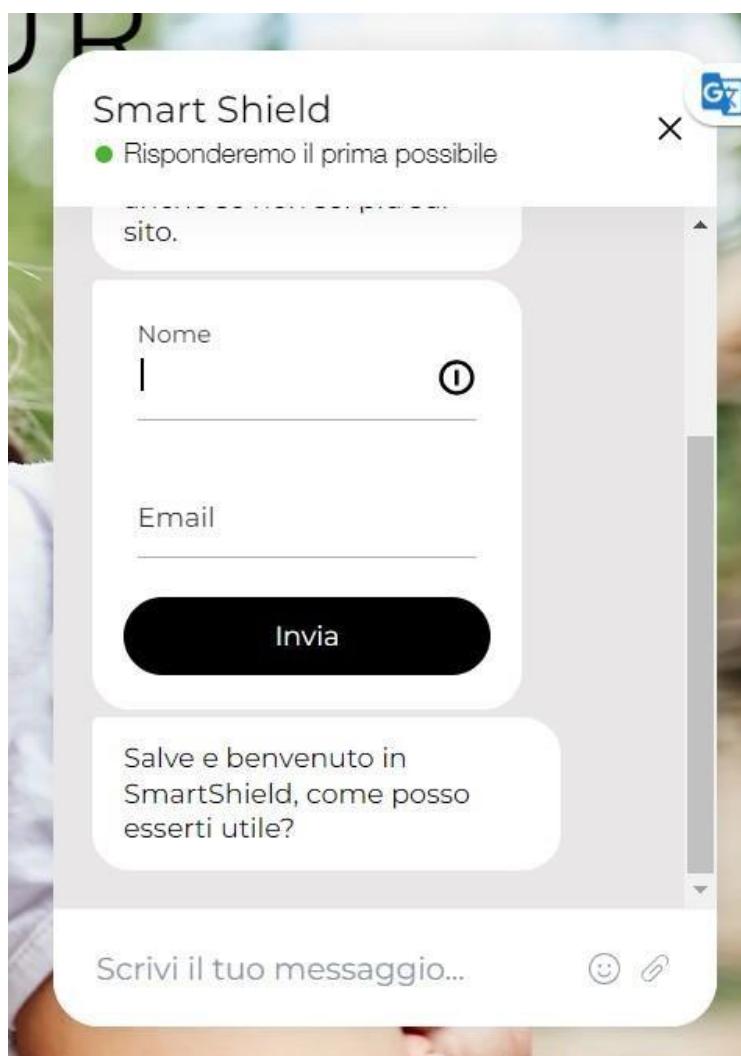
Un approccio diverso e
un nuovo metodo di
manifattura.

Leggi altro →

Sul sito web, in qualsiasi pagina ci si trovi è presente un piccolo pulsante connesso h/24 che offre la possibilità di parlare in diretta con il nostro centralino call center.

Premendo sul pulsante “**Chattiamo**” si inizia a parlare con l’operatore.

Prima di inviare un messaggio viene visualizzato un messaggio automatico di benvenuto.



SMARTSHIELD

Tecnologia

Tel: 243 456798

ISCRIVITI

Chi siamo

smartshieldenterprise@gmail.com

Ricevi le notizie e gli aggiornamenti di SmartShied.

Lavoro

C.I.S. Nola 80035, Isola 8

Email *

Iscriviti

© 2035 by SmartShieldEnterprise



PRODOTTI

Questa è nella nostra sezione dedicata ai Prodotti, il cuore pulsante della nostra offerta di sicurezza informatica. Qui potrete scoprire una vasta gamma di soluzioni progettate per proteggere voi, la vostra famiglia e la vostra azienda da ogni minaccia digitale.

Immaginate di entrare in un negozio virtuale pieno zeppo di strumenti progettati per proteggere il vostro mondo digitale. Da antivirus a firewall, da software di protezione dei dati a strumenti di monitoraggio delle minacce, abbiamo tutto ciò di cui avete bisogno per costruire un'armatura digitale inviolabile.

I nostri prodotti non sono solo strumenti, ma partner affidabili nella vostra battaglia contro le minacce informatiche. Ogni prodotto è stato sviluppato con cura e attenzione per garantire la massima efficacia e sicurezza. Siamo fieri di offrire soluzioni di qualità che si adattano alle esigenze di privati, piccole imprese e aziende di grandi dimensioni.

Nella nostra sezione Prodotti, potrete esplorare una vasta gamma di opzioni, ciascuna accompagnata da una descrizione dettagliata delle sue funzionalità e benefici. Che state alla ricerca di una protezione antivirus completa o di strumenti avanzati di crittografia dei dati, siamo sicuri che troverete ciò che fa al caso vostro.

Ma non finisce qui. Siamo consapevoli che navigare nel vasto mare della sicurezza informatica può essere intimidatorio. È per questo che siamo sempre qui per voi, pronti a offrire consulenza e assistenza personalizzata. Il nostro team di esperti è disponibile per rispondere alle vostre domande, chiarire i dubbi e aiutarvi a trovare la soluzione perfetta per le vostre esigenze specifiche.

Esplorate la nostra sezione Prodotti e iniziate il vostro viaggio verso una sicurezza informatica senza compromessi. Siamo qui per proteggere ciò che conta di più per voi, un clic alla volta.



AD HOC FOR BUSINESS
€ 999,99



FOR BUSINESS
€ 29,90



CLASSIC
€ 9,99



LITE
€ 0,00





AD HOC FOR BUSINESS

€ 999,99

[Aggiungi al carrello](#)

AD HOC FOR BUSINESS, INCLUDE tutti i prodotti inclusi nel piano For Business a cui possono essere aggiunte caratteristiche, strumenti e modalità create su misura per te, in modo da essere al sicuro da qualsiasi minaccia.

- Copertura multi-dispositivo
- Gestione centralizzata degli account
- Controllo genitoriale avanzato
- Backup familiare condiviso
- Controllo dei dispositivi smart home
- Filtri di navigazione familiare
- Allerta di geolocalizzazione familiare
- Monitoraggio dell'utilizzo del tempo familiare
Sicurezza dei social media familiari
- Formazione sulla sicurezza informatica familiare
- Gestione delle password familiare
- Eventi di sicurezza familiari
- Sicurezza avanzata dei server
- Protezione endpoint aziendale
- Sicurezza del cloud e delle applicazioni
- Firewall avanzato
- Protezione avanzata contro il ransomware
- Formazione alla sicurezza per i dipendenti
- Audit di sicurezza e compliance
- Supporto tecnico prioritario
- Analisi forense digitale
- Protezione dell'integrità dei dati
- Gestione delle vulnerabilità
- Assicurazione contro le frodi



FOR BUSINESS

€ 29,90

[Aggiungi al carrello](#)

INCLUDE:

- Copertura multi-dispositivo
- Gestione centralizzata degli account
- Controllo genitoriale avanzato
- Protezione per tutte le età
- Supporto dedicato per la famiglia
- Prezzo scontato
- Privacy e sicurezza dei dati familiari
- Backup familiare condiviso
- Controllo dei dispositivi smart home
- Filtri di navigazione familiare
- Allerta di geolocalizzazione familiare
- Monitoraggio dell'utilizzo del tempo familiare
- Sicurezza dei social media familiari
- Formazione sulla sicurezza informatica familiare
- Gestione delle password familiare
- Eventi di sicurezza familiari
- Sicurezza avanzata dei server
- Protezione endpoint aziendale
- Sicurezza del cloud e delle applicazioni
- Firewall avanzato
- Protezione avanzata contro il ransomware
- Formazione alla sicurezza per i dipendenti
- Audit di sicurezza e compliance
- Supporto tecnico prioritario
- Analisi forense digitale
- Protezione dell'integrità dei dati
- Gestione delle vulnerabilità



CLASSIC

€ 9,99

[Aggiungi al carrello](#)

INCLUDE:

- Protezione della webcam
- Firewall personale
- Controllo genitoriale
- Monitoraggio dell'identità
- Protezione del Wi-Fi
- Crittografia dei dati
- Backup automatico
- Sicurezza delle transazioni online
- Protezione da ransomware
- Notifiche di sicurezza personalizzate
- Sicurezza delle reti Wi-Fi pubbliche
- Blocco delle app malevoli
- Protezione in tempo reale
- Scansione antivirus
- Protezione anti-phishing
- Firewall integrato
- Protezione da ransomware
- Aggiornamenti automatici
- Quarantena e rimozione di file
- Rapporti dettagliati
- Modalità gioco/silenziosa
- Protezione dei dispositivi USB
- Supporto tecnico
- Interfaccia utente intuitiva
- Controllo genitoriale
- Pulizia del sistema
- Protezione della privacy



LITE

€ 0,00

[Aggiungi al carrello](#)

- Protezione in tempo reale
- Scansione antivirus
- Protezione anti-phishing
- Firewall integrato
- Protezione da ransomware
- Aggiornamenti automatici
- Quarantena e rimozione di file
- Rapporti dettagliati
- Modalità gioco/silenziosa
- Protezione dei dispositivi USB
- Interfaccia utente intuitiva
- Pulizia del sistema
- Protezione della privacy



FAMILY

€ 12,90

[Aggiungi al carrello](#)

INCLUDE:

- Copertura multi-dispositivo
- Gestione centralizzata degli account
- Controllo genitoriale avanzato
- Protezione per tutte le età
- Supporto dedicato per la famiglia
- Prezzo scontato
- Privacy e sicurezza dei dati familiari
- Backup familiare condiviso
- Controllo dei dispositivi smart home
- Filtri di navigazione familiare
- Allerta di geolocalizzazione familiare
- Monitoraggio dell'utilizzo del tempo familiare
- Sicurezza dei social media familiari
- Formazione sulla sicurezza informatica familiare
- Gestione delle password familiare
- Eventi di sicurezza familiari

CARRELLO

Una volta che il cliente avrà selezionato i prodotti desiderati e completato l'acquisto, sarà immediatamente reindirizzato al proprio carrello virtuale, dove potrà visualizzare tutti gli articoli acquistati. Qui avrà la possibilità di rivedere l'ordine, apportare eventuali modifiche e procedere al pagamento in modo sicuro e protetto.

Dopo aver completato il processo di pagamento, riceverà istruzioni dettagliate su come scaricare e installare i nuovi prodotti sul proprio dispositivo. Il processo è progettato per essere semplice e intuitivo, consentendo al cliente di iniziare a utilizzare le nuove soluzioni di sicurezza informatica nel minor tempo possibile.

Una volta scaricati e installati i prodotti, il cliente potrà usufruirne immediatamente sul proprio dispositivo. Sia che si tratti di un computer desktop, un laptop, uno smartphone o un tablet, i prodotti saranno pronti per proteggerlo da qualsiasi minaccia digitale possa presentarsi.

Una volta che il cliente si sarà registrato e effettuato l'accesso al proprio account, i prodotti saranno automaticamente resi disponibili su tutti i suoi dispositivi. Questo significa che potrà godere della massima protezione ovunque si trovi, sia che sia a casa, in ufficio o in viaggio.

L'azienda è qui per rendere l'esperienza del cliente il più fluida e conveniente possibile, garantendo che la sicurezza sia sempre al primo posto, indipendentemente da quale dispositivo stia utilizzando.

tenza Chi sian 4

> Carrello

etro | Avanti >

 FAMILY
€ 12,90
[- 1 +]

 FOR BUSINESS
€ 29,90
[- 1 +]

 CLASSIC
€ 9,99
[- 1 +]

Subtotale
€ 52,79

Vedi carrello

PROCEDURE D'ACQUISTO

La maggior parte delle nostre vendite avverrà tramite il sito web prima illustrato:

<https://smartshieldenterpr.wixsite.com/smart-shield>

Qui è possibile scaricare qualsiasi tipologia di prodotto, nel caso in cui si dovesse necessitare di un prodotto ancorapiù specifico, con determinate automazioni o strumenti, si potrà chiedere una consulenza.

Il prodotto in questione è la gamma “**AD HOC FOR BUSINESS**”, il prezzo sul sito è simbolico in quanto va poi concordato dopo consulenza.

Il cliente una volta contattato il centralino comunicherà con un addetto call center, una volta espressa la volontà di un prodotto ad hoc sarà subito trasferito ad un addetto vendite, nel caso non ci fosse un addetto vendite disponibile allora verranno chiesti i recapiti telefonici e successivamente contattato.

L'addetto presenterà un questionario al cliente e dopo un attento confronto presenterà tutte le richieste del cliente agli sviluppatori, questi provvederanno ad una stima di costi e prezzi, oltre che alle tempistiche e alla fattibilità del prodotto.

L'addetto vendite farà quindi da **broker** tra l'ufficio sviluppo e il cliente, ovviamente cercando di giungere a compromessi per finalizzare la vendita, concordate poi le tempistiche il cliente sarà dotato di un prodotto forbusiness classico per se e per tutta la sua azienda, questi in modo da avere comunque un prodotto sicuro ed utilizzabile dopo pochi giorni, in attesa poi del prodotto “sartoriale” che richiederà leggermente più tempo.

Qualsiasi vendita essendo una transazione elettronica sarà completamente tracciabile, su richiesta sarà possibile ricevere fattura elettronica in modo da detrarne l'iva per chi ne farà un utilizzo aziendale.

Tutti i diritti di recesso, reclamo, rimborso ecc... sono quelli sanciti dal Codice dei consumatori, e da tutti i decreti riguardanti i prodotti digitali.

7. Piano economico-finanziario

La Start-Up avrà un capitale sociale concordato di 16.000 €, i soci valutano che il primo anno di attività riuscirà a conquistare il 5% del mercato fra piccole e medie imprese(PMI), per poi passare al secondo anno riuscendo a raggiungere il 12% fra utenti privati(5%), famiglie(5%) e PMI(2%). Al terzo anno la Start-Up raggiungerà una percentuale totale pari al 15% del mercato tra utenti privati(10%), famiglie(10%) e PMI(5%).

I dati dall'analisi di Marketing dimostra che i principali competitors nel mercato saranno: Avast (34,5%), Bitdefender (32,2%), Norton 360 (14,3%), AVG (10,3%) e Webroot (2,4%). E la Start-Up intende raggiungere una solida posizione nel mercato raggiungendo al terzo anno il 15%(vendendo 2.178.500 unità) del mercato e stare al terzo posto contro i competitors(in questo caso Avast e Bitdefender).

Al primo anno di esercizio la Start-Up raggiunge un Reddito Netto di € 2.646.153. Al fine di svolgere la propria attività, i soci hanno preventivato costi per il primo anno pari a € 1.736.000 (vedi tabella “Fonti di Finanziamenti”).

Di seguito le tabelle economico-finanziarie:

Smart Shield S.r.l. - CIS di Nola, isola 8 - smartshieldenterprise@gmail.com -
<https://smartshieldenterpr.wixsite.com/smart-shield>

Ipotesi	Anno 1	Anno 2	Anno 3
Volumi	435.700	1.086.400	2.178.500
Prezzo	18	18	18
Incidenza materiali (sui ricavi)	10%	10%	10%
Provvigioni	10%	10%	10%
Fatturato realizzabile con 1 addetto diretto	100.000	100.000	100.000
Costo annuo di 1 addetto:	20.000	20.000	20.000
Addetti indiretti	4	4	4
Costo annuo di 1 addetto:	30.000	30.000	30.000
Incidenza TFR sul costo del lavoro	5,556%	5,556%	5,556%
Costi fissi di struttura	37.200	37.200	37.200
Costi di Sviluppo	100.000	200.000	300.000
Immobilizzazioni (investimento nell'anno)	450.000	225.000	215.000
Periodo di ammortamento (anni)	10	10	10
Tempi pagamento clienti (mesi)	1	2	3
Tempi pagamento fornitori (mesi)	2	2	2
Tempi rotazione scorte materie prime (mesi)	1	1	1
% oneri finanziari su debiti onerosi	10%	10%	10%
% imposte su reddito a.i. (acconto 100%)	40%	40%	40%
% IVA su Vendite, Acquisti e Immobilizzazioni	20%	20%	20%
Acconto sulle imposte	100%		
Capitale sociale	16.000	16.000	16.000
Riserve	20.000		
Conto Economico	Anno 1	Anno 2	Anno 3
+ Ricavi di vendita	7.668.320	19.120.640	38.341.600
- Costo materiali	766.832	1.912.064	3.834.160
- Provvigioni	766.832	1.912.064	3.834.160
= Margine di contribuzione	6.134.656	15.296.512	30.673.280
- Manodopera diretta	1.533.664	3.824.128	7.668.320
- Accantonamento TFR MDO diretta	85.204	212.452	426.018
= MDC - Costo MDO diretta	4.515.788	11.259.932	22.578.942
- Costi fissi di struttura	37.200	37.200	37.200
- Manodopera indiretta	120.000	120.000	120.000
- Accantonamento TFR MDO indiretta	6.667	6.667	6.667
- Costi di sviluppo	100.000	200.000	300.000
= EBITDA	4.251.922	10.896.066	22.115.076
- Ammortamenti (inserirlo prima nello SP)	45.000	67.500	89.000
= EBIT (Reddito Operativo)	4.206.922	10.828.566	22.026.076
- Oneri (Gestione finanziaria)	100.000	122.500	144.000
= Reddito ante imposte	4.106.922	10.706.066	21.882.076
- Imposte	1.642.769	4.282.426	8.752.830
= Reddito netto	2.464.153	6.423.639	13.129.245

Stato Patrimoniale			
IMPIEGHI	Anno 1	Anno 2	Anno 3
+ Attivo circolante	830.735	3.983.467	11.821.993
+ Crediti verso clienti	766.832	3.824.128	11.502.480
+ Erario c.to IVA attivo	-	-	-
+ Scorte	63.903	159.339	319.513
+ Immobilizzazioni operative nette	405.000	562.500	688.500
+ Immobilizzazioni lorde	450.000	675.000	890.000
- Fondo ammortamento	45.000	112.500	201.500
= Totale Impieghi	1.235.735	4.545.967	12.510.493
Calcolo Erario conto iva	Anno 1	Anno 2	Anno 2
+ IVA su Acquisti	334.173	812.266	1.601.104
+ IVA su Immobilizzazioni	90.000	45.000	43.000
- IVA su vendite	(1.533.664)	(3.824.128)	(7.668.320)
Somma algebrica IVA dell'anno	(1.109.491)	(2.966.862)	(6.024.216)
Recupero crediti IVA	-	-	-
Erario conto IVA	(92.458)	(247.239)	(502.018)

FONTI	Anno 1	Anno 2	Anno 3
+ Passivo circolante	2.159.269	4.010.150	11.599.625
+ Debiti verso fornitori	334.173	812.266	1.601.104
+ Fondo imposte	1.642.769	2.639.658	8.752.830
+ Fondo TFR	91.870	310.988	743.673
+ Erario c.to IVA passivo	92.458	247.239	502.018
+ Debiti finanziari	(3.423.688)	(8.387.976)	(21.142.170)
+ Scoperti di c/c e castelletto	(3.473.688)	(8.487.976)	(21.242.170)
+ Finanziamenti a medio/lungo termine	50.000	100.000	100.000
+ Mezzi Propri	2.500.153	8.923.793	22.053.038
+ Capitale sociale	16.000	16.000	16.000
+ Riserve	20.000	2.484.153	8.907.793
+ Reddito netto	2.464.153	6.423.639	13.129.245
= Totale Fonti	1.235.735	4.545.967	12.510.493
+ Attivo circolante	830.735	3.983.467	11.821.993
- Passivo circolante	(2.159.269)	(4.010.150)	(11.599.625)
= CCN Operativo	(1.328.535)	(26.684)	222.368
+ Immobilizzazioni operative nette	405.000	562.500	688.500
= Capitale investito netto operativo	(923.535)	535.816	910.868
- Autofinanziamento	2.484.153	8.907.793	22.037.038
= Fabbisogno finanziario	(3.407.688)	(8.371.976)	(21.126.170)

7.1 STRUTTURA FINANZIARIA

Voci di testo	Tipologia / Dettagli	Unità necessarie 1° Anno	Costo Totale 1° Anno (in €)	Costo Totale 2° Anno (in €)	Costo Totale 3° Anno (in €)
Fiscalità	Commercialista	1	18.000	18.000	18.000
Affitto	Sede operativa (CIS Int., Nola)	1	37.200	37.200	37.200
Gestione	Collaboratori (4 addetti)	2 al marketing 2 alle centraline	18.000 14.400	18.000 14.400	18.000 14.400
Immobilizzazioni	Marchi / Certificazioni / Brevetti / Licenze	11 totale	91.000	/	/
Spese Promozionali	Web, video prom, giornali e porta a porta	/	85.000	120.000	140.000
Attrezzature/PC	Attrezzature HW, CPU, GPU, RAM, SSD ecc...		25.300	/	/
Totale Investimenti			€ 288.900	€ 207.600	€ 227.600

FONTI DI FINANZIAMENTO	1° Anno (in €)	2° Anno (in €)
Capitale Sociale	16.000	/
Programma di Finanziamento "Resto Al Sud"	80.000	120.000
Fondo "Smart&Start Italia"	1.500.000	/
Riserve	/	20.000
TOTALE Finanziamenti	€ 1.596.000	€ 140.000

TARIFFARIO:

Tipologia di abbonamento	Costo (in €)	Dispositivi	Totale (12 mesi in €)
Singolo Utente	9.90	1	118,8
Famiglia	12.90	5	154,8
Azienda	29.90	---	358,8

* oltre a queste tipologie esiste una versione gratuita con presenza di banner pubblicitari.

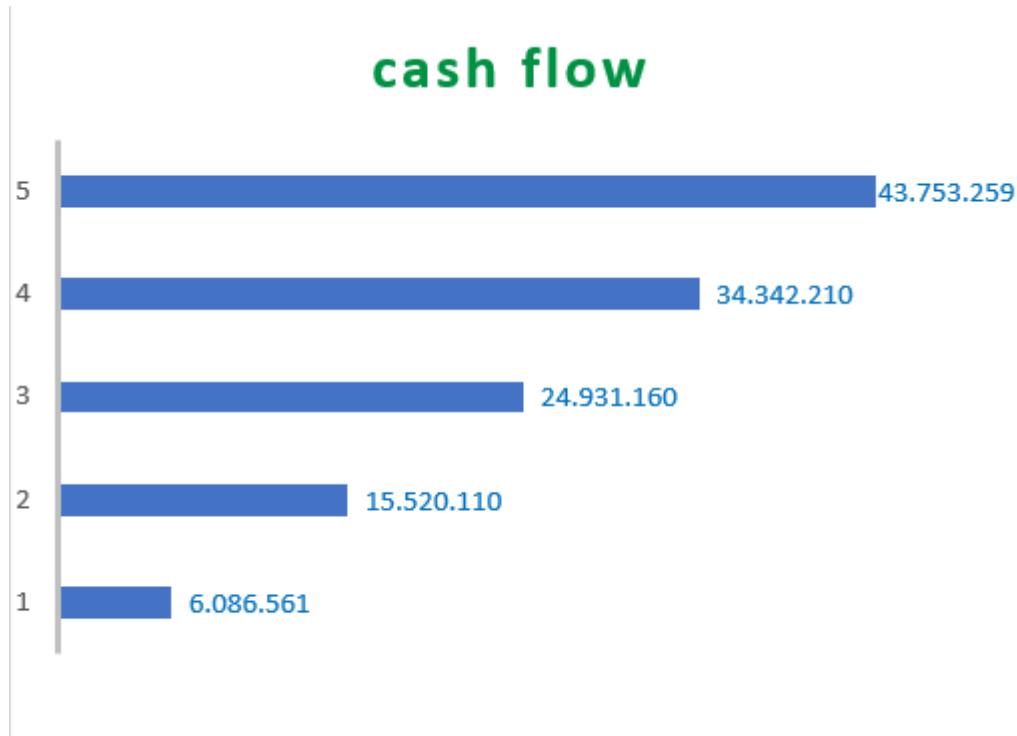
7.2 PROIEZIONI FUTURE

Di seguito le proiezioni future, il *Calcolo VAN* con annesso grafico “cash flow”:

Foglio **Calcolo VAN**:

	1	2	3	4	5
EBIT	4.206.922	10.828.566	17.450.210	24.071.854	30.693.498
Ammortamenti	45.000	67.500	67.500	67.500	67.500
Accantonamenti	91.870	219.118	346.366	473.614	600.862
Oneri finanziari	100.000	122.500	145.000	167.500	190.000
Imposte	1.642.769	4.282.426	6.922.084	9.561.742	12.201.399
Flusso di cassa	6.086.561	15.520.110	24.931.160	34.342.210	43.753.259
	Tasso Rend.	8,0%			
	VAN	€ 93.753.138,14			

Grafico **CASH FLOW**:



7. Bibliografia

"Se io ho una mela e tu hai una mela e ce le scambiamo, ciascuno di noi avrà ancora una mela. Ma se io ho un'idea e tu hai un'idea e ce le scambiamo, ciascuno di noi avrà due idee."

Semicit.. George Bernard Shaw

8. Sitografia

- <https://www.punto-informatico.it/> crescita pmi
- <https://www.analisidifesa.it/>
- Rapporto Cluist 2023 sulla sicurezza ICT in Italia, Security Summit, Astrea, Milano, 2023, pp 5-10
- Gratteri, N., & Nicaso, A. (2023). Il grifone. Come la tecnologia sta cambiando il volto della 'ndrangheta, pp 35-36

Tutta la Sitografia del piano Marketing

Definizione sul mercato e situazione italiana:

<https://www.swascan.com/>

Dimensioni del Mercato globale e nazionale:

<https://www.marketsandmarkets.com/>

Numero di Utenti e Domanda Potenziale:

<https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-mercato-all-a-soglia-dei-2-miliardi-ora-serve-una-strategia-long-term/>

Numero di Imprese Presenti:

<https://www.agid.gov.it/it/argomenti/intelligenza-artificiale>

Domanda di Mercato:

<https://www.marketsandmarkets.com/>

Concorrenza:

<https://support.norton.com/sp/en/us/home/current/solutions/v53370843>

<https://www.bitdefender.com/solutions/antivirus.html>

<https://www.avast.com/premium-security>

<https://www.avg.com/en-us/internet-security>

<https://www.av-test.org/en/>

<https://www.pcmag.com/>

<https://www.techradar.com/>

quote di mercato dei 5 antivirus in Italia a maggio 2024:

Smart Shield S.r.l. - CIS di Nola, isola 8 - smartshieldenterprise@gmail.com -
<https://smartshieldenterpr.wixsite.com/smart-shield>

<https://www.osservatori.net/it/ricerche/osservatori-attivi/cybersecurity-data-protection>

Punti di forza e debolezza dei prodotti dei nostri concorrenti

<https://www.bitdefender.com/>

<https://www.webroot.com/us/en>

<https://us.norton.com/>

<https://account.avast.com/>

<https://www.avg.com/>

<https://www.pc当地.com/>

<https://www.av-test.org/en/>

<https://www.av-comparatives.org/>

<https://nsslabs.com/>

<https://www.idc.com/>

<https://www.gartner.com/en>

<https://www.statista.com/>

Strategia marketing

<https://www.pc当地.com/reviews/antivirus>

Stima della domanda

ricerca di mercato:

<https://www.marketsandmarkets.com/PressReleases/artificial-intelligence-security.asp>

Questa tabella è basata su questi dati ricavati da internet:

<http://dati.istat.it/>

<https://www.istat.it/it/files/2020/12/C03.pdf>

<https://www.osservatori.net/it/home>

Smart Shield S.r.l. - CIS di Nola, isola 8 - smartshieldenterprise@gmail.com -
<https://smartshieldenterpr.wixsite.com/smart-shield>

<https://www.istat.it/it/archivio/popolazione>

<https://www.osservatori.net/it/home>

<https://www.bancaditalia.it/>

brevetti, certificazioni e licenze:

<https://uibm.mise.gov.it/index.php/it/>

<https://www.wipo.int/>

<https://www.epo.org/en>

<https://www.av-test.org/en/>

<https://www.virusbulletin.com/testing/vb100>

<https://www.commoncriteriaportal.org/>

<https://www.iso.org/home.html>

<https://www.copyright.gov/>

<https://www.uspto.gov/>

<https://www.uspto.gov/>

<https://iapp.org/>

<https://www.bis.gov/>

Costi della Sede(300 mq2):

<https://www.casa.it/vendita/capannoni/nola/>

Costi dei diversi componenti(CPU, GPU, RAM, SSD ecc.):

- <https://www.idealo.it/spcat/3016/componenti-pc.html>

FONDI DI FINANZIAMENTO:

- “Resto Al Sud”: <https://www.invitalia.it/cosa-facciamo/creiamo-nuove-aziende/resto-al-sud>
- “Smart&Start Italia”: <https://www.invitalia.it/cosa-facciamo/creiamo-nuove-aziende/smartstart-italia>

Smart Shield S.r.l. - CIS di Nola, isola 8 - smartshieldenterprise@gmail.com -
<https://smartshieldenterpr.wixsite.com/smart-shield>
