



Università degli Studi di Padova



Catch em All - *CAPTCHA: Umano o Sovraumano?*

Email: catchemallswe3@gmail.com

Piano di progetto

Versione	(modifica)
Approvazione	(modifica)
Redazione	(modifica)
Verifica	(modifica)
Stato	(In sviluppo)
Uso	(modifica)
Distribuzione	(modifica)

Registro delle modifiche

Versione	Data	Descrizione
0.0.1	23/11/2022	Creazione del documento e stesura dell'Introduzione, dell'Analisi dei rischi e del modello di

Indice

1	Introduzione	2
1.1	Scopo del documento	2
1.2	Scopo del prodotto	2
1.3	Glossario	2
1.4	Riferimenti	2
1.4.1	Riferimenti normativi	2
1.5	Riferimenti informativi	3
2	Analisi dei rischi	4
2.1	Rischi personali	4
2.2	Rischi tecnologici	7

1 Introduzione

1.1 Scopo del documento

Nel seguente documento viene esposto in modo dettagliato la pianificazione delle attività da svolgere per lo sviluppo del progetto, trattando i seguenti punti:

- Analisi dei rischi;
- Modello dello sviluppo adottato;
- Suddivisione dei compiti tra i membri del gruppo;
- Stima dei costi e delle risorse necessarie;

1.2 Scopo del prodotto

Gli attuali sistema di sicurezza di rilevazione dei bot rispetto agli esseri umani, al fine di bloccare azioni con fini malevoli nel web, oggi giorno viene effettuato tramite test CAPTCHA. Viene evidenziato, nel capitolato “CAPTCHA: Umano o Sovrumano?” una criticità in questi sistemi, in quanto grazie ai notevoli progressi nel campo dell’intelligenza artificiale, task che si ritenevano impossibili da svolgere per una macchina, ora vengono effettuate spesso meglio delle persone, superando le barriere poste attualmente nei motori di ricerca. Dal proponente “Zucchetti S.p.A” viene richiesto lo sviluppo di un applicazione web contenente una pagina di login contenente un sistema in grado di rilevare in modo ottimale ed efficiente i bot rispetto agli esseri umani.

1.3 Glossario

Per risolvere ambiguità relative al linguaggio utilizzato nei documenti prodotti, è stato creato un documento denominato “Glossario”. Questo documento fornisce le definizioni relative a tutti i termini tecnici utilizzati nei vari documenti, segnalando questi termini con l’apice G accanto alla parola.

1.4 Riferimenti

1.4.1 Riferimenti normativi

- Norme di Progetto v1.0.0; (a caso)
- Capitolato d’appalto C1 "CAPTCHA: Umano o Sovrumano?" <https://www.math.unipd.it/~tullio/IS-1/2022/Progetto/C1.pdf>
- Slide PD2 del corso di Ingegneria del Software - Regolamento del Progetto Didattico: <https://www.math.unipd.it/~tullio/IS-1/2022/Dispense/PD02.pdf>

1.5 Riferimenti informativi

- Analisi dei Requisiti v2.0.0; (a caso)
- Slide T04 del corso di Ingegneria del Software - Gestione di progetto: <https://www.math.unipd.it/~tullio/IS-1/2022/Dispense/T04.pdf>
- Slide T02 del corso di Ingegneria del Software - Processi di ciclo di vita del software: <https://www.math.unipd.it/~tullio/IS-1/2022/Dispense/T02.pdf>

2 Analisi dei rischi

Grazie ad un'attenta analisi dei rischi si pone l'obiettivo di prevedere e mitigare rischi e problematiche che nascono durante lo sviluppo del progetto, cercando strategie per minimizzarli. La gestione dei rischi avviene tramite le 4 attività seguenti:

- **Identificazione** dei possibili eventi che potrebbero causare problemi durante l'avanzamento;
- **Analisi** del problema, tramite una valutazione delle conseguenze negative e una stima di con cui si possa verificare e della gravità di esso;
- **Pianificazione** della metodologia per impedire il verificarsi dei rischi individuati e i comportamenti da adottare nel caso in cui si presentassero;
- **Monitoraggio** per rilevare tutti gli eventuali nuovi rischi da effettuare durante tutto il periodo di sviluppo del progetto;

I rischi sono stati suddivisi in tre categorie:

- Rischi personali;
- Rischi tecnologici;
- Rischi organizzativi;
- Rischi legati ai requisiti;

2.1 Rischi personali

Inesperienza in ambito tecnologico	
Descrizione:	Nessun componente del team ha un'elevata esperienza con le tecnologie scelte per lo sviluppo del progetto.
Identificazione:	Il componente comunica al resto del team i problemi riscontrati.
Precauzioni:	Studio approfondito dei software da utilizzare tramite manuali e tutorial online.
Pericolosità:	Alta.
Stima di manifestazione:	Media.
Conseguenze:	Ritardi o inadempienze nello svolgere i lavori assegnati.
Piano di contingenza:	Il componente riscontrato un problema, dovrà consultare la documentazione ufficiale o i tutorial online. In caso di necessità potrà richiedere ai componenti con più esperienza di ragionare insieme ai problemi riscontrati per trovare una soluzione.

Difficoltà nella comunicazione interna	
Descrizione:	Ciascun componente ha impegni fissi e straordinari durante tutto l'arco della settimana, non riuscendo ad essere sempre tutti disponibili contemporaneamente per dei meeting interni.
Identificazione:	Ogni membro deve dichiarare gli impegni fissi settimanali al resto del team nei primi meeting effettuati, permettendo una mappatura degli impegni di ciascuna persona in un singolo calendario.
Precauzioni:	La comunicazione di impegni straordinari che non permettono di effettuare il meeting settimanale di tutto il team deve avvenire tramite l'app messaggistica whatsapp.
Pericolosità:	Media.
Stima di manifestazione:	Media.
Conseguenze:	Possibili ritardi e mancanza di comunicazione efficiente del singolo individuo.
Piano di contingenza:	Il team concorda una data e un orario per effettuare un meeting di routine ogni settimana in cui tutti possono partecipare che non si sovrappone con gli impegni fissi di ciascun membro tramite la piattaforma Discord. In caso di impegni straordinari di uno o più membri nell'orario del meeting concordato, il responsabile si occupa di trovare un altro orario accessibile a tutti. In caso di impossibilità, il resto del team effettua il meeting come concordato e si occupa di stilare dettagliatamente in un documento Word tutti i punti affrontati per rendere informata la persona e si richiede un feedback da ritornare alla persona interessata.

Difficoltà nella comunicazione esterna	
Descrizione:	La comunicazione con il proponente che avviene esclusivamente tramite email e meeting non è sempre accessibile a tutti i componenti del team.
Identificazione:	Come già dichiarato ogni componente ha degli impegni fissi e straordinari a cui vanno sovrapposti quelli del proponente per effettuare dei meeting insieme. Inoltre la comunicazione tramite email non è sempre efficiente, poiché non è sempre ottenibile una risposta veloce.
Precauzioni:	Il team tramite comunicazione via email organizza meeting accessibili a tutti i componenti, proponendo diverse date e orari concordate tra il gruppo al proponente, che comunicherà le sue disponibilità.
Pericolosità:	Media.
Stima di manifestazione:	Media.
Conseguenze:	Possibili ritardi nella comunicazione dello stato dello sviluppo del progetto o problemi riscontrati.
Piano di contingenza:	Il team ad ogni necessità di comunicare delle informazioni o domande al proponente, durante il meeting settimanale concorda diverse date e orari accessibili a tutti e tempestivamente le comunica al proponente per organizzare una riunione. In caso di un'impossibilità nella sovrapposizione degli impegni tra le parti, se possibile si cerca di effettuare una comunicazione efficiente tramite email, altrimenti effettua il meeting nella data proposta dal proponente in cui più componenti del team sono disponibili. A termine della riunione, viene redatto il verbale, come ad ogni meeting, in cui vengono elencati tutti i punti affrontati che sarà poi visualizzato dai componenti mancanti al meeting per renderli informati.

Conflitti interni per lo sviluppo del progetto	
Descrizione:	Nella tecnologie lasciate libere da utilizzare e nei diversi sistemi da implementare per ottenere il risultato richiesto, è comune avere diversi punti di vista tra i componenti del team.
Identificazione:	Ciascun componente in maniera professionale espone il proprio punto di vista al resto del team.
Precauzioni:	Non è possibile decidere autonomamente una tecnologia da utilizzare o un sistema da implementare senza l'approvazione comune.
Pericolosità:	Alta.
Stima di manifestazione:	Alta.
Conseguenze:	Il capitolato viene svolto in un clima avverso.
Piano di contingenza:	Ogni componente con un diverso punto di vista è invitato a fornire una documentazione al fine motivare la sua idea in maniera professionale. Il team tutto riunito, ascoltate le proposte deciderà in maniera democratica la proposta ritenuta migliore e ciascun componente si adegnerà alla scelta decisa.

2.2 Rischi tecnologici

Implementazione in diversi motori di ricerca, ognuno con delle proprie caratteristiche.	
Descrizione:	Ad oggi, per visitare il web è possibile utilizzare diversi motori di ricerca, ognuno diverso tra loro.
Identificazione:	Sviluppato il progetto, bisognerà rilevare errori e bug relativi ad ogni motore di ricerca.
Precauzioni:	Documentazione e studio dei problemi che potrebbero nascere.
Pericolosità:	Media.
Stima di manifestazione:	Media.
Conseguenze:	Bug e errori caratteristici di ogni singolo motore di ricerca.
Piano di contingenza:	Sviluppo consapevole dei problemi esistenti che utilizza soluzioni efficaci e applicabili a tutti i motori di ricerca.

Problemi Hardware	
Descrizione:	Ciascun membro lavora su un computer in remoto, il quale può essere soggetti a guasti e mancanza di connessione.
Identificazione:	Il membro comunica al resto del team il problema.
Precauzioni:	Tutti i file devono avere una copia di backup in remoto su GitHub.
Pericolosità:	Media.
Stima di manifestazione:	Bassa.
Conseguenze:	Problemi nell'avanzamento del singolo individuo nel progetto.
Piano di contingenza:	Utilizzare un altro dispositivo disponibile oppure nel caso non fosse disponibile rivolgersi all'ateneo per richiedere l'utilizzo di un computer di un laboratorio.

Problemi software	
Descrizione:	Per svolgere qualsiasi attività inerente al progetto il team utilizza software di terze parti, che sono soggetti a bug e ad non essere operativi e utilizzabili.
Identificazione:	I problemi identificati dovranno essere comunicati al resto del team.
Precauzioni:	Dovranno essere effettuati backup in chiavetta ogni settimana per ridurre al minimo le perdite di dati.
Pericolosità:	Media.
Stima di manifestazione:	Bassa.
Conseguenze:	Perdite di dati e indisponibilità nello svolgere le attività.
Piano di contingenza:	In caso di problematiche gravi e durature, il responsabile della settimana dovrà decidere un software alternativo a quello non più utilizzabile.