Analisi dei Requisiti

Versione: 0.1.0

Registro delle versioni

Versione	Data	Autore	Descrizione delle modifiche
0.2.0	14/01/2025	Lorenzo Grolla	Stesura UC Autenticazione
0.1.0	19/12/2025	Alessandro Morabito	Inizio stesura

Indice

1 Introduzione

1.1 Scopo del documento

Con il presente documento il gruppo Byte Holders stabilisce i requisiti funzionali e non funzionali del software CodeGuardian.

Questo documento è rivolto:

- all'Azienda Var Group, destinatari anche del software sviluppato
- al gruppo Byte Holders, che farà riferimento a questo documento nel corso del progetto
- ai professori Tullio Vardanega e Riccardo Cardin

All'interno del documento si proponge una visione generale del software proposto nella Sezione 2, per poi passare in rassegna i casi d'uso individuati nella Sezione 3.

Per la redazione del documento si è fatto riferimento allo standard IEEE 830-1998.

1.2 Scopo del prodotto

Il prodotto CodeGuardian permetterà di effettuare analisi della qualità di repository GitHub, con una particolare attenzione in merito ai permessi di visualizzazione delle informazioni e lancio delle stesse analisi.

CodeGuardian si propone come soluzione per team di sviluppo eterogenei che vogliono poter monitorare lo stato di repository GitHub e ottenere informazioni aggregate su insemi di progetti analizzati.

1.3 Glossario

Per evitare ambiguità, nel corso del documento si farà riferimento a termini indicati nel *Glossario*[G] utilizzando la lettera *G* ad apice della formula corrispondente, che viene indicata in corsivo (ad es. *formula in glossario*[G]). La corrispondenza di termini è a meno di coniugazioni e declinazioni.

1.4 Definizioni, acronimi e abbreviazioni

1.4.1 *Caso d'uso*[G]

Un Caso d'uso è un insieme di scenari che hanno in comune uno scopo finale per un utente.

1.4.2 *Scenario*[G]

1.4.3 *Attore*[G]

1.5 Riferimenti

1.5.1 Riferimenti normativi

- Norme Di Progetto
  https://byte-holders.github.io/Documentazione/RTB/Norme_Di_Progetto.pdf
- 830-1998 - IEEE Recommended Practice for Software Requirements Specifications
  https://ieeexplore.ieee.org/document/720574

- Capitolato
  https://www.math.unipd.it/~tullio/IS-1/2025/Progetto/C2.pdf

1.5.2 Riferimenti informativi

- *Glossario*[G]
  https://byte-holders.github.io/Documentazione/RTB/Glossario.pdf
- Specifica UML 2.5.1
  https://www.omg.org/spec/UML/2.5.1/PDF

2 Descrizione generale

2.1 Prospettiva del prodotto

Il gruppo Byte Holders propone il software CodeGuardian, un sistema ad agenti che permette di analizzare la qualità del codice, il livello di sicurezza e di manutenzione per una repository GitHub. L'esito dell'analisi sarà disponibile sotto forma di report agli utenti, ai quali sono proposte eventuali soluzioni alle problematiche individuate.

Il gruppo Byte Holders ha offerto particolare attenzione alla rolistica all'interno dell'applicazione, che si è tradotta nella distinzione di tipologie di utenti in base ai loro permessi.

A tutti gli utenti sarà comune la presenza di una dashboard che comprenderà vari workspace, nonché la capacità di effettuare ricerche avanzate al loro interno.

Il prodotto si propone quindi come soluzione per diverse tipologie di utenti, come quelle individuate in prima sessione di *Design Thinking*, che condividono gli stessi progetti.

2.2 Funzioni del prodotto

2.3 Caratteristiche dell'utente

3 Casi d'uso

3.1 Lista degli Attori

Nella creazione dei casi d'uso sono stati individuati i seguenti attori:

- **Utente non Autenticato**
  Un utente non riconosciuto dal sistema
- **Utente Autenticato**
  Utente generico riconosciuto dal sistema
- **Utente Permesso OWASP** (eredita da *Utente autenticato*)
  Utente Autenticato con il permesso per la visione completa delle informazioni su OWASP
- **Utente Permesso Utenti/Ruoli** (eredita da *Utente autenticato*)
  Utente Autenticato con il permesso per la gestione degli utenti e dei ruoli
- **Utente Permesso Test** (eredita da *Utente autenticato*)
  Utente Autenticato con il permesso per la visione completa delle informazioni sui test
- **Utente Permesso Documentazione** (eredita da *Utente autenticato*)
  Utente Autenticato con il permesso per la visione completa delle informazioni sulla documentazione

- **Utente Permesso Scansione** (eredita da *Utente autenticato*)
  Utente Autenticato con il permesso per il lancio di una scansione
- **Utente Permesso Qualità Codice** (eredita da *Utente autenticato*)
  Utente Autenticato con il permesso per la visione completa delle informazioni sulla qualità del codice
- **Utente Permesso Informazioni Tecniche** (eredita da *Utente autenticato*)
  Utente Autenticato con il permesso per la visione completa delle informazioni tecniche di una repository

3.2 Struttura generale di un caso d'uso

Si è deciso di descrivere ciascun *caso d'uso*[G] seguendo la seguente struttura (sottolineati i campi sempre popolati):

Codice	Codice identificativo utilizzato per far riferimento al *caso d'uso*[G] corrente
Titolo	Titolo del *caso d'uso*[G] corrente
Attori principali	Attori che agiscono sul sistema dando inizio allo scenario
Attori secondari	Attori di supporto che agiscono in risposta a stimoli del sistema
Precondizioni	Condizioni necessarie per l'esecuzione del *caso d'uso*[G] corrente
Postcondizioni	Condizioni in cui viene lasciato il sistema al termine dello *scenario principale*[G]
Scenario principale	Descrizione degli eventi che avvengono all'interno dello *scenario principale*[G]
Inclusioni	Lista dei riferimenti a *casi d'uso*[G] terzi *inclusi*[G] dal *caso d'uso*[G] corrente e al quale si fa riferimento nella sezione *Scenario principale*
Scenari alternativi	Descrizione delle situazione che portano a *scenari alternativi*[G]
Eredita da	Codice del *caso d'uso*[G] terzo da cui eredita il *caso d'uso*[G] corrente (non ammettiamo ereditarietà multipla)

3.3 Lista dei *casi d'uso*[G]

3.3.1 UC1 - Registrazione

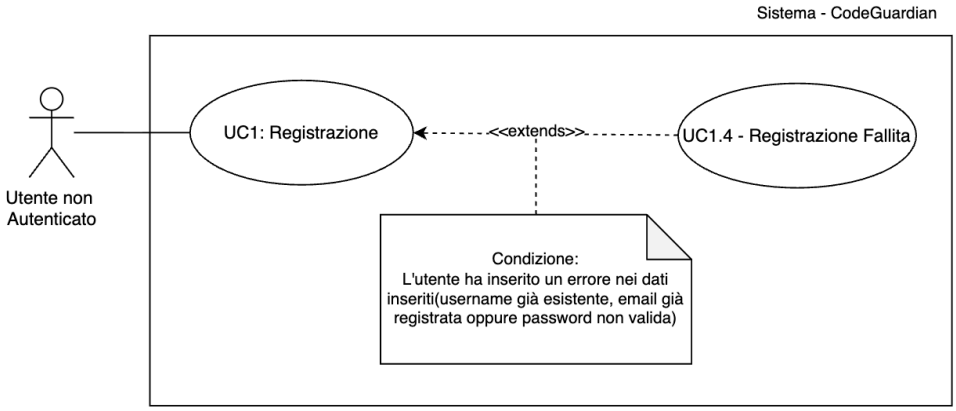

Figura 1: UC1 - Registrazione

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente non possiede ancora un account attivo nel sistema
- **Postcondizioni:** Viene creato un nuovo profilo utente nel sistema CodeGuardian con stato "da confermare".
- **Scenario principale:**
  1. L'utente accede alla pagina di registrazione
  2. L'utente inserisce l'username (UC1.1)
  3. L'utente inserisce l'email (UC1.2)
  4. L'utente inserisce la password (UC1.3)
  5. L'utente conferma la registrazione
  6. Il sistema valida i dati e crea l'utente su Amazon Cognito
  7. Il sistema invia un codice OTP all'email fornita
- **Inclusioni:**
  - UC1.1 - Inserimento username
  - UC1.2 - Inserimento email
  - UC1.3 - Inserimento password
- **Estensioni:**
  - UC1.4 - Registrazione fallita

Il caso d'Uso UC1 include ulteriori casi d'uso come rappresentato nella seguente immagine:

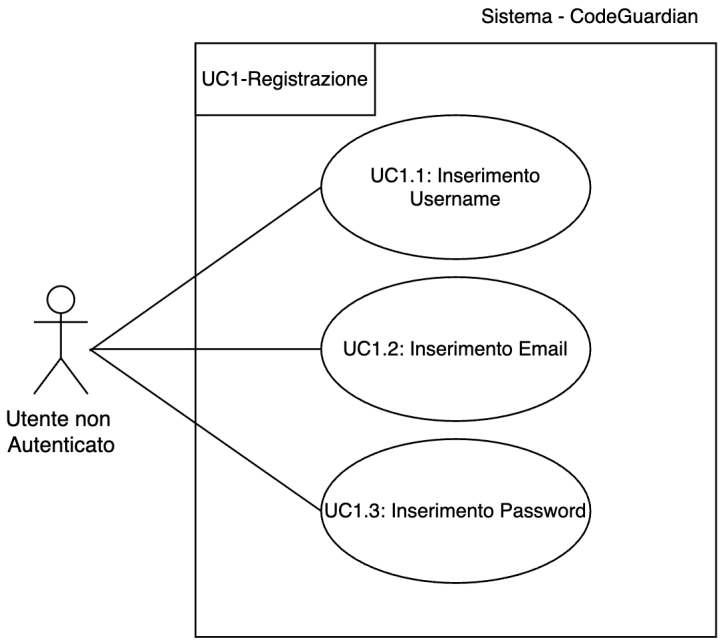

Figura 2: Inclusioni di UC1: UC1.1,UC1.2,UC1.3

3.3.2 UC1.1 - Inserimento username

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente si trova nella pagina di registrazione
- **Scenario principale:** L'utente digita l'username scelto nell'apposito campo.
- **Postcondizioni:** L'username è inserito nel sistema.

3.3.3 UC1.2 - Inserimento email

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente si trova nella pagina di registrazione
- **Scenario principale:** L'utente digita il proprio indirizzo email nell'apposito campo.
- **Postcondizioni:** L'email è inserita nel sistema.

3.3.4 UC1.3 - Inserimento password

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente si trova nella pagina di registrazione
- **Scenario principale:** L'utente digita la password desiderata nell'apposito campo.
- **Postcondizioni:** La password è inserita nel sistema.

3.3.5 UC1.4 - Registrazione fallita

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente ha tentato la conferma della registrazione con dati non validi
- **Scenario principale:**
  1. Il sistema rileva un errore nei dati inseriti (username già esistente, email già registrata oppure password non conforme ai requisiti di sicurezza)
  2. Il sistema mostra un messaggio di errore specifico all'utente
  3. Il sistema permette all'utente di correggere i dati mantenendo quelli validi
- **Postcondizioni:** La registrazione non viene completata; l'utente rimane nella pagina di registrazione.

3.3.6 UC2 - Conferma registrazione

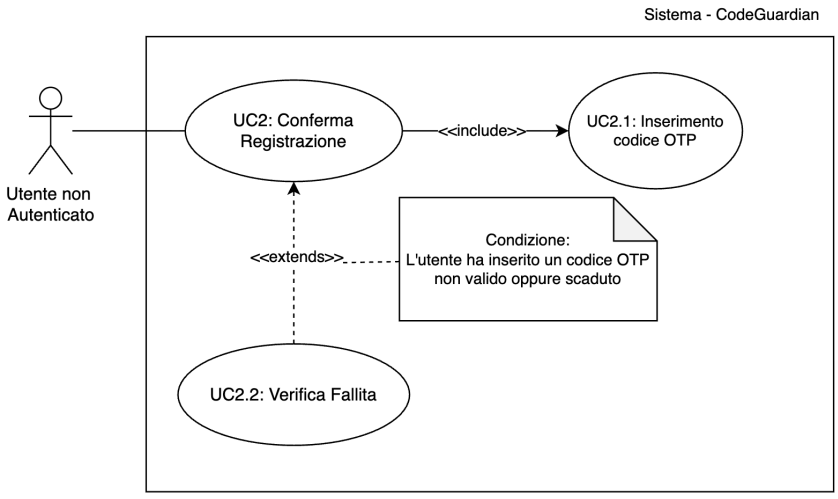

Figura 3: UC2 - Conferma Registrazione

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente ha completato la prima fase di registrazione (UC1)
  - L'utente ha ricevuto il codice OTP via email
- **Postcondizioni:** L'account viene attivato e l'utente può effettuare il login.
- **Scenario principale:**
  1. L'utente accede alla pagina di conferma registrazione
  2. Il sistema richiede il codice di verifica
  3. L'utente inserisce il codice OTP (UC2.1)
  4. L'utente conferma l'invio
  5. Il sistema verifica il codice e attiva l'account
- **Inclusioni:**
  - UC2.1 - Inserimento codice OTP
- **Estensioni:**
  - UC2.2 - Verifica fallita

3.3.7 UC2.1 - Inserimento codice OTP

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente si trova nella pagina di conferma registrazione
- **Scenario principale:** L'utente inserisce il codice numerico ricevuto via email nell'apposito campo.
- **Postcondizioni:** Il codice OTP è inserito nel sistema.

3.3.8 UC2.2 - Verifica fallita

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente ha inviato un codice OTP errato o scaduto
- **Scenario principale:**
  1. Il sistema rileva che il codice non è valido o è scaduto
  2. Il sistema mostra un messaggio di errore "Codice non valido o scaduto"

3. Il sistema offre l'opzione per richiedere un nuovo codice OTP

- **Postcondizioni:** L'account rimane nello stato "da confermare".

3.3.9 UC3 - Login

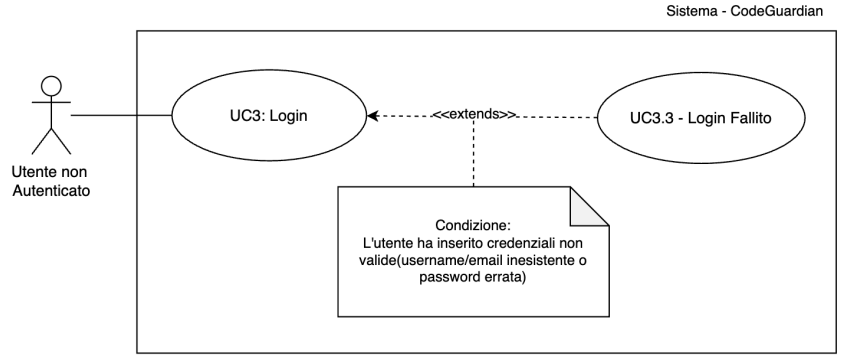

Figura 4: UC3 - Login

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente possiede un account attivo nel sistema
- **Postcondizioni:** L'utente è autenticato e accede alla home del sistema
- **Scenario principale:**
  1. L'utente accede alla pagina di login
  2. L'utente inserisce l'username (UC3.1)
  3. L'utente inserisce la password (UC3.2)
  4. L'utente conferma l'accesso
  5. Il sistema valida le credenziali tramite Amazon Cognito
  6. Il sistema reindirizza l'utente alla home
- **Inclusioni:**
  - UC3.1 - Inserimento username o email
  - UC3.2 - Inserimento password
- **Estensioni:**
  - UC3.3 - Login fallito
- **Scenari alternativi:**
  - UC4 - Recupero password (accessibile dalla pagina di login)

Il caso d'Uso UC3 include ulteriori casi d'uso come rappresentato nella seguente immagine:

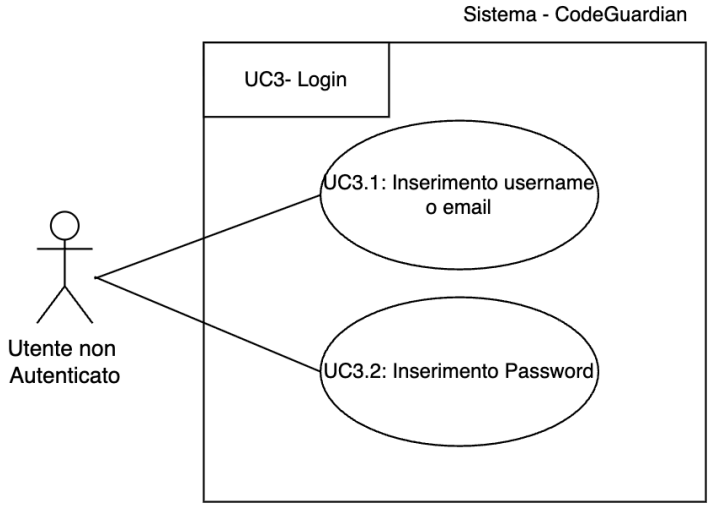

Figura 5: Inclusioni di UC3: UC3.1,UC3.2

3.3.10 UC3.1 - Inserimento username o email

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente si trova nella pagina di login
- **Scenario principale:** L'utente inserisce il proprio username o email nell'apposito campo.
- **Postcondizioni:** L'username è inserito nel sistema.

3.3.11 UC3.2 - Inserimento password

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente si trova nella pagina di login
- **Scenario principale:** L'utente inserisce la propria password nell'apposito campo.
- **Postcondizioni:** La password è inserita nel sistema.

3.3.12 UC3.3 - Login fallito

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**

  - Il sistema è attivo e funzionante
  - L'utente ha inviato credenziali non valide

- **Scenario principale:**

  1. Il sistema verifica che le credenziali non corrispondono a nessun account attivo
  2. Il sistema mostra il messaggio "Username o password errati"
  3. Il sistema permette di riprovare l'inserimento delle credenziali

- **Postcondizioni:** L'utente rimane non autenticato.

3.3.13 UC4 - Recupero password

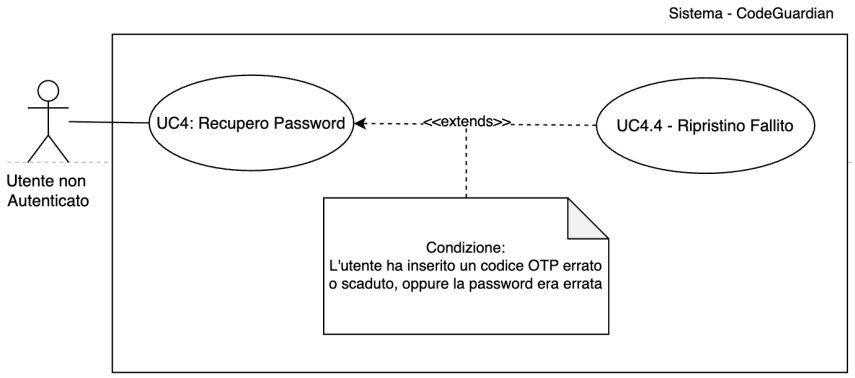

Figura 6: UC4

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**

  - Il sistema è attivo e funzionante
  - L'utente possiede un account registrato
  - L'utente ha dimenticato la password

- **Postcondizioni:** La password viene reimpostata con successo.
- **Scenario principale:**

  1. L'utente accede alla funzionalità di recupero password dalla pagina di login
  2. L'utente inserisce l'email associata al proprio account (UC4.1)
  3. L'utente conferma la richiesta
  4. Il sistema valida l'email e genera un codice OTP
  5. Il sistema invia il codice OTP via email
  6. L'utente inserisce il codice OTP ricevuto (UC4.2)
  7. L'utente inserisce la nuova password (UC4.3)
  8. L'utente conferma il cambio password

9. Il sistema valida il codice OTP, verifica che la nuova password rispetti i requisiti di sicurezza e aggiorna la password
10. Il sistema conferma l'aggiornamento e reindirizza alla pagina di login

- **Inclusioni:**
  - UC4.1 - Inserimento email per recupero
  - UC4.2 - Inserimento codice OTP
  - UC4.3 - Inserimento nuova password
- **Estensioni:**
  - UC4.4 - Ripristino fallito

Il caso d'Uso UC4 include ulteriori casi d'uso come rappresentato nella seguente immagine:

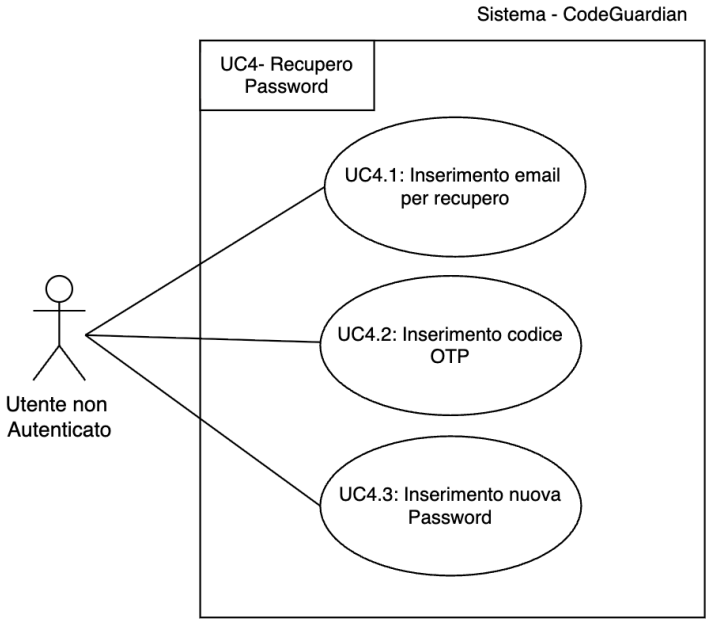

Figura 7: Inclusioni di UC4: UC4.1,UC4.2,UC4.3

3.3.14 UC4.1 - Inserimento email per recupero

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente si trova nella pagina di recupero password
- **Scenario principale:** L'utente inserisce l'email associata all'account nell'apposito campo e conferma la richiesta.
- **Postcondizioni:** Il sistema invia il codice OTP all'email fornita.

3.3.15 UC4.2 - Inserimento codice OTP

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente ha ricevuto il codice OTP via email
  - L'utente si trova nella pagina di reset password
- **Scenario principale:** L'utente inserisce il codice OTP ricevuto via email nell'apposito campo.
- **Postcondizioni:** Il codice OTP è inserito nel sistema.

3.3.16 UC4.3 - Inserimento nuova password

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente ha inserito il codice OTP
  - L'utente si trova nella pagina di reset password
- **Scenario principale:** L'utente inserisce la nuova password desiderata nell'apposito campo.
- **Postcondizioni:** La nuova password è inserita nel sistema.

3.3.17 UC4.4 - Ripristino fallito

- **Attori principali:** Utente non Autenticato
- **Precondizioni:**
  - Il sistema è attivo e funzionante
  - L'utente ha inserito un codice OTP non valido o scaduto, oppure una password non conforme ai requisiti
- **Scenario principale:**
  1. Il sistema rileva che il codice OTP è errato o scaduto, oppure che la password non rispetta i requisiti di sicurezza
  2. Il sistema mostra un messaggio di errore specifico
  3. Il sistema impedisce il cambio password e permette di richiedere un nuovo codice o correggere la password
- **Postcondizioni:** La password rimane invariata.