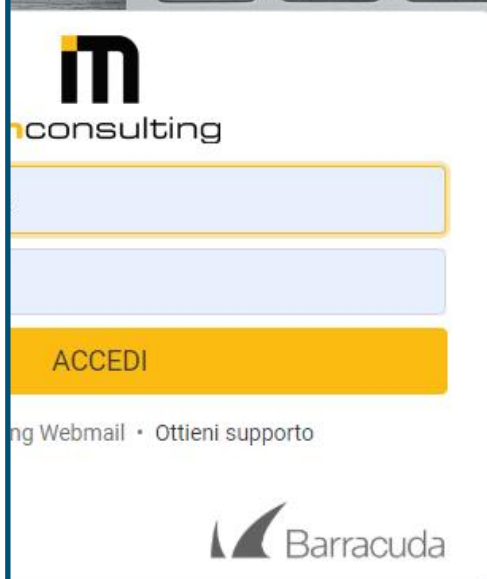


IMC WebMail: Autenticazione a 2-Step



I.M. CONSULTING s.r.l.

Autore: Masi Elisabetta
Tassinari Andrea

Descrizione ambiente di sviluppo

Lo sviluppo dell'applicazione nasce come supporto alle aziende, che considerano la comunicazione con gli utenti esterni un aspetto fondamentale per il ciclo produttivo, e agli stessi utenti finali, che desiderano scambiare informazioni in modo funzionale.

Per lo scambio di informazioni con i propri clienti e tra i membri dei team di lavoro, spesso le aziende scelgono di utilizzare lo strumento della posta elettronica.

Con l'introduzione delle nuove tecnologie, l'utilizzo dello strumento ha visto aprirsi nuove possibilità. Sfruttando al meglio la rete di navigazione offerta dal Web, la posta elettronica ha visto un'evoluzione sui propri sistemi. Questi infatti sono passati dall'utilizzo di strumenti statici, come la classica posta elettronica, a strumenti applicativi, che sfruttano la rete Internet in modo da rendere lo scambio di informazioni più efficiente. Si parla in questo caso di "**Web Mail**".

Cos'è una Web Mail?

Un'applicazione Web Mail è un servizio di posta elettronica accessibile direttamente dalla rete Internet attraverso il proprio browser (Firefox, Safari, Chrome ecc...).

Come il classico servizio di posta elettronica, essa offre una suite di funzionalità per la gestione e lo scambio di informazioni tra utenti diversi, sfruttando al meglio lo strumento delle e-mail.

Offre la possibilità di organizzare uno o più account di posta elettronica, monitorando lo scambio di mail che ne comporta attraverso lo strumento della navigazione web.

Diversamente da una casella di posta statica, un'applicazione Web Mail offre la possibilità ad un utente di accedere ai propri dati da un qualsiasi dispositivo remoto, semplicemente collegandosi alla rete Internet.

Come applicazione web infatti, essa raggruppa tutte le informazioni in un archivio centralizzato, il quale, a seconda della necessità, distribuisce le informazioni tra gli utenti.

Ogni utente può, quindi, visualizzare i messaggi e rispondere inviando mail a sua volta. Grazie alla navigazione web: ha la possibilità di eseguire l'intera suite di funzionalità standard accedendo al proprio account da qualsiasi punto nella rete.

Grazie alla sincronizzazione dei dati: accedendo da un qualsiasi dispositivo, avrà la garanzia di avere un ottimo allineamento delle informazioni.

Il programma applicativo sviluppato vede come protagonista un'applicazione Web Mail particolare.

Il suo utilizzo è indirizzato alle aziende la cui comunicazione con la clientela e i membri del team ricopre un ruolo importante all'interno del flusso produttivo.

Ogni membro dell'organismo aziendale viene supportato nello svolgimento della propria mansione.

Nello stesso modo, lo sviluppo dell'applicazione è indirizzato ad ogni singolo utente finale che desidera un servizio di casella di posta più funzionale.

Entrambe le tipologie di figure sfruttano infatti la suite di funzionalità offerte dal servizio web per ottenere una migliore interoperabilità con la propria casella di posta.



Figura 1 - Login IMC WebMail

Come sviluppatori si è posti l'obiettivo di mantenere lo strumento sempre in aggiornamento rispetto alle nuove tecnologie e misure di sicurezza, che sono sempre in evoluzione.

Un ultimo aggiornamento implementato riprende l'aspetto della sicurezza.

Un utente per accedere alla propria casella di posta sulla rete, deve autenticarsi segnalando un proprio *nome utente* seguito da una *password*.

Secondo i canoni standard infissi dal Cybersecurity, non sempre questa misura di sicurezza può essere ritenuta irresistibile. A questo proposito, le maggiori industrie informatiche hanno introdotto l'idea di un'autenticazione più sofisticata. Essa prevede l'inserimento dei dati personali dell'utente, seguiti da un codice univoco, auto generato e usabile solo una volta.

La nuova tecnologia è stata introdotta anche nel mondo delle applicazioni web di posta elettronica sotto forma di nuovo plugin.

Nuovo Plugin: Autenticazione a 2-step

Il nuovo plugin sviluppato pone come obiettivo principale quello di garantire una maggiore sicurezza per l'utente che usufruisce del servizio web e per le informazioni che questo scambia sulla rete.

Il servizio di controllo in due step offre all'utente la possibilità di inserire al processo di autenticazione una misura di controllo aggiuntiva. A seguito della conferma dei propri dati da parte del sistema, l'utente è chiamato ad inserire un codice numerico speciale, auto generato dal sistema all'occasione ed eliminato una volta utilizzato.

Si parla di "**AUTENTICAZIONE A 2 STEP**".

Essa suddivide l'accesso dell'utente al proprio account in due passaggi.

- ✚ Il primo richiede l'inserimento di uno *username* (solitamente l'indirizzo di posta elettronica dell'utente) e una *password*.
- ✚ Un secondo step vede l'inserimento di un codice di autenticazione generato e inviato all'utente dal sistema, al momento della richiesta: il *codice OTP*.

Il codice auto generato dal sistema identifica l'utente in modo univoco e ne certifica la personalità.

In questo modo si limita l'accesso alla casella di posta solo agli utenti autorizzati. Aumentando il controllo verso gli utenti malintenzionati e limitando il rischio di danneggiamento per l'intero sistema.

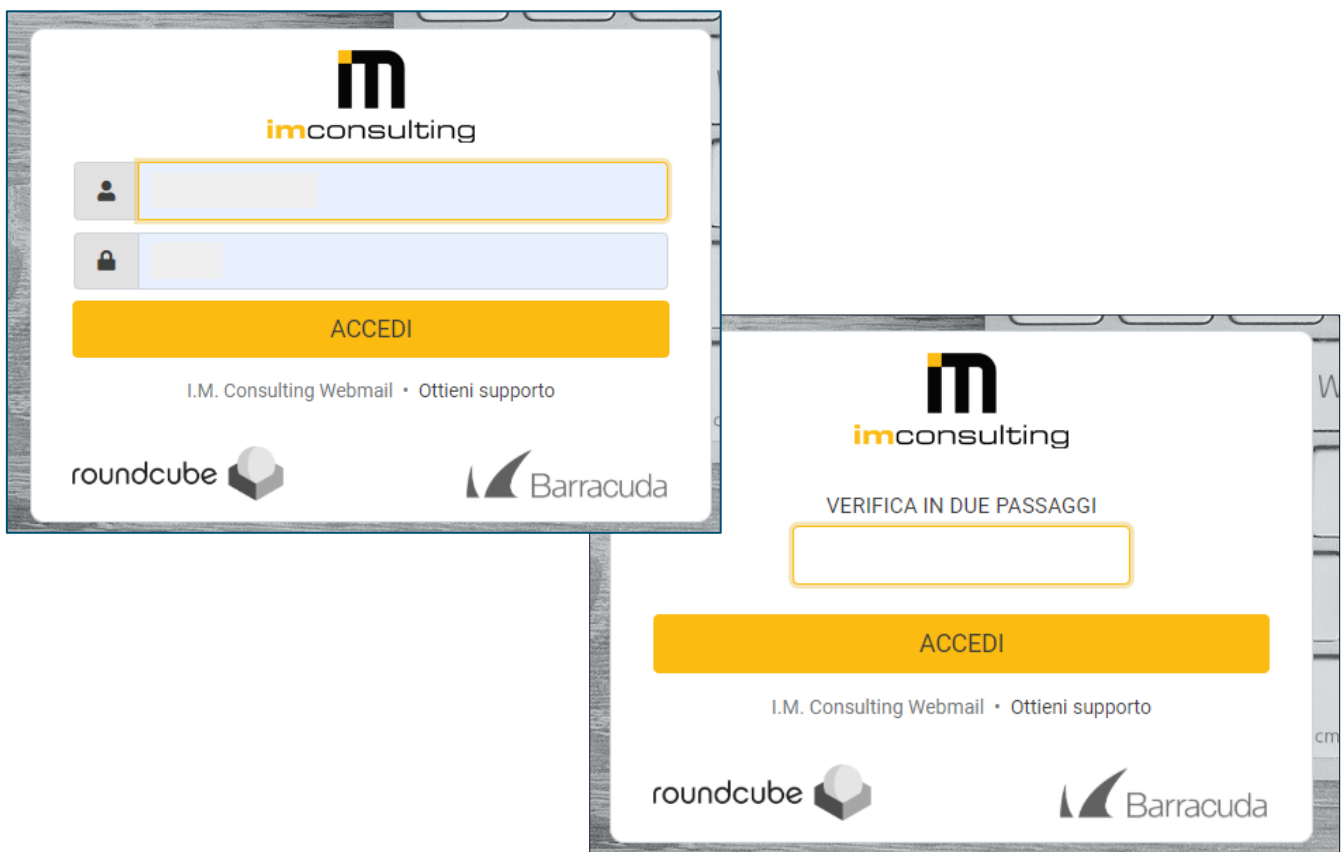


Figura 2 - Login IMC WebMail con autenticazione in 2-step

Codice OTP

Il codice auto generato dal sistema prende il nome di **OTP (One Time Password)**.

Si tratta di un codice numerico o alfanumerico “usa e getta”, generato dal sistema per essere utilizzato solo una volta, dopodiché viene eliminato. Esso è consultabile dall’utente all’occorrenza mediante dispositivi e applicazioni particolari.

Così come una password, il suo compito è quello di certificare l’autenticità di un utente che vuole accedere al proprio profilo su una piattaforma, salvaguardando la sicurezza delle informazioni e limitando l’accesso a enti non autorizzati.

Poiché si tratta di una password temporanea, il codice OTP non può essere memorizzato ma verrà generato come nuovo ogni volta che occorre. Sono diversi gli ambienti in cui viene utilizzato. Un esempio può essere legato alla gestione dei conti correnti, dove la banca fornisce un piccolo dispositivo con un pulsante da premere. All’occorrenza esso genera una chiave numerica di sei cifre o alfanumerica che l’utente potrà visualizzare direttamente dal display. Un’altra modalità prevede ad esempio, l’invio di un messaggio sms che l’utente riceve direttamente sul proprio smartphone al momento dell’operazione da effettuare.



Figura 3 - Generatori di codici OTP

Grazie alle nuove tecnologie, molte aziende e istituti bancari hanno deciso di adottare l’invio di codici OTP mediante l’utilizzo di applicazioni specifiche. L’utente ha la possibilità di installare sul proprio dispositivo mobile l’applicazione, consigliata dall’azienda a cui si fa riferimento, e consultare di volta in volta il nuovo codice di autenticazione.

Come per numerose aziende, anche l’applicazione WebMail di cui si sta svolgendo l’analisi, prevede l’introduzione di una seconda applicazione in grado di generare codici OTP secondo le necessità dell’utente che ne fa uso.

Lo scopo principale è quello di garantire un’autenticazione sicura all’interno del sistema ed evitare l’intromissione da parte di chi non è autorizzato.

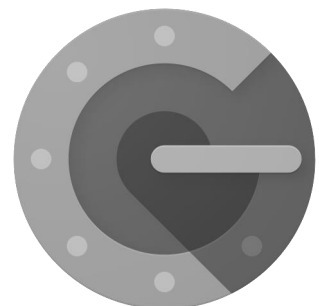


Figura 4 - Applicazione Google Authenticator

A chi è indirizzata l'applicazione?

L'applicazione così sviluppata è indirizzata a:

- tutte le aziende che vedono nello strumento della web mail una modalità agevolata per la comunicazione tra i membri del team di lavoro e con il cliente finale;
- tutti i singoli utenti che fanno della propria casella di posta uno strumento di comunicazione

Grazie al nuovo plugin, ogni utente avrà la certezza di utilizzare uno strumento sicuro e la rete di lavoro aziendale verrà salvaguardata dal rischio di danni alla produzione e intromissioni da enti non autorizzati. La comunicazione con i propri clienti sarà sempre controllata e l'accesso all'account di ogni utente verrà certificato da una modalità di autenticazione più sofisticata.

STRUMENTI DI LAVORO

La nuova versione del servizio WebMail prevede l'utilizzo di una suite di strumenti utili alla buona gestione dell'intera applicazione.

- ✚ Primo fra tutti, l'utente dovrà procurarsi l'accesso al servizio di WebMail, creando un account e facendo richiesta presso l'azienda produttrice.
- ✚ Un secondo elemento necessario è lo strumento di autenticazione.
Accedendo ai principali store presenti sui sistemi del proprio dispositivo mobile, l'utente ha la possibilità di scaricare un'applicazione per la generazione di codici di autenticazione.
- ✚ Infine, il passaggio più importante sarà nella sincronizzazione tra i due strumenti. L'utente dovrà abilitare sulla piattaforma web il plugin per il controllo di sicurezza e sincronizzare i dati con l'applicazione presente sul proprio dispositivo mobile.

La guida che segue vuole essere un supporto all'utente che si trova alle prime armi con l'utilizzo di una strumentazione come la seguente.

Si andranno a descrivere i vari passaggi che l'utente dovrà eseguire per sfruttare al meglio l'applicazione. Grazie all'utilizzo di grafici e immagini illustrative si vuole raggiungere una più vasta gamma di utenti, supportandoli nella gestione e nell'utilizzo dell'applicazione web mail.

Servizio webmail:

IMC Webmail

Lo strumento principale per il servizio di posta elettronica è l'applicazione web mail; che nel sistema in esame prende nome di: **IMC WebMail**.

L'applicazione WebMail è sviluppata da parte di *I.M. Consulting* per supportare le aziende nella comunicazione di informazioni tramite lo scambio di mail.

Accedendo con un proprio account, ogni utente ha la possibilità di consultare la propria posta elettronica e comunicare con gli altri in qualsiasi posto si trovi.

Grazie infatti al collegamento in rete, il sistema offre una rete di organizzazione dei dati sicura e affidabile.

Ogni azienda che usufruisce del servizio avrà diritto ad una sezione riservata della piattaforma e ad uno spazio di archiviazione presso gli archivi centralizzati.



Figura 5 - IMC Webmail - Login

Come ottenere l'applicazione web?

Un'azienda o un singolo utente interessato al servizio web di posta elettronica, può inviare una richiesta alla società fornitrice; la quale si occuperà di supportare il nuovo cliente: dalla fase iniziale di impostazione degli account fino alla manutenzione del servizio nel tempo.

Applicazione per la generazione di codici OTP: **Google Authenticator**

Un secondo strumento necessario all'utente è l'applicazione responsabile della generazione dei codici di autenticazione e la gestione che ne segue.

Google Authenticator è un'applicazione sviluppata dall'azienda statunitense *Google* come servizio di generazione automatica di token e distribuita come applicazione per i principali sistemi operativi mobile (es. Android e iOS).

Grazie agli algoritmi HOPT e TOTP, l'applicazione genera codici di autenticazione **OTP**, collegandosi alle diverse piattaforme grazie alla scansione di *codici QR code*.

In riferimento all'applicazione WebMail, l'utente ha la possibilità di accedere alle impostazioni di sistema e sincronizzare l'applicazione Google con il servizio web.

Grazie alla scansione del codice QR code, l'utente può visualizzare i codici OTP dall'applicazione Google, sul proprio dispositivo mobile, e inserirli nell'applicazione webmail in fase di autenticazione, durante il login alla propria casella di posta.

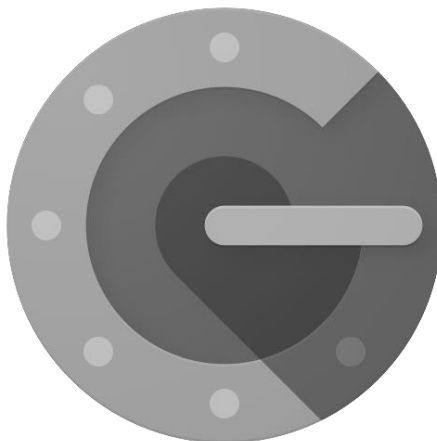


Figura 6 - Applicazione Google Authenticator

Come ottenere l'applicazione mobile?

L'utente ha la possibilità di scaricare l'applicazione *Google Authenticator* da un qualsiasi Play store, accessibile direttamente dal proprio dispositivo.

Avviando una ricerca per nome, l'utente può scaricare il generatore e installarlo sul proprio dispositivo.

In questo modo, ogni volta che vorrà accedere alla propria casella di posta elettronica sul web, visualizzerà il nuovo codice, generato all'occorrenza dall'applicazione.

Plugin di Autenticazione a 2-Step :

RoundCube

Un ultimo strumento fondamentale per la nuova applicazione web è il plugin **RoundCube**.

Ad esso è affidata la responsabilità di gestire la nuova modalità di autenticazione con l'inserimento delle informazioni in due passaggi: username e password seguiti dal codice OTP.

L'obiettivo è quello di mantenere alta la sicurezza dei dati per ogni utente, limitando sempre più il rischio di intromissioni da parte di chi non è autorizzato.

L'accesso quindi ad ogni piattaforma, e più in particolare di una webmail, prevede un processo di autenticazione, nel quale l'utente deve certificare la propria personalità.

Grazie al plugin *RoundCube* il processo risulta ancora più raffinato grazie all'introduzione di un nuovo passaggio.

In riferimento all'applicazione web in esame l'utente sarà chiamato a:

- a. Indicare il proprio *username* seguito da una *password*
- b. Se confermati come corretti da parte del sistema, quest'ultimo richiede l'inserimento di un *codice OTP*. Un codice di autenticazione a sei cifre generato in modo automatico dal sistema e visualizzato dall'utente sulla piattaforma di Google Authenticator.



Figura 7 - Plugin di autenticazione RoundCube

Come ottenere l'applicazione mobile?

Ogni utente, in possesso di un profilo sulla casella di posta IMC WebMail, ha la possibilità di attivare il plugin *RoundCube*, e con lui lo strumento di autenticazione a 2-step, in ogni momento.

Visualizzando la pagina di impostazioni del sistema può selezionare la voce "*Verifica in 2-step come Google*" dal menu di navigazione.

Qui, l'utente visualizza un flag "*Attiva*", selezionando il quale attiva il servizio di autenticazione.

Una volta salvate le modifiche, al successivo accesso, l'utente noterà l'attivazione del servizio di autenticazione a 2-step mediante la richiesta del codice OTP da parte del sistema.

MANUALE ISTRUZIONI:

IMC WebMail con Autenticazione a 2-Step

Con lo sviluppo dell'applicazione IMC WebMail, l'azienda offre ad ogni cliente la possibilità di gestire la comunicazione con i propri clienti in modo funzionale.

Ogni utente possiede un account personale e ad ogni azienda è riservato uno spazio di archiviazione presso i sistemi centralizzati.

Grazie alla nuova versione dell'applicazione, l'utente non solo ha la sicurezza di utilizzare un sistema efficiente ma anche sicuro ed affidabile.

Grazie all'introduzione del metodo di autenticazione, per ogni account di posta elettronica viene diminuito il rischio di accesso da parte di enti non autorizzati. Aumenta, nello stesso tempo, la certezza di sapere chi usa lo strumento.

Nel capitolo seguente si vuole concentrare l'attenzione sulla parte che riguarda la nuova modalità di accesso di un utente tramite la sua autenticazione certificata.

Ci si vuole soffermare sulla descrizione accurata dei passaggi da seguire, aiutandosi con illustrazioni e diagrammi.

Per una descrizione più ampia sulle funzionalità dell'applicazione web per la posta elettronica si rimanda a un manuale specifico.

Come autenticarsi sul sistema?

Come viene descritto nelle sezioni precedenti, l'autenticazione di un utente sul sistema di webmail avviene in due passaggi:

1. USERNAME + PASSWORD

Una volta avviata l'applicazione web, il sistema mostra una prima pagina di login.

In essa richiede all'utente di inserire il proprio username identificativo e indicare una password per la certificazione.

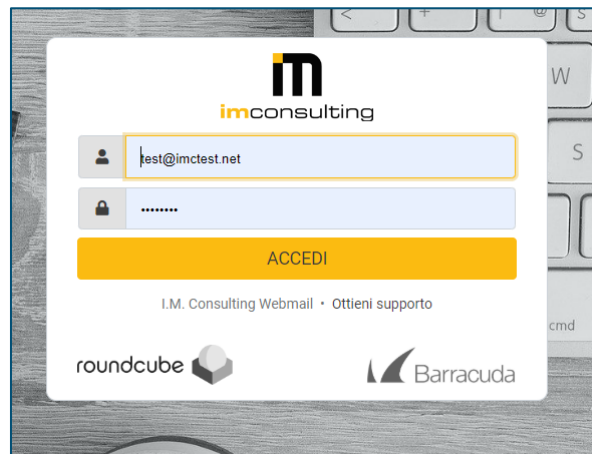


Figura 8 - Primo step: Login con username e password

In un secondo passaggio, il sistema verifica la correttezza dei dati ricevuti: controllando la validità dello username e se la password inserita corrisponde al profilo indicato.

Nel caso in cui:

- a. I dati vengano accertati, il primo passaggio di autenticazione risulta confermato e viene mostrata una nuova pagina di richiesta.

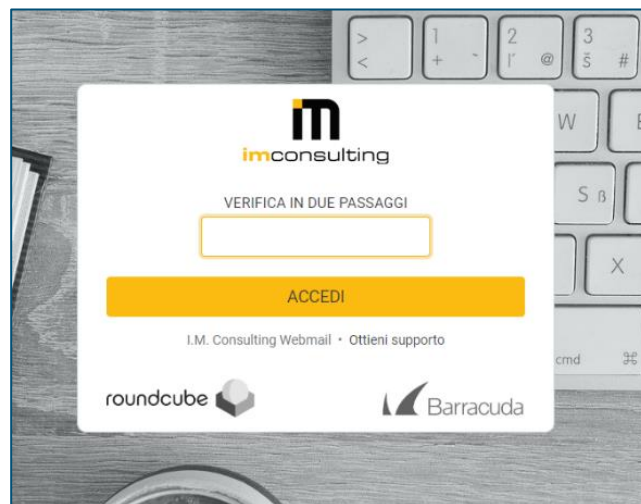


Figura 9 - Secondo step: Login con codice OTP

- b. In caso contrario il sistema notifica l'utente con un messaggio di errore. Quest'ultimo sarà costretto a controllare i dati inseriti e apportare le dovute modifiche.

Nel momento in cui l'errore dovesse persistere, il sistema è pensato per verificare la corretta personalità dell'utente, inserendo un'ulteriore test **CAPTCHA** (*Completely Automated Public Turing test to tell Computers and Humans Apart*). Un test pubblico eseguito dal sistema per capire se l'utente sia un'entità umana oppure un computer.

In questi casi viene integrato come strumento di difesa nei confronti di programmi conosciuti come *bot*. Applicazioni dannose che cercano di attaccare i siti online attraverso form di inserimento dati come quello in esame.

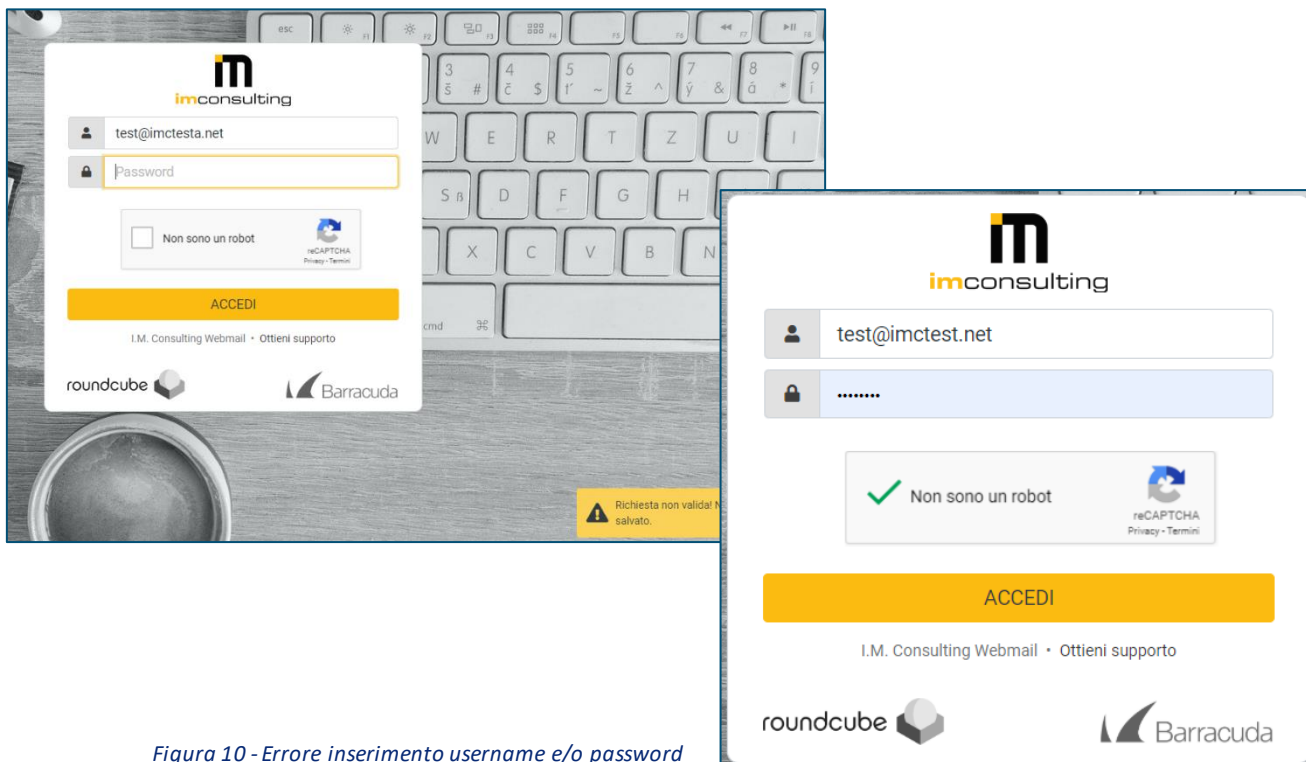


Figura 10 - Errore inserimento username e/o password

2. CODICE OTP

Il secondo passaggio per una corretta autenticazione vede protagonista un *codice OTP*.

L'acronimo di *One Time Password*, indica una password generata come codice numerico dal sistema per essere utilizzata solo una volta.

A differenza della password statica, il codice OTP viene generato come *nuovo* ogni volta che l'utente vuole eseguire l'accesso nel sistema. Una volta utilizzato, infatti, la chiave numerica non potrà più essere riutilizzata, garantendo così una buona sicurezza ed evitando possibili repliche e spiacevoli inconvenienti.

In particolare:

- a. L'utente accede all'applicazione *Google Authenticator* tramite il proprio dispositivo mobile;

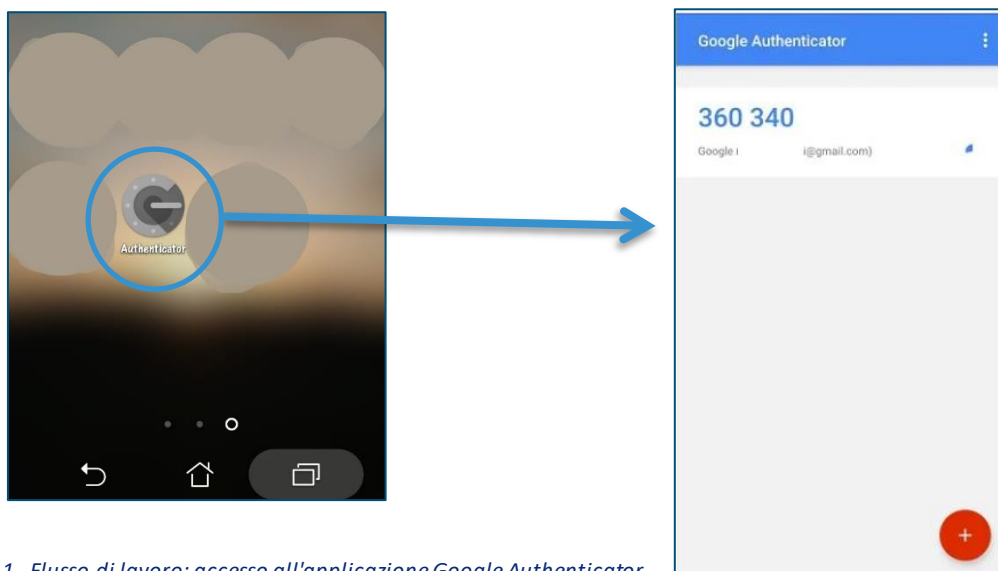


Figura 11 - Flusso di lavoro: accesso all'applicazione Google Authenticator

- b. Visualizza il codice OTP auto generato dal sistema;

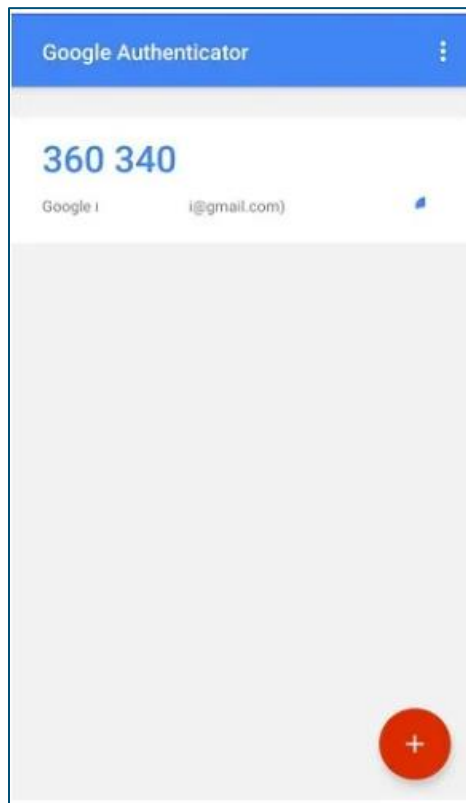


Figura 12 - Flusso di lavoro: visualizzazione del codice OTP

- c. Inserisce il codice numerico a sei cifre sul form presente nella pagina web di login;

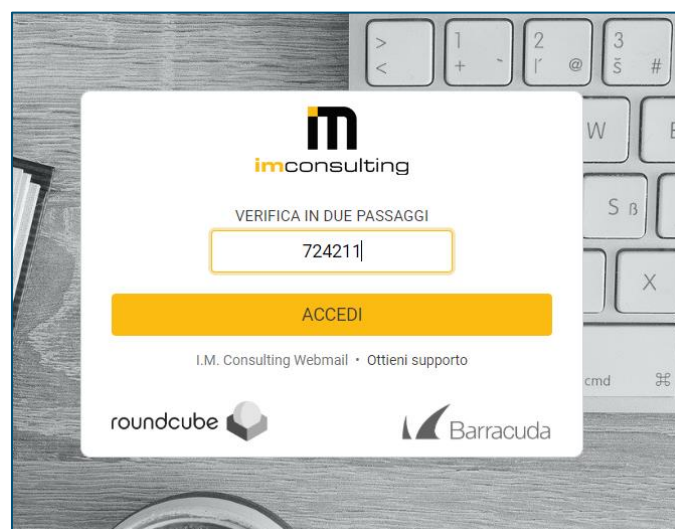


Figura 13 - Flusso di lavoro: Login con codice OTP

- d. Il sistema ha il compito di verificare la correttezza del codice rispetto ai dati personali dell'utente inseriti durante il primo passaggio.

- e. In caso di conferma, il sistema abilita all'utente l'accesso alla propria applicazione webmail. In caso contrario, verrà richiesto nuovamente l'inserimento dei dati corretti.

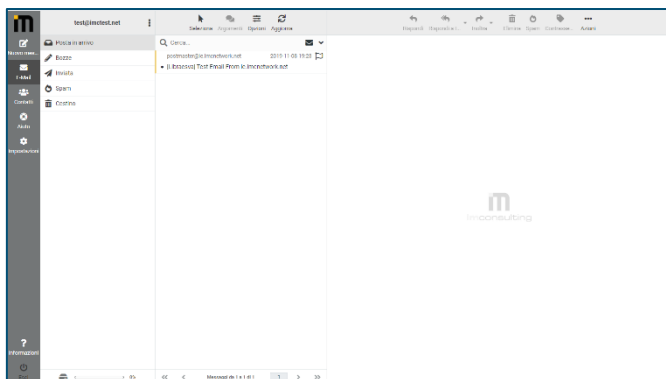


Figura 15 - Flusso di lavoro: Conferma codice OTP corretto



Figura 14 - Flusso di lavoro: Errore inserimento codice OTP

Una volta completato con successo l'autenticazione, il login può considerarsi concluso. L'utente può quindi accedere alla propria casella di posta e sfruttare la suite di funzionalità offerte.

Come configurare il metodo di autenticazione per codice OTP?

Per poter utilizzare al meglio la modalità di autenticazione a 2-step è necessario apportare alcune modifiche al sistema di posta elettronica web.

Seguendo qualche accortezza sarà possibile utilizzare agevolmente lo strumento, rendendo l'intero sistema molto più efficiente.

1) SCARICARE APPLICAZIONE GOOGLE AUTHENTICATOR

Come prima cosa è necessario scaricare l'applicazione per la generazione di codici OTP, che, come descritto in precedenza, prende il nome di **Google Authenticator**.

Seguendo una semplice sequenza di passaggi l'utente è in grado di scaricare e installare l'applicazione sul proprio dispositivo mobile.

In particolare:

- 1) Accede alla piattaforma **Play Store** presente sul proprio dispositivo (riconoscibile dal logo come il seguente)



Figura 16 - Logo Google Play Store

2) Effettua il login, inserendo i propri dati, e si autentica come utente Google

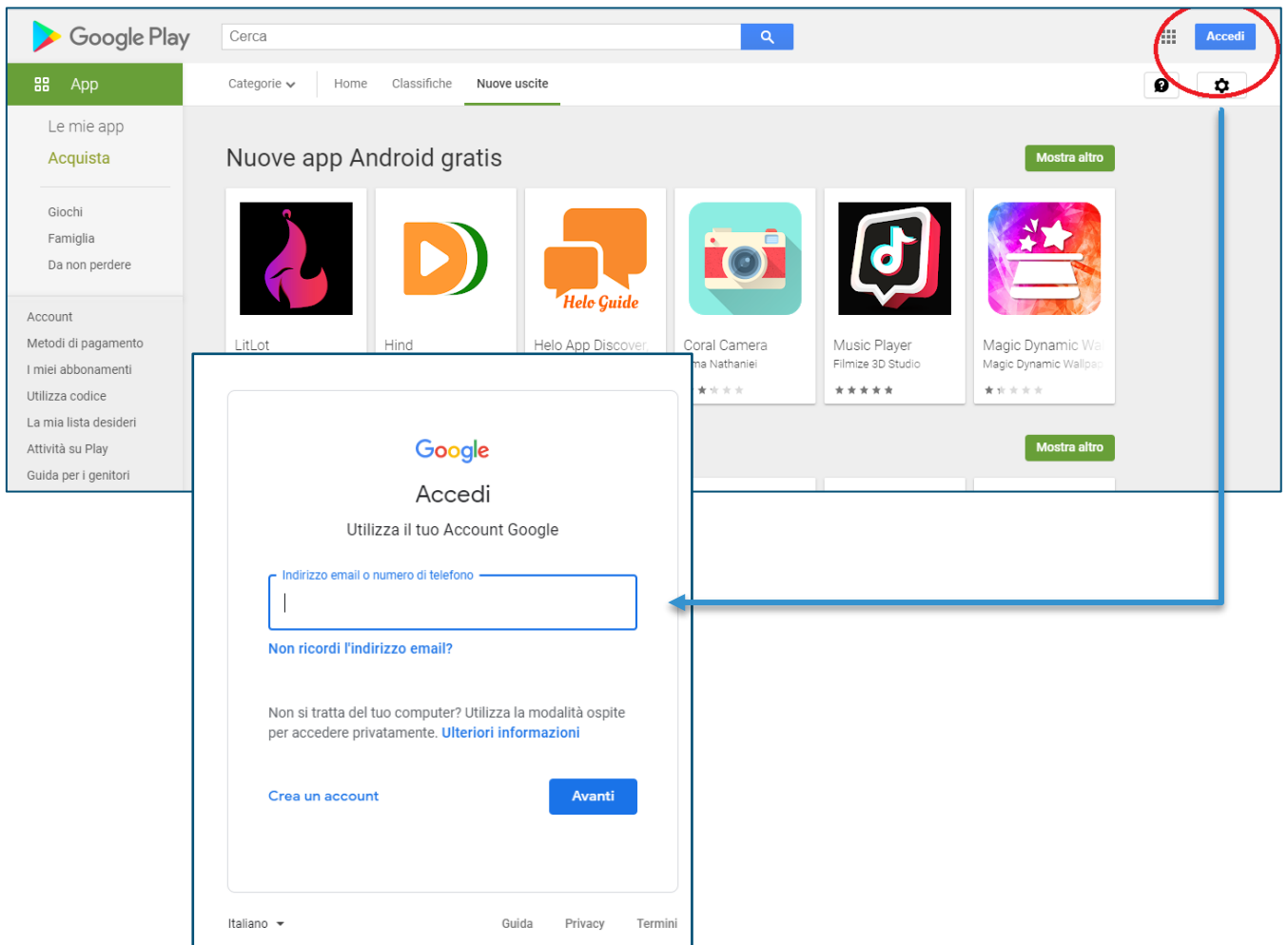


Figura 17: Flusso di lavoro: Accesso a Google Play Store

3) Avvia una ricerca tra le applicazioni con il nome "Google Authenticator"

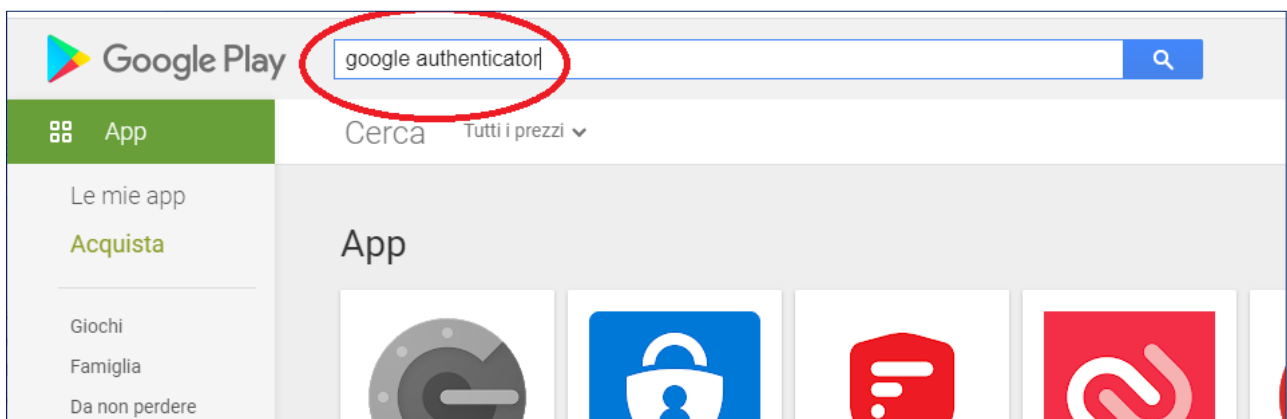


Figura 18 - Flusso di lavoro: Ricerca applicazione

4) Seleziona l'omonima applicazione dalla griglia dei risultati della ricerca

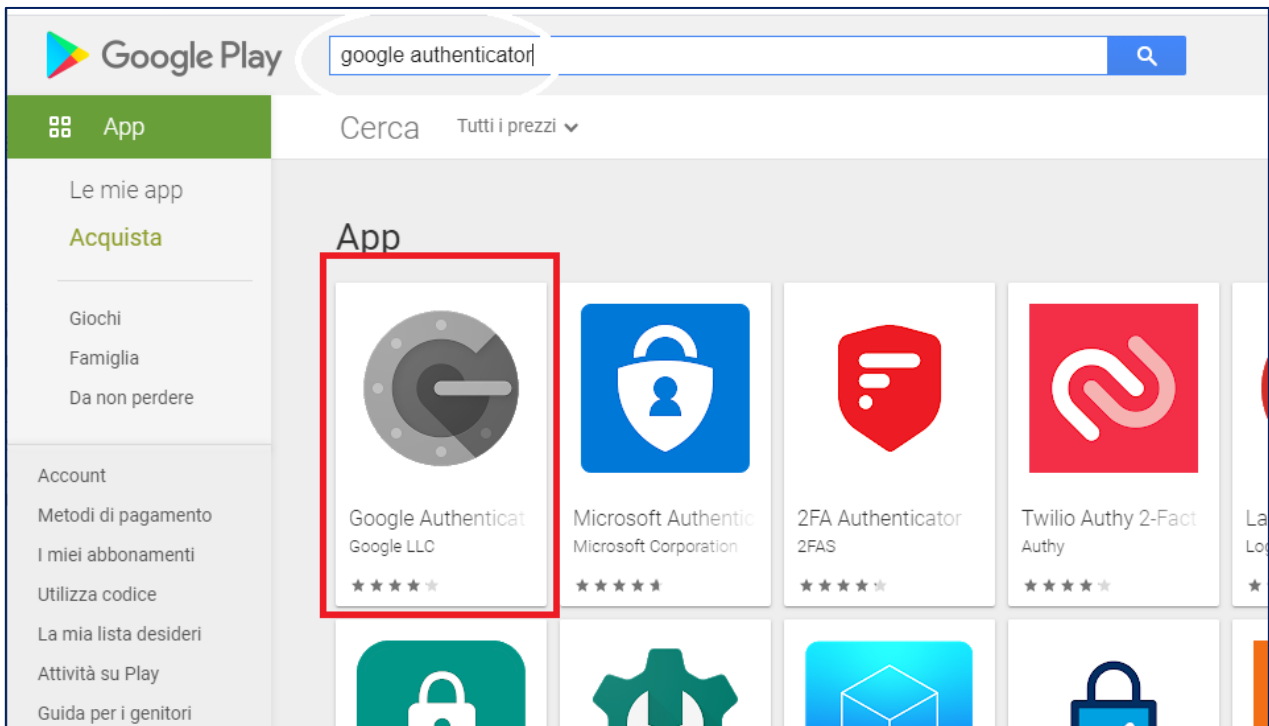


Figura 19 - Flusso di lavoro: Selezione applicazione come risultato della ricerca

5) Visualizzata la pagina profilo dell'applicazione Google Authenticator

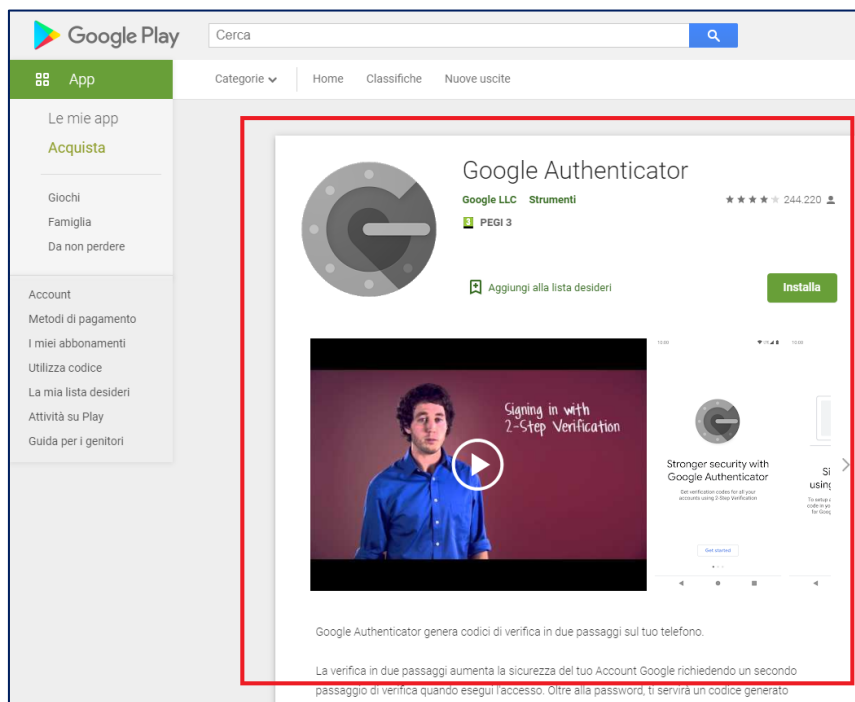


Figura 20 - Flusso di lavoro: Visualizzazione profilo applicazione

- 6) L'utente seleziona il bottone **"Installa"**, per avviare il download e l'installazione dell'applicazione, e attende il completamento dell'operazione

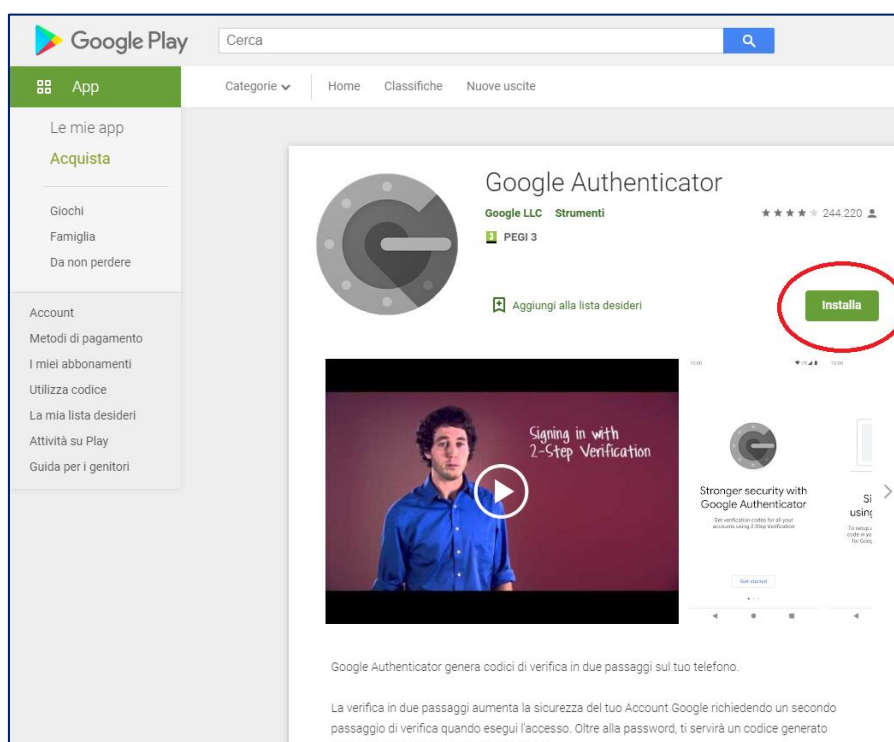


Figura 21 - Flusso di lavoro: Installazione applicazione

Nel caso in cui l'utente non sia loggato correttamente, il sistema lo invita, con un messaggio a video, a procedere con l'autenticazione prima di poter procedere all'installazione dell'applicazione.

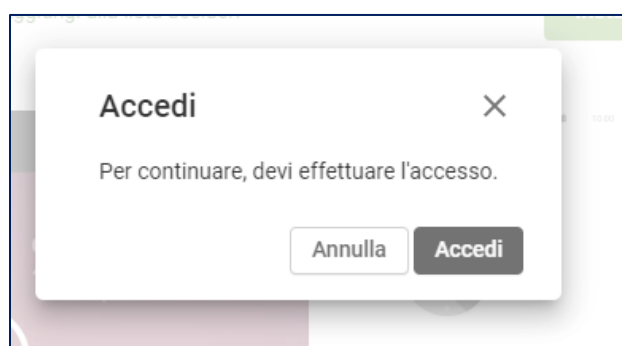


Figura 22 - Flusso di lavoro: Errore di mancato accesso alla piattaforma

- 7) Una volta completato con successo l'installazione, il sistema offre la possibilità di aprire l'applicazione sul proprio dispositivo e avviare le procedure di gestione codici.

2) CONFIGURARE AUTENTICAZIONE 2-STEP

Una volta in possesso dell'applicazione per la generazione dei codici OTP, l'utente può proseguire con la modifica delle impostazioni sulla propria casella di posta elettronica web e infine, con la sincronizzazione dei dati tra le due applicazioni in uso.

Come per il passo precedente, l'utente è chiamato a seguire una sequenza di passaggi semplici, allo scopo di rendere la propria interoperabilità con l'applicazione ancora più sicura ed efficiente.

- 1) Per prima cosa accede al proprio profilo inserendo il proprio **nome utente** e **password**.

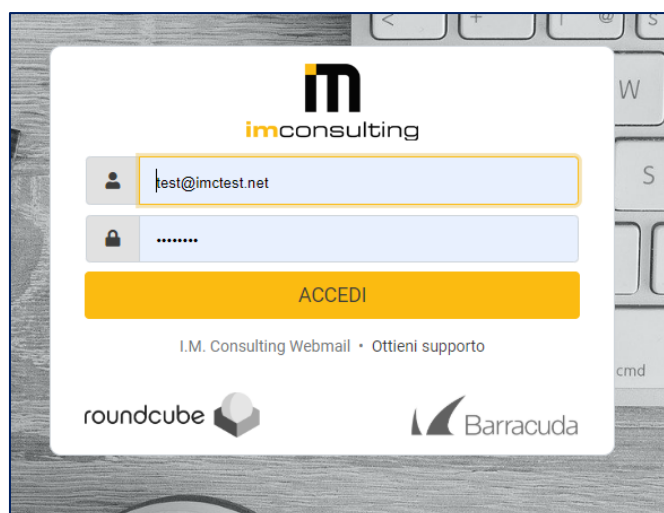


Figura 23: Flusso di lavoro: Login a IMC WebMail

- 2) Una volta visualizzata la pagina iniziale dell'applicazione web concentra l'attenzione sul menù di navigazione posto nella parte laterale della maschera.

Selezionando la voce di menu "**Impostazioni**" visualizza una nuova pagina web dove sono riportate tutte le impostazioni di sistema, personalizzate secondo le necessità dell'utente che ne fa uso.

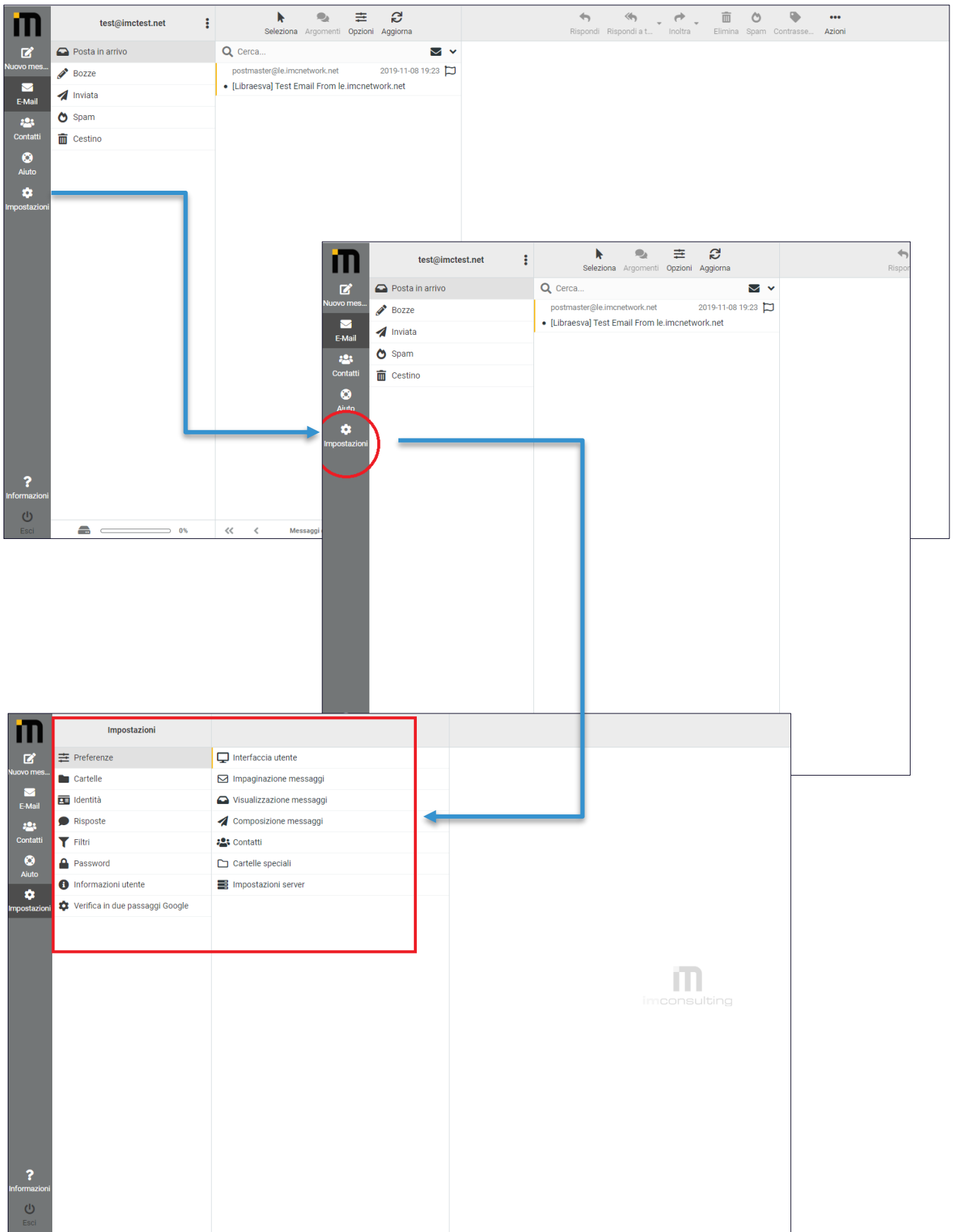


Figura 24 - Flusso di lavoro: pagina "impostazioni" piattaforma

3) Nel menu di navigazione laterale l'utente seleziona la voce **“Verifica in 2-step come Google”** e visualizza una nuova pagina web per l'impostazione dei metodi di autenticazione.

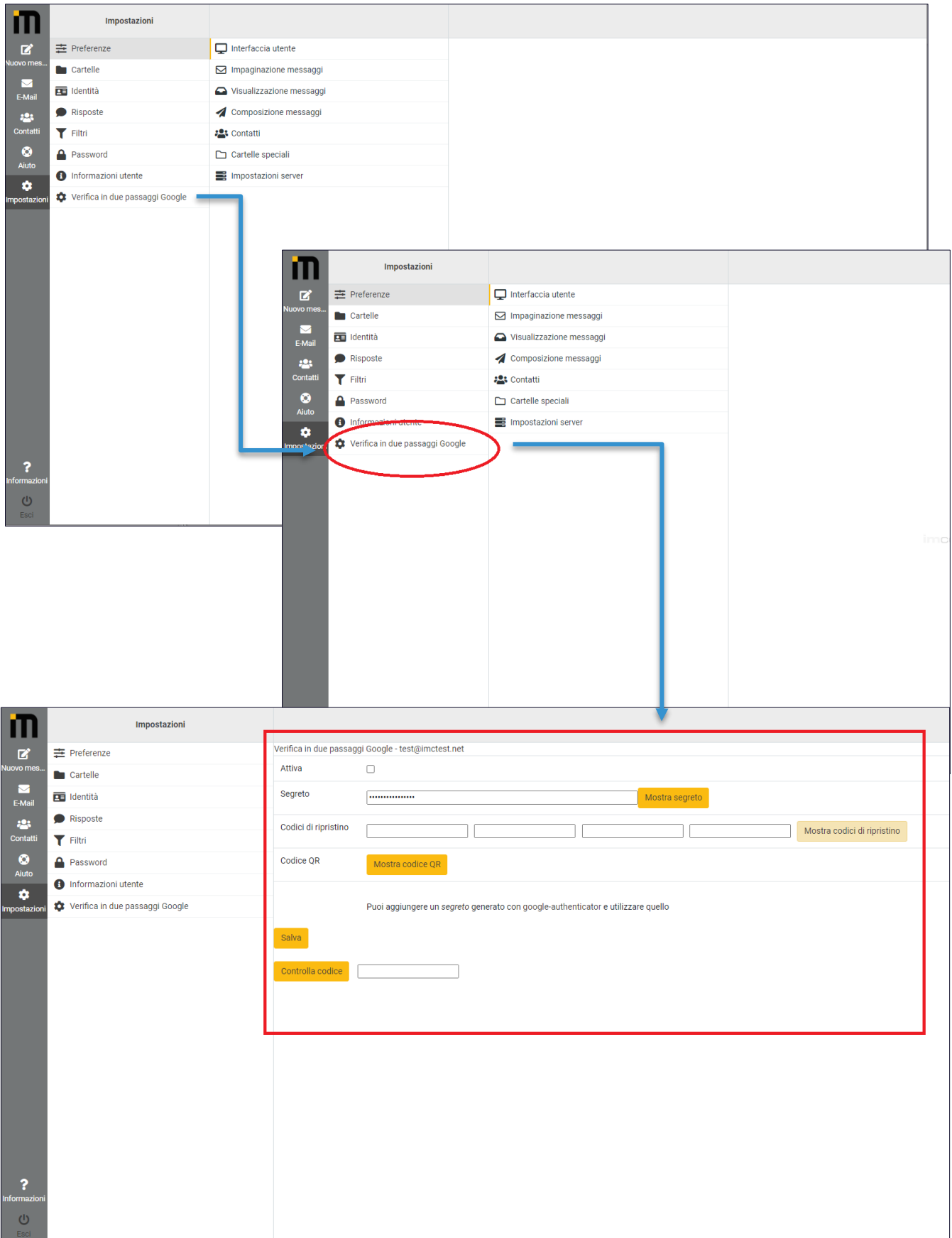
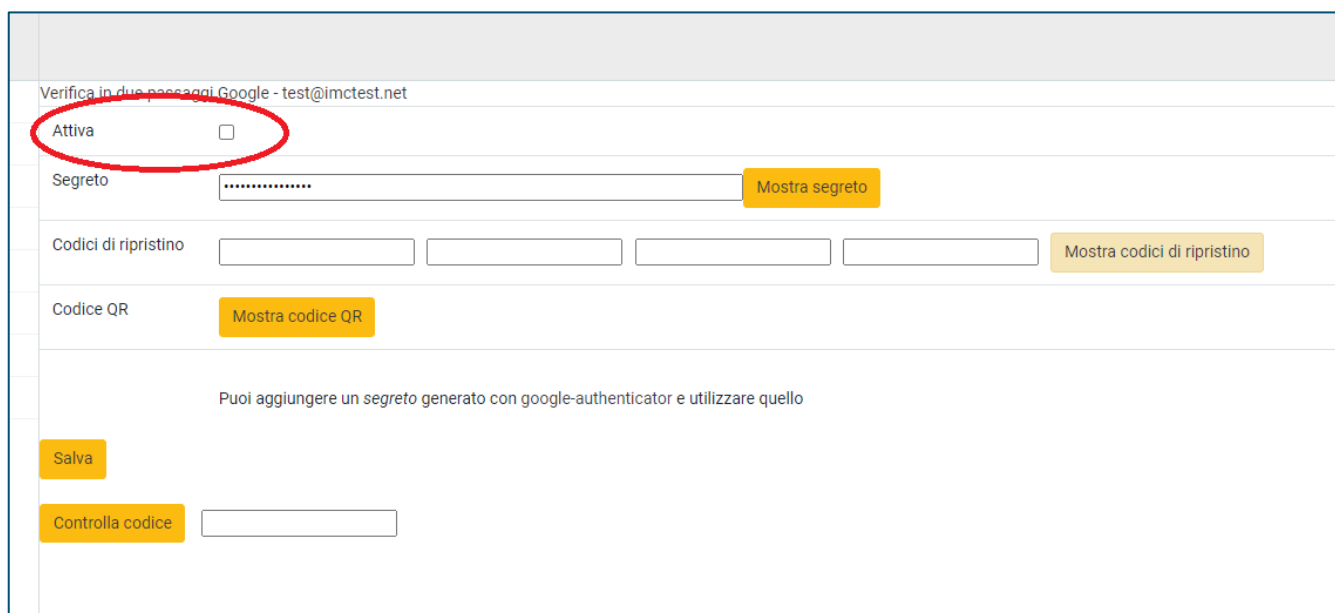


Figura 25 - Flusso di lavoro: Pagina "Verifica in 2-step come Google"

- 4) A questo punto l'utente è in grado di attivare la modalità di autenticazione in 2-step e personalizzare il proprio profilo.

Come per le impostazioni generali dell'account, segue un procedimento a step che vede il susseguirsi di un insieme di operazioni fondamentali che l'utente è chiamato a eseguire in sequenza.

- A. Seleziona il flag "**Attiva**" come vero, per attivare il servizio di autenticazione a 2-step



Verifica in due passaggi Google - test@imctest.net

Attiva

Segreto Mostra segreto

Codici di ripristino Mostra codici di ripristino

Codice QR Mostra codice QR

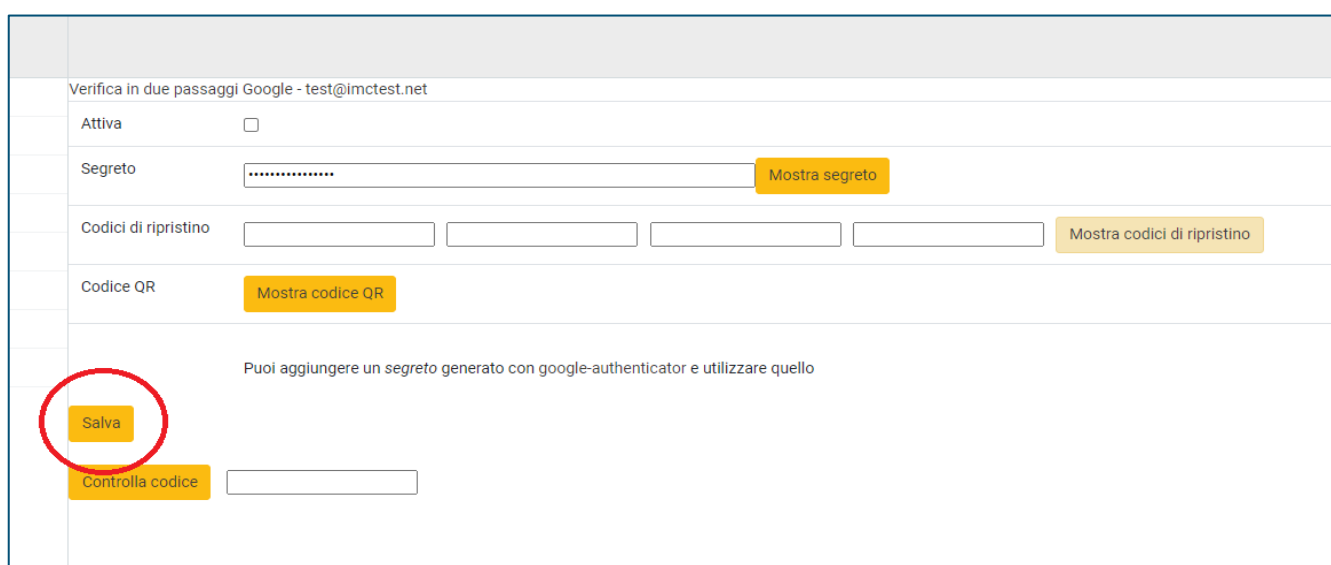
Puoi aggiungere un segreto generato con google-authenticator e utilizzare quello

Salva

Controlla codice

Figura 26 - Flusso di lavoro: Attivazione servizio di autenticazione

- B. Salva la modifica di impostazione selezionando l'omonimo bottone "**Salva**"



Verifica in due passaggi Google - test@imctest.net

Attiva

Segreto Mostra segreto

Codici di ripristino Mostra codici di ripristino

Codice QR Mostra codice QR

Puoi aggiungere un segreto generato con google-authenticator e utilizzare quello

Salva

Controlla codice

Figura 27 - Flusso di lavoro: Salvataggio modifiche

C. Una volta completato con successo il salvataggio dei dati, il sistema notifica l'utente con un messaggio in fondo alla pagina.

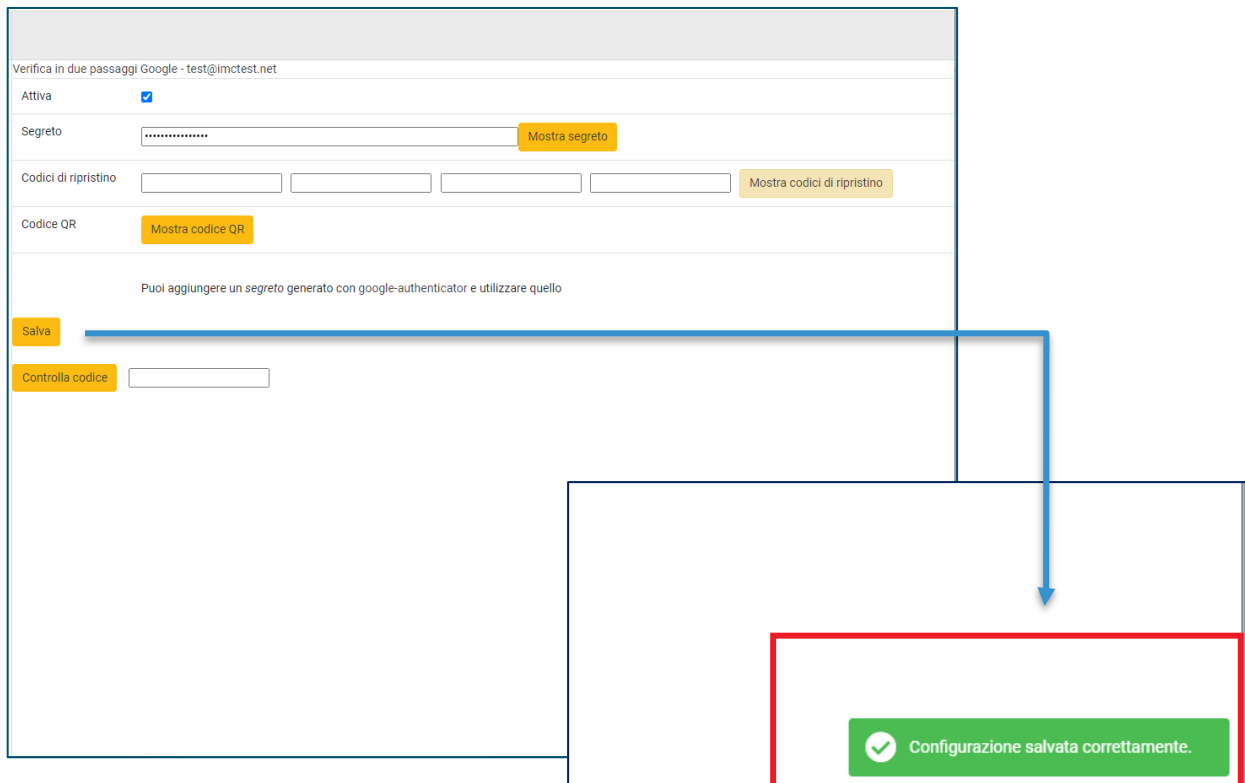


Figura 28 - Flusso di lavoro: Messaggio di conferma salvataggio

D. L'utente seleziona il bottone **"Genera Segreto"** per generare un nuovo codice. In risposta, il sistema genera un codice alfanumerico e, in corrispondenza, crea un codice QR code, notificando l'utente mediante l'abilitazione dell'omonimo bottone. Lasciato inizialmente offuscato, l'utente ha la possibilità di visualizzare i codici una volta selezionato il bottone **"Mostra segreto"** e **"Mostra codice QR"**.

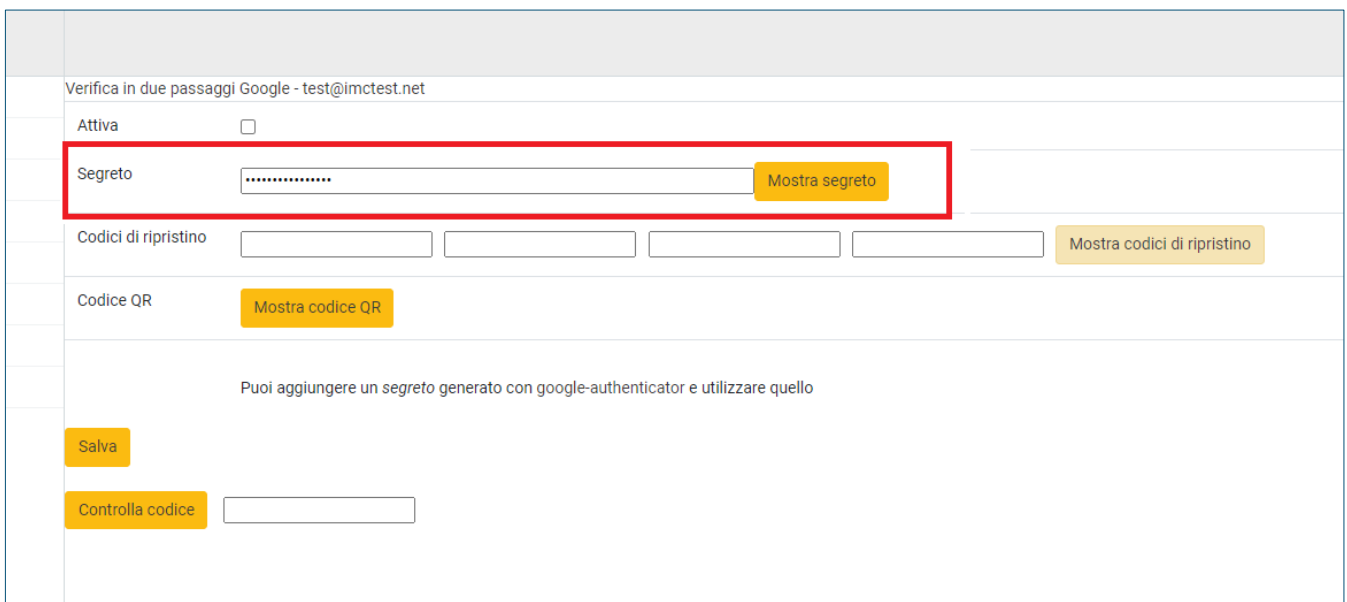


Figura 29 - Flusso di lavoro: Generazione codice segreto

Verifica in due passaggi Google - test@imctest.net

Attiva

Segreto Mostra segreto

Codici di ripristino Mostra codici di ripristino

Codice QR Mostra codice QR

Puoi aggiungere un segreto generato con google-authenticator e utilizzare quello

Salva

Controlla codice

Figura 30 - Flusso di lavoro: Generazione codice QR code

- E. Selezionando il bottone “**Mostra codice QR**”, l’utente visualizza il codice QR code generato in corrispondenza del codice segreto di cui si fa riferimento al punto precedente


Verifica in due passaggi Google - test@imctest.net

Attiva

Segreto Mostra segreto

Codici di ripristino Mostra codici di ripristino

Codice QR Nascondi codice QR



Puoi aggiungere un segreto generato con google-authenticator e utilizzare quello

Salva

Controlla codice

Figura 31 - Flusso di lavoro: Visualizzazione codice QR code

F. L'utente accede all'applicazione **Google Authenticator** dal proprio dispositivo mobile

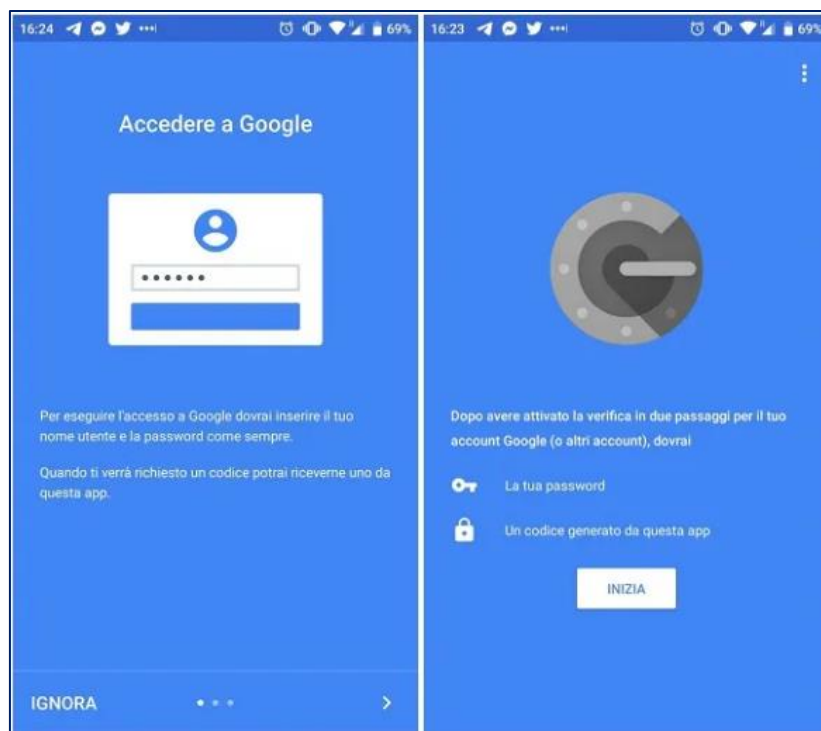


Figura 32 - Flusso di lavoro: Accesso all'applicazione Google Authenticator

G. Selezionando il bottone “+” attiva la sincronizzazione con una nuova piattaforma

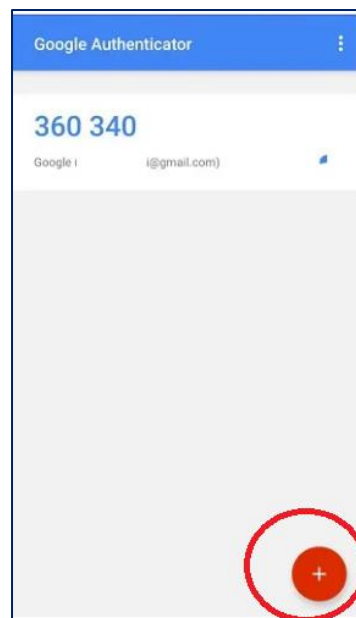


Figura 33 - Flusso di lavoro: Attivazione nuova sincronizzazione

H. Selezionando la voce “**Scansione Nuovo QR code**” l'utente avvia una nuova scannerizzazione. Il sistema mostra sul dispositivo uno scanner e un insieme di istruzioni da seguire: inquadrando con la propria fotocamera il QR code riportato sulla pagina web, il sistema riconosce il codice e abilita la sincronizzazione.

- I. Una volta attivato il servizio, l'applicazione mobile notifica all'utente una nuova sincronizzazione e attiva un nuovo generatore di codici numerici OPT legati al QR appena scansionato

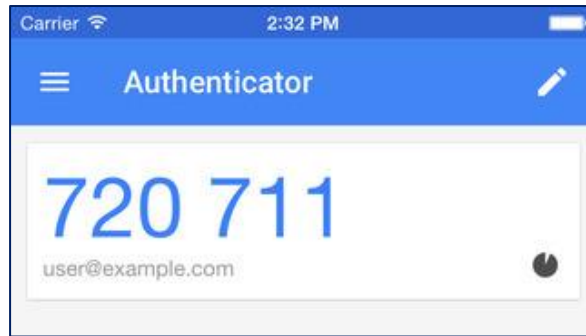



Figura 34 - Flusso di lavoro: Generazione codice OTP

Accanto al codice un simbolo dinamico notificherà all'utente il tempo rimanente per l'utilizzo del codice, al termine del quale quest'ultimo verrà cancellato e sostituito con un nuovo.

- J. Per verificare la correttezza e accertarsi che il collegamento tra i dispositivi sia concluso con successo, l'utente può riportare nella pagina web il codice indicato dall'applicazione Google.

-  Selezionando il bottone **“Verifica Codice”**, il sistema notificherà se il collegamento tra le due applicazioni risulta effettivamente attivo.

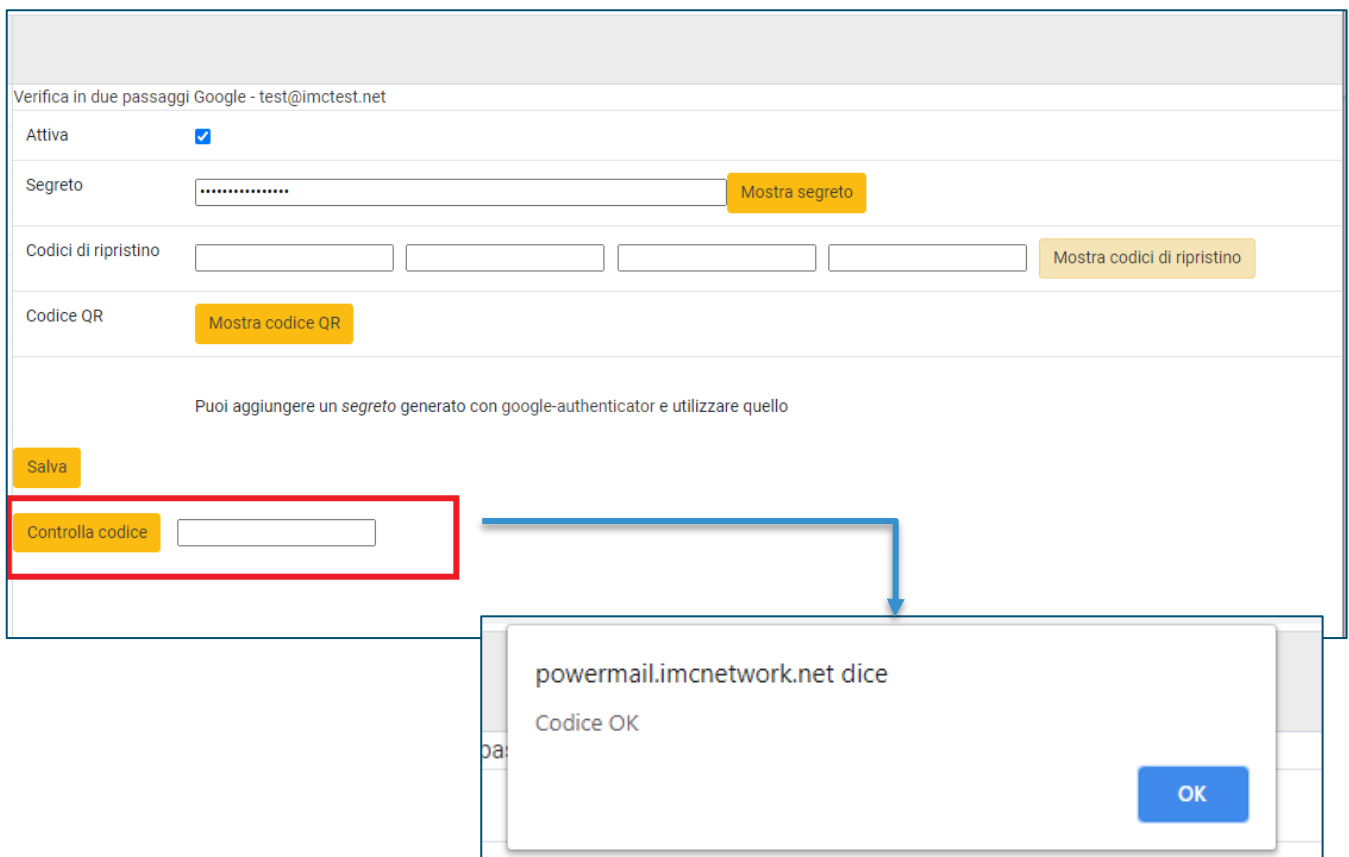


Figura 35 - Flusso di controllo: Verifica codice OTP generato

Procedendo in questo modo, dal prossimo accesso alla piattaforma web, ogni qualvolta che l'utente esegue il login alla propria casella di posta mediante l'applicazione webmail, il sistema richiederà dapprima uno username seguito da una password; e in un secondo momento il codice generato dall'applicazione Google.

In questo modo si avrà sempre la certezza di avere una corretta gestione della casella di posta e un utilizzo dei dati affidabile da parte dell'utente.



Figura 36 - Flusso di lavoro: Login a IMC WebMail con autenticazione a 2-step

Come annullamento del metodo di autenticazione a 2-step?

L'utente avrà sempre la possibilità di annullare la modalità di autenticazione in 2-step e riportare l'applicazione web alle impostazioni originali.

Ripercorrendo la sequenza di operazioni:

- a. nella pagina **Impostazioni** → **Verifica in 2-step come Google l'utente**
- b. disabilita il flag "**Attiva**"
- c. e salva le modifiche selezionando il bottone "**Salva**".

In questo modo, una volta che l'utente esegue nuovamente il login alla piattaforma webmail, il sistema non richiederà più l'autenticazione tramite codice OTP, ma semplicemente il nome utente seguito dalla password.

Come modificare il codice QR code?

In caso di necessità, l'utente ha la possibilità di modificare il codice segreto e generare un nuovo codice QR code.

Onde evitare spiacevoli conseguenze, è importante che questi segua una sequenza di operazioni semplici:

- a. nella pagina **Impostazioni** → **Verifica in 2-step come Google l'utente**
- b. seleziona e cancella il codice segreto da modificare
- c. seleziona il bottone "**Genera un nuovo codice segreto**"
- d. salva le modifiche selezionando il bottone "**Salva**"
- e. visualizza il nuovo codice QR code selezionando il bottone "**Mostra codice QR**" ed esegue nuovamente la scannerizzazione mediante l'applicazione mobile Google Authenticator
- f. Verifica la correttezza del codice: riportandolo nella casella di testo sulla pagina web e selezionando il bottone "**Verifica codice**"
- g. In caso di conferma da parte del sistema, il codice è stato modificato con successo e potrà essere utilizzato fin dal prossimo accesso alla piattaforma.

Possibili errori generati dall'utente

Durante la gestione della piattaforma webmail e in particolare nella fase di impostazione dei metodi di autenticazione possono verificarsi alcuni errori legati spesso all'inesperienza dell'utente.

Errore nell'inserimento delle credenziali

Si verifica quando l'utente inserisce un nome utente e/o una password errati. In questi casi il sistema annulla l'operazione e segnala l'errore all'utente invitandolo ad inserire una sequenza di dati corretta. Nel caso in cui l'errore persista, il sistema inserisce un doppio controllo, attraverso un codice detto **CAPTCHA**, studiato per verificare la corretta identità dell'utente (se umana o meccanica), allo scopo di evitare intromissioni e danneggiamenti al sistema.

Errore nell'inserimento del codice OPT

Un secondo caso può verificarsi quando un utente inserisce un codice OPT errato. A causa di poca attenzione oppure di latenza nell'inserimento di un codice numerico già scaduto.

In questi casi il sistema notifica l'errore all'utente annullando l'operazione e riavviando l'intera procedura di autenticazione.

Esso mostra nuovamente la pagina iniziale invitando: l'utente ad inserire ancora una volta le proprie credenziali e l'applicazione Google a generare un nuovo codice OPT.

Errore nella gestione del codice QR code

Può capitare che l'utente modifichi erroneamente il codice QR code, seguendo in modo non corretto la sequenza di operazioni per l'impostazione del metodo di autenticazione a 2-step.

L'errore causa un danneggiamento al collegamento tra le due applicazioni con ripercussione sul buon funzionamento dell'intero sistema.

L'utente non sarà più in grado, infatti, di svolgere correttamente l'accesso alla piattaforma a causa della mancata corrispondenza tra l'applicazione web e il codice OPT generato dall'applicazione mobile. Sarà quindi invitato a contattare l'azienda produttrice e richiedere un intervento mediante Help Desk.

SINCRONIZZAZIONE TRALE DUE VERSIONI

Al termine del processo di strutturazione della nuova WebMail, l'utente è chiamato a personalizzare la propria casella di posta secondo le proprie esigenze e all'ambiente di lavoro.

Non garantendo una compatibilità tra le due versioni, il sistema specifica che tutte le eventuali personalizzazioni (come: impostazioni di visualizzazione, rubriche, firma ecc.), che l'utente ha impostato sulla versione antecedente, non possono essere automaticamente migrate.

Onde evitare il rischio di perdita di dati importanti per l'utente, è possibile equilibrare gli ambienti di lavoro, riportando anche nella nuova versione di posta elettronica le personalizzazioni scelte dall'utente nella versione precedente.

Tra le operazioni più frequenti sviluppate dall'utente durante la fase di sincronizzazione, si ricorda la migrazione di:

- ✚ I contatti di rubrica
- ✚ La firma

Copia dei Contatti in Rubrica

La prima operazione di migrazione prevede la *copia dei contatti presenti in rubrica*.

Allo scopo di limitare il rischio di perdita di dati importanti, l'utente è chiamato a seguire una sequenza di operazioni di esportazione e importazione tra le due diverse caselle di posta.

ESPORTAZIONE

Come prima fase, l'utente è chiamato ad:

- accedere, con il proprio account, alla **vecchia** versione della webmail ed
- esportare il gruppo di contatti che desidera riportare nella nuova versione di posta elettronica.

L'operazione di *esportazione* è composta a sua volta, da una sequenza semplice di funzioni:

- 1) Nel menù di navigazione riportato nella parte in alto della pagina, seleziona la voce **"Rubrica"**



Figura 37 - Flusso di operazioni: migrazione rubrica

- 2) Il sistema mostra una nuova pagina con un menù di navigazione laterale. Le voci riportano la lista di gruppi che compongono l'intera rubrica (per default "Rubrica Personale") dell'utente e in corrispondenza l'insieme di contatti che comprende ogni gruppo.

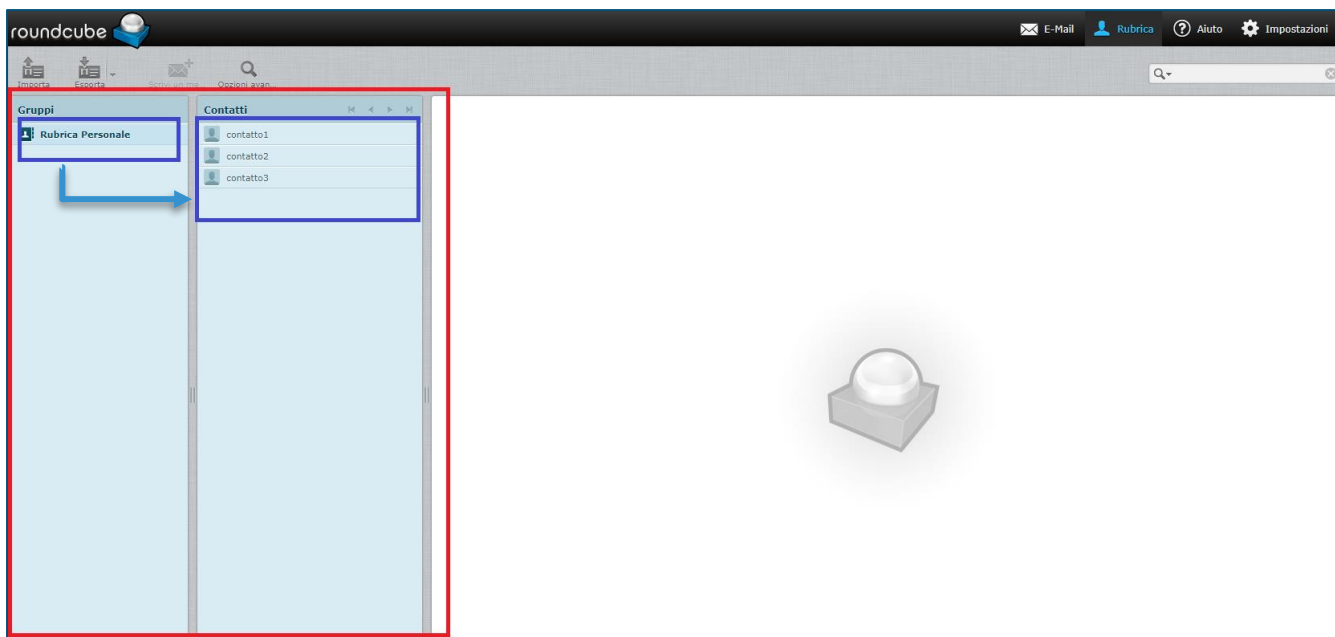


Figura 38 - Flusso di operazioni: migrazione rubrica

Selezionando ogni gruppo, nella prima colonna, il sistema mostra l'insieme dei contatti che questo comprende, nella seconda colonna.

- 3) L'utente seleziona il gruppo di contatti che desidera esportare nella nuova versione di posta elettronica.
- 4) A questo punto, nella parte superiore della scheda viene abilitato un menù di navigazione tra cui l'utente seleziona il bottone "**Esporta**".
In via alternativa, l'utente ha anche la possibilità di esportare interamente l'insieme di tutti i gruppi presenti in rubrica. Espandendo la voce di menu "Esporta" può visualizzare una seconda voce di dettaglio "**Esporta tutto**", con la quale il sistema avvia l'esportazione complessiva dei contatti presenti in rubrica
- 5) Dopo aver settato correttamente le modalità di esportazione, il sistema provvederà a creare un file apposito che l'utente ritroverà nella cartella *Download* presente sul proprio computer.

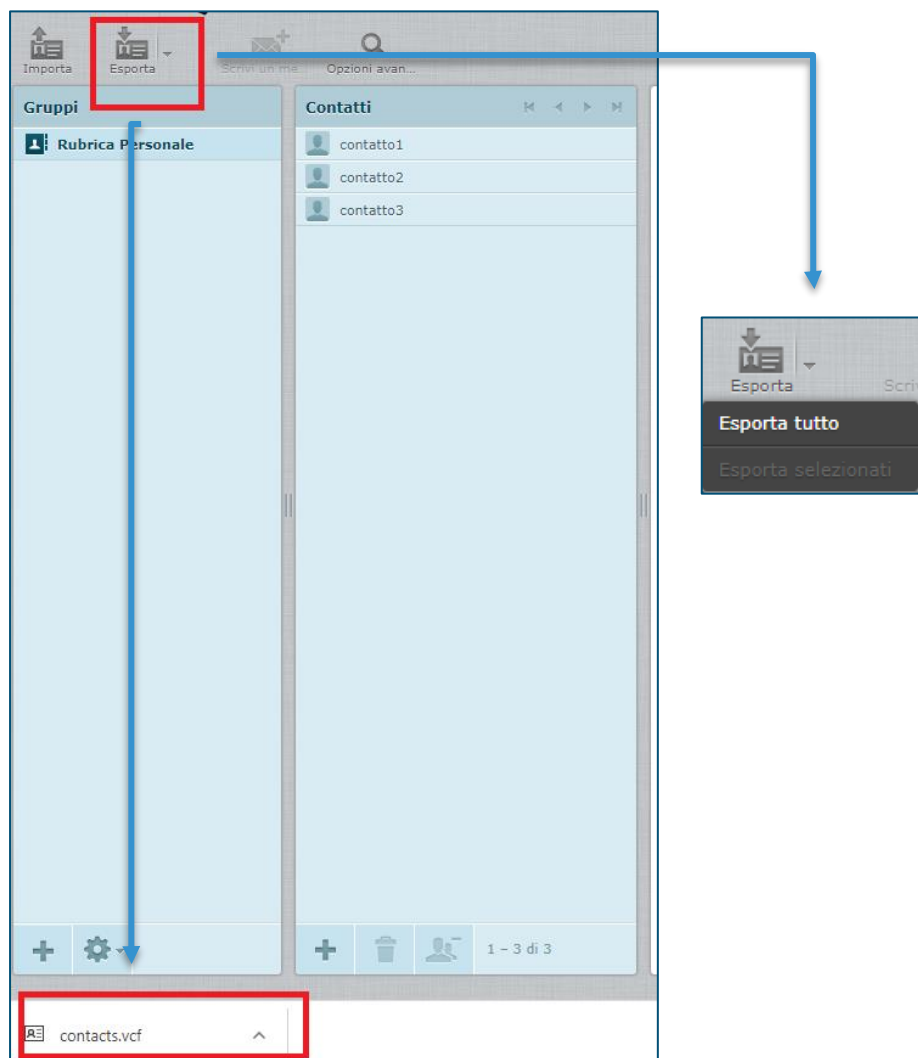


Figura 39 - Flusso di operazioni: esportazione della rubrica

A questo punto l'operazione di esportazione può ritenersi conclusa.

L'utente può proseguire con la seconda operazione che prevede l'utilizzo integrale della versione **nuova** di webmail.

IMPORTAZIONE

Come per l'operazione di esportazione, l'utente è chiamato a seguire una sequenza di attività semplici che permetteranno al sistema di reimpostare le personalizzazioni apportate dall'utente in modo tempestivo ed efficiente.

- 1) Accede alla propria casella di posta nella nuova versione di WebMail, seguendo le procedure esplicitate nei paragrafi precedenti

- 2) Nel menù di navigazione iniziale l'utente seleziona la voce **"Contatti"** e accede alla pagina di personalizzazione della propria casella di posta nella sezione **Rubrica**.

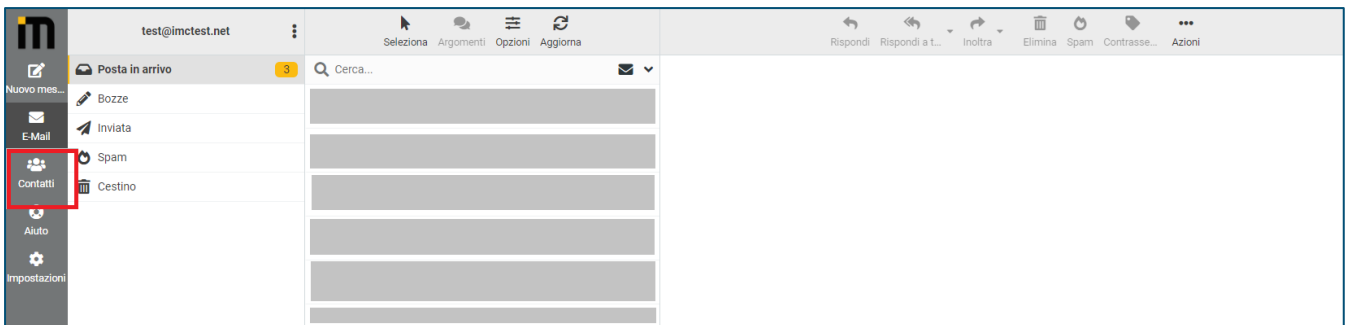


Figura 40 - Flusso di operazioni: Importazione Rubrica

- 3) La struttura tabellare della scheda web è simile a quella proposta nella versione precedente. Il sistema mostra in una prima colonna l'elenco dei gruppi mentre in una seconda la lista di contatti in corrispondenza di ogni insieme.

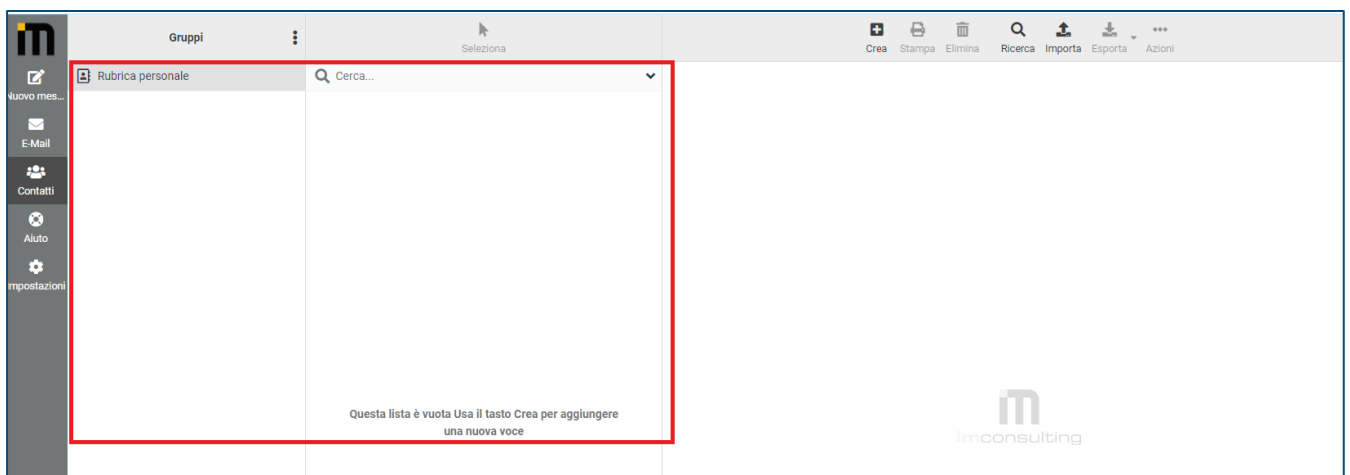


Figura 41 - Flusso di operazioni: Importazione Rubrica

- 4) Nel menù di navigazione presente nella parte iniziale della scheda, l'utente seleziona la voce **"Importa"**

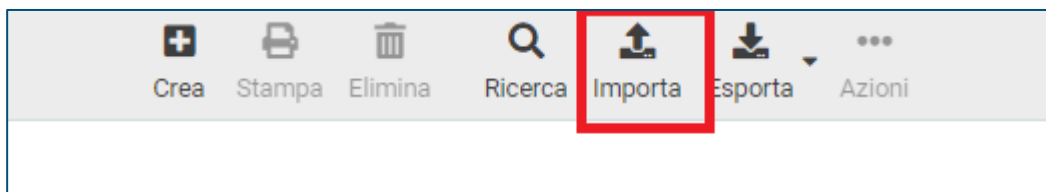


Figura 42 - Flusso di operazioni: Importazione Rubrica

Il sistema richiede di selezionare il file da importare (il documento processato in modo automatico durante la fase di esportazione dei contatti dalla versione precedente della WebMail – vedi paragrafo precedente) e le impostazioni generali per vincolare il processo di personalizzazione.

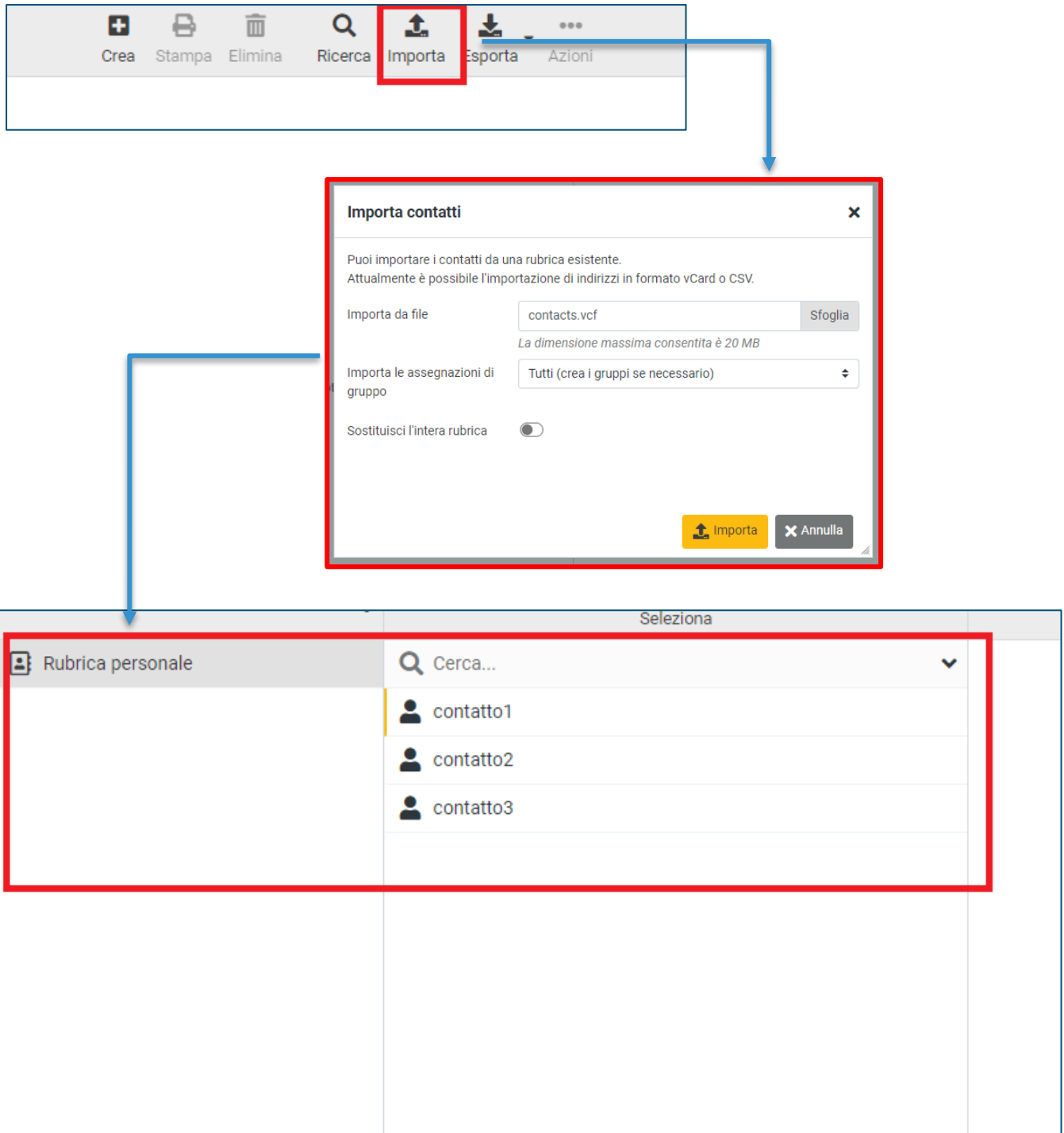


Figura 43 - Flusso di operazioni: Importazione Rubrica

Al termine del processo di importazione l'utente troverà l'insieme dei contatti, che formavano la propria rubrica nella precedente WebMail, riportati correttamente anche nella nuova versione della casella di posta.

Da questo momento avrà la possibilità di procedere autonomamente nella gestione dei propri contatti con terze parti, senza il dubbio di essere incorso nella perdita di dati importanti.

Copia firma digitale

Una seconda richiesta di personalizzazione, alzata frequentemente da diversi utenti, è legata alla gestione della propria firma digitale.

Ogni l'azienda predispone una mail aziendale per i membri del proprio team e in corrispondenza una firma digitale, impostata automaticamente in calce ad ogni messaggio di posta elettronica.

Come per la rubrica di contatti, anche questa personalizzazione non può essere riportata automaticamente nella nuova WebMail, bensì necessita di un processo di migrazione dedicato. Seppur si tratti di una sequenza di operazioni più semplice rispetto a quella esposta precedentemente, prevede anch'essa una prima parte dedicata alla copia dei dati dalla versione WebMail più vecchia e una fase di importazione e aggiornamento della versione più nuova.

La sequenza di operazioni vede innanzitutto protagonista la versione di WebMail precedente.

- 1) Nel menù di navigazione iniziale l'utente seleziona la voce "**Impostazioni**" visualizzando un nuovo sottomenù le cui voci rappresentano i principali ambienti di personalizzazione su cui l'utente può agire
- 2) L'utente seleziona la voce "**Identità**" e nella seconda colonna visualizza come identità il proprio account (in questo caso "test")
- 3) Una volta evidenziata l'account desiderato, il sistema mostra nella parte centrale della pagina le caratteristiche identificative dell'account in esame.
Tra queste l'attenzione dell'utente deve focalizzarsi sulla parte riferita alla gestione della firma.
- 4) Copia l'intero contenuto della casella di testo che trova sotto la sezione "**Firma**" ed esce dalla pagina

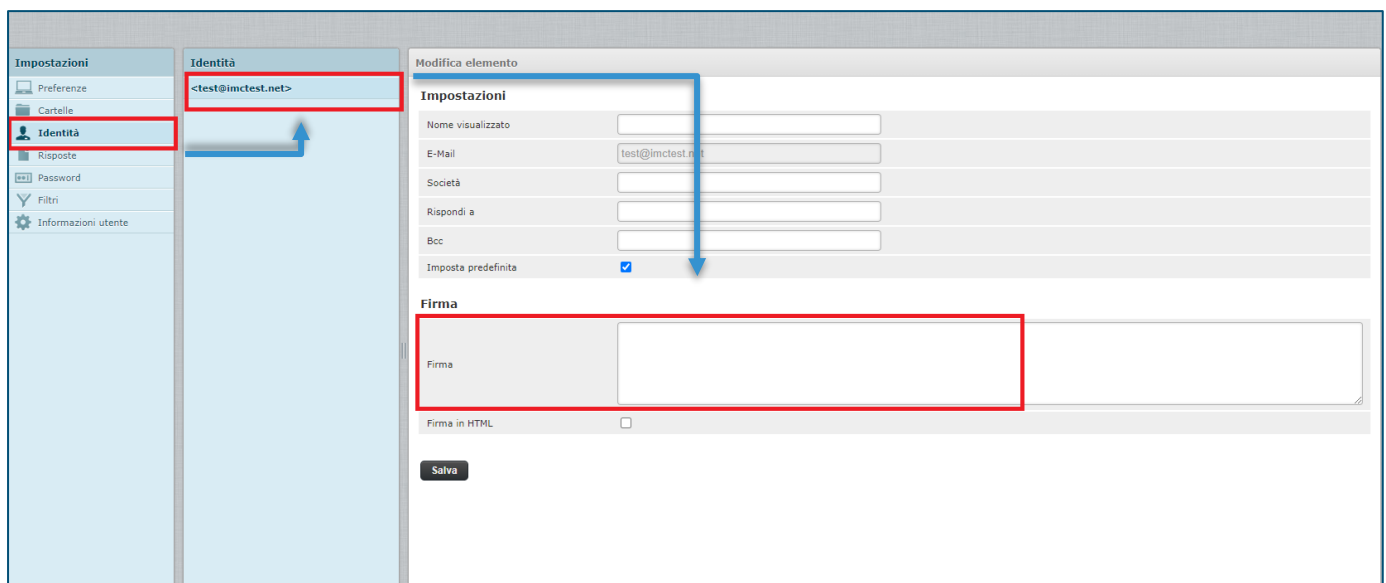


Figura 44 - Flusso di operazioni: Migrazione firma digitale

A questo punto l'attenzione si sposta nella nuova versione della WebMail:

- 1) In modo similare alla versione precedente, l'utente seleziona nel menù principale la voce **"Impostazioni"**

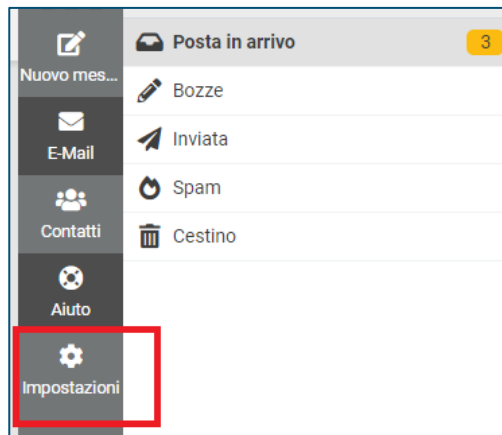


Figura 45: Flusso di operazioni: Copia firma digitale su nuova WebMail

- 2) Il sistema mostra una nuova pagina con un menù di navigazione. L'utente seleziona la voce **"Identità"** e nella seconda colonna l'account per cui si desidera copiare la firma digitale.
- 3) L'attenzione si presta a questo punto alla sezione **"Firma"** che l'utente trova nella pagina che viene visualizzata con i dati principali dell'account in esame.
- 4) Ricopia il contenuto (precedentemente copiato dalla vecchia casella di posta) e riporta il codice per la composizione della firma digitale in calce ogni messaggio di posta elettronica.
- 5) Al termine salve le nuove modifiche e procede con l'invio di una mail di verifica.

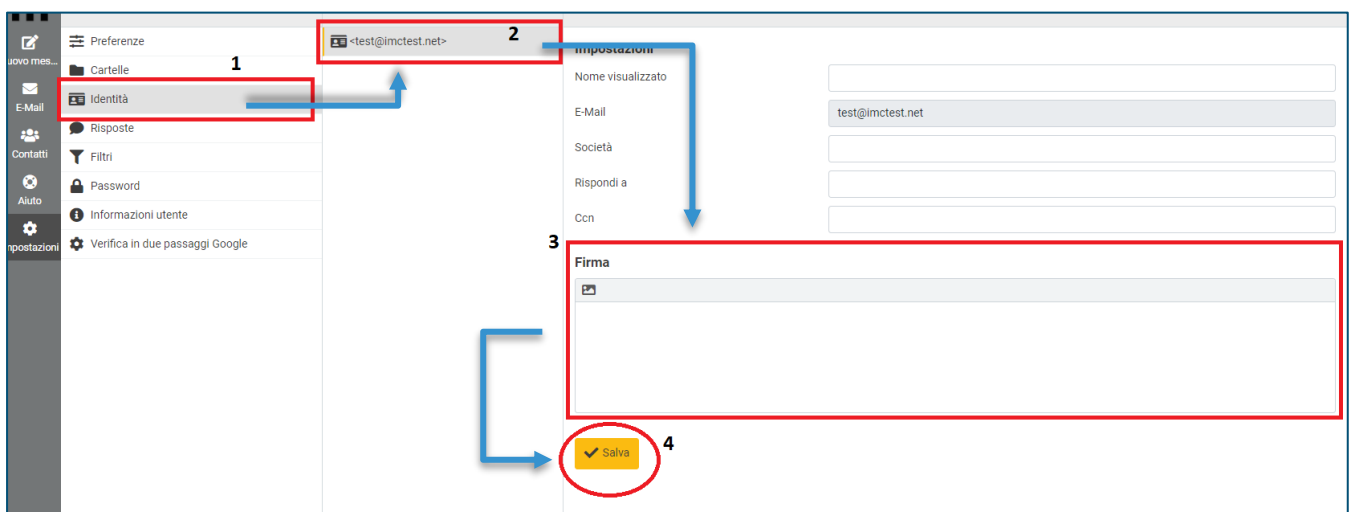


Figura 46 - Flusso di operazioni: Migrazione firma digitale nella nuova versione WebMail

Al termine della sequenza di operazioni, l'utente noterà un riequilibrio delle impostazioni di personalizzazione rispetto alla versione WebMail precedente.