Titolo	ControlloAccesso	
Descrizione	Ogni accesso al sistema deve essere controllato	
Misuse case	FurtoCredenziali, AccessoNonAutorizzato	
Pre-condizioni	L'attaccante conosce o ha dedotto l'email di un Utente	
Post-condizioni	Il sistema blocca temporaneamente l'accesso dell'Utente e registra le attività sospette nel log di sistema	
Scenario Principale	**Sistema**	**Attaccante**
		Effettua ripetuti tentativi di login utilizzando email note e attacco a dizionario
	Verifica le credenziali immesse. Dopo un numero definito di tentativi errati, blocca temporaneamente ulteriori tentativi per quell'account	
	Registra l'evento anomalo nel log	
Scenario di Attacco Avvenuto con Successo	**Sistema**	**Attaccante**
		Attacco a dizionario riuscito
	Verifica le credenziali immesse e concede l'accesso	
		Naviga tra le funzionalità alla ricerca di dati sensibili
	Registra tutte le operazioni effettuate dall'account nel log di sistema. Controlli di monitoraggio rilevano pattern di accesso anomali	

Titolo	ProtezioneDati	
Descrizione	I dati finanziari, i documenti PDF e le informazioni sulle abitazioni devono essere accessibili solo ai Membri autorizzati della Famiglia	
Misuse case	EsfiltrazioneDati, AccessoNonAutorizzatoDati	
Pre-condizioni	L'attaccante ha ottenuto accesso al sistema (account compromesso o vulnerabilità) e conosce o indovina riferimenti a risorse di altre famiglie	
Post-condizioni	Il sistema verifica famiglia e ruolo su ogni richiesta di accesso, valida e sanitizza tutti gli input, verifica tipo e dimensione dei PDF caricati, minimizza la visibilità nelle liste, traccia tutte le operazioni sui dati sensibili, nega richieste non autorizzate	
Scenario Principale	**Sistema**	**Attaccante**
		Tenta di accedere a dati di una Famiglia diversa dalla propria
	Verifica appartenenza e Ruolo del Membro. Nega l'accesso e registra il tentativo di accesso nel log	
		Tenta di caricare un PDF malevolo
	Verifica tipo e dimensione del file PDF. Rifiuta e registra il tentativo	
		Tenta di inserire movimenti finanziari con dati malevoli
	Validazione dei dati e sanitizzazione delle stringhe. Rifiuta la richiesta e registra il tentativo di inserimento malevolo	
Scenario di Attacco Avvenuto con Successo	**Sistema**	**Attaccante**
		Sfrutta vulnerabilità di controllo accessi per accedere a dati di altre famiglie. Scarica sistematicamente grandi volumi di dati sensibili
	Fornisce i dati richiesti. Le operazioni sono tracciate nel log. Controlli periodici sui log evidenziano volumi anomali di accesso ai dati o accessi sospetti	

Titolo	GestioneSicuraInviti	
Descrizione	L'adesione tramite codice d'invito deve prevenire indovinamento e abuso dei tentativi	
Misuse case	AbusoCodiciInvito, GuessingCodici	
Pre-condizioni	L'attaccante ha intercettato o tenta di indovinare un codice invito valido	
Post-condizioni	Il sistema limita i tentativi di inserimento codici errati, consente al Capofamiglia di rigenerare il codice (univoco e difficilmente prevedibile), registra tutti i tentativi nel log	
Scenario Principale	**Sistema**	**Attaccante**
		Prova sequenze di codici alfanumerici cercando di indovinare un codice valido
	Verifica validità del codice. Dopo un numero limitato di tentativi errati, blocca temporaneamente ulteriori tentativi	
	Registra ogni tentativo nel log	
Scenario di Attacco Avvenuto con Successo	**Sistema**	**Attaccante**
		Indovina o intercetta un codice invito valido
	Accetta il codice e aggiunge il Membro alla Famiglia. Traccia l'uso del codice nei log	
	Il Capofamiglia può rimuovere il Membro non autorizzato	
	Il Capofamiglia può rigenerare il codice invito	

Titolo	ProtezioneLog	
Descrizione	I log di sistema devono essere non modificabili, garantendo l'integrità delle tracce per audit e analisi	
Misuse case	ManomissioneLog, AccessoNonAutorizzatoLog	
Pre-condizioni	L'attaccante ha ottenuto privilegi elevati o ha sfruttato vulnerabilità per accedere ai file di log	
Post-condizioni	Il sistema consente la consultazione dei log solo agli amministratori, conserva i log in modalità append-only	
Scenario Principale	**Sistema**	**Attaccante**
		Prova a visualizzare, modificare o eliminare voci dei log di sistema per nascondere tracce di attività malevole
	Richiede autorizzazione amministrativa per accesso ai log e nega l'accesso	
	Mantiene i log in modalità append-only	
Scenario di Attacco Avvenuto con Successo	**Sistema**	**Attaccante**
		Consulta i log e tenta di eliminare o modificare voci che documentano le proprie attività malevole
	Il sistema mantiene i log in modalità append-only, rendendo difficile la modifica completa	
	L'analisi successiva può rilevare incongruenze o gap nei log per indagini forensi	

Requisiti di Sicurezza

Dall'analisi del rischio emergono **requisiti di sicurezza** fondamentali per **proteggere** i **beni identificati**: credenziali di accesso con privilegi al sistema, dati personali tutelati dal GDPR, informazioni finanziarie strettamente private, documenti PDF contenenti contratti e fatture, e codici invito che controllano l'accesso alle famiglie.
L'**analisi delle minacce** ha identificato attacchi a dizionario sulle credenziali, sottrazione di dati sensibili, abuso dei codici invito e accesso fraudolento ai log. Per ciascuna minaccia sono stati **individuati controlli** con relativa fattibilità: requisiti di complessità password, limitazione dei tentativi, controllo degli accessi basato sul ruolo, validazione degli input, generazione di codici non prevedibili e registrazione in modalità non modificabile. L'analisi tecnologica ha **confermato vulnerabilità note** associate alle tecnologie impiegate, rafforzando la **necessità dei controlli individuati**.
La modellazione di scenari di attacco ha permesso di **identificare meccanismi di difesa concreti**: controllo degli accessi contro furti di credenziali, protezione dei dati contro esfiltrazione, gestione sicura degli inviti contro guessing, e protezione dei log per garantire integrità delle tracce. Per **garantire sicurezza** elevata e **gestione semplificata** del ruolo critico di **Amministratore**, tale account non sarà soggetto a registrazione dinamica ma **fornito in fase di configurazione iniziale**.

ID	Requisito funzionale di sicurezza
RF27	Il sistema deve bloccare temporaneamente l'accesso dopo ripetuti tentativi falliti consecutivi, sia per autenticazione che per adesione a una famiglia
RF28	Il sistema deve creare un log per tracciare tutte le operazioni critiche effettuate dagli Utenti, registrando: timestamp, email dell'Utente, tipo operazione, esito
RF29	Il sistema deve impedire l'accesso ai log di sistema a Utenti non autorizzati. Solo gli Amministratori possono consultare i log
RF30	Il Capofamiglia deve poter rigenerare il codice invito della propria Famiglia
RF31	Il sistema deve validare tipo e dimensione dei file PDF caricati, rifiutando file di tipo diverso o che superano la soglia massima consentita di 10 MB
RF32	Il sistema deve applicare controlli di coerenza prima dell'inserimento di nuovi movimenti finanziari
RF33	Il sistema deve verificare che ogni operazione su dati sensibili (Spese, Introiti, Abitazioni, Contratti) sia eseguita da un Membro appartenente alla Famiglia proprietaria dei dati con il Ruolo autorizzato.

ID	Requisito non funzionale di sicurezza
RN9	La password deve essere di almeno 8 caratteri e contenere almeno una lettera maiuscola, una lettera minuscola e un numero
RN10	Il numero massimo di tentativi falliti prima del blocco temporaneo di almeno 15 minuti deve essere 5 sia per l'autenticazione che per l'adesione a una famiglia
RN11	I codici invito devono essere univoci, generati in modo non prevedibile
RN12	I log di sicurezza devono essere conservati in modalità append-only e devono essere sottoposti ad analisi con cadenza almeno settimanale

Aggiornamento Vocabolario

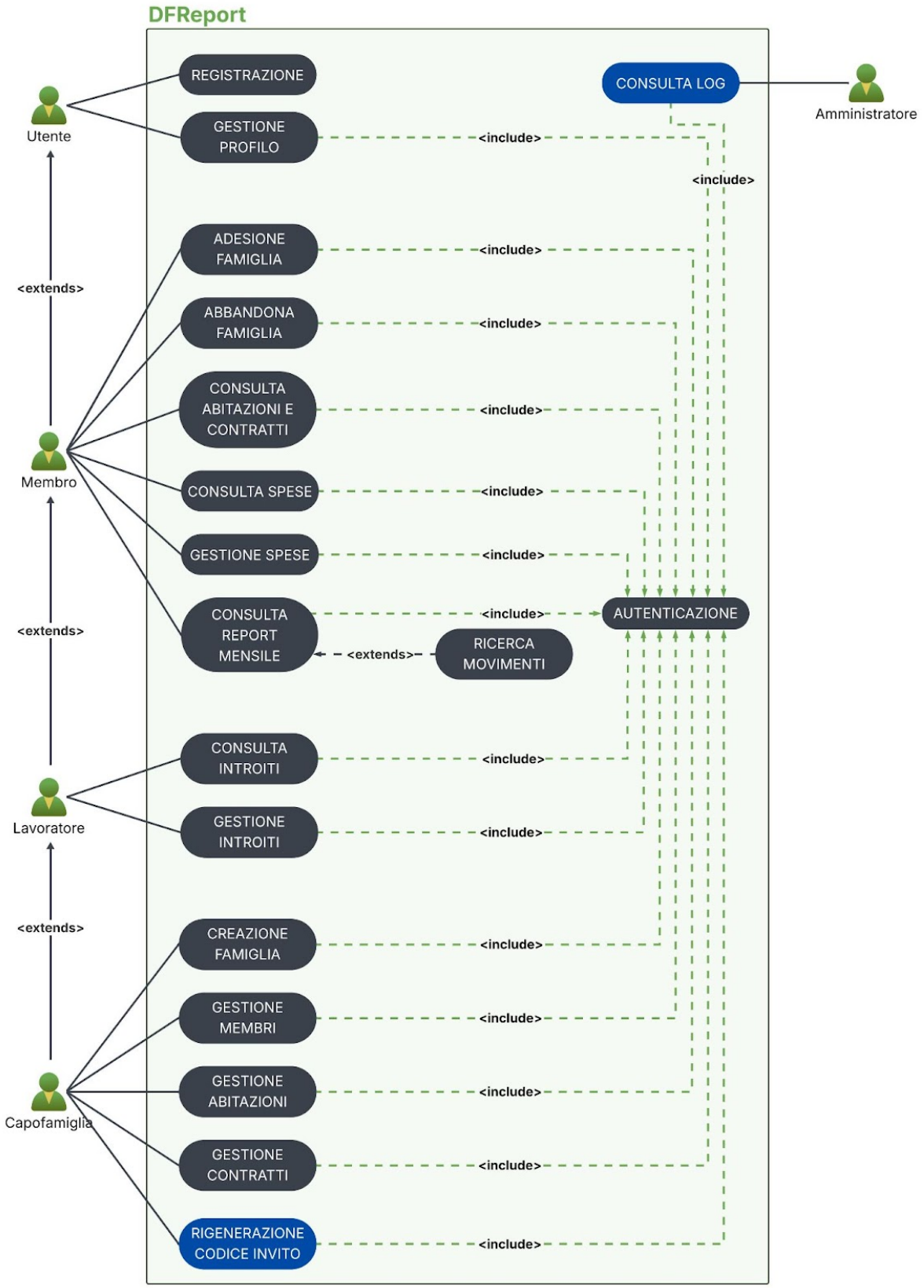
Vocabolo	Significato	Sinonimi
Amministratore	Ruolo privilegiato predisposto in fase di configurazione iniziale del sistema, dotato di autorità esclusiva per consultare i log di sicurezza e supervisionare l'integrità del sistema	Admin
Log di Sicurezza	Registro permanente in cui il sistema traccia tutte le operazioni critiche degli Utenti. Il log è gestito in modalità append-only per garantire l'integrità e l'immutabilità delle voci registrate	
Voce di Log	Singola registrazione all'interno del Log di Sicurezza che documenta un'operazione critica. Ogni voce contiene obbligatoriamente: timestamp dell'operazione, email dell'Utente che l'ha eseguita, tipo di operazione effettuata ed esito (successo o fallimento)	
Operazione Critica	Azione svolta da un Utente che deve essere obbligatoriamente tracciata nel Log di Sicurezza per finalità di audit e sicurezza. Include tutte le operazioni che comportano accesso, modifica o cancellazione di dati sensibili, nonché tentativi di autenticazione e di adesione a famiglie	

Scenari d’uso nuovi

Titolo	ConsultaLog
Descrizione	L'Amministratore consulta i log di sicurezza per analizzare le operazioni critiche registrate dal sistema
Attori	Amministratore
Relazioni	Autenticazione
Pre-condizioni	
Post-condizioni	I log di sicurezza vengono visualizzati; la consultazione viene registrata nel log
Scenario principale	1. Autenticazione 2. Il Sistema mostra le Voci di Log 3. L’Amministratore, per ogni Voce di Log, visualizza timestamp, email dell’Utente a cui è riferita, tipo operazione ed esito (successo o fallimento) 4. Il Sistema registra l'operazione nel log di sicurezza
Scenari alternativi	**A) Nessuna Voce di Log** 2. Il Sistema mostra all’Amministratore un messaggio che indica l'assenza di Voci di Log
Requisiti non funzionali	RN2, RN3, RN4, RN5, RN6, RN8, RN12

Titolo	RigenerazioneCodiceInvito
Descrizione	Il Capofamiglia rigenera il codice invito della propria Famiglia
Attori	Capofamiglia
Relazioni	Autenticazione
Pre-condizioni	Il Capofamiglia ha creato una Famiglia
Post-condizioni	• Nuovo codice invito associato alla Famiglia • Operazione registrata nel log
Scenario principale	1. Autenticazione 2. Il Capofamiglia richiede la rigenerazione del codice 3. Il Capofamiglia conferma la rigenerazione 4. Il Sistema dissocia il codice esistente dalla Famiglia 5. Il Sistema mostra un nuovo codice invito univoco e casuale e l’associa alla Famiglia 6. Il Sistema registra l'operazione nel log di sicurezza
Scenari alternativi	
Requisiti non funzionali	RN1, RN2, RN3, RN4, RN5, RN11

Casi d’uso aggiornati



Scenari d’uso aggiornati

Nel paragrafo vengono presentati 7 **scenari d'uso rappresentativi** che **esemplificano** le diverse tipologie di **modifiche** introdotte dall'analisi del rischio. Gli **scenari** sono stati **selezionati** per coprire tutti i requisiti di sicurezza funzionali e non funzionali identificati, **evitando ridondanze**.
Gli scenari d'uso **non riportati** per esteso **seguono pattern analoghi** a quelli presentati e sono stati ugualmente aggiornati secondo i medesimi principi.

Titolo	Registrazione
Descrizione	L’utilizzatore del sistema crea un nuovo profilo Utente
Attori	Utente
Relazioni	
Pre-condizioni	
Post-condizioni	• Viene creato un nuovo profilo Utente • Operazione registrata nel log di sicurezza
Scenario principale	1. L’Utente inserisce: nome, cognome, data di nascita, email, password 2. Il Sistema verifica univocità e validità e-mail 3. Il Sistema verifica che la password contenga almeno 8 caratteri di cui una lettera maiuscola, una minuscola e un numero 4. Il Sistema memorizza i dati dell’Utente 5. Il Sistema registra l'operazione di registrazione nel log 6. Il Sistema reindirizza l’Utente all’Autenticazione
Scenari alternativi	**A) Email già in uso o non valida** 3. Il Sistema mostra all’Utente un messaggio di errore e gli si dà la possibilità di reinserire l’email **B) Password non conforme ai requisiti di sicurezza** 4. Il Sistema mostra all'Utente un errore specificando i requisiti e gli si dà la possibilità di reinserire la password
Requisiti non funzionali	RN2, RN3, RN6, RN8, RN9, RN12

Titolo	Autenticazione
Descrizione	L’Utente inserisce le proprie credenziali e si autentica sulla piattaforma
Attori	Utente
Relazioni	Tutti i casi d’uso autenticati
Pre-condizioni	L’Utente si è precedentemente registrato e conosce le proprie credenziali d’accesso
Post-condizioni	● L’Utente è autenticato nel sistema ● Tentativo di autenticazione registrato nel log
Scenario principale	1. L’Utente inserisce e-mail e password 2. Il Sistema verifica che le credenziali inserite corrispondano a quelle di un Utente già registrato 3. L’Utente viene autorizzato a usufruire del sistema 4. Il Sistema registra il tentativo riuscito nel log
Scenari alternativi	**A) Credenziali fornite non riconosciute** 3. Il Sistema registra il tentativo fallito nel log di sicurezza 4. Viene mostrato all’Utente un messaggio di errore e gli si dà la possibilità di riprovare l’Autenticazione **B) Credenziali errate inserite 5 volte consecutive** 3. Il Sistema registra i tentativi falliti nel log di sicurezza 4. Il Sistema blocca temporaneamente l'accesso per 15 minuti e mostra all'Utente un messaggio sul blocco temporaneo 5. Dopo 15 minuti, il Sistema consente nuovi tentativi
Requisiti non funzionali	RN2, RN3, RN4, RN6, RN8, RN9, RN10, RN12

Titolo	CreazioneFamiglia
Descrizione	Il Capofamiglia crea una Famiglia
Attori	Capofamiglia
Relazioni	Autenticazione
Pre-condizioni	Il Capofamiglia non è associato a una Famiglia
Post-condizioni	• Famiglia creata con un'Abitazione • Codice invito univoco e casuale associato alla Famiglia • Operazione registrata nel log di sicurezza
Scenario principale	1. Autenticazione 2. Il Capofamiglia inserisce il cognome familiare 3. Il Sistema crea la Famiglia 4. Il Sistema mostra un codice invito di 6 caratteri alfanumerici univoco e casuale e l'associa alla Famiglia 5. Il Sistema registra l'operazione nel log di sicurezza
Scenari alternativi	**A) Il Capofamiglia non inserisce le informazioni obbligatorie richieste** 3. Viene mostrato al Capofamiglia un invito ad inserire i dati mancanti
Requisiti non funzionali	RN2, RN3, RN5, RN6, RN11, RN12

** Lo scenario **GestioneProfilo** segue un pattern analogo a **CreazioneFamiglia** per quanto riguarda gli aggiornamenti di sicurezza: registra i log dell'operazione, ma non include la generazione del codice invito*

Titolo	AdesioneFamiglia
Descrizione	Un Membro si unisce ad una Famiglia
Attori	Membro
Relazioni	Autenticazione
Pre-condizioni	Il Membro non è associato a una Famiglia e conosce il codice invito associato alla Famiglia a cui vuole aderire
Post-condizioni	• Il Membro è aggiunto alla Famiglia • Operazione registrata nel log di sicurezza
Scenario principale	1. Autenticazione 2. Il Membro inserisce il codice invito 3. Il Sistema verifica che il codice invito sia associato a una Famiglia esistente 4. Il Sistema aggiunge il Membro alla Famiglia 5. Il Sistema registra il tentativo riuscito nel log
Scenari alternativi	**A) Codice fornito non riconosciuto** 4. Il Sistema registra il tentativo fallito nel log di sicurezza 5. Viene mostrato al Membro un messaggio di errore e gli si dà la possibilità di reinserire il codice invito **B) Codice errato inserito 5 volte consecutive** 4. Il Sistema registra i tentativi falliti consecutivi nel log di sicurezza 5. Il Sistema blocca temporaneamente l'adesione per 15 minuti e mostra all'Utente un messaggio sul blocco temporaneo 6. Dopo 15 minuti, il Sistema consente nuovi tentativi
Requisiti non funzionali	RN2, RN3, RN10, RN12

Titolo	GestioneContratti
Descrizione	Il Capofamiglia crea o elimina un Contratto
Attori	Capofamiglia
Relazioni	Autenticazione
Pre-condizioni	• Il Capofamiglia ha creato una Famiglia • La Famiglia ha associata almeno un'Abitazione
Post-condizioni	• Il Sistema crea o elimina il Contratto • Operazione registrata nel log di sicurezza
Scenario principale	1. Autenticazione 2. Il Sistema verifica che l'Utente sia il Capofamiglia della Famiglia 3. Il Capofamiglia sceglie tra: - Creazione nuovo Contratto - Eliminazione Contratto esistente 4. Il Capofamiglia fornisce rispettivamente: - Abitazione a cui associarlo e tipo utenza, fornitore, piano tariffario, data inizio, durata, periodicità, costo periodico, scadenze pagamenti, allegato PDF opzionale. - Contratto da eliminare e conferma dell'azione 5. Se fornito un allegato, il Sistema valida che il file sia effettivamente di tipo PDF e che la dimensione ≤ 10 MB 6. Il sistema esegue l'azione richiesta 7. Il Sistema registra l'operazione nel log di sicurezza
Scenari alternativi	**A) Il Capofamiglia non inserisce le informazioni obbligatorie richieste** 5. Viene mostrato al Capofamiglia un invito ad inserire i dati mancanti **B) Nessun Contratto da eliminare** 4. Il Sistema mostra un avviso che indica l'assenza di Contratti **C) L'Utente non è il Capofamiglia della Famiglia** 3. Viene mostrato all'Utente un messaggio di errore **D) File PDF non valido o dimensione superiore a 10 MB** 6. Il Sistema mostra un messaggio di errore specificando il problema e richiede un file conforme
Requisiti non funzionali	RN2, RN3, RN4, RN5, RN6, RN12
Punti Aperti	Conseguenze dell'eliminazione di un'Abitazione sui Contratti associati

** Gli scenari **GestioneAbitazione** e **GestioneMembri** seguono un pattern analogo a **GestioneContratti** per quanto riguarda gli aggiornamenti di sicurezza: verificano il ruolo del Capofamiglia, l'appartenenza alla Famiglia e registrano i log dell'operazione, ma non includono la validazione del file caricato*

Titolo	ConsultaSpese
Descrizione	Il Membro consulta le spese personali
Attori	Membro
Relazioni	Autenticazione
Pre-condizioni	Il Membro è associato a una Famiglia
Post-condizioni	Il Sistema mostra le informazioni relative alle Spese personali
Scenario principale	1. Autenticazione 2. Il Sistema verifica che l'Utente sia un Membro della Famiglia 3. Il Sistema mostra le Spese di cui il Membro è responsabile 4. Il Membro, per ogni Spesa, visualizza descrizione, importo, data e categoria 5. Il Sistema registra l'operazione di consultazione nel log di sicurezza
Scenari alternativi	**A) Nessuna Spesa di cui il Membro è responsabile** 3. Il Sistema mostra al Membro un messaggio che indica l'assenza di Spese personali **B) L'Utente non è un Membro della Famiglia** 3. Viene mostrato all'Utente un messaggio di errore
Requisiti non funzionali	RN1, RN2, RN3, RN4, RN5, RN6, RN7

** Gli scenari di **Consultazione** seguono un pattern completamente analogo a **ConsultaSpese**: verificano l'appartenenza del Membro alla Famiglia e registrano il log dell'operazione*

Titolo	GestioneSpese
Descrizione	Il Membro crea o elimina una Spesa personale o familiare
Attori	Membro
Relazioni	Autenticazione
Pre-condizioni	Il Membro è associato a una Famiglia
Post-condizioni	• Il Sistema crea o elimina la Spesa • Operazione registrata nel log di sicurezza
Scenario principale	1. Autenticazione 2. Il Sistema verifica che l'Utente sia un Membro della Famiglia 3. Il Membro sceglie tra: - Creazione nuova Spesa - Eliminazione Spesa esistente 4. Il Membro fornisce rispettivamente: - Descrizione, importo, data, categoria e responsabile (tra Membro stesso o Famiglia) - Spesa da eliminare e conferma dell'azione 5. Se si sta creando una nuova Spesa, il Sistema applica controlli di coerenza 6. Il sistema esegue l'azione richiesta 7. Il Sistema registra l'operazione nel log di sicurezza
Scenari alternativi	**A) Il Membro non inserisce le informazioni obbligatorie richieste** 5. Mostrato al Membro un invito ad inserire i dati mancanti **B) Nessuna Spesa da eliminare** 4. Il Sistema mostra un avviso che indica l'assenza di Spese **C) L'Utente non è un Membro della Famiglia** 3. Viene mostrato all'Utente un messaggio di errore **C) Dati non coerenti** 6. Il Sistema mostra un messaggio di errore specificando il problema e richiede dati corretti
Requisiti non funzionali	RN1, RN2, RN3, RN5, RN6, RN7, RN12

** Lo scenario **GestioneIntroiti** segue un pattern analogo a **GestioneSpese** per quanto riguarda gli aggiornamenti di sicurezza: verifica il ruolo del Lavoratore, l'appartenenza alla Famiglia, controlla la coerenza dei dati inseriti e registra i log dell'operazione*