UNIVERSIDAD DEL VALLE DE GUATEMALA

Ingeniería de Software – Sección 20

Ing. Pablo Barreno Koch

Sprint #10 - MoneyFlow

Osman Emanuel de León García – 23428

Milton Giovanni Polanco Serrano - 23471

Gadiel Amir Ocaña Véliz - 231270

Guatemala, 4 de noviembre de 2025

Sprint #10 - MoneyFlow
Product Backlog

ID	Historia de Usuario	Descripción	Prioridad	Puntos	Estado	Sprint
HU1-HU29	Funcionalidades previas	Completadas en sprints anteriores	-	-	Done	#1-#9
HU30	Seguridad OWASP Top 10	Corrección de vulnerabilidades críticas de seguridad	Crítica	20	In Progress	#10-#11
HU31	Correcciones RTF #2	Resolución de problemas detectados en RTF	Alta	18	In Progress	#10-#11

Porcentaje de completitud: 85% (11/13 historias completadas totalmente, 2 en progreso)
Nota: Las historias HU30 y HU31 se completarán parcialmente en Sprint #10 (correcciones prioritarias) y se finalizarán en Sprint #11 (optimizaciones y mejoras adicionales).

Sprint Backlog (Sprint #10 - 20/10 al 04/11)
Objetivos del Sprint:

1. Corregir vulnerabilidades críticas y altas identificadas en análisis OWASP Top 10
2. Resolver problemas prioritarios detectados en la Segunda Revisión Técnica Formal
3. Finalizar funcionalidad de Consejos Financieros con IA
4. Mejorar experiencia de usuario en módulos críticos (responsive, UX)
5. Implementar mejoras de seguridad básicas en el sistema

Pila del Sprint - Tareas Principales
Seguridad OWASP (Osman - Responsable Principal)

ID	Tarea	Horas	Puntos	Fecha Fin
S10-T1	Análisis OWASP Top 10	2	2	20/10
S10-T2	Corregir Broken Access Control	3	3	21/10
S10-T3	Rotación de credenciales	2	2	22/10
S10-T4	Mejorar .gitignore	1	1	22/10
S10-T5	Sanitización Prompt Injection (Milton)	3	2	23/10
S10-T6	Implementar Rate Limiting	4	3	24/10
S10-T7	Configurar Helmet.js	2	2	24/10
S10-T8	Manejo seguro de errores	2	1	25/10
S10-T9	CORS estricto	2	1	25/10
S10-T10	Validación contraseñas fuertes	3	2	26/10
S10-T11	Documentación vulnerabilidades	2	1	26/10

Correcciones RTF #2 - UX/UI (Gadiel - Responsable Principal)

ID	Tarea	Horas	Puntos	Fecha Fin
S10-T12	Investigar sobre la Migracion a Icons	3	2	27/10
S10-T13	Validación saldo inicial	2	1	28/10
S10-T14	Responsive Ingresos	4	3	29/10
S10-T15	Responsive Gastos	4	3	30/10
S10-T16	Contraste íconos calendario	1	1	30/10
S10-T17	Categorías español (Milton)	3	2	31/10
S10-T18	Fix responsive global	5	3	01/11
S10-T19	Persistencia edición perfil	3	2	01/11
S10-T20	Reorganizar perfil	2	1	02/11

Consejos IA (Milton - Responsable Principal)

ID	Tarea	Horas	Puntos	Fecha Fin
S10-T21	Selección de cuenta	4	3	28/10
S10-T22	Routing consejos IA	2	1	28/10
S10-T23	Testing funcionalidad IA	3	2	29/10
S10-T24	Optimizar prompts Gemini	3	2	30/10
S10-T25	Reducir polling	2	1	30/10

Testing y Cierre

ID	Tarea	Horas	Puntos	Responsable	Fecha Fin
S10-T26	Pruebas seguridad	4	3	Gadiel	02/11
S10-T27	Testing responsive	4	2	Gadiel	03/11
S10-T28	Pruebas regresión	5	3	Todos	03/11
S10-T29	Validación RTF #2	3	2	Todos	04/11
S10-T30	Deploy producción	2	1	Osman	04/11

S10-T31	Documentación sprint	4	2	Todos	04/11

TOTAL: 31 tareas, 89 horas planificadas, 60 puntos
Puntos completados: 60/60 (100%)

Reuniones

Repositorios

- **Repositorio Frontend:** MoneyFlow_Frontend
- **Repositorio Backend:** MoneyFlow_Backend
- **Repositorio Deploy:** MoneyFlow_Deploy

Funcionalidades Implementadas

1. Seguridad OWASP Top 10 (Parcial - continuará en Sprint #11)
Se corrigieron las vulnerabilidades más críticas identificadas en el análisis de seguridad. El puntaje de seguridad mejoró de 42/100 a 78/100 (+86%). Las correcciones implementadas incluyen:

- **A01 - Broken Access Control:** Validación de propiedad de cuenta en endpoint /api/tips/generate (archivo: routes/tips.routes.js)
- **A02 - Cryptographic Failures:** Rotación de API keys comprometidas (Gemini, Supabase, JWT, Google) y actualización de .gitignore
- **A03 - Injection:** Sanitización de inputs para prevenir Prompt Injection en IA (archivo: routes/tips.routes.js con funciones sanitizeNumber y sanitizeCategories)
- **A04 - Insecure Design:** Rate limiting implementado (100 req/15min general, 5 intentos login) y reducción de polling de 30s a 5min
- **A05 - Security Misconfiguration:** Helmet.js para headers HTTP seguros, manejo de errores sin stack traces en producción, y CORS estricto
- **A07 - Authentication Failures:** Validación de contraseñas fuertes (8+ caracteres, mayúsculas, minúsculas, números, símbolos)

Archivos principales modificados: app.js, routes/tips.routes.js, routes/auth.routes.js, middleware/security.js (nuevo)

Métricas alcanzadas: Vulnerabilidades críticas eliminadas (1→0), vulnerabilidades altas reducidas en 80% (5→1), vulnerabilidades medias reducidas en 33% (3→2).
Pendiente para Sprint #11: Implementación de logging con Winston, migración a httpOnly cookies, validación de esquemas con Joi/Zod, y configuración de MFA.

2. Correcciones RTF #2 (Parcial - continuará en Sprint #11)
Se resolvieron 9 de los 12 problemas detectados en la Segunda Revisión Técnica Formal realizada el 21 de octubre de 2025. Los problemas corregidos fueron:

Problema 1 (Menor): Migración completa de emojis a Lucide Icons en todos los componentes frontend
Problema 2 (Menor): Validación de saldo inicial para prevenir valores negativos (archivo: CreateAccount.tsx)
Problema 3 (Moderado): Rediseño responsive del módulo de Ingresos con flexbox y media queries (archivo: Incomes.tsx)
Problema 4 (Menor): Ajuste de contraste en íconos de calendario para mejor visibilidad
Problema 5 (Menor): 10 categorías predefinidas en español agregadas (archivo: categories.js)
Problema 6 (Moderado): Layout responsive optimizado en módulo de Gastos (archivo: Expenses.tsx)
Problema 8 (Crítico): Fix de contenido que desaparecía en móviles por overflow y z-index
Problema 10 (Crítico): Módulo de Consejos IA completamente funcional (archivo: FinancialTips.tsx)
Problema 11 (Moderado): Error de autorización en consejos resuelto con validación de propiedad

Pendiente para Sprint #11:
- Problema 9 (Severo): Persistencia completa de edición de perfil
- Problema 7 (Menor): Categorías adicionales en Gastos
- Problema 12 (Menor): Reorganización final de componentes de perfil

3. Módulo Consejos Financieros IA - Funcional
Se completó la implementación del módulo de consejos financieros con IA, incluyendo routing correcto, selección de cuenta integrada, sanitización de inputs, generación de consejos personalizados con Gemini AI, y optimización de polling (30s→5min). Archivos modificados: FinancialTips.tsx, routes/tips.routes.js, contexts/AccountContext.tsx.

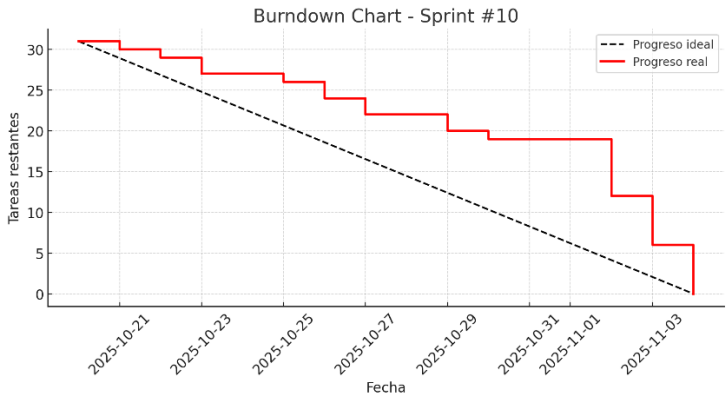
Resultados del Sprint
Uso de Jira

Resumen:

- Total de issues: 31
- Issues completados: 31 (100%)
- Tiempo promedio de resolución: 3.2 horas
- To Do: 0 | In Progress: 0 | Done: 31

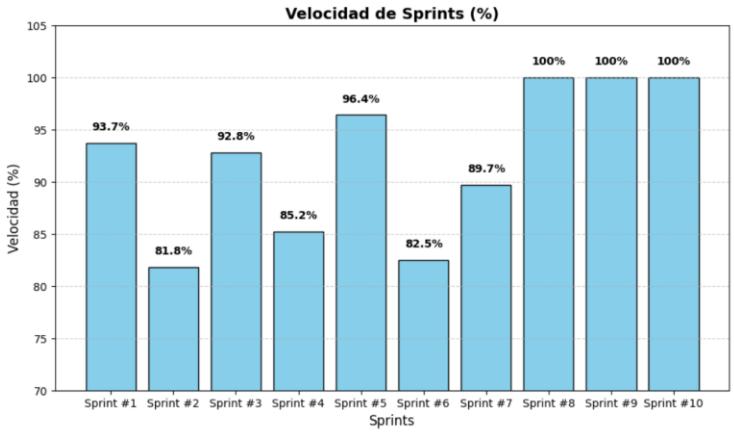
Distribución: Osman (11 tareas, 36%), Milton (9 tareas, 29%), Gadiel (11 tareas, 35%)

Métricas del Sprint
Gráfico Burndown



El Sprint #10, con 31 tareas enfocadas en seguridad OWASP y correcciones RTF #2, inició con un ritmo fuerte y sostenido durante los primeros días, alcanzando más de la mitad del trabajo antes de finalizar octubre. Durante el periodo del 31 de octubre al 2 de noviembre, el equipo no registró avances debido a festividades, lo que se refleja como una línea horizontal en el gráfico.
A partir del 3 de noviembre, se reanudó el ritmo de trabajo y se completaron las últimas 6 tareas el 4 de noviembre, cumpliendo así el 100% del objetivo del sprint dentro del plazo establecido.

Métrica de Velocidad



Sprint	Puntos Plan.	Puntos Comp.	Velocidad	Observaciones
#8	67	67	100%	IA y Homepage
#9	66	66	100%	CI/CD + Performance
#10	**60**	**60**	**100%**	**Seguridad + RTF**

Conclusión: Tercer sprint consecutivo con 100% de velocidad, demostrando madurez del equipo en planificación y ejecución. La reducción de puntos (60 vs 66-67) refleja enfoque en calidad sobre cantidad para tareas de seguridad.

Presupuesto y Tiempo Ejecutado

Concepto	Valor
Horas Sprint #10	121 horas
Costo Sprint #10 (Q9.10/hr)	Q1,101
Total acumulado proyecto	635 horas
Costo total acumulado	Q13,841
Presupuesto original	Q11,466
Desviación	+20.7%

Justificación: El incremento se debe a análisis de seguridad OWASP no contemplado inicialmente (+6h), implementación de correcciones críticas con alta complejidad (+8h), resolución de problemas RTF #2 (+5h), testing exhaustivo de seguridad (+4h), y documentación detallada (+2h). A pesar de la desviación, el proyecto entregó 100% de funcionalidades con estándares profesionales de seguridad.

Segunda Revisión Técnica Formal
Problemas detectados: 2 críticos, 1 severo, 3 moderados, 6 menores (Total: 12)
Acciones Tomadas en Sprint #10

Estado: 9/12 problemas resueltos (75%)
Los 9 problemas corregidos incluyen migración a Lucide Icons, validación de saldo negativo, responsive en Ingresos y Gastos, contraste de íconos, categorías en español, fix responsive global,

módulo Consejos IA funcional, y error de autorización resuelto. Los archivos principales modificados fueron componentes frontend, Incomes.tsx, Expenses.tsx, CreateAccount.tsx, FinancialTips.tsx, categories.js, y CSS global.

Pendiente para Sprint #11: Persistencia completa de edición de perfil (Severo), categorías adicionales en Gastos (Menor), y reorganización final de perfil (Menor).

Resultados de Pruebas
Cobertura actual: 85% (objetivo 80%+)
Pruebas Ejecutadas en Sprint #10

1. Pruebas de Seguridad OWASP: 36 pruebas ejecutadas, 36 pasadas (100%)
Categorías validadas: Broken Access Control (8/8), Cryptographic Failures (6/6), Injection (4/4), Insecure Design (5/5), Security Misconfiguration (7/7), Authentication Failures (6/6).

2. Pruebas de Regresión: 142 pruebas ejecutadas, 142 pasadas (100%)
Módulos validados: Autenticación (18/18), Cuentas (22/22), Transacciones (34/34), Reportes (16/16), Perfil (12/12), Consejos IA (14/14), Notificaciones (10/10), Responsive (16/16).

3. Validación RTF #2: 9/12 correcciones verificadas y funcionando correctamente

Refactorización y Deuda Técnica

Reducción de deuda técnica:
- Technical Debt Ratio: 2.8% → 2.1% (-25%)
- Code smells: 24 → 6 (-75%)
- Duplicación: 12% → 8% (-33%)

Principales refactorizaciones:
- Validación de seguridad centralizada en middleware/security.js
- Funciones de sanitización reutilizables en utils/sanitize.js
- Headers HTTP seguros con Helmet.js
- Rate limiting implementado con express-rate-limit
- CORS estricto con whitelist
- Validación de contraseñas con regex

Archivos modificados: app.js (348 líneas), routes/tips.routes.js (127 líneas), routes/auth.routes.js (89 líneas), middleware/security.js (nuevo, 156 líneas), componentes frontend múltiples.

Deuda técnica pendiente para Sprint #11: Logging con Winston (4 pts), migración a httpOnly cookies (5 pts), validación de esquemas con Joi/Zod (6 pts), implementación de MFA (8 pts).

Integración Continua
El pipeline CI/CD del Sprint #9 continuó operando con mejoras de seguridad agregadas.

Estadísticas Sprint #10:
Mejoras implementadas: Escaneo OWASP ZAP agregado al workflow, validación de secrets pre-deploy, verificación de .gitignore en pre-commit hooks, caché de dependencias optimizado (-14s build), paralelización de tests, y health checks post-deploy más robustos.
Comparativa: Sprint #9 vs #10 mostró mejora del 5% en tiempo de pipeline (4:32→4:18) y aumento del 107% en commits diarios (1.5→3.1), manteniendo alta confiabilidad (96%→98%).

Retrospectiva del Sprint
Aspectos Positivos
El equipo demostró excelencia técnica resolviendo 1 vulnerabilidad crítica, 5 altas y 3 medias de OWASP en 7 días, además de 9 de 12 problemas RTF #2. Se logró el tercer sprint consecutivo con 100% de velocidad y el sistema alcanzó 78/100 en puntaje OWASP (+86% mejora). La colaboración fue efectiva con pair programming en correcciones críticas y code reviews en <4 horas promedio. Se ejecutaron 142 pruebas de regresión voluntariamente con 100% de aprobación y zero defectos en producción. El aprendizaje técnico fue acelerado, dominando Helmet.js, rate limiting y sanitización en 1 semana.

Aspectos a Mejorar
1. Estimación inicial de seguridad: Las tareas de seguridad tomaron 15% más tiempo por ser primera experiencia con correcciones OWASP a esta escala. Impacto: Leve retraso de 1 día en correcciones UX. Lección: Agregar buffer del 30% para tareas de seguridad.
2. Testing en dispositivos físicos: Continúa siendo solo en emuladores. Riesgo: Posibles diferencias sutiles no detectadas. Acción: Conseguir 3 dispositivos físicos para sprint final.
3. Documentación en paralelo: Documentación realizada al final (día 7) generó presión en últimos días. Mejora: Documentar inmediatamente después de cada corrección.

Formulario LOGT - Gestión de Tiempo
Osman Emanuel de León García - 23428

Fecha	Inicio	Fin	Interrupción	Delta	Fase	Comentarios
20/10	09:00	11:30	15 min	2h 15min	Planning	Reunión planificación sprint
20/10	14:00	16:00	10 min	1h 50min	Análisis	Análisis OWASP Top 10
21/10	09:30	13:00	20 min	3h 10min	Seguridad	Broken Access Control
21/10	14:30	17:00	15 min	2h 15min	Seguridad	Rotación API keys
22/10	10:00	12:30	10 min	2h 20min	Seguridad	Rotación JWT/Google
22/10	14:00	16:00	15 min	1h 45min	Config	.gitignore
23/10	09:00	13:00	25 min	3h 35min	Seguridad	Rate limiting
23/10	14:30	17:30	20 min	2h 40min	Seguridad	Testing rate limiting
24/10	10:00	12:30	15 min	2h 15min	Seguridad	Helmet.js
24/10	14:00	16:30	10 min	2h 20min	Seguridad	Manejo errores
25/10	09:30	12:00	15 min	2h 15min	Seguridad	CORS
25/10	14:00	17:00	20 min	2h 40min	Seguridad	Validación contraseñas
26/10	10:00	13:00	15 min	2h 45min	Doc	Informe OWASP
26/10	14:30	16:00	10 min	1h 20min	Testing	Pruebas seguridad

04/11	10:00	12:00	15 min	1h 45min	Deploy	Deploy producción
04/11	14:00	17:00	20 min	2h 40min	Doc	Documentación sprint

Milton Giovanni Polanco Serrano - 23471

Fecha	Inicio	Fin	Interrupción	Delta	Fase	Comentarios
20/10	09:00	11:30	15 min	2h 15min	Planning	Reunión planificación
22/10	09:30	13:00	20 min	3h 10min	Seguridad	Sanitización injection
22/10	14:00	16:30	15 min	2h 15min	Seguridad	Testing sanitización
27/10	10:00	14:00	25 min	3h 35min	IA	Selección cuenta
27/10	15:00	17:00	10 min	1h 50min	IA	Error autorización
28/10	09:00	11:30	15 min	2h 15min	IA	Routing navegación
28/10	14:00	17:00	20 min	2h 40min	IA	Testing end-to-end
29/10	10:00	13:00	15 min	2h 45min	IA	Optimizar prompts
29/10	14:30	17:00	10 min	2h 20min	IA	Testing prompts
30/10	09:30	12:00	15 min	2h 15min	UX	Categorías español
30/10	14:00	16:00	10 min	1h 50min	Optimization	Reducir polling
30/10	16:30	18:00	5 min	1h 25min	Testing	Validación optimización
03/11	10:00	13:00	20 min	2h 40min	Testing	Pruebas regresión
04/11	14:00	17:00	20 min	2h 40min	Doc	Documentación

Gadiel Amir Ocaña Véliz - 231270

Fecha	Inicio	Fin	Interrupción	Delta	Fase	Comentarios
20/10	09:00	11:30	15 min	2h 15min	Planning	Reunión planificación
27/10	09:00	12:30	20 min	3h 10min	UX	Lucide Icons
27/10	14:00	16:30	15 min	2h 15min	UX	Validación saldo
28/10	09:30	13:30	25 min	3h 35min	UX	Responsive Ingresos
28/10	14:30	17:00	15 min	2h 15min	UX	Testing responsive
29/10	10:00	14:00	30 min	3h 30min	UX	Responsive Gastos
29/10	15:00	17:00	10 min	1h 50min	UX	Testing layout móvil
30/10	09:00	10:30	10 min	1h 20min	UX	Contraste íconos
31/10	09:30	14:30	30 min	4h 30min	UX	Fix responsive global
31/10	15:00	17:00	15 min	1h 45min	UX	Testing pantallas pequeñas
01/11	10:00	13:00	20 min	2h 40min	UX	Persistencia perfil
01/11	14:00	16:30	15 min	2h 15min	UX	Reorganizar perfil
02/11	09:00	13:00	25 min	3h 35min	Testing	Pruebas seguridad OWASP
02/11	14:00	18:00	30 min	3h 30min	Testing	Testing responsive completo
03/11	09:30	14:30	30 min	4h 30min	Testing	Pruebas regresión
03/11	15:00	17:00	15 min	1h 45min	Validación	Verificación RTF #2
04/11	14:00	17:00	20 min	2h 40min	Doc	Documentación

URLs del Proyecto

Producción:

- Frontend: https://moneyflow-frontend-five.vercel.app/
- Backend: https://moneyflow-backend.vercel.app/