

Evaluación de banca digital

Banco Lumbré | Pentest y riesgo empresarial | Simulación

Cliente

Banco Lumbré (entidad ficticia)

Evaluador

Sebastián Latorre Muñoz · Autor de la muestra |
Pentester Junior

Fecha

2026-10-07

Versión

1.0

Tabla de contenidos

1. Control del documento y procedencia	3
2. Resumen ejecutivo	4
3. Alcance, arquitectura y contexto de negocio	5
4. Metodología, reglas y cobertura diseñada	8
5. Apetito de riesgo, tolerancias, capacidad y BIA	10
6. Modelo e índice de riesgo empresarial	13
7. Registro y consolidación de riesgos	16
8. Tratamiento, responsables, plazos e inversión	18
9. Cobertura de control, indicadores y seguimiento	21
10. Gobierno de aceptación, supuestos y cierre	26
11. Resumen de hallazgos	28
12. Hallazgos	29
13. Narrativa de ataque y límites de encadenamiento	58
14. Referencias, glosario y límites de la entrega	59

1 Control del documento y procedencia

DOCUMENTO PÚBLICO DE SIMULACIÓN. NO ES UNA EVALUACIÓN DE UN CLIENTE.

Banco Lumbre es una entidad completamente ficticia. No existe una relación comercial, contratación, autorización de un banco real ni evaluación de infraestructura financiera real. La arquitectura, los actores, los hallazgos y las evidencias son contruidos para demostrar metodología y elaboración de informes con report-gen 0.21.2. Todos los dominios pertenecen al espacio .example y todos los registros, importes e identidades son canarios sintéticos.

Campo	Registro
Identificador	BL-SIM-2026-001
Versión y fecha	1.0 2026-10-07
Clasificación	PÚBLICO SIMULACIÓN EDUCATIVA
Autor	Sebastián Latorre Muñoz Portafolio iphobiuss
Herramienta	report-gen 0.21.2, exportadores originales
Revisión	Diseño documental y exportación; no evaluación empírica bancaria
Distribución	Pública para portafolio. No contiene información de un banco real

Procedencia y estado de ejecución

Dimensión	Límite
Origen del contenido	Escenario redactado para portafolio; no procede de un cliente ni de un engagement real.
Origen de evidencias	Evidencias ilustrativas contruidas para este escenario. Los extractos no son resultados de solicitudes a sistemas reales. E01A-E12B son identificadores documentales, no prueba de ejecución.
Ejecución	NO EJECUTADO contra un banco ni contra la arquitectura descrita
Retest	NO EJECUTADO. Los criterios y resultados esperados se presentan como plan de validación.
Estado de hallazgos	CONDICIONES VULNERABLES DEFINIDAS EN EL MODELO, no vulnerabilidades descubiertas en una entidad real
Valoración de riesgo	Estimaciones ordinales y decisiones de gobierno ficticias para el escenario; no mediciones de pérdidas ni evaluación regulatoria.
Publicación	Muestra pública de metodología y capacidad de comunicación; no acredita experiencia laboral bancaria ni una certificación de cumplimiento.
Límite del generador	report-gen genera las salidas del informe. La revisión de integridad de esas salidas verifica la exportación del documento, no la veracidad empírica de los hallazgos sintéticos.

Control de versión y distribución

Versión	Fecha	Cambio
1.0	2026-10-07	Primera muestra pública completa del caso ficticio, sin retest ejecutado

2 Resumen ejecutivo

El escenario concentra su riesgo empresarial en la separación de funciones, la asignación de privilegios y la confiabilidad de las evidencias. La prioridad no es cerrar doce tickets por igual: primero deben impedirse aprobaciones independientes omitidas y accesos privilegiados no gobernados, después limitar la exposición de información y las rutas de propagación.

Banco digital ficticio orientado a personas y pequeñas empresas. Ofrece cuentas de pago, transferencias internas, consulta de movimientos, extractos y gestión de beneficiarios. Las operaciones empresariales de mayor importe requieren separación entre preparador y aprobador.

Decisión requerida en el escenario: priorizar identidad, independencia de aprobación, privilegios de despliegue y trazabilidad antes de habilitar nuevas integraciones. No se solicita autorización a una institución real.

Se definen **12 condiciones vulnerables**, sobre **8 activos ficticios**. La valoración empresarial del modelo contiene **1 riesgo crítico, 8 altos y 3 moderados**. Hay **5 tratamientos P0, 4 P1 y 3 P2**. Los 12 índices actuales superan el objetivo ordinario IRN ≤5; 9 tienen IRN ≥12. Los tres restantes necesitarían una excepción documentada y temporal si siguieran abiertos, que aquí no está aprobada. El máximo actual es 20/25; no se calcula una suma de índices ni pérdida económica.

Pregunta ejecutiva	Respuesta del escenario
Qué amenaza el negocio	Pagos sin independencia, privilegios no gobernados, exposición de información y trazas modificables
Qué está demostrado	Coherencia documental de condiciones, artefactos sintéticos y su exportación; no ejecución real
Qué debe tratarse primero	F02/F04/F06/F07/F10: control de pagos, identidad, autorizadores, CI y auditoría
Qué inversión se propone	CLP 24.180.000 ficticios: 62 jornadas × CLP 300.000 más contingencia del 30 %; no cotización
Qué cambia tras corregir	Se reevaluará P; el impacto permanece y el residual es objetivo pendiente
Qué falta para cerrar	Implementar, comprobar controles positivos/negativos, observar operación y aprobar el cierre

Decisiones de dirección

Aprobar un tratamiento prioritario de control de pagos, identidad y trazabilidad; Asignar un propietario único por tratamiento y presupuesto ficticio verificable; Definir quién acepta excepciones, por cuánto tiempo y con qué controles; Autorizar un retest de alcance acotado como siguiente etapa de un eventual laboratorio; Mantener públicamente el rótulo de simulación y los límites de evidencia.

Controles definidos y su límite

MFA existente en el flujo ordinario; Acceso de cliente requiere autenticación; La identidad de búsqueda carece de permiso de escritura de datos; La identidad de integración no entrega credenciales en la respuesta canario; Entornos y propietarios están documentados.

Son controles compensatorios definidos en el guion, no fortalezas observadas en una entidad real ni prueba de que bloquean todas las variantes.

3 Alcance, arquitectura y contexto de negocio

Objetivos

- Evaluar el aislamiento entre clientes y los permisos por función de los operadores.
- Modelar la independencia de aprobación y la integridad del ciclo de vida de un pago.
- Revisar autenticación, recuperación MFA, revocación y privilegios derivados de identidad corporativa.
- Identificar fronteras de confianza entre Internet, operaciones, integraciones, AD, CI y datos.
- Relacionar condiciones técnicas con impacto en el negocio y apetito de riesgo ficticio.
- Definir tratamientos accionables, responsables, dependencias y criterios de cierre verificables.
- Demostrar un informe ejecutivo y técnico completo generado con report-gen 0.21.2.

Contexto y criticidad

50.000 relaciones de cliente ficticias y 120 operadores, valores de diseño para dimensionar impacto; no es el volumen de datos consultados ni una estadística de clientes reales.

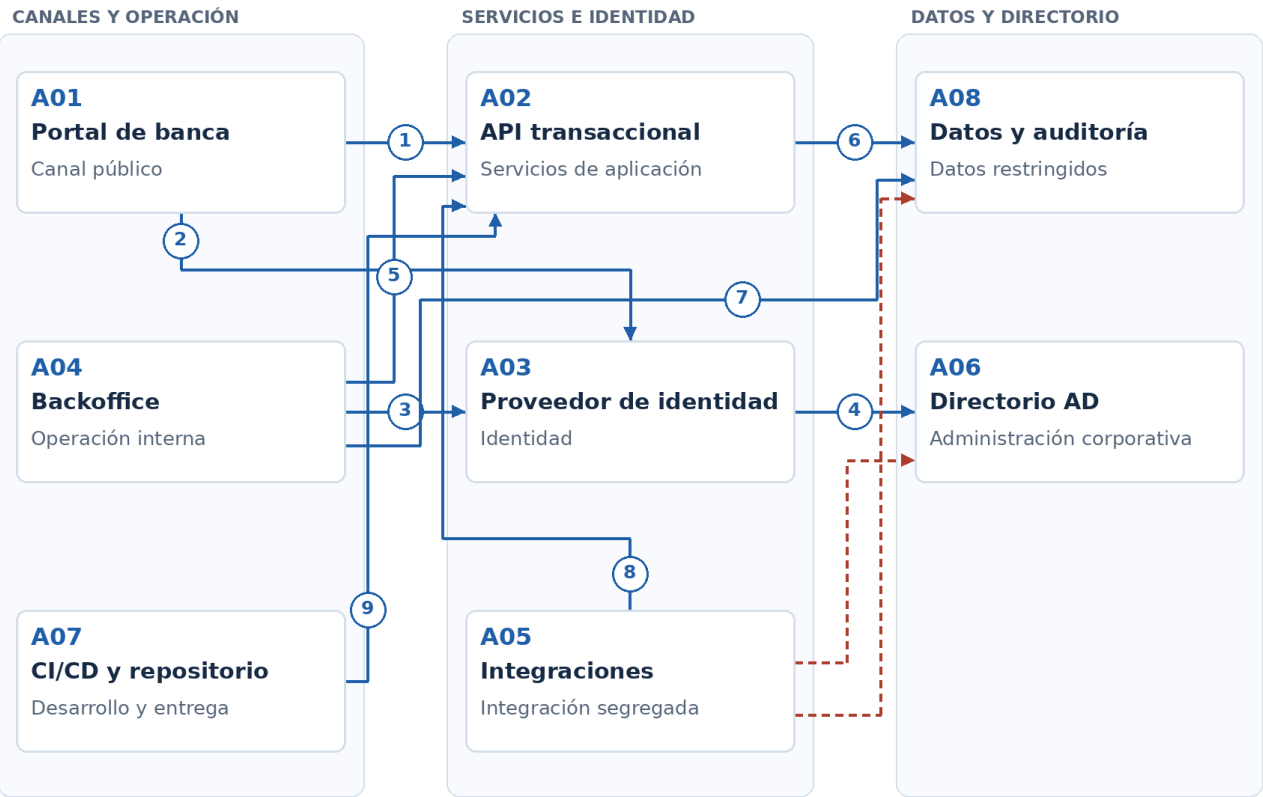
El escenario prioriza impedir pagos sin aprobación independiente, acceso cruzado a información y alteración de trazas. La continuidad se aborda por dependencias y condiciones de tratamiento; no se ejecutan pruebas de carga ni de recuperación ante desastres.

Activo	Zona / propietario	Función y dependencia
A01 Portal de banca digital	Canal público / Gerencia de Canales Digitales	Interfaz de cliente para movimientos, extractos y preparación de pagos Depende de: A02, A03
A02 API transaccional	Servicios de aplicación / Plataforma de Pagos	Autorización por objeto, pagos y emisión de eventos Depende de: A03, A08
A03 Proveedor de identidad	Identidad / IAM	SSO, factores de autenticación, recuperación y revocación Depende de: A06
A04 Backoffice de operaciones	Operación interna / Operaciones y Prevención de Fraude	Soporte, búsqueda, conciliación, aprobación y exportación Depende de: A02, A03, A06, A08
A05 Plataforma de integraciones	Integración segregada / Integraciones	Webhooks empresariales y comunicación con servicios internos definidos Depende de: A02
A06 Directorio corporativo AD	Administración corporativa / Infraestructura e IAM	Grupos corporativos y delegación de altas y bajas Depende de: ninguna descrita
A07 CI/CD y repositorio	Desarrollo y entrega / Ingeniería de Plataforma	Construcción y despliegue de componentes firmados Depende de: A02, A04, A05
A08 Plataforma de datos y auditoría	Datos restringidos / Datos y SOC	Registro de operaciones sintéticas, vistas de consulta y eventos de auditoría Depende de: ninguna descrita

SIMULACIÓN · EVIDENCIA SINTÉTICA · NO EJECUTADO

Arquitectura lógica y fronteras de confianza

Diseño ficticio. Las líneas representan relaciones del modelo, no conexiones observadas en un banco.



Banco Lumbre (entidad ficticia) | report-gen 0.21.2 | Escenario documental, no captura real

Arquitectura sintética: activos y flujos previstos, no infraestructura real

El canal público A01 consume A02 y autentica mediante A03. Los operadores usan A04 desde la zona interna. A03 recibe pertenencias aprobadas de A06. A05 gestiona únicamente destinos empresariales autorizados. A07 despliega mediante identidades de corta duración y aprobación por entorno como diseño objetivo. A08 recibe operaciones y eventos a través de interfaces separadas. El modelo vulnerable contiene excepciones explícitas a estas fronteras, descritas en F01-F12.

Frontera	Origen → destino	Control esperado
TB01	Cliente → A01/A02	Autenticación más autorización de sujeto, objeto y acción
TB02	Preparador → A02/A04	Aprobador independiente y vinculación de autorización a la operación
TB03	Soporte → A03/A04	Recuperación con verificación independiente y permisos por función
TB04	A05 → A06/A08	Denegación de conectividad no aprobada y autenticación de servicio

Frontera	Origen → destino	Control esperado
TB05	A06 → A04	Delegación mínima y control dual de grupos sensibles
TB06	A07 → Aplicaciones	Identidad efímera, entorno acotado y revisión de despliegue
TB07	Aplicación → A08	Separación de escritura operativa, consulta y auditoría inmutable

Incluido / excluido

Incluido:

- A01-A08 y sus fronteras de confianza descritas
- Autorización por objeto y función
- Lógica de aprobación de pagos sintéticos
- Identidad, sesiones y recuperación
- Entradas de backoffice e integraciones
- Privilegios AD y CI definidos en el modelo
- Integridad de eventos y restricciones de acceso a datos

Excluido:

- Infraestructura real o nombres fuera de .example
- SWIFT, tarjetas de pago, adquirencia, cajeros y redes de compensación
- Aplicaciones móviles nativas
- Sucursales, seguridad física y personal real
- Phishing, pretexting y campañas contra personas
- DoS, estrés, ransomware, borrado o degradación de servicios
- Validación de PCI DSS, ISO 27001 o cumplimiento normativo bancario
- Compromiso de proveedores reales, hardware HSM o algoritmos criptográficos
- Pruebas empíricas de restauración, BCP/DR y RTO/RPO

Roles y matriz inicial

Actor	Rol	Permiso legítimo
U01 cliente-canario-a	Cliente	Consultar únicamente documentos propios y preparar pagos de su relación
U02 cliente-canario-b	Cliente de control	Dueño de documentos de contraste
U03 operador-preparador	Preparador	Crear pago sintético; no aprobar el propio
U04 operador-aprobador	Aprobador	Aprobar pagos ajenos después de revisión y factor requerido
U05 soporte-consulta	Soporte limitado	Ver caso asignado y metadatos mínimos; no exportar clientes ni resetear factores privilegiados
U06 mesa-ayuda-iam	Helpdesk delegado	Operar recuperación estándar bajo aprobación; no asignar autorización de pagos
U07 runner-lector	Lector de artefactos CI	Leer el artefacto de una compilación; no desplegar ni administrar
U08 svc-integracion	Identidad de integración	Contactar solo servicios expresamente autorizados
U09 svc-pagos	Identidad de aplicación	Agregar eventos; no actualizar ni eliminar evidencias

4 Metodología, reglas y cobertura diseñada

Evaluación guiada por amenazas y fronteras de confianza. La secuencia integra entendimiento de negocio, matriz de permisos, revisión de autenticación, pruebas de lógica, entradas y privilegios, correlación de evidencias, tratamiento y criterios de retest.

OWASP API Security Top 10 2023, OWASP Cheat Sheet Series y documentación oficial de Microsoft y GitHub se utilizan como referencias técnicas. Las etiquetas no representan certificación, auditoría de cumplimiento ni cobertura exhaustiva de un estándar.

Fase	Entregable del guion
M01 Definición	Activos A01-A08, roles U01-U09, reglas, datos canario y supuestos
M02 Diseño de pruebas	Checks de sujeto/objeto/acción, estados del pago y fronteras
M03 Construcción del escenario	Condiciones vulnerables F01-F12 y evidencias ilustrativas E01A-E12B
M04 Análisis	Precondición, límite demostrado en el modelo, impacto potencial y controles
M05 Tratamiento	R01-R12, dependencias, responsables y aceptación por criterio
M06 Validación prevista	Retest pendiente y controles positivos/negativos; no se asigna estado corregido sin ejecución

Reglas del ejercicio y límites operativos

Regla	Registro
Autorización	La autorización es un documento ficticio del propio ejercicio. No autoriza pruebas contra instituciones, personas o infraestructura externas.
Ventana del guion	Ventana de evaluación representada D1-D5. Son hitos del guion, no una bitácora de trabajo ejecutado.
Límite de datos	Solo dos cuentas cliente, dos pagos sintéticos y un dataset canario de 20 clientes ficticios. Ninguna consulta masiva se ejecuta; las magnitudes empresariales son supuestos separados.
Cambios permitidos	Únicamente cambios reversibles a una membresía canario, un evento canario y una nota de soporte en el guion. No borrar objetos ni modificar configuración real.
Límite de solicitudes	Plan de pruebas de baja frecuencia: máximo 2 solicitudes por segundo y 500 solicitudes por día en un eventual laboratorio; no ejecutado aquí.
Comunicación	Canales y responsables se identifican por rol; no se inventan firmas, correos ni cargos de personas reales.
Limpieza prevista	El plan contempla restaurar membresías, invalidar tokens de prueba, retirar marcadores y registrar el antes/después. No se declara limpieza ejecutada sobre infraestructura inexistente.
Gestión de evidencia	Cada figura y extracto lleva Simulación / evidencia sintética. No se publican tokens utilizables, hashes de contraseña, PII, números de cuenta válidos ni identificadores tributarios.

Condiciones de parada del plan:

- Aparición de datos no canario
- Destino fuera del inventario
- Efecto sobre una operación no sintética
- Respuesta que indique degradación

- Necesidad de privilegios o técnicas fuera del supuesto inicial

Cobertura diseñada, no ejecutada

La matriz enumera controles considerados en el guion y la ficha que los representa. No equivale a un porcentaje de cobertura probado ni a resultados passed/failed sobre un banco.

Activo	Áreas representadas	Fichas / límites
A01	Objetos de cliente, flujo de pagos, sesión y mensajes de error	F01, F02, F03 No probado: Compatibilidad móvil nativa, carga y exposición externa real
A02	Autorización por objeto, independencia de aprobación, integración y eventos	F01, F02, F07, F10 No probado: Liquidación real y conectividad a redes financieras
A03	Refresh, baja, recuperación y reautenticación	F03, F04, F06 No probado: Biometría, dispositivos físicos y resistencia empírica de MFA
A04	Roles, aprobación, búsquedas, exportaciones y renderizado	F02, F03, F04, F06, F09, F11, F12 No probado: Ingeniería social y estaciones reales de operador
A05	Destinos de webhook y fronteras de red	F05, F08 No probado: Proveedores reales y disponibilidad de integraciones
A06	Delegación y pertenencias sensibles	F06, F08 No probado: Domain Admin, DCSync, bosque completo y persistencia
A07	Artefactos, alcance y ciclo de credenciales	F07 No probado: Compromiso de repositorios reales y publicación de software malicioso
A08	Lectura restringida, conexión y mutabilidad de eventos	F05, F08, F09, F10, F11 No probado: Backups, restauración, cifrado HSM y BCP/DR

La coherencia del modelo puede revisarse documentalmente. La confianza de una vulnerabilidad real sería indeterminada hasta ejecutar pruebas en un entorno autorizado. El informe no convierte evidencia inventada en confirmación técnica.

5 Apetito de riesgo, tolerancias, capacidad y BIA

Método de riesgo y límites del caso

Banco Lumbré, sus activos, artefactos y decisiones son ficticios. Las evidencias se construyeron para mostrar redacción y exportación con report-gen 0.21.2; no registran pruebas realizadas en un banco. El método sirve para explicar decisiones de negocio y sus condiciones, no para certificar cumplimiento.

La matriz y sus umbrales son una política propuesta para este escenario. Se inspira en evaluación por escenarios y registro de incertidumbre (RB01), integración de riesgo y objetivos (RB02/RB03), y marcos de apetito/resiliencia bancaria (RB05/RB06). Ninguna referencia aprueba los números del caso. CVSS describe severidad técnica; el índice empresarial incluye contexto y objetivos del negocio (RB04).

Concepto	Uso en el caso
Apetito	Orientación estratégica sobre tipos de riesgo que el negocio está dispuesto a asumir para alcanzar objetivos.
Tolerancia	Límites operativos específicos que concretan el apetito; los define el guion y no una autoridad supervisora.
Capacidad	Límite de exposición que permitirían recursos y obligaciones. No equivale a lo deseado ni a un permiso; aquí no fue demostrado financiera u operativamente.
Riesgo inherente	Escenario contrafactual manteniendo activo, función, actor y exposición, sin acreditar eficacia de controles mitigadores.
Exposición actual del modelo	Exposición estimada con las condiciones narradas y el resultado sintético acotado. No es residual medido de un banco.
Objetivo residual	Proyección tras implantar y probar controles propuestos. Es meta y no cierre, aprobación o retest.
Cobertura de controles	Fracción de objetivos de control evaluados, desglosada entre diseño, implementación y operación; no porcentaje de riesgo eliminado.
Confianza	Calidad y límites de información. Menor confianza nunca reduce automáticamente el índice.

Horizonte: 12 meses hipotéticos desde T0. P es plausibilidad ordinal: no una probabilidad o tasa anual. La confianza en una narración sintética no convierte un artefacto en una ejecución real.

Apetito, tolerancias y operaciones críticas

El directorio ficticio prioriza pagos íntegros, confidencialidad y reconstrucción de eventos. Prefiere retrasar integraciones a mantener autorizaciones defectuosas. No promete riesgo cero: «0» limita rutas o permisos conocidos, no la probabilidad de incidentes.

RTO es el objetivo de recuperación; tolerancia, el máximo de afectación; capacidad, un límite de recursos no demostrado. Cumplir RTO exige integridad, conciliación y RPO. Las ventanas asumidas no autorizan operar hasta ellas. No se evalúan capital, liquidez ni solvencia.

OP01 • Autorización y registro de pagos

Dimensión	Definición propuesta
Apetito	Bajo para fraude y alteración de autorizaciones; el crecimiento digital no justifica una autoaprobación conocida.

Dimensión	Definición propuesta
Tolerancia	0 rutas conocidas de autoaprobación abiertas en producción; 100 % de transiciones de aprobación con maker y checker distintos y autorizados. Interrupción crítica máxima de 60 min por evento en el escenario BIA.
Capacidad	No determinada financieramente. Se asume una ventana operativa máxima de 120 min para el ejercicio, sin ensayo de continuidad que la valide.
Recuperación (RTO / RPO)	RTO: 30 min. RPO: 0 transacciones ya confirmadas al cliente; los mensajes pendientes requieren deduplicación y conciliación.
Dependencias	A02, A03, A04, A06, A07, A08
Límite cualitativo	Una ruta conocida de omisión de independencia de aprobación o alteración de autorizadores impide aceptación rutinaria.

OP02 • Consulta de saldos, extractos y datos de cliente

Dimensión	Definición propuesta
Apetito	Bajo para acceso indebido a datos; se admite degradación temporal de funcionalidades de consulta antes que exponer registros financieros.
Tolerancia	0 rutas conocidas de lectura o exportación fuera del ámbito autorizado; acceso revocado deja de ser renovable antes de 5 min. Máximo 120 min de interrupción de consulta con canal alternativo.
Capacidad	No determinada financieramente. Ventana de soporte manual de 240 min asumida para el guion, sin evidencia de carga o dotación.
Recuperación (RTO / RPO)	RTO: 60 min. RPO: 15 min para réplicas de consulta, conservando el libro de pagos como fuente autoritativa.
Dependencias	A01, A02, A03, A04, A08
Límite cualitativo	Autorización ausente sobre extractos o exportaciones no se compensa con cifrado en tránsito.

OP03 • Conciliación, cierre diario y evidencia financiera

Dimensión	Definición propuesta
Apetito	Muy bajo para pérdida de integridad y trazabilidad; no se acepta borrar o reescribir registros financieros desde la identidad de aplicación.
Tolerancia	0 identidades de aplicación con UPDATE/DELETE sobre auditoría cerrada; 100 % de eventos de aprobación correlacionables. Interrupción máxima de 4 h del cierre en el guion.
Capacidad	No determinada financieramente. Se asume una reconstrucción manual máxima de 8 h, condicionada a conservar evidencias externas e íntegras.
Recuperación (RTO / RPO)	RTO: 120 min. RPO: 0 eventos financieros confirmados; replicas y colas se reconcilian antes de declarar cierre.
Dependencias	A02, A04, A07, A08
Límite cualitativo	Auditoría alterable y sin copia independiente impide aceptación rutinaria, aunque el índice descendiera.

OP04 · Alta de integraciones y cambios de plataforma

Dimensión	Definición propuesta
Apetito	Moderado para retrasar integraciones; bajo para otorgar acceso transversal o privilegios de despliegue.
Tolerancia	0 flujos no aprobados hacia AD/datos; 100 % de artefactos de despliegue sin secretos de larga vida. Se admite posponer integraciones para conservar aislamiento.
Capacidad	No determinada financieramente. El costo de posponer un alta no fue modelado ni equiparado a una pérdida financiera.
Recuperación (RTO / RPO)	RTO: 240 min. RPO: Configuraciones desde control de versiones y copias verificadas; objetivo 24 h para cambios no financieros.
Dependencias	A05, A06, A07, A08
Límite cualitativo	Un secreto crítico activo o una delegación que controla autorizadores requiere contención, no una excepción administrativa ordinaria.

6 Modelo e índice de riesgo empresarial

Escala de plausibilidad P

P	Nivel	Criterio
1	Excepcional	El escenario requiere varias condiciones extraordinarias y barreras independientes eficaces. Una ausencia de prueba no basta para asignar 1.
2	Poco plausible	Exige acceso restringido, especialización o encadenamientos no observados; hay barreras relevantes respaldadas en el guion. Identificar cada prerequisite.
3	Plausible	Requiere rol interno, identidad de servicio o acceso de integración específico; una técnica habitual permite el resultado acotado. No demuestra acceso desde Internet.
4	Muy plausible	Con una cuenta común de cliente u operador y esfuerzo bajo, el guion permite repetir el fallo de una barrera central. El alcance del daño aún depende de controles y procesos adicionales.
5	Altamente facilitado	Superficie ampliamente accesible y repetible a escala, sin barrera pertinente en el modelo. Reservado para una exposición así sustentada; no equivale a certeza ni a frecuencia anual.

Se registran actor, acceso inicial y barreras. Una ruta autenticada no se presenta como anónima; un socket abierto no se interpreta como ejecución. Una técnica conocida no determina una frecuencia real. P sólo ordena la plausibilidad dentro del guion.

Escala de impacto I

Se asigna un nivel por dimensión y se usa el máximo: $I = \max(\text{fraude, datos, disponibilidad, integridad})$. No se suman ni se promedian los impactos.

Impacto 1 • Menor

Dimensión	Criterio
Fraude	Sin movimiento de valor; corrección local sin perjuicio a un cliente.
Datos	Datos públicos o sintéticos sin sensibilidad; sin datos de clientes reales.
Disponibilidad	Interrupción puntual menor de 5 min y alternativa operativa disponible.
Integridad y trazabilidad	Cambio de presentación reversible; registros de negocio y auditoría íntegros.

Impacto 2 • Limitado

Dimensión	Criterio
Fraude	Intento bloqueado antes de aprobar; trabajo operativo acotado sin asiento comprometido.
Datos	Metadatos internos de baja sensibilidad y alcance restringido.
Disponibilidad	De 5 a menos de 15 min; una función no crítica degradada.
Integridad y trazabilidad	Error aislado reconciliable antes del compromiso, con evidencia completa.

Impacto 3 • Material

Dimensión	Criterio
Fraude	Manipulación de un trámite o capacidad preparatoria de fraude que exige pasos adicionales para afectar un pago.
Datos	Datos internos confidenciales o un subconjunto acotado de información personal; impacto dependiente del contenido y alcance.
Disponibilidad	De 15 a menos de 30 min en operación crítica o degradación relevante de un canal.
Integridad y trazabilidad	Estado intermedio o nota operativa manipulable; requiere conciliación, sin prueba de pérdida irreversible del libro.

Impacto 4 • Grave

Dimensión	Criterio
Fraude	Toma de cuenta relevante o capacidad de operar indebidamente que alcanza controles de autorización; daño financiero condicionado, no cuantificado.
Datos	Extractos o datos financieros de clientes accesibles fuera de su ámbito; recuperación/ confidencialidad comprometidas.
Disponibilidad	De 30 a 60 min inclusive en operación crítica; exige continuidad y atención extraordinaria.
Integridad y trazabilidad	Operación o identidad privilegiada comprometida con posibilidad de afectar múltiples registros y conciliación intensiva.

Impacto 5 • Extremo

Dimensión	Criterio
Fraude	La barrera de aprobación independiente de pagos puede omitirse, o una identidad crítica habilita alteración generalizada; no afirma fraude consumado.
Datos	Conjunto amplio de datos financieros y secretos de identidad con efectos difíciles de contener; sólo asignar si el modelo sostiene ese alcance.
Disponibilidad	Más de 60 min en operación crítica o afectación que supera la tolerancia definida.
Integridad y trazabilidad	Capacidad de alterar autorizadores, despliegues críticos o auditoría financiera comprometida; amenaza al registro confiable y a la reconstrucción.

Los tiempos de esta escala son criterios locales para OP01. Cada proceso conserva su tolerancia particular: el incumplimiento de una tolerancia o límite cualitativo prevalece sobre la cifra. No se asignaron pérdidas, multas o daño reputacional monetario sin datos.

Matriz e índice de riesgo de negocio

$IRN = P \times I$, con ambas escalas ordinales 1–5. El producto toma valores de 1 a 25 y permite priorizar; no mide porcentaje, dinero ni probabilidad. Sus bandas son locales: Bajo 1–5; Moderado 6–11; Alto 12–19; Crítico 20–25.

P / I	1	2	3	4	5
1	1 Bajo	2 Bajo	3 Bajo	4 Bajo	5 Bajo
2	2 Bajo	4 Bajo	6 Moderado	8 Moderado	10 Moderado

P / I	1	2	3	4	5
3	3 Bajo	6 Moderado	9 Moderado	12 Alto	15 Alto
4	4 Bajo	8 Moderado	12 Alto	16 Alto	20 Crítico
5	5 Bajo	10 Moderado	15 Alto	20 Crítico	25 Crítico

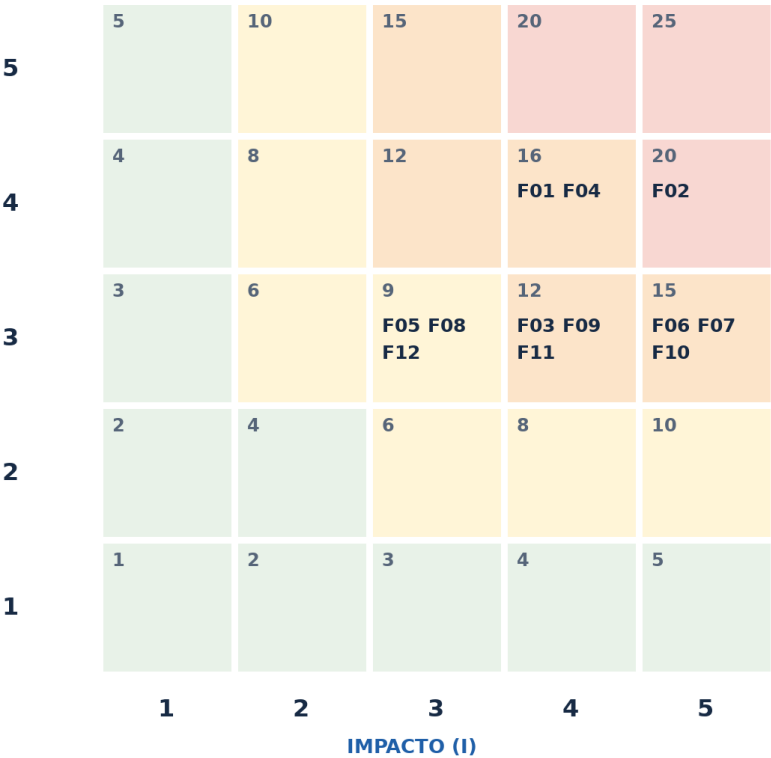
No se suman índices de hallazgo para obtener riesgo total. La diferencia entre índices no es un porcentaje de mejora. El impacto se conserva en la meta salvo reducción del daño sustentada; por eso el plan actúa principalmente sobre P.

SIMULACIÓN · EVIDENCIA SINTÉTICA · NO EJECUTADO

Matriz de riesgo empresarial actual del modelo

Escala ordinal 1-5. IRN = P × I. No representa pérdida esperada, porcentaje ni dato estadístico.

PLAUSIBILIDAD (P)



Posiciones: condiciones F01-F12 del guion. El residual objetivo depende de tratamiento y retest futuro.

Banco Lumbré (entidad ficticia) | report-gen 0.21.2 | Escenario documental, no captura real

Matriz IRN de los doce hallazgos sintéticos; no estadística real

7 Registro y consolidación de riesgos

Registro trazable de exposiciones

Inherente: escenario sin crédito de controles. Actual del modelo: exposición estimada con las condiciones narradas. Para estos 12 hallazgos no se acredita una reducción por barreras no probadas, por lo que ambos valores coinciden. Es preferible mostrar esa igualdad a fabricar una reducción por mencionar MFA, WAF, TLS o registros.

La última columna es una meta: todos los retests están pendientes. Una meta ≤ 5 no demuestra que el riesgo ya sea aceptable.

ID / activos	Inherente P×I	Actual	Meta residual	Prioridad
F01 / A01, A02	4×4=16	16 Alto	2×4=8 pendiente	P1
F02 / A02, A04	4×5=20	20 Crítico	1×5=5 pendiente	P0
F03 / A03, A01, A04	3×4=12	12 Alto	1×4=4 pendiente	P1
F04 / A03, A04	4×4=16	16 Alto	1×4=4 pendiente	P0
F05 / A05, A08	3×3=9	9 Moderado	1×3=3 pendiente	P2
F06 / A06, A03, A04	3×5=15	15 Alto	1×5=5 pendiente	P0
F07 / A07, A02	3×5=15	15 Alto	1×5=5 pendiente	P0
F08 / A05, A06, A08	3×3=9	9 Moderado	1×3=3 pendiente	P2
F09 / A04, A08	3×4=12	12 Alto	1×4=4 pendiente	P1
F10 / A02, A08	3×5=15	15 Alto	1×5=5 pendiente	P0
F11 / A04, A08	3×4=12	12 Alto	1×4=4 pendiente	P1
F12 / A04	3×3=9	9 Moderado	1×3=3 pendiente	P2

ID	Límite de evidencia y justificación
F01	El fallo permite lectura entre dos clientes sintéticos. No se acredita lectura de toda la cartera ni fraude.
F02	La transición a aprobado está representada en el guion; el sistema de liquidación y dinero real están fuera de alcance.
F03	Access token de 5 min no compensa un refresh token de 7 días renovable tras la revocación.
F04	Se representa alteración del factor MFA. No equivale a login sin contraseña; una toma de sesión requiere un paso adicional. I4/P0 responde al factor privilegiado y a la política propuesta, sin compromiso de operadores demostrado.
F05	Sólo contacto y estado de un canario de diagnóstico, sin credenciales ni operaciones. I3 de datos es un impacto condicionado a que otra ruta interna responda con contenido confidencial; no está demostrado.
F06	El modelo permite modificar sólo el grupo financiero, no administrar el dominio. La membresía no significa por sí sola que se haya liquidado un pago.
F07	Un lector CI obtiene un secreto sintético con alcance de despliegue de producción en el modelo. No equivale a firmar código ni a root del host; no se ejecuta un despliegue destructivo.
F08	Un socket TCP abierto sólo prueba conectividad. La autenticación de AD/datos sigue siendo una barrera en el modelo. I3 de disponibilidad requiere un escenario posterior adicional, sin prueba DoS ni interrupción.

ID	Límite de evidencia y justificación
F09	Lectura acotada de filas sintéticas de una vista de conciliación, mediante rol read-only. I4 refleja sensibilidad financiera en el escenario, no alcance total de la cartera; modificación, dump completo y ejecución no están representados.
F10	El writer puede modificar un evento de auditoría, no saldos ni transacciones. I5 se refiere al registro confiable y a la reconstrucción; no afirma fraude consumado ni una investigación real ocultada.
F11	Exportación de 20 filas canario desde un catálogo técnicamente accesible, sin el permiso funcional debido. Distinta de BOLA; I4 se basa en la sensibilidad financiera del conjunto, no en el volumen de la cartera.
F12	Sólo marcador visual en la sesión de un operador. Cookies HttpOnly y step-up conservan barreras sobre pagos en el modelo. I3 refleja manipulación operativa condicionada; no se demuestra exfiltración ni una operación financiera.

Vista consolidada y dependencias

La cartera demostrativa se consolida en seis exposiciones de negocio, manteniendo las referencias a sus hallazgos. El máximo de cada grupo funciona como una envolvente de prioridad, no como probabilidad de la cadena completa. Una entrada compartida, el mismo cliente o una barrera común no se cuentan como pérdidas independientes.

Exposición	Hallazgos	Índice actual	Dependencia
D-01 Exposición de datos de clientes	F01, F09, F11	16 Alto	Mismos datos de clientes por tres entradas. No son tres pérdidas independientes.
D-02 Aprobación indebida de pagos	F02, F06	20 Crítico	La membresía de autorizadores y el backend de aprobación sostienen una misma barrera de negocio.
D-03 Persistencia o suplantación de identidad operativa	F03, F04, F12	16 Alto	Identidad, recuperación y notas internas pueden compartir sesiones; no se afirma una cadena completa ejecutada.
D-04 Acceso entre zonas no autorizado	F05, F08	9 Moderado	Contactar un canario y tener acceso TCP no equivalen a comprometer AD o datos.
D-05 Alteración de software crítico	F07	15 Alto	Secreto y rol de despliegue se consideran una sola exposición habilitadora.
D-06 Pérdida de evidencia financiera confiable	F10	15 Alto	Agrava la reconstrucción de D-02, pero no se suma como un nuevo monto de fraude.

Índice de postura del alcance: 20/25, Crítico, porque la exposición D-02 incluye F02=20 y vulnera independencia de aprobación. Distribución: 1 exposición Crítica, 4 Altas, 1 Moderada. No es un promedio, una probabilidad ni el riesgo global de Banco Lumbré. En hallazgos: 1 Crítico de negocio, 8 Altos y 3 Moderados. La severidad técnica puede tener otra distribución.

Los 12 hallazgos superan el objetivo ordinario $IRN \leq 5$. Nueve tienen $IRN \geq 12$ y requieren contención/plan; tres son Moderados y son elegibles para una excepción temporal, pero no hay ninguna aprobada. El plan proyecta un máximo residual de 8, debido a F01: aún es Moderado y exige reevaluación/decisión. No se anuncia un estado Verde ficticio tras la propuesta.

8 Tratamiento, responsables, plazos e inversión

Prioridades y plazos propuestos

Estos son SLA internos ficticios de respuesta a hallazgos, no plazos regulatorios ni compromisos vigentes de una entidad. El reloj parte en T0, aprobación del plan. Distinguir horas/días corridos de días hábiles. Prioridad no equivale automáticamente a CVSS.

Prioridad	Disparador	Triage	Contención	Arreglo	Retest
P0	Barrera de integridad de pagos, autorizadores, despliegue o auditoría comprometida; prevalece aunque el índice sea 12–19.	4 h corridas	24 h corridas	7 días corridos	Antes de restituir la ruta; máximo 2 días después del arreglo
P1	Índice actual ≥ 12 sin el disparador P0; datos, acceso o identidad de impacto grave.	1 día hábil	3 días hábiles	30 días corridos	5 días hábiles desde el arreglo
P2	Índice 6–11 y efecto acotado; no existe evidencia de red line comprometida.	3 días hábiles	10 días hábiles si la ruta sigue expuesta	60 días corridos	10 días hábiles desde el arreglo
P3	Índice 1–5 sin límite cualitativo vulnerado; mantenimiento y mejora.	10 días hábiles	Según necesidad documentada	90 días corridos	En la siguiente ventana, antes de cerrar

Prioridad	Hallazgos	Autoridad y seguimiento
P0	F02, F04, F06, F07, F10	Gerente responsable + CISO + CRO; escalamiento al Comité de Riesgo el mismo día.
P1	F01, F03, F09, F11	Owner de negocio + CISO + CRO; excepción temporal con vencimiento.
P2	F05, F08, F12	Owner de negocio + CISO; Riesgo revisa las excepciones.
P3	Ninguno en este caso	Owner de negocio, con revisión de Seguridad.

Una dependencia o disponibilidad insuficiente obliga a escalar, no a mover silenciosamente la fecha. Contener no equivale a arreglar; corregir no equivale a verificar.

Plan de trabajo 0–90 días

Ola	Ventana	Objetivo / hallazgos	Trabajo
W0	0–24 h desde T0	Contener barreras críticas (F02, F04, F06, F07, F10)	Suspender ruta de autoaprobación y recuperación vulnerable, retirar delegación, revocar credencial y preservar auditoría independiente; verificar impacto funcional antes de restituir.
W1	Días 1–7 desde T0	Arreglar P0 y validar condiciones de reapertura (F02, F04, F06, F07, F10)	Implementar controles permanentes, regresión permitida/prohibida, registro correlacionable y revisión del owner. Reabrir sólo tras resultados documentados.
W2	Días 8–30 desde T0	Cerrar exposición de datos y persistencia de acceso (F01, F03, F09, F11)	Arreglos de autorización, revocación, consultas y exportación; retest por dos identidades y caso permitido. Consolidar KRIs.

Ola	Ventana	Objetivo / hallazgos	Trabajo
W3	Días 31–60 desde T0	Reducir rutas internas y XSS (F05, F08, F12)	Listas de salida, segmentación y escape contextual; probar denegaciones y flujos necesarios, revisar dependencias de las seis exposiciones.
W4	Días 61–90 desde T0	Integrar prácticas y demostrar operación sostenida (F01, F02, F03, F04, F05, F06, F07, F08, F09, F10, F11, F12)	Ensayo de continuidad seguro, revisión de permisos, prueba de auditoría y tablero de riesgo. No llamar cerrado un hallazgo que sólo tenga una tarea terminada.

Conservar versión de código, configuración, tester y evidencias nuevas por cambio R01–R12. Cada fase necesita un control de salida, un responsable y un punto de reversión seguro. Si un ensayo amenaza datos o integridad, detenerlo y reevaluar el alcance; este caso no ejecuta pruebas destructivas.

Escenario de inversión, sin falsa precisión financiera

Presupuesto ilustrativo: 62 jornadas-persona a una tarifa inventada de CLP 300.000 por jornada. Se incluye para mostrar trazabilidad de decisiones de respuesta, no como cotización, salario, pérdida esperada o estimación de ROI. Jornadas agregadas no equivalen a duración calendario.

Frente	Hallazgos	Jornadas	Costo CLP ficticio
Identidad y aprobaciones	F02, F03, F04, F06	20	6.000.000
Autorización, consulta y exportación	F01, F09, F11, F12	18	5.400.000
Plataforma, redes y auditoría	F05, F07, F08, F10	16	4.800.000
Retest independiente y gobierno	F01, F02, F03, F04, F05, F06, F07, F08, F09, F10, F11, F12	8	2.400.000

Base CLP 18.600.000 + contingencia de planificación 30 % (CLP 5.580.000) = CLP 24.180.000. Impuestos, licencias y costos de interrupción no están incluidos. Se prioriza el paquete por barreras de negocio y dependencias, sin repartir beneficios monetarios inventados entre hallazgos.

Una evaluación económica real necesitaría volumen de operaciones, montos expuestos, fraude histórico, capacidad de recuperación, costos de contención, contratos y obligaciones verificadas. Tampoco se infiere capacidad financiera a partir de este presupuesto de remediación.

Trazabilidad del tratamiento

Tratamiento	Objetivo de control	Responsable / prioridad
R01 → F01	Autorización por objeto y relación cliente-cuenta en cada lectura; regresión cruzada con dos identidades.	Gerencia de Canales Digitales P1
R02 → F02	Separación maker-checker en el backend y política de identidad/rol; rechazar la autoaprobación por API.	Gerencia de Pagos P0
R03 → F03	Revocación de familias de refresh tokens y bloqueo del sujeto; verificación de eventos de baja y cambio de credencial.	Gerencia de Identidad P1
R04 → F04	Verificar identidad por canal independiente y aprobación dual para recuperación privilegiada; trazabilidad de solicitudes.	Gerencia de Operaciones e Identidad P0
R05 → F05	Lista de destinos y resolución validada; proxy de salida y bloqueo de rangos internos según flujos autorizados.	Gerencia de Integraciones P2

Tratamiento	Objetivo de control	Responsable / prioridad
R06 → F06	Retirar delegaciones excesivas, separar administración de identidad y aprobación financiera; cambios con revisión dual.	Gerencia de Infraestructura y Pagos P0
R07 → F07	Revocar el secreto sintético equivalente, reducir permisos, credenciales efímeras y escaneo de artefactos antes de publicar.	Gerencia de Ingeniería de Plataforma P0
R08 → F08	Segmentación por flujos explícitos y política deny-by-default; validar tanto rechazos como comunicaciones necesarias.	Gerencia de Redes P2
R09 → F09	Consultas parametrizadas, rol de base de datos de mínimo privilegio y pruebas negativas del buscador.	Gerencia de Aplicaciones Internas P1
R10 → F10	Separar escritura de aplicación y retención de auditoría; almacenamiento inmutable y conciliación independiente.	Gerencia de Datos y Control Financiero P0
R11 → F11	Autorizar la función de exportación por rol y finalidad, controles de volumen y registro de descargas.	Gerencia de Datos y Operaciones P1
R12 → F12	Escape contextual, saneamiento adecuado y CSP como defensa adicional; pruebas de notas con datos no confiables.	Gerencia de Aplicaciones Internas P2

Las correcciones detalladas y los criterios prospectivos de comprobación están en cada ficha F01–F12. Las fechas del documento no inician el SLA: T0 sería la aprobación del plan en un eventual laboratorio. No hay fechas objetivo vigentes asignadas ni compromisos de un cliente.

Cobertura de control, indicadores y seguimiento

Cobertura de controles y confianza

Doce objetivos de control se vinculan uno a uno con R01–R12. Escribir una recomendación da cobertura de diseño propuesta, no evidencia de instalación ni de operación. Estado común: 12/12 objetivos definidos; 0/12 verificados en una entidad real; 0/12 remediaciones cerradas con retest. No se dice que los 12 controles están probados.

ID / cambio	Objetivo de control	Estado
F01 / R01	Autorización por objeto y relación cliente-cuenta en cada lectura; regresión cruzada con dos identidades.	Propuesto; implementación y retest pendientes
F02 / R02	Separación maker-checker en el backend y política de identidad/rol; rechazar la autoaprobación por API.	Propuesto; implementación y retest pendientes
F03 / R03	Revocación de familias de refresh tokens y bloqueo del sujeto; verificación de eventos de baja y cambio de credencial.	Propuesto; implementación y retest pendientes
F04 / R04	Verificar identidad por canal independiente y aprobación dual para recuperación privilegiada; trazabilidad de solicitudes.	Propuesto; implementación y retest pendientes
F05 / R05	Lista de destinos y resolución validada; proxy de salida y bloqueo de rangos internos según flujos autorizados.	Propuesto; implementación y retest pendientes
F06 / R06	Retirar delegaciones excesivas, separar administración de identidad y aprobación financiera; cambios con revisión dual.	Propuesto; implementación y retest pendientes
F07 / R07	Revocar el secreto sintético equivalente, reducir permisos, credenciales efímeras y escaneo de artefactos antes de publicar.	Propuesto; implementación y retest pendientes
F08 / R08	Segmentación por flujos explícitos y política deny-by-default; validar tanto rechazos como comunicaciones necesarias.	Propuesto; implementación y retest pendientes
F09 / R09	Consultas parametrizadas, rol de base de datos de mínimo privilegio y pruebas negativas del buscador.	Propuesto; implementación y retest pendientes
F10 / R10	Separar escritura de aplicación y retención de auditoría; almacenamiento inmutable y conciliación independiente.	Propuesto; implementación y retest pendientes
F11 / R11	Autorizar la función de exportación por rol y finalidad, controles de volumen y registro de descargas.	Propuesto; implementación y retest pendientes
F12 / R12	Escape contextual, saneamiento adecuado y CSP como defensa adicional; pruebas de notas con datos no confiables.	Propuesto; implementación y retest pendientes

Confianza: media en coherencia del guion, no evaluada en el mundo real. Las capturas y transcripciones sintéticas sostienen la narración; no sostienen actividad comercial, exposición real o eficacia de controles. Menor confianza no baja P ni I. Registrar incertidumbres, pedir prueba del alcance y separar escenarios alternativos del resultado demostrado.

Indicadores de riesgo KRI

Los umbrales se definen antes de medir. No evaluado es un estado distinto de Verde. Las pocas líneas base numéricas describen rutas/identidades incluidas en el guion; no son indicadores observados en producción.

KRI01 • Rutas conocidas de autoaprobación abiertas

Campo	Definición
Definición y unidad	Cantidad de rutas API/UI en que el mismo sujeto puede crear y aprobar una instrucción de pago sin independencia efectiva. Unidad: rutas
Verde / ámbar / rojo	0 / No aplica: cualquier ruta dispara rojo / ≥ 1
Frecuencia	Diaria mientras P0 esté abierto; mensual después
Responsable y fichas	Gerencia de Pagos F02, F06
Línea base del guion	1 ruta F02 en el guion; no es una medición de producción.

KRI02 • Rutas de datos de cliente fuera del ámbito autorizado

Campo	Definición
Definición y unidad	Cantidad de rutas distintas con evidencia de lectura/exportación indebida; contar una ruta una vez aunque tenga varias capturas. Unidad: rutas
Verde / ámbar / rojo	0 / Pendiente de evidencia se informa como no evaluado, no verde / ≥ 1
Frecuencia	Semanal y después de cambios de autorización
Responsable y fichas	Gerencia de Datos F01, F09, F11
Línea base del guion	3 rutas sintéticas distintas en el guion.

KRI03 • Latencia de revocación efectiva

Campo	Definición
Definición y unidad	Tiempo desde evento de baja hasta rechazo tanto del token activo como de la renovación; informar máximo y tamaño de muestra. Unidad: minutos
Verde / ámbar / rojo	≤ 5 min / > 5 y ≤ 15 min / > 15 min o todavía renovable
Frecuencia	Semanal, tras cambios de IdP y ante bajas críticas
Responsable y fichas	Gerencia de Identidad F03
Línea base del guion	Renovación sintética representada después de revocar; no se midieron 7 días de ejecución.

KRI04 • Identidades capaces de modificar auditoría cerrada

Campo	Definición
Definición y unidad	Identidades operativas con permisos de modificación/borrado sobre eventos financieros finalizados, excluyendo procedimiento de retención aprobado e independiente. Unidad: identidades
Verde / ámbar / rojo	0 / Inventario incompleto: no evaluado / ≥ 1
Frecuencia	Diaria durante contención; mensual tras estabilizar
Responsable y fichas	Gerencia de Control Financiero F10
Línea base del guion	1 identidad de aplicación sintética representada.

KRI05 • Excepciones de riesgo vencidas

Campo	Definición
Definición y unidad	Aceptaciones o extensiones cuya fecha final pasó sin renovación documentada, revisión de controles o cierre verificado. Unidad: excepciones
Verde / ámbar / rojo	0 / Vencen en ≤ 7 días / ≥ 1 vencida
Frecuencia	Semanal; aviso a 14 y 7 días del vencimiento
Responsable y fichas	Oficina de Riesgo Alcance transversal; sin ficha individual
Línea base del guion	No medido; ninguna excepción está aprobada en este caso.

KRI06 • Tiempo de indisponibilidad de pagos por evento

Campo	Definición
Definición y unidad	Tiempo de afectación de OP01 medido desde la primera incapacidad de prestar la operación hasta recuperar un servicio íntegro y reconciliado. Unidad: minutos/evento
Verde / ámbar / rojo	≤ 15 min / > 15 y ≤ 60 min / > 60 min
Frecuencia	Por incidente y ensayo de continuidad
Responsable y fichas	Gerencia de Continuidad F07
Línea base del guion	No medido; el caso no ejecuta DoS ni un ensayo de recuperación.

KRI07 • Flujos de integración fuera de la matriz aprobada

Campo	Definición
Definición y unidad	Número de combinaciones origen-destino-servicio accesibles y sin aprobación vigente. La conectividad no se presenta como acceso a datos. Unidad: flujos
Verde / ámbar / rojo	0 / Matriz desactualizada: no evaluado / ≥ 1
Frecuencia	Semanal y después de cada regla de red
Responsable y fichas	Gerencia de Redes F05, F08
Línea base del guion	Flujos sintéticos E05/E08; inventario completo no evaluado.

KRI08 • Credenciales críticas de larga vida expuestas

Campo	Definición
Definición y unidad	Credenciales activas de despliegue o privilegio financiero accesibles en artefactos no autorizados; deduplicar por identificador del secreto. Unidad: credenciales
Verde / ámbar / rojo	0 / Rotación iniciada pero no verificada / ≥ 1 activa expuesta
Frecuencia	Cada build y revisión diaria de contención
Responsable y fichas	Gerencia de Plataforma F07
Línea base del guion	1 credencial sintética modelada; no existe secreto real publicado.

Los indicadores y sus valores son definidos para el caso ficticio; no representan mediciones operativas del banco. Una excepción requiere decisiones documentadas y vencimiento.

Indicadores de ejecución KPI

Los KPI siguientes evalúan la ejecución del plan propuesto. Las metas no son resultados alcanzados; las líneas base del guion se conservan sin inventar retests ni mediciones.

KPI01 • Remediaciones cerradas con retest

Campo	Definición
Fórmula	Remediaciones con prueba negativa y funcional satisfactoria / 12 remediaciones × 100.
Meta	100 % al finalizar el plan, sin usar la cantidad de commits como sustituto.
Línea base del guion	0/12 cerradas; no se realizó retest.
Responsable	CISO

KPI02 • Cumplimiento de plazo P0

Campo	Definición
Fórmula	P0 contenidos y corregidos dentro de sus plazos / 5 P0 × 100; reportar contención y arreglo por separado.
Meta	100 % para ambos hitos.
Línea base del guion	No medido; plazos de un plan propuesto, no incidente real.
Responsable	CIO

KPI03 • Cobertura de pruebas de autorización

Campo	Definición
Fórmula	Casos de autorización ejecutados que incluyen sujetos permitidos y prohibidos / catálogo aplicable aprobado × 100; acompañar aprobados, fallidos y no ejecutados.
Meta	100 % del catálogo crítico antes de liberación.
Línea base del guion	Catálogo propuesto; ejecución no realizada.
Responsable	Gerencia de Calidad

KPI04 • Propietarios y fecha de cierre asignados

Campo	Definición
Fórmula	Hallazgos con owner de negocio, responsable técnico y fecha explícita / 12 × 100.
Meta	100 % antes de iniciar implementación.
Línea base del guion	12/12 owners propuestos; 0/12 asignaciones aprobadas por una entidad real.
Responsable	Oficina de Riesgo

KPI05 • Controles relevantes con prueba vigente

Campo	Definición
Fórmula	Objetivos de control con diseño, implementación y operación evaluados / 12 objetivos aplicables × 100; desglosar cada dimensión, sin convertirlo a reducción del riesgo.
Meta	100 % de los 12 objetivos antes de cerrar el proyecto.
Línea base del guion	0/12 verificados en un banco real; 12/12 objetivos especificados en el caso.
Responsable	CISO

KPI06 • Ensayo de recuperación dentro de tolerancia

Campo	Definición
Fórmula	Operaciones críticas recuperadas íntegras dentro del RTO y tolerancia / operaciones incluidas en el ensayo × 100.
Meta	100 %, con revisión de RPO y conciliación además del tiempo.
Línea base del guion	No medido; ningún ensayo de continuidad fue ejecutado.
Responsable	Gerencia de Continuidad

10 Gobierno de aceptación, supuestos y cierre

Decisiones, aceptación y cierre

Objetivo ordinario: IRN ≤ 5 por exposición y ningún límite cualitativo vulnerado. IRN 6–11 admite una excepción propuesta de hasta 30 días con owner, controles compensatorios comprobables y fecha de término. IRN ≥ 12 exige contención y plan; una autorización de emergencia por hasta 7 días debe documentar por qué cambiar de inmediato dañaría más la operación. La excepción no reetiqueta el riesgo como Bajo.

Los límites cualitativos prevalecen: autoaprobación de pagos, cambio no independiente de autorizadores, secreto crítico activo expuesto, auditoría alterable sin copia independiente y lectura de cliente fuera de ámbito. No son aceptables de forma rutinaria aunque un cálculo aislado parezca pequeño.

Rol	Responsabilidad
Directorio	Define apetito y exige seguimiento; no hay acta real aprobada.
Owner de negocio	Rinde cuentas por el riesgo del proceso; Seguridad no sustituye al dueño del negocio.
Responsable técnico	Implanta el arreglo y entrega evidencia.
CISO	Revisa eficacia técnica y condiciones de seguridad.
CRO	Desafía evaluación, acumulaciones y excepción frente al apetito.
Control financiero	Valida integridad y conciliación.
Retest independiente	Repite fallo y caso permitido con identidad independiente; no aprueba su propio desarrollo.
Auditoría interna	Aseguramiento posterior, sin asumir la gestión ni aprobar el control que auditará.

Una decisión contiene: ID de decisión; Hallazgo y escenario consolidado; Owner de negocio responsable; Motivo y alternativas rechazadas; Exposición actual y límites cualitativos; Control compensatorio y evidencia; Autoridad que aprueba; Fecha de inicio y vencimiento; Hito y responsable de corrección; KRI y frecuencia; Condición de revocación; Resultado de revisión/retest.

Ejemplo DEC-01 para F08: Gerencia de Redes propone una excepción hasta T0+30 días para completar la segmentación, condicionada a restringir el flujo, verificar la regla y revisar KRI07. Sólo se probó conectividad en el guion; lectura o ejecución no demostradas tampoco son imposibles. Estado: propuesta sin aprobación y sin prueba nueva.

Cierre: Un ticket terminado o un commit no cierra un hallazgo. Arreglo implementado y negativo del fallo deben pasar junto con la función legítima. Probar API y UI, roles, revocación y objetos adicionales según riesgo. Documentar evidencia nueva, fecha, versión, tester y límites. Reevaluar P, I, IRN y decisión; no copiar automáticamente la meta. Excepción vencida, cambio relevante o KRI rojo reabre y escala la decisión.

Supuestos y condiciones de revisión

ID	Supuesto o límite
AS01	Entorno, identidades y registros son sintéticos; las cuentas no pertenecen a clientes reales.
AS02	T0 es la aprobación ficticia del plan, no una fecha real de inicio de incidente.
AS03	Capacidades y objetivos BIA son supuestos de diseño; no hubo ensayo de continuidad ni evaluación de solvencia.
AS04	El índice considera las condiciones del guion, no amenazas ni frecuencia observadas en una entidad.

ID	Supuesto o límite
AS05	No se representa una cadena completa desde Internet hasta liquidación, AD y libro contable; cada enlace conserva sus prerequisites.
AS06	No hay mitigaciones ejecutadas ni retest. Todos los valores objetivo son proyecciones.
AS07	No hay análisis de obligación legal local, multas, capital regulatorio ni declaración de cumplimiento.
AS08	Las cifras CLP corresponden sólo al ejercicio de planificación de respuesta; no cuantifican una pérdida económica probable.

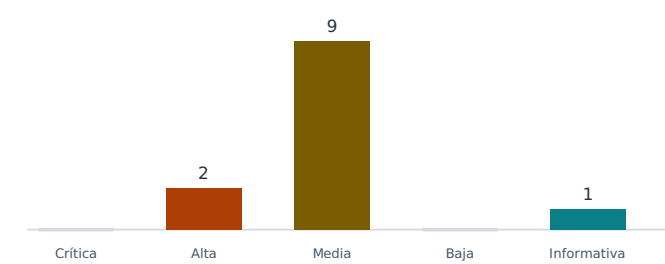
El registro debe revisarse si cambian roles, alcance de datos, controles, exposición, canal, proveedor o arquitectura. Las decisiones propuestas y sus vencimientos requieren una autoridad real antes de aplicar este método a una organización.

Estado de cada ficha

Todos los hallazgos tienen **estado abierto y verificación técnica sin verificar**, porque no se ejecutó la arquitectura descrita. Hay **0 registros de retest**. Los extractos A/B son evidencias sintéticas construidas, no capturas de resultados obtenidos. Ningún tratamiento se declara eficaz o aceptado por una entidad real.

11 Resumen de hallazgos

La evaluación identificó 12 hallazgos con la siguiente clasificación de severidad: 2 alta, 9 media, 1 informativa.



#	Severidad	Hallazgo	Pág.
1	Alta (7.1)	Delegación AD sobre autorizadores financieros	41
2	Alta (8.1)	Credencial de despliegue expuesta en CI	43
3	Media (6.5)	Acceso cruzado a extractos	29
4	Media (6.5)	Autoaprobación de pagos por el preparador	31
5	Media (6.5)	Refresh renovable tras la revocación	34
6	Media (4.9)	Recuperación MFA sin verificación independiente	36
7	Media (4.3)	Webhook hacia destino interno no autorizado	39
8	Media (6.5)	Inyección SQL en búsqueda de conciliación	48
9	Media (4.9)	Auditoría financiera modificable por aplicación	50
10	Media (6.5)	Exportación de clientes por un rol de consulta	53
11	Media (5.4)	Script almacenado en notas de backoffice	55
12	Informativa (0.0)	Conectividad de integración no aprobada	46

12 Hallazgos

F01 Acceso cruzado a extractos		Media 6.5
CWE	CWE-639	
CVSS 3.1	6.5 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	
Descripción (incl. causa raíz)	SIMULACIÓN: condición definida en el guion; sin verificación contra un sistema real. Nombre completo: Acceso cruzado a extractos por falta de autorización del objeto. La API del modelo autentica al solicitante, pero recupera el extracto usando únicamente su identificador. El cliente A puede recibir el extracto canario del cliente B sin una relación autorizada. Conocer el identificador es una precondition; la aleatoriedad del ID no repara la autorización. Causa raíz: La consulta no vincula el objeto con el conjunto de relaciones permitidas al sujeto ni verifica la acción de descarga. El control de propiedad de la interfaz no se replica en la API.	
Impacto de seguridad	La misma condición en un entorno real podría exponer información financiera y hábitos de transacción, generar reclamaciones e investigaciones y erosionar confianza. El alcance de una posible extracción masiva no está demostrado en el guion. Riesgo de negocio: inherente y actual 16/25 (Alto), P=4, I=4. Residual objetivo 8/25, pendiente. Prioridad P1. Límite: El fallo permite lectura entre dos clientes sintéticos. No se acredita lectura de toda la cartera ni fraude.	
Dominio afectado	GET api.bancolumbre.example/v1/extractos/{extracto_id}	
Remediación	Aplicar una política central de sujeto, objeto y acción en servidor para cada lectura y descarga. Consultar el recurso dentro del ámbito autorizado y fallar de forma cerrada. Mantener IDs opacos como defensa complementaria, nunca como control principal. Responsable de riesgo: Gerencia de Canales Digitales. Tratamiento R01. Estado abierto y sin verificar; 0 retests.	
Referencias	- https://api-security.owasp.org/editions/2023/en/0xa1-broken-object-level-authorization/ - https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html	

Procedimiento detallado

- Justificación de severidad técnica** AV:N/AC:L por endpoint de red determinista. PR:L por cliente autenticado. C:H estima el peor caso razonable de un extracto financiero sensible bajo la condición del modelo; no representa extracción completa observada. I/A:N: no escritura ni indisponibilidad atribuida. CVSS representa la consecuencia técnica acotada del guion y no sustituye el riesgo empresarial.
- Actor y preconditiones del guion** U01 cliente-canario-a; objeto de contraste perteneciente a U02. Sesión cliente válida U01; Identificador del objeto de U02 suministrado por el dataset de contraste; Permiso normal para descargar los propios extractos.
- Paso documental 1 (no ejecutado)** Obtener un extracto propio y registrar su propietario canario como control positivo.
- Paso documental 2 (no ejecutado)** Mantener la sesión U01 y sustituir exclusivamente el identificador por el objeto de U02.

5. **Paso documental 3 (no ejecutado)** Comparar sujeto, propietario y resultado del modelo, sin enumerar identificadores ni descargar otros registros.
6. **E01A · transcripción sintética completa** El modelo construye una violación de la relación sujeto-objeto; no demuestra una extracción real.

```
Sujeto: cliente-canario-a
Objeto: EXT-CANARIO-B-001
Propietario declarado en dataset: cliente-canario-b
Respuesta ilustrada: 200
Contenido: EXTRACTO_CANARIO_B / cuenta TEST-B / movimientos ficticios
```

7. **E01B · transcripción sintética completa** Separa falta de autenticación de falta de autorización por objeto.

```
U01 → EXT-CANARIO-A-001: permitido
U01 → EXT-CANARIO-B-001: permitido indebidamente
Anónimo → EXT-CANARIO-B-001: denegado
Objetivo corregido: acceso cruzado denegado sin revelar existencia
```

8. Estos extractos se construyeron para el modelo. No son respuestas capturadas de una infraestructura real.

SIMULACIÓN · EVIDENCIA SINTÉTICA · NO EJECUTADO

F01 · Acceso cruzado a extractos

Extractos abreviados. Transcripciones completas en el informe; no son capturas de un sistema real.

E01A · Extracto HTTP sintético

Sujeto: cliente-canario-a
Extracto B ajeno: entregado a A
El modelo construye una violación de la relación sujeto-objeto; no demuestra una extracción real.

E01B · Matriz de autorización

Objeto propio: permitido
Objeto ajeno: acceso indebido
Separa falta de autenticación de falta de autorización por objeto.

Banco Lumbre ficticio | extractos ilustrativos | Véase la transcripción A/B y los límites de la ficha

Figura 1. SIMULACIÓN · E01A: cliente A recibe extracto de cliente B; E01B: control positivo y denegación anónima. Evidencia sintética no ejecutada.

9. **Resultado definido en el modelo** Lectura de un único extracto ajeno compuesto por registros canario.
10. **Controles actuales definidos** Sesión autenticada obligatoria; Solo dos cuentas y un objeto de contraste en el escenario. No se les atribuye una eficacia real ni rebaja automática del índice.
11. **Límites del resultado** No modificación de datos; No acceso anónimo; No enumeración masiva; No demuestra que todos los endpoints compartan la misma falla; No atribuir una multa ni una pérdida monetaria sin datos y análisis independientes.
12. **Contención propuesta** Limitar temporalmente la descarga a una consulta que incluya las relaciones autorizadas del sujeto; registrar denegaciones sin incluir el documento.
13. **Prevención y dependencias** Matriz de autorización automatizada con dos clientes, productos propios, compartidos y ajenos; revisión de todos los handlers que reciben identificadores. Dependencias: Inventario de relaciones cliente-producto; Política de cuentas compartidas y poderes. Responsable técnico: Plataforma de Pagos / responsable de API.
14. **Retest prospectivo: control positivo** PENDIENTE; no ejecutado. U01 descarga su extracto y una cuenta compartida expresamente autorizada.
15. **Retest prospectivo: control negativo** U01 no obtiene objetos de U02 al variar IDs por ruta, query o cuerpo; denegación consistente y sin contenido financiero.

16. Criterio de cierre y regresión Todas las combinaciones de la matriz sujeto-objeto-acción quedan verificadas; evidencia de respuesta y trazabilidad de la política adjuntas. Confirmar que alias, exportación y caché no reabren el acceso cruzado. La meta residual se reevaluará tras implementar y probar; aquí no se declara corregido.

17. Activos afectados

- portal.bancolumbre.example
- api.bancolumbre.example

F02 Autoaprobación de pagos por el preparador

Media 6.5

CWE	CWE-863
CVSS 3.1	6.5 <code>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N</code>
Descripción (incl. causa raíz)	SIMULACIÓN: condición definida en el guion; sin verificación contra un sistema real. Nombre completo: El preparador puede aprobar su propio pago omitiendo la independencia de funciones. La interfaz evita que el preparador pulse Aprobar, pero el modelo de API admite la transición pendiente→aprobado cuando U03 la solicita para un pago creado por él mismo. U03 satisface su propio factor de operación canario; el servidor comprueba identidad y factor, pero no exige rol de aprobador ni una identidad distinta del preparador. Autenticación reforzada del mismo actor no constituye independencia de funciones. Causa raíz: El estado del pago y la separación maker-checker se validan en la interfaz. La función de aprobación valida el factor del sujeto, pero no contrasta rol vigente, sujeto creador y versión del pago como condiciones independientes de autorización.
Impacto de seguridad	Un preparador que satisface su propio factor, o un actor con control de su sesión y factor, podría originar instrucciones sin segunda revisión. El escenario no demuestra que una cuenta comprometida sin su factor pueda operar. La ausencia del control preventivo de independencia es material aunque no se cuantifique pérdida ni liquidación. Riesgo de negocio: inherente y actual 20/25 (Crítico), P=4, I=5. Residual objetivo 5/25, pendiente. Prioridad P0. Límite: La transición a aprobado está representada en el guion; el sistema de liquidación y dinero real están fuera de alcance.
Dominio afectado	<code>POST api.bancolumbre.example/v1/pagos/{pago_id}/aprobar</code>
Remediación	Implementar máquina de estados en servidor con rol vigente de aprobador y subject distinto de created_by. Vincular autorización a importe, destinatario, versión y operación exactos. Invalidar aprobación si cambian esos datos y registrar cada intento. Ejecutar la transición de forma atómica. Responsable de riesgo: Gerencia de Pagos. Tratamiento R02. Estado abierto y sin verificar; 0 retests.
Referencias	• https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html • https://cheatsheetseries.owasp.org/cheatsheets/Transaction_Authorization_Cheat_Sheet.html

Procedimiento detallado

- Justificación de severidad técnica** PR:L es un preparador que opera sus propios pagos. I:H representa la pérdida de autorización independiente sobre la instrucción. C/A:N por ausencia de fuga o indisponibilidad. CVSS 6,5 no incluye

fraude económico, monto, apetito ni criticidad empresarial. CVSS representa la consecuencia técnica acotada del guion y no sustituye el riesgo empresarial.

2. **Actor y precondiciones del guion** U03 operador-preparador. Sesión interna U03 con permiso para crear pagos; Pago sintético preparado por U03; Conocimiento del endpoint de aprobación; U03 puede satisfacer su propio factor de operación canario; no se requiere ni se elude el factor de un aprobador independiente.
3. **Paso documental 1 (no ejecutado)** Crear PAY-CANARIO-001 con destino y cantidad ficticios y registrar created_by=U03.
4. **Paso documental 2 (no ejecutado)** Solicitar la transición de aprobación con la misma sesión U03 y su propio factor de operación canario válido.
5. **Paso documental 3 (no ejecutado)** Comparar el estado y las identidades registradas; el guion concluye cuando el estado sintético es aprobado, antes de cualquier liquidación.
6. **E02A · transcripción sintética completa** Ilustra pérdida de independencia; no demuestra transferencia de fondos.

Pago: PAY-CANARIO-001
 Antes: pendiente / created_by=operador-preparador
 Solicitud de aprobación: subject=operador-preparador
 Factor por operación del mismo sujeto: válido en el modelo
 Después ilustrado: aprobado / approved_by=operador-preparador
 Liquidación: no existe en este modelo

7. **E02B · transcripción sintética completa** La autenticación y un rol genérico de operador son insuficientes para autorizar la transición.

Preparador → crear propio: permitido
 Preparador → aprobar propio: debe denegarse
 Aprobador distinto → aprobar pendiente válido: permitido con factor de operación
 Aprobador → aprobar pago ya modificado: requiere nueva revisión

8. Estos extractos se construyeron para el modelo. No son respuestas capturadas de una infraestructura real.

SIMULACIÓN · EVIDENCIA SINTÉTICA · NO EJECUTADO

F02 · Autoaprobación de pagos por el preparador

Extractos abreviados. Transcripciones completas en el informe; no son capturas de un sistema real.

E02A · Estado antes/después sintético

Autoaprobación: aceptada en el guion
 Liquidación: fuera del modelo

Ilustra pérdida de independencia; no demuestra transferencia de fondos.

E02B · Matriz de negocio

Meta: un aprobador independiente
 Factor propio ≠ persona distinta

La autenticación y un rol genérico de operador son insuficientes para autorizar la transición.

Banco Lumbre ficticio | extractos ilustrativos | Véase la transcripción A/B y los límites de la ficha

Figura 2. SIMULACIÓN · E02A: transición aceptada para el mismo actor; E02B: contraste de roles esperado. Evidencia sintética no ejecutada.

9. **Resultado definido en el modelo** Un pago sintético alcanza aprobado con creador y aprobador iguales.
10. **Controles actuales definidos** Sesión interna requerida; Control visual en la interfaz; MFA de inicio de sesión ordinario; Factor por operación del sujeto, insuficiente para reemplazar aprobador independiente. No se les atribuye una eficacia real ni rebaja automática del índice.
11. **Límites del resultado** No hay acceso de cliente a funciones internas; No se elude el proceso bancario real de compensación; No se demuestra modificación de saldo; La cantidad del pago es canario y no se convierte en pérdida

observada; El factor por operación permanece requerido para el sujeto; la falla es independencia y rol, no un bypass del factor.

- 12. Contención propuesta** Suspenden en el modelo la aprobación API por roles genéricos y exigen una revisión independiente registrada antes de liberar la transición.
- 13. Prevención y dependencias** Pruebas de independencia y estados inválidos como requisito de release; control de asignación incompatible de roles y alertas por coincidencia de actores. Dependencias: R04 recuperación de identidad privilegiada; R06 gobierno de grupos sensibles; Diseño de autorización por operación. Responsable técnico: Plataforma de Pagos / Operaciones.
- 14. Retest prospectivo: control positivo** PENDIENTE; no ejecutado. U04 distinto de U03 aprueba una operación pendiente válida con los requisitos definidos.
- 15. Retest prospectivo: control negativo** El creador no aprueba su pago por API, UI, rol mixto ni sesión reutilizada; cambios de operación invalidan la autorización previa.
- 16. Criterio de cierre y regresión** Independencia, autorización y atomicidad verificadas con matriz de estados y registro íntegro. Verificar que reintentos no duplican la transición; la prueba de idempotencia es control de regresión y no otro hallazgo confirmado. La meta residual se reevaluará tras implementar y probar; aquí no se declara corregido.
- 17. Activos afectados**
 - api.bancolumbre.example
 - operaciones.bancolumbre.example

F03 Refresh renovable tras la revocación

Media 6.5

CWE CWE-613

CVSS 3.1 6.5 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

Descripción (incl. causa raíz)

SIMULACIÓN: condición definida en el guion; sin verificación contra un sistema real.**Nombre completo:** Las familias refresh sobreviven a la revocación y mantienen acceso más allá de la baja.

El modelo invalida la sesión web y registra revoke-all, pero no revoca la familia de refresh ni valida session_version en nuevas renovaciones. Un token refresh anterior produce otro access token después del evento de baja/revocación. El TTL corto del access token no limita esta ruta cuando el refresh conserva siete días de vigencia.

Causa raíz: La revocación actúa sobre la cookie de sesión, mientras el endpoint de renovación consulta solo expiración y firma del refresh. El cambio de estado de identidad y la versión de sesión no se propagan al verificador.

Impacto de seguridad

Una baja, incidente o recuperación de cuenta podría dejar acceso persistente al canal o a información operativa. El efecto depende del rol y de los permisos vigentes; no se presume acceso de administrador para todas las cuentas.

Riesgo de negocio: inherente y actual 12/25 (Alto), P=3, I=4. Residual objetivo 4/25, pendiente. Prioridad P1.

Límite: Access token de 5 min no compensa un refresh token de 7 días renovable tras la revocación.

Dominio afectado

POST id.bancolumbre.example/oauth/token y evento de revocación total

Remediación

Vincular cada refresh a familia, usuario, versión de sesión y estado activo; revocar la familia ante baja, reset de credenciales o revoke-all. Usar rotación y detección de reutilización para familias donde corresponda. Definir cómo se limita un access token ya emitido hasta su expiración y cuándo exigir consulta de estado para operaciones sensibles.

Responsable de riesgo: Gerencia de Identidad. Tratamiento R03. Estado abierto y sin verificar; 0 retests.

Referencias

- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

Procedimiento detallado

- Justificación de severidad técnica** PR:L requiere la familia refresh previa. C:H representa acceso continuado a información financiera sensible del rol. I/A:N para no atribuir una capacidad de operación no representada. La vigencia temporal y la baja son contexto empresarial, no una suma al CVSS. CVSS representa la consecuencia técnica acotada del guion y no sustituye el riesgo empresarial.
- Actor y precondiciones del guion** Cuenta canario autenticada antes de revoke-all. Posesión de una familia refresh legítima antes del evento; Cuenta y servicio del escenario usan refresh de siete días; Access token definido con TTL de cinco minutos.
- Paso documental 1 (no ejecutado)** Representar una sesión inicial de usuario canario y conservar únicamente el identificador redactado de la familia.
- Paso documental 2 (no ejecutado)** Modelar revoke-all por baja de operador y registrar el nuevo estado de identidad.
- Paso documental 3 (no ejecutado)** Representar una renovación posterior al TTL del access token anterior; el guion devuelve otro access token y una lectura canario.

6. **E03A - transcripción sintética completa** Aísla el refresh posterior de la validez residual de un access token de cinco minutos.

```
T0: familia REF-CANARIO-01 emitida
T1: revoke-all / usuario deshabilitado / session_version=2
T1+6 min: familia anterior todavía aceptada
Resultado ilustrado: access token nuevo / lectura canario 200
Tokens: omitidos; identificador de familia no es credencial
```

7. **E03B - transcripción sintética completa** El fallo es propagación de revocación, no ausencia total de expiración.

```
Access token vencido: denegado
Refresh vencido: denegado
Refresh vigente de familia revocada: aceptado indebidamente
Objetivo: invalid_grant sin emitir access token nuevo
```

8. Estos extractos se construyeron para el modelo. No son respuestas capturadas de una infraestructura real.

SIMULACIÓN · EVIDENCIA SINTÉTICA · NO EJECUTADO

F03 · Refresh renovable tras la revocación

Extractos abreviados. Transcripciones completas en el informe; no son capturas de un sistema real.

E03A · Línea temporal sintética

Cuenta: canario revocado
Refresh: renovable tras la baja
Aísla el refresh posterior de la validez residual de un access token de cinco minutos.

E03B · Control de contraste

Access vencido: denegado
Refresh revocado: permiso indebido
El fallo es propagación de revocación, no ausencia total de expiración.

Banco Lumbre ficticio | extractos ilustrativos | Véase la transcripción A/B y los límites de la ficha

Figura 3. SIMULACIÓN · E03A: nueva sesión tras revocación total; E03B: expiración ordinaria funciona, revocación no. Evidencia sintética no ejecutada.

9. **Resultado definido en el modelo** Una familia revocada renueva sesión y permite una lectura canario después de vencer el access token anterior.
10. **Controles actuales definidos** Access token de cinco minutos; Expiración de refresh de siete días; MFA en autenticación normal. No se les atribuye una eficacia real ni rebaja automática del índice.
11. **Límites del resultado** No demuestra robo de refresh; MFA ordinario no se declara inexistente; No se atribuyen siete días de actividad observada; es el máximo de vigencia configurado; La revocación de grupo y la autorización en cada operación pueden limitar el impacto y deben validarse por separado.
12. **Contención propuesta** Invalidar las familias afectadas y suspender renovación para cuentas dadas de baja; revisar propagación de revoke-all en consumidores.
13. **Prevención y dependencias** Contrato automatizado de ciclo completo: login, renovación, revocación, baja, cambios de rol y recuperación; monitorizar renovaciones posteriores a esos eventos sin registrar tokens. Dependencias: Inventario de consumidores de identidad; Política de sesión y propagación de baja. Responsable técnico: IAM / Seguridad de Aplicaciones.
14. **Retest prospectivo: control positivo** PENDIENTE; no ejecutado. Una familia activa rota y renueva dentro de su política sin bloquear usuarios legítimos.
15. **Retest prospectivo: control negativo** Tras revoke-all o baja, familias anteriores no emiten nuevas sesiones en ningún consumidor; repetir después del TTL del access token.

16. Criterio de cierre y regresión Propagación y ventanas residuales documentadas y verificadas para cliente y backoffice. Cambios de rol y recuperación no mantienen autorizaciones antiguas. La meta residual se reevaluará tras implementar y probar; aquí no se declara corregido.

17. Activos afectados

- id.bancolumbre.example
- portal.bancolumbre.example
- operaciones.bancolumbre.example

F04 Recuperación MFA sin verificación independiente		Media 4.9
CWE	CWE-287	
CVSS 3.1	4.9 CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N	
Descripción (incl. causa raíz)	SIMULACIÓN: condición definida en el guion; sin verificación contra un sistema real. Nombre completo: Recuperación MFA privilegiada sin verificación independiente de identidad. El guion permite que un único helpdesk solicite y apruebe el cambio del factor de una cuenta operativa usando un número de ticket y datos presentes en la ficha del usuario. No requiere aprobación independiente ni verificación de un factor existente. El destinatario de enrolamiento se introduce en el mismo formulario. Causa raíz: La recuperación es tratada como una tarea administrativa común, sin controles equivalentes a la sensibilidad del rol ni separación entre solicitud, verificación y aprobación.	
Impacto de seguridad	Una cuenta helpdesk comprometida o un abuso interno podría alterar el factor de una identidad operativa y debilitar el control de recuperación. La apropiación posterior requeriría satisfacer autenticación primaria y otras barreras, incluida una contraseña si la política la exige; ese requisito no se demuestra. Si se obtuviera acceso a una cuenta preparadora por una vía adicional, F02 amplificaría el riesgo. No es una cadena ejecutada. Riesgo de negocio: inherente y actual 16/25 (Alto), P=4, I=4. Residual objetivo 4/25, pendiente. Prioridad P0. Límite: Se representa alteración del factor MFA. No equivale a login sin contraseña; una toma de sesión requiere un paso adicional. I4/P0 responde al factor privilegiado y a la política propuesta, sin compromiso de operadores demostrado.	
Dominio afectado	Flujo interno de recuperación de factor de operadores	
Remediación	Separar solicitud, verificación y aprobación; emplear canales previamente registrados y un procedimiento alternativo seguro cuando se pierde el factor. El helpdesk no debe cambiar libremente el destinatario y aprobar a la vez. Notificar al titular por canal independiente, invalidar sesiones afectadas y establecer enfriamiento o autorización reforzada para operaciones sensibles según política. Responsable de riesgo: Gerencia de Operaciones e Identidad. Tratamiento R04. Estado abierto y sin verificar; 0 retests.	
Referencias	• https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html • https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html	

Procedimiento detallado

- 1. **Justificación de severidad técnica** PR:H porque el actor posee permiso administrativo helpdesk sobre recuperación de identidad. I:H representa la modificación no gobernada del factor, un elemento crítico de identidad. C/A:N porque el guion no aporta contraseña base ni login ni lectura de datos. Una toma de cuenta posterior requeriría condiciones adicionales y se analiza como impacto potencial empresarial, sin incorporarla como resultado directo al vector. CVSS representa la consecuencia técnica acotada del guion y no sustituye el riesgo empresarial.
- 2. **Actor y precondiciones del guion** U06 mesa-ayuda-iam sobre cuenta canario de operador. Sesión helpdesk U06; Datos y ticket canario suministrados en el escenario; Cuenta objetivo de operador incluida en el alcance; Acceso al destinatario canario designado en el propio guion; La autenticación primaria y otras barreras siguen requeridas; el guion no representa obtención de la contraseña base ni un login exitoso.
- 3. **Paso documental 1 (no ejecutado)** Representar el restablecimiento para operador-canario mediante ticket SIM-REC-001.
- 4. **Paso documental 2 (no ejecutado)** Usar el mismo actor para enviar y aprobar la solicitud y fijar destino usuario-simulado@bancolumbre.example.
- 5. **Paso documental 3 (no ejecutado)** Registrar que el modelo emite una autorización de enrolamiento sin prueba independiente; no enviar correo ni contactar personas.
- 6. **E04A · transcripción sintética completa** El modelo muestra una vía de recuperación sin independencia, no una campaña de suplantación ejecutada.

Ticket: SIM-REC-001
Requested_by: mesa-ayuda-iam
Approved_by: mesa-ayuda-iam
Identidad objetivo: operador-canario
Factor existente verificado: no
Destino de enrolamiento: campo editable del mismo flujo
Resultado ilustrado: enrolamiento habilitado

- 7. **E04B · transcripción sintética completa** La observación no es que el banco carezca de MFA; es que la recuperación permite cambiarlo con menor garantía.

Login normal de operador: exige MFA
Reset privilegiado: no exige prueba independiente ni segundo aprobador
Objetivo: recovery pending hasta validación de identidad por canal previamente registrado

- 8. Estos extractos se construyeron para el modelo. No son respuestas capturadas de una infraestructura real.

SIMULACIÓN · EVIDENCIA SINTÉTICA · NO EJECUTADO

F04 · Recuperación MFA sin verificación independiente

Extractos abreviados. Transcripciones completas en el informe; no son capturas de un sistema real.

E04A · Registro de decisión sintético

Reset: solicita mesa de ayuda
Validación independiente: ausente
El modelo muestra una vía de recuperación sin independencia, no una campaña de suplantación ejecutada.

E04B · Control de contraste

Login normal: requiere MFA
Reset: sin prueba independiente
La observación no es que el banco carezca de MFA; es que la recuperación permite cambiarlo con menor garantía.

Banco Lumbré ficticio | extractos ilustrativos | Véase la transcripción A/B y los límites de la ficha

Figura 4. SIMULACIÓN · E04A: un actor controla el restablecimiento; E04B: el MFA ordinario permanece habilitado. Evidencia sintética no ejecutada.

- 9. **Resultado definido en el modelo** Emisión de autorización de enrolamiento para un destino controlado dentro del guion.

- 10. Controles actuales definidos** Helpdesk autenticado; Ticket obligatorio; MFA en el login normal. No se les atribuye una eficacia real ni rebaja automática del índice.
- 11. Límites del resultado** No se obtuvo una contraseña real; No hubo contacto con empleados; No se ejecutó login real ni transferencia; No se afirma que todas las identidades puedan resetearse por esta ruta; Cambio del factor y autorización de enrolamiento no equivalen por sí solos a login ni a apropiación de cuenta.
- 12. Contención propuesta** Retirar temporalmente el reset unilateral para operadores sensibles y usar recuperación asistida bajo control dual.
- 13. Prevención y dependencias** Revisión periódica de operadores habilitados para recuperar factores, monitoreo de destino nuevo y doble rol, y ejercicios de procedimiento con identidades canario. Dependencias: R03 revocación completa; Catálogo de roles sensibles; Procedimiento de contingencia de identidad. Responsable técnico: IAM / Operaciones / Prevención de Fraude.
- 14. Retest prospectivo: control positivo** PENDIENTE; no ejecutado. Un usuario legítimo recupera acceso por el flujo de contingencia completo con evidencias de verificación.
- 15. Retest prospectivo: control negativo** Un helpdesk único no crea, aprueba y redirige recuperación de un operador sensible; no se aceptan datos públicos como prueba única.
- 16. Criterio de cierre y regresión** Control dual, canales independientes, notificación y revocación acreditados en el eventual laboratorio. El procedimiento no crea una indisponibilidad permanente para quien perdió todos los factores. La meta residual se reevaluará tras implementar y probar; aquí no se declara corregido.
- 17. Activos afectados**
 - id.bancolumbre.example
 - operaciones.bancolumbre.example

F05 Webhook hacia destino interno no autorizado

Media 4.3

CWE	CWE-918
CVSS 3.1	4.3 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
Descripción (incl. causa raíz)	SIMULACIÓN: condición definida en el guion; sin verificación contra un sistema real. Nombre completo: Validación de webhook permite solicitudes a un destino interno no autorizado. La validación del webhook del modelo solicita una URL indicada por el usuario y devuelve parte de la respuesta. Acepta un destino de diagnóstico interno fuera de la lista aprobada. El servicio de contraste devuelve solo un marcador, sin credenciales, secretos ni funciones administrativas. Causa raíz: El verificador valida sintaxis HTTPS, pero no impone destino aprobado ni restricciones de salida independientes de la entrada.
Impacto de seguridad	Puede aumentar exposición de servicios internos y facilitar reconocimiento. El riesgo de acciones privilegiadas requeriría interfaces o credenciales adicionales no demostradas en este escenario. Riesgo de negocio: inherente y actual 9/25 (Moderado), P=3, I=3. Residual objetivo 3/25, pendiente. Prioridad P2. Límite: Sólo contacto y estado de un canario de diagnóstico, sin credenciales ni operaciones. I3 de datos es un impacto condicionado a que otra ruta interna responda con contenido confidencial; no está demostrado.
Dominio afectado	POST integraciones.bancolumbre.example/v1/webhooks/validar
Remediación	Aplicar política de destinos, resolución controlada y restricciones de salida de red. Validar host/IP resultantes y redirecciones según el caso de uso, evitando resolución a destinos prohibidos; no delegar autenticación de servicios internos a la mera pertenencia a la red. Responsable de riesgo: Gerencia de Integraciones. Tratamiento R05. Estado abierto y sin verificar; 0 retests.
Referencias	https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

Procedimiento detallado

- Justificación de severidad técnica** C:L se limita a información interna de diagnóstico canario. No asignar C:H, I:H o A:H sin funciones, secretos o efectos adicionales. La conectividad de F08 no se incorpora como cadena confirmada. CVSS representa la consecuencia técnica acotada del guion y no sustituye el riesgo empresarial.
- Actor y precondiciones del guion** Administrador empresarial canario con permiso de registrar webhooks. Sesión empresarial con capacidad de gestionar webhooks; Nombre interno canario proporcionado por el guion; Servicio diagnóstico ficticio accesible desde A05.
- Paso documental 1 (no ejecutado)** Representar una validación hacia receptor-canario.bancolumbre.example como caso legítimo.
- Paso documental 2 (no ejecutado)** Cambiar únicamente la URL al destino diagnostico.datos.bancolumbre.example/canario, no autorizado para empresas.
- Paso documental 3 (no ejecutado)** Registrar el marcador devuelto y detener el escenario; no explorar rangos internos, metadatos cloud ni protocolos adicionales.
- E05A • transcripción sintética completa** Ilustra cruce no aprobado de frontera. La lectura del marcador no equivale a compromiso de datos.

```
Origen lógico: servicio de validación A05
Destino solicitado: https://diagnostico.datos.bancolumbre.example/canario
Destino aprobado: no
Resultado ilustrado: 200 / MARCADOR_DIAGNOSTICO_INTERNO
Secretos en respuesta: ninguno
```

7. **E05B • transcripción sintética completa** El problema permanece aunque exista validación de esquema.

```
Receptor empresarial canario aprobado: permitido
Diagnóstico interno: permitido indebidamente
Esquema no HTTPS: rechazado en el modelo
Objetivo: bloquear destino interno desde aplicación y red
```

8. Estos extractos se construyeron para el modelo. No son respuestas capturadas de una infraestructura real.

SIMULACIÓN • EVIDENCIA SINTÉTICA • NO EJECUTADO

F05 • Webhook hacia destino interno no autorizado

Extractos abreviados. Transcripciones completas en el informe; no son capturas de un sistema real.

E05A • Respuesta sintética

```
Destino interno: no aprobado
Respuesta: marcador, sin secretos

Ilustra cruce no aprobado de frontera. La lectura
del marcador no equivale a compromiso de datos.
```

E05B • Matriz de destinos

```
Receptor aprobado: permitido
Destino interno: permiso indebido

El problema permanece aunque exista validación
de esquema.
```

Banco Lumbre ficticio | extractos ilustrativos | Véase la transcripción A/B y los límites de la ficha

Figura 5. SIMULACIÓN • E05A: respuesta interna reflejada al solicitante; E05B: diferencia entre URL válida y destino autorizado. Evidencia sintética no ejecutada.

9. **Resultado definido en el modelo** Lectura de un marcador interno mediante el verificador de webhook.
10. **Controles actuales definidos** Registro de webhook requiere autenticación; Esquema HTTPS requerido; Destino canario sin secretos y sin operación financiera. No se les atribuye una eficacia real ni rebaja automática del índice.
11. **Límites del resultado** No acceso a cloud metadata; No robo de credenciales; No ejecución de comandos; No escritura de datos ni escaneo de red; F08 es un escenario de conectividad independiente, no consecuencia probada de F05.
12. **Contención propuesta** Restringir la validación a destinos empresariales aprobados y eliminar la devolución del cuerpo de diagnósticos internos.
13. **Prevención y dependencias** Tests de destinos internos, IPv4/IPv6, redirección y resolución cambiante; actualización segura de receptores autorizados sin bloquear integraciones legítimas. Dependencias: R08 matriz de flujos de red; Inventario de receptores empresariales. Responsable técnico: Integraciones / Redes.
14. **Retest prospectivo: control positivo** PENDIENTE; no ejecutado. Receptor autorizado recibe únicamente la validación esperada.
15. **Retest prospectivo: control negativo** Destinos internos y sus variantes no se contactan ni reflejan; verificar denegación en la capa de aplicación y en egreso.
16. **Criterio de cierre y regresión** Capturas o trazas canario demuestran ausencia de solicitud al destino prohibido. Revalidar cada salto y cada actualización DNS sin incluir destinos externos al alcance. La meta residual se reevaluará tras implementar y probar; aquí no se declara corregido.
17. **Activos afectados**
- integraciones.bancolumbre.example

F06 Delegación AD sobre autorizadores financieros		Alta 7.1
CWE	CWE-269	
CVSS 3.1	7.1 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N	
Descripción (incl. causa raíz)	SIMULACIÓN: condición definida en el guion; sin verificación contra un sistema real. Nombre completo: Delegación AD permite asignar el grupo de autorizadores financieros sin control dual. El modelo delega Modify Group Membership al helpdesk sobre una OU que contiene grupos financieros. U06 agrega una cuenta canario a G-Autorizadores-Pagos. La regla de A03 transforma esa pertenencia en rol de aprobador de A04. Se describe esa regla de aplicación explícitamente; no se presume que pertenencia AD equivalga siempre a permiso financiero. Causa raíz: Una delegación de tareas ordinarias hereda alcance sobre un grupo crítico, sin separación de OU, lista de grupos permitidos ni aprobación independiente de privilegio financiero.	
Impacto de seguridad	Un delegado de soporte podría otorgar capacidad de autorización financiera fuera del proceso de altas. El impacto depende del control dual de pagos y del gobierno de roles; se requiere cerrar tanto el privilegio como el flujo de negocio. Riesgo de negocio: inherente y actual 15/25 (Alto), P=3, I=5. Residual objetivo 5/25, pendiente. Prioridad P0. Límite: El modelo permite modificar sólo el grupo financiero, no administrar el dominio. La membresía no significa por sí sola que se haya liquidado un pago.	
Dominio afectado	OU=Operaciones / grupo G-Autorizadores-Pagos del directorio ficticio	
Remediación	Separar los grupos sensibles del ámbito delegado de tareas ordinarias. Delegar únicamente objetos y acciones necesarios, exigir aprobación independiente de rol financiero y registrar cambios y sincronización. Revisar pertenencias anidadas y permisos efectivos, sin confiar solo en el nombre del grupo. Responsable de riesgo: Gerencia de Infraestructura y Pagos. Tratamiento R06. Estado abierto y sin verificar; 0 retests.	
Referencias	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/delegation-control-wizard	

Procedimiento detallado

- Justificación de severidad técnica** PR:L es la delegación específica sobre membresías y no administración del dominio. C:L/I:H corresponden al rol financiero definido por el mapeo explícito, dentro del mismo ámbito corporativo de autorización. No puntuar Domain Admin, DCSync o impacto global del bosque. CVSS representa la consecuencia técnica acotada del guion y no sustituye el riesgo empresarial.
- Actor y precondiciones del guion** U06 mesa-ayuda-iam. Cuenta U06 con permiso delegado de modificar membresías; Grupo financiero incluido en la herencia de la OU; Mapeo grupo→rol configurado en el modelo de A03/A04.
- Paso documental 1 (no ejecutado)** Comparar membresía inicial de operador-canario sin rol aprobador.
- Paso documental 2 (no ejecutado)** Representar alta reversible de esa única cuenta en G-Autorizadores-Pagos por U06.

5. **Paso documental 3 (no ejecutado)** Registrar el rol resultante en A04 después de la sincronización; no aprobar pagos ni tocar grupos de administración del dominio.
6. **E06A · transcripción sintética completa** Ilustra un permiso efectivo acotado, no GenericAll sobre el dominio.

```
Principal delegado: mesa-ayuda-iam
Permiso: Modify Group Membership
Ámbito heredado: OU=Operaciones
Objeto sensible incluido: G-Autorizadores-Pagos
Cuenta añadida: operador-canario
Aprobación independiente: ausente
```

7. **E06B · transcripción sintética completa** El impacto se limita al rol definido por la regla, sin atribuir DCSync ni control de DC.

```
Antes: operador-canario / rol=consulta
Regla: G-Autorizadores-Pagos → aprobador
Después ilustrado: rol=aprobador
Domain Admins: no modificado
Objetivo: helpdesk denegado para este grupo
```

8. Estos extractos se construyeron para el modelo. No son respuestas capturadas de una infraestructura real.

SIMULACIÓN · EVIDENCIA SINTÉTICA · NO EJECUTADO

F06 · Delegación AD sobre autorizadores financieros

Extractos abreviados. Transcripciones completas en el informe; no son capturas de un sistema real.

E06A · Matriz ACL y membresía sintética

Helpdesk: agrega miembro canario
Aprobación independiente: ausente
Ilustra un permiso efectivo acotado, no GenericAll sobre el dominio.

E06B · Regla de rol y contraste

Grupo financiero → rol aprobador
No Domain Admin ni DCSync
El impacto se limita al rol definido por la regla, sin atribuir DCSync ni control de DC.

Banco Lumbre ficticio | extractos ilustrativos | Véase la transcripción A/B y los límites de la ficha

Figura 6. SIMULACIÓN · E06A: delegación ordinaria alcanza grupo financiero; E06B: mapeo explícito a la aplicación. Evidencia sintética no ejecutada.

9. **Resultado definido en el modelo** Una cuenta canario obtiene rol de aprobador mediante modificación de grupo no gobernada.
10. **Controles actuales definidos** Helpdesk usa cuenta identificada; Delegación acotada por OU en el diseño, aunque el ámbito sea demasiado amplio; Solo una membresía canario ilustrada. No se les atribuye una eficacia real ni rebaja automática del índice.
11. **Límites del resultado** No compromiso del dominio; No membresía Domain Admin; No DCSync; No lectura de contraseñas; No se ejecuta pago; el rol resultante es el límite del guion.
12. **Contención propuesta** Retirar el permiso heredado sobre grupos financieros, revisar pertenencias y congelar altas fuera del workflow aprobado.
13. **Prevención y dependencias** Recertificación periódica del propietario de negocio, detección de altas fuera de ticket y matriz de incompatibilidad de roles. Dependencias: R02 independencia de aprobación; R03 revocación tras cambio de rol; Mapa de grupos y reglas de claims. Responsable técnico: Infraestructura e IAM / Operaciones.
14. **Retest prospectivo: control positivo** PENDIENTE; no ejecutado. Workflow aprobado incorpora una cuenta con ticket, segundo aprobador y trazabilidad.

15. Retest prospectivo: control negativo U06 no modifica el grupo financiero ni sus rutas anidadas; retirar membresía revoca la autorización según la ventana definida.
16. Criterio de cierre y regresión Permiso efectivo y claims verificados antes y después, incluyendo herencia y anidación. La corrección no impide altas ordinarias autorizadas en grupos no sensibles. La meta residual se reevaluará tras implementar y probar; aquí no se declara corregido.
17. Activos afectados
 - dc01.corp.bancolumbre.example
 - id.bancolumbre.example
 - operaciones.bancolumbre.example

F07 Credencial de despliegue expuesta en CI		Alta 8.1
CWE	CWE-522	
CVSS 3.1	8.1 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N	
Descripción (incl. causa raíz)	SIMULACIÓN: condición definida en el guion; sin verificación contra un sistema real. Nombre completo: Credencial de despliegue excesiva queda expuesta en un artefacto de CI. Un artefacto del modelo contiene un campo de credencial de despliegue que debe haber sido excluido. La identidad asociada autoriza publicación en dos entornos y modificación de una configuración de API, aunque el job solo construye una versión de prueba. El valor publicado es TEST-NO-ES-CREDENCIAL y no es utilizable. Causa raíz: La plantilla de diagnóstico serializa el entorno completo del job y la misma identidad permanente se comparte entre tareas y entornos. La ruta de lectura del artefacto tiene mayor audiencia que la ruta de despliegue.	
Impacto de seguridad	Si un secreto válido quedara expuesto con esos permisos en una plataforma real, un lector podría intentar cambios no autorizados de aplicación. El riesgo afecta integridad de entrega y continuidad; no se declara software malicioso publicado ni un despliegue demostrado. Riesgo de negocio: inherente y actual 15/25 (Alto), P=3, I=5. Residual objetivo 5/25, pendiente. Prioridad P0. Límite: Un lector CI obtiene un secreto sintético con alcance de despliegue de producción en el modelo. No equivale a firmar código ni a root del host; no se ejecuta un despliegue destructivo.	
Dominio afectado	Artefacto de diagnóstico de compilación y política de identidad deploy-canario	
Remediación	Excluir secretos de logs y artefactos por diseño, permitir solo campos diagnósticos necesarios y aplicar escaneo antes de publicación. Separar identidades por job y entorno, usar credenciales breves federadas cuando la plataforma lo soporte y exigir aprobación para despliegues sensibles. Responsable de riesgo: Gerencia de Ingeniería de Plataforma. Tratamiento R07. Estado abierto y sin verificar; 0 retests.	
Referencias	• https://docs.github.com/en/actions/reference/security/secure-use	

Procedimiento detallado

1. Justificación de severidad técnica PR:L requiere rol lector de artefactos. C:H/I:H son estimaciones para un secreto válido con el alcance documental indicado en el modelo de despliegue. A:N evita atribuir caída no demostrada. El valor

publicado es no funcional y la política, no una autenticación, sustenta el supuesto. CVSS representa la consecuencia técnica acotada del guion y no sustituye el riesgo empresarial.

2. **Actor y precondiciones del guion** U07 runner-lector. Acceso lector U07 a artefactos del proyecto; Artefacto de diagnóstico sintético disponible; Política de la identidad incluida para revisión.
3. **Paso documental 1 (no ejecutado)** Representar lectura del artefacto por U07 sin permiso directo de despliegue.
4. **Paso documental 2 (no ejecutado)** Identificar el campo canario y correlacionarlo con el sujeto deploy-canario de la política.
5. **Paso documental 3 (no ejecutado)** Comparar permisos del sujeto con necesidades del job. No autenticar con el valor, publicar código ni ejecutar un despliegue.
6. **E07A · transcripción sintética completa** Demuestra documentalmente el diseño inseguro del modelo, no la validez de un secreto.

```
Artefacto: build-diagnostico-canario.json
Lector: runner-lector
Campo indebidamente exportado: DEPLOY_CREDENTIAL
Valor seguro publicado: TEST-NO-ES-CREDENCIAL
Identidad asociada en modelo: deploy-canario
```

7. **E07B · transcripción sintética completa** No confundir permiso de configuración con control root ni con firma de releases.

```
Job solicitado: build de prueba
Necesidad: lectura de código y escritura de artefacto de prueba
Identidad modelada: deploy:test + deploy:prod + api:config:write
Aprobación separada de producción: ausente
Objetivo: identidad efímera ligada a job y entorno
```

8. Estos extractos se construyeron para el modelo. No son respuestas capturadas de una infraestructura real.

SIMULACIÓN · EVIDENCIA SINTÉTICA · NO EJECUTADO

F07 · Credencial de despliegue expuesta en CI

Extractos abreviados. Transcripciones completas en el informe; no son capturas de un sistema real.

E07A · Archivo de diagnóstico sintético

Artefacto CI: secreto de muestra
Credencial: sintética, no válida
Demuestra documentalmente el diseño inseguro del modelo, no la validez de un secreto.

E07B · Matriz de permisos sintética

Rol: despliegue de test y prod
Aprobación de prod: ausente
No confundir permiso de configuración con control root ni con firma de releases.

Banco Lumbre ficticio | extractos ilustrativos | Véase la transcripción A/B y los límites de la ficha

Figura 7. SIMULACIÓN · E07A: campo de credencial en artefacto legible; E07B: alcance superior a la tarea. Evidencia sintética no ejecutada.

9. **Resultado definido en el modelo** Lectura del campo canario y comprobación documental de permisos excesivos.
10. **Controles actuales definidos** Artefacto exige rol lector del proyecto; El modelo distingue build de deploy, aunque reutilice identidad. No se les atribuye una eficacia real ni rebaja automática del índice.
11. **Límites del resultado** Credencial publicada no funcional; No autenticación con secretos; No despliegue; No ejecución en runner; No atribuir capacidad de firmar artefactos o tomar el host sin evidencia adicional.
12. **Contención propuesta** Retirar el artefacto con el campo, revocar la identidad afectada y revisar accesos a salidas de diagnóstico. En este ejercicio solo se retiran campos canario.

- 13. Prevención y dependencias** Permisos mínimos declarativos por workflow, comprobación de alcance, prueba negativa con lector y detección de campos sensibles con canarios. Dependencias: Proveedor de identidad de workloads; Catálogo de entornos y aprobadores; Política de retención de artefactos. Responsable técnico: Ingeniería de Plataforma / Seguridad de Desarrollo.
- 14. Retest prospectivo: control positivo** PENDIENTE; no ejecutado. El job autorizado construye y publica su artefacto sin valores sensibles; el despliegue aprobado funciona solo en su entorno.
- 15. Retest prospectivo: control negativo** Lector de artefacto no obtiene credenciales; identidad de prueba no modifica producción ni configuración ajena.
- 16. Criterio de cierre y regresión** Artefactos, políticas y denegaciones se verifican conjuntamente; eliminar el campo no basta si queda la identidad excesiva compartida. Errores de herramientas y stdout/stderr no reintroducen campos sensibles. La meta residual se reevaluará tras implementar y probar; aquí no se declara corregido.
- 17. Activos afectados**
 - ci.bancolumbre.example
 - api.bancolumbre.example

F08 Conectividad de integración no aprobada

Informativa 0.0

CWE	CWE-284
CVSS 3.1	0.0 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:N
Descripción (incl. causa raíz)	SIMULACIÓN: condición definida en el guion; sin verificación contra un sistema real. Nombre completo: La zona de integración conserva conectividad no aprobada hacia AD y datos. El diseño aprobado permite a A05 contactar interfaces específicas de A02. La configuración ficticia conserva flujos hacia LDAP de A06 y el listener de datos A08 sin justificación de negocio. El extracto ilustra conexión TCP aceptada; autenticación y permisos de servicio siguen activos. Causa raíz: Una excepción temporal de red se convirtió en regla amplia y no existe recertificación de flujo con propietario, vencimiento y dependencia documentada.
Impacto de seguridad	Aumenta la superficie para movimiento lateral y reduce la contención si otra condición permite credenciales o ejecución. La magnitud depende de controles de servicio que el guion no elude. Riesgo de negocio: inherente y actual 9/25 (Moderado), P=3, I=3. Residual objetivo 3/25, pendiente. Prioridad P2. Límite: Un socket TCP abierto sólo prueba conectividad. La autenticación de AD/datos sigue siendo una barrera en el modelo. I3 de disponibilidad requiere un escenario posterior adicional, sin prueba DoS ni interrupción.
Dominio afectado	Matriz de flujos desde A05 hacia dc01.corp.bancolumbre.example y datos.bancolumbre.example
Remediación	Aplicar denegación por defecto con reglas por origen, destino, puerto y finalidad. Segregar administración de integración, exigir identidades de servicio específicas y recertificar excepciones con dueño y vencimiento. Responsable de riesgo: Gerencia de Redes. Tratamiento R08. Estado abierto y sin verificar; 0 retests.
Referencias	- https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html - https://cheatsheetseries.owasp.org/cheatsheets/Network_Segmentation_Cheat_Sheet.html

Procedimiento detallado

- Justificación de severidad técnica** C/I/A:N porque conectividad TCP sin acceso autenticado no demuestra impacto directo. Base 0,0 e Informativo. La exposición de frontera puede conservar prioridad de negocio P2 como agravante condicionado; no convertir un puerto abierto en compromiso. CVSS representa la consecuencia técnica acotada del guion y no sustituye el riesgo empresarial.
- Actor y precondiciones del guion** U08 svc-integracion / punto de origen asumido. Punto de origen en A05 proporcionado para prueba; no se afirma que un SSRF entregue shell; Destino y puerto conocidos del inventario; Sin credenciales adicionales de AD o base de datos.
- Paso documental 1 (no ejecutado)** Comparar la matriz de flujos necesaria con reglas de red del modelo.
- Paso documental 2 (no ejecutado)** Representar una conexión canario a cada listener fuera de la lista aprobada.
- Paso documental 3 (no ejecutado)** Registrar conectividad y negativa de autenticación sin consultar datos, enumerar AD ni intentar escalada.

6. **E08A - transcripción sintética completa** Un puerto alcanzable acredita exposición de frontera en el modelo, no acceso a datos.

A05 → A02 interfaz integración: permitido / requerido
 A05 → A06 LDAP: permitido / no requerido
 A05 → A08 listener datos: permitido / no requerido
 Propietario de excepción: no definido
 Vencimiento: no definido

7. **E08B - transcripción sintética completa** No elevar a compromiso de dominio ni de base por conectividad aislada.

Conexión TCP ilustrada: establecida
 Autenticación con identidad de integración a AD/datos: denegada
 Lectura de información: no realizada
 Objetivo: conexión de red denegada para estos flujos

8. Estos extractos se construyeron para el modelo. No son respuestas capturadas de una infraestructura real.

SIMULACIÓN · EVIDENCIA SINTÉTICA · NO EJECUTADO

F08 · Conectividad de integración no aprobada

Extractos abreviados. Transcripciones completas en el informe; no son capturas de un sistema real.

E08A · Tabla de flujos sintética

LDAP/datos: flujos no requeridos
 Excepción: sin dueño ni plazo
 Un puerto alcanzable acredita exposición de frontera en el modelo, no acceso a datos.

E08B · Contraste de conectividad y autorizac...

TCP: conexión establecida
 Autenticación: denegada
 No elevar a compromiso de dominio ni de base por conectividad aislada.

Banco Lumbre ficticio | extractos ilustrativos | Véase la transcripción A/B y los límites de la ficha

Figura 8. SIMULACIÓN · E08A: conectividad excede la matriz de negocio; E08B: autenticación permanece como límite. Evidencia sintética no ejecutada.

9. **Resultado definido en el modelo** Dos listeners fuera de la matriz de flujos son alcanzables desde el origen supuesto.
10. **Controles actuales definidos** Autenticación de AD y datos mantiene la denegación; Solo conexiones a destinos del inventario representadas. No se les atribuye una eficacia real ni rebaja automática del índice.
11. **Límites del resultado** No credenciales; No lectura ni escritura; No explotación de LDAP o motor de datos; No barrido de puertos; No cadena ejecutada F05→F08.
12. **Contención propuesta** Retirar los dos flujos innecesarios después de confirmar dependencias del escenario y registrar toda excepción restante.
13. **Prevención y dependencias** Pruebas periódicas de matriz permitida/prohibida y detección de cambios de reglas; no sustituir autorización de servicio por firewall. Dependencias: Inventario de flujos; R05 validación del destino webhook; Procedimiento de cambio y rollback. Responsable técnico: Redes / Arquitectura / propietario de Integraciones.
14. **Retest prospectivo: control positivo** PENDIENTE; no ejecutado. Las integraciones aprobadas continúan funcionando.
15. **Retest prospectivo: control negativo** A05 no establece los flujos prohibidos ni por ruta alternativa autorizada en el alcance.
16. **Criterio de cierre y regresión** Evidencia desde el punto de origen demuestra denegación y ausencia de impacto en flujos necesarios. Se prueban rollback y excepciones con vencimiento sin habilitar una regla amplia temporal. La meta residual se reevaluará tras implementar y probar; aquí no se declara corregido.

17. Activos afectados

- integraciones.bancolumbre.example
- dc01.corp.bancolumbre.example
- datos.bancolumbre.example

F09 Inyección SQL en búsqueda de conciliación

Media 6.5

CWE	CWE-89
CVSS 3.1	6.5 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Descripción (incl. causa raíz)	SIMULACIÓN: condición definida en el guion; sin verificación contra un sistema real. Nombre completo: Búsqueda de conciliación concatena entrada y permite ampliar la lectura de la vista. La revisión de código construida para el modelo muestra que referencia se concatena en una consulta. El guion de contraste modifica la condición lógica y obtiene filas canario fuera de la cartera asignada. La identidad de búsqueda es solo lectura y tiene acceso únicamente a una vista de conciliación. Causa raíz: Entrada de usuario pasa a sintaxis SQL en lugar de un parámetro de datos; el filtro de cartera comparte la expresión vulnerable y no se refuerza en una capa independiente.
Impacto de seguridad	Expone información financiera fuera de la cartera autorizada y puede afectar decisiones operativas basadas en su consulta. La identidad de solo lectura limita la modificación de datos, pero no corrige la exposición de la vista. No se atribuye alteración del registro transaccional, de saldos ni de resultados de conciliación almacenados. Riesgo de negocio: inherente y actual 12/25 (Alto), P=3, I=4. Residual objetivo 4/25, pendiente. Prioridad P1. Límite: Lectura acotada de filas sintéticas de una vista de conciliación, mediante rol read-only. I4 refleja sensibilidad financiera en el escenario, no alcance total de la cartera; modificación, dump completo y ejecución no están representados.
Dominio afectado	GET operaciones.bancolumbre.example/conciliacion/buscar?referencia={valor}
Remediación	Reemplazar concatenación por consultas parametrizadas. Mantener listas permitidas para elementos no parametrizables y aplicar la autorización de cartera antes e independientemente de filtros. Conservar privilegio mínimo de datos y errores sin detalles del motor. Responsable de riesgo: Gerencia de Aplicaciones Internas. Tratamiento R09. Estado abierto y sin verificar; 0 retests.
Referencias	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Procedimiento detallado

- Justificación de severidad técnica** PR:L requiere buscador interno. C:H estima información financiera sensible en la vista alcanzable. I/A:N porque la identidad es solo lectura y no hay salida del ámbito de la vista. No añadir RCE ni escritura al vector. CVSS representa la consecuencia técnica acotada del guion y no sustituye el riesgo empresarial.
- Actor y precondiciones del guion** Operador canario con permiso de buscar su cartera. Cuenta de operador con función de búsqueda; Entrada controlable referencia; Consulta construida con concatenación en el modelo.
- Paso documental 1 (no ejecutado)** Representar consulta ordinaria por REF-CANARIO-A y registrar una fila de la cartera asignada.

4. **Paso documental 2 (no ejecutado)** Usar una entrada booleana de contraste definida en el guion sin extraer tablas ni campos nuevos.
5. **Paso documental 3 (no ejecutado)** Comparar el conjunto resultante con dos filas de otra cartera, manteniendo la prueba en lectura y dentro del dataset.
6. **E09A • transcripción sintética completa** El pseudocódigo ilustra la causa; no atribuye código vulnerable a un proveedor.

```
Implementación vulnerable del modelo:  
consulta = texto_SQL + referencia_recibida + texto_filtro_cartera  
Ejecución: concatenación de texto  
Objetivo: consulta constante con parámetros enlazados y ámbito independiente  
Código de producción real: no existe
```

7. **E09B • transcripción sintética completa** La lectura modelada no prueba escritura, RCE ni acceso al conjunto del motor.

```
Referencia ordinaria: 1 fila / cartera A  
Contraste lógico del modelo: 3 filas / carteras A y B  
Cuenta de datos: SELECT sobre vista conciliación  
UPDATE/DELETE: no permitido por la identidad  
Datos: 20 registros canario totales
```

8. Estos extractos se construyeron para el modelo. No son respuestas capturadas de una infraestructura real.

SIMULACIÓN • EVIDENCIA SINTÉTICA • NO EJECUTADO

F09 • Inyección SQL en búsqueda de conciliación

Extractos abreviados. Transcripciones completas en el informe; no son capturas de un sistema real.

E09A • Pseudocódigo sintético de revisión

SQL: concatenación de entrada
Meta: parámetros y ámbito
El pseudocódigo ilustra la causa; no atribuye código vulnerable a un proveedor.

E09B • Matriz de resultados sintética

Contraste: 3 filas de A y B
Cuenta SELECT: sin UPDATE/DELETE
La lectura modelada no prueba escritura, RCE ni acceso a todo el motor.

Banco Lumbre ficticio | extractos ilustrativos | Véase la transcripción A/B y los límites de la ficha

Figura 9. SIMULACIÓN • E09A: flujo de entrada hacia sintaxis SQL; E09B: lectura ampliada con control de no escritura. Evidencia sintética no ejecutada.

9. **Resultado definido en el modelo** Lectura de dos registros canario adicionales fuera de la cartera del operador.
10. **Controles actuales definidos** Sesión interna requerida; Cuenta de datos de solo lectura; Acceso limitado a vista de conciliación. No se les atribuye una eficacia real ni rebaja automática del índice.
11. **Límites del resultado** No modificación; No ejecución de comandos; No enumeración del motor; No extracción de tablas fuera de la vista; No se usa SQLMap ni se afirma automatización ejecutada.
12. **Contención propuesta** Deshabilitar temporalmente las expresiones de búsqueda libres y usar consulta parametrizada fija dentro de la cartera permitida.
13. **Prevención y dependencias** Revisión de sinks de consulta, pruebas de entradas límite y contratos de aislamiento de cartera; no tratar WAF o escape manual como reemplazo de parametrización. Dependencias: Inventario de consultas de conciliación; Política de carteras y filas visibles. Responsable técnico: Desarrollo de Backoffice / Datos.
14. **Retest prospectivo: control positivo** PENDIENTE; no ejecutado. Búsquedas legítimas, caracteres válidos y referencias exactas funcionan sin regresión.
15. **Retest prospectivo: control negativo** Las entradas de contraste se tratan como datos y nunca amplían la cartera; no aparecen errores de sintaxis ni respuestas diferenciadas por predicados SQL.

16. **Criterio de cierre y regresión** Parametrización acreditada en revisión y resultados, con permiso de datos limitado verificado. Otros filtros, ordenamientos y exportaciones no reintroducen concatenación. La meta residual se reevaluará tras implementar y probar; aquí no se declara corregido.
17. **Activos afectados**
 - operaciones.bancolumbre.example
 - datos.bancolumbre.example

F10 Auditoría financiera modificable por aplicación		Media 4.9
CWE	CWE-732	
CVSS 3.1	4.9 CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N	
Descripción (incl. causa raíz)	SIMULACIÓN: condición definida en el guion; sin verificación contra un sistema real. Nombre completo: La identidad de aplicación puede modificar eventos históricos de auditoría. El servicio emisor del modelo dispone de INSERT, UPDATE y DELETE sobre el repositorio que después se usa como fuente única de auditoría. Se ilustra el cambio reversible del campo actor en un evento canario histórico. El permiso no modifica el registro transaccional ni los saldos del modelo. Causa raíz: La identidad de aplicación comparte permisos de administración de evidencia. No hay un destino independiente de solo adición o protección que haga observable el cambio de un registro histórico.	
Impacto de seguridad	Una investigación podría depender de una traza manipulable por el mismo sistema investigado. Reduce confianza en atribución y reconstrucción y puede prolongar respuesta a incidentes. No equivale automáticamente a fraude financiero ni a incumplimiento legal determinado. Riesgo de negocio: inherente y actual 15/25 (Alto), P=3, I=5. Residual objetivo 5/25, pendiente. Prioridad P0. Límite: El writer puede modificar un evento de auditoría, no saldos ni transacciones. I5 se refiere al registro confiable y a la reconstrucción; no afirma fraude consumado ni una investigación real ocultada.	
Dominio afectado	Permisos de svc-pagos sobre colección de eventos de auditoría	
Remediación	Separar emisión, consulta y administración. Usar un destino de solo adición con retención e integridad protegidas y una copia independiente cuando el riesgo lo requiera. Definir control de cambios administrativos, alertas de modificación y sincronización temporal. Evitar incluir secretos o PII innecesaria en las trazas. Responsable de riesgo: Gerencia de Datos y Control Financiero. Tratamiento R10. Estado abierto y sin verificar; 0 retests.	
Referencias	https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html	

Procedimiento detallado

1. **Justificación de severidad técnica** PR:H requiere por supuesto una identidad de aplicación con acceso a configuración/ permisos de evidencia; no se descubrió una ruta inicial para obtenerla. I:H por pérdida de integridad de fuente auditora; C/A:N sin lectura nueva ni borrado representados. El CVSS moderado no reduce la criticidad empresarial de reconstrucción. CVSS representa la consecuencia técnica acotada del guion y no sustituye el riesgo empresarial.

2. **Actor y precondiciones del guion U09** svc-pagos asumida para revisión de permisos. Revisión autorizada de permisos de la identidad U09, suministrados en el modelo; Un evento canario histórico; Sin atribuir compromiso previo de svc-pagos a otra ficha.
3. **Paso documental 1 (no ejecutado)** Registrar evento AUD-CANARIO-001 con actor=operador-canario y versión original.
4. **Paso documental 2 (no ejecutado)** Representar una actualización de actor por svc-pagos y comparar el evento histórico.
5. **Paso documental 3 (no ejecutado)** Restaurar el valor en la narrativa y conservar ambos extractos; no borrar eventos ni alterar operaciones.
6. **E10A · transcripción sintética completa** El permiso de mutar evidencia no implica permiso de cambiar saldo o transacción.

```
Identidad: svc-pagos
Necesidad: INSERT evento nuevo
Permisos modelados: INSERT + UPDATE + DELETE
Destino independiente: ausente
Protección de evento histórico: no definida
```

7. **E10B · transcripción sintética completa** La evidencia ilustra capacidad de alterar una fuente de auditoría, sin afirmar encubrimiento real.

```
Evento: AUD-CANARIO-001
Antes: actor=operador-canario
Después ilustrado: actor=actor-sustituido-canario
Aviso de integridad en canal independiente: ausente
Registro transaccional: intacto
Restauración: prevista dentro del guion
```

8. Estos extractos se construyeron para el modelo. No son respuestas capturadas de una infraestructura real.

SIMULACIÓN · EVIDENCIA SINTÉTICA · NO EJECUTADO

F10 · Auditoría financiera modificable por aplicación

Extractos abreviados. Transcripciones completas en el informe; no son capturas de un sistema real.

E10A · Política de permisos sintética

svc-pagos: INSERT/UPDATE/DELETE
Copia independiente: ausente

El permiso de mutar evidencia no implica permiso de cambiar saldo o transacción.

E10B · Antes/después sintético

Evento canario: actor alterable
Registro transaccional: intacto

La evidencia ilustra capacidad de alterar una fuente de auditoría, sin afirmar encubrimiento real.

Banco Lumbre ficticio | extractos ilustrativos | Véase la transcripción A/B y los límites de la ficha

Figura 10. SIMULACIÓN · E10A: emisor posee permiso de mutación histórica; E10B: evento histórico cambiado sin rastro independiente. Evidencia sintética no ejecutada.

9. **Resultado definido en el modelo** Un campo de un evento canario se modifica usando la identidad emisora.
10. **Controles actuales definidos** Servicio identificable como emisor; Repositorio transaccional separado; Eventos sintéticos con identificador correlacionable. No se les atribuye una eficacia real ni rebaja automática del índice.
11. **Límites del resultado** No eventos reales; No borrado; No cambios de pago o saldo; No compromiso demostrado de identidad; No se asigna fuerza probatoria legal al registro o al hash de este informe.
12. **Contención propuesta** Retirar UPDATE/DELETE del emisor y conservar copia de referencia de los eventos durante el tratamiento, con acceso independiente.

- 13. Prevención y dependencias** Verificar permisos efectivos y monitorizar operaciones administrativas; ensayar reconstrucción con eventos canario y controles de pérdida, secuencia y correlación. Dependencias: Política de retención e integridad; Propietario de la evidencia independiente; Separación de identidades de aplicación y datos. Responsable técnico: SOC / Datos / Plataforma de Pagos.
- 14. Retest prospectivo: control positivo** PENDIENTE; no ejecutado. svc-pagos agrega eventos y el SOC consulta la secuencia completa.
- 15. Retest prospectivo: control negativo** svc-pagos no modifica ni elimina un evento histórico; un administrador excepcional deja rastro independiente y alerta.
- 16. Criterio de cierre y regresión** Privilegios, canal independiente y reconstrucción canario verificados; un hash local aislado no basta. La retención y las tareas de mantenimiento no eliminan silenciosamente evidencia requerida. La meta residual se reevaluará tras implementar y probar; aquí no se declara corregido.
- 17. Activos afectados**
 - api.bancolumbre.example
 - datos.bancolumbre.example

F11 Exportación de clientes por un rol de consulta

Media 6.5

CWE	CWE-862
CVSS 3.1	6.5 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Descripción (incl. causa raíz)	SIMULACIÓN: condición definida en el guion; sin verificación contra un sistema real. Nombre completo: El rol de consulta puede invocar una exportación masiva no autorizada. El modelo oculta Exportar para soporte-consulta, pero el endpoint solo comprueba que existe una sesión interna. U05 invoca la función y recibe los 20 clientes canario del dataset, incluidos registros sin caso asignado. La función en sí exige un rol distinto; por ello es BFLA, no una segunda BOLA de extractos. Causa raíz: No hay permiso funcional de exportación en servidor, ámbito de cartera ni validación de finalidad. La interfaz se usa como frontera de autorización y el resultado incluye campos no necesarios para soporte.
Impacto de seguridad	Podría facilitar extracción por una cuenta interna limitada y ampliar información disponible para abuso. Las consecuencias dependen del universo real y de los campos; el guion no muestra una fuga ni el volumen empresarial asumido. Riesgo de negocio: inherente y actual 12/25 (Alto), P=3, I=4. Residual objetivo 4/25, pendiente. Prioridad P1. Límite: Exportación de 20 filas canario desde un catálogo técnicamente accesible, sin el permiso funcional debido. Distinta de BOLA; I4 se basa en la sensibilidad financiera del conjunto, no en el volumen de la cartera.
Dominio afectado	POST operaciones.bancolumbre.example/clientes/exportar
Remediación	Comprobar permiso exportar y autorización por filas/columnas en servidor. Exigir finalidad para exportaciones sensibles, minimizar campos, establecer volumen y periodo permitidos y generar eventos independientes con identidad y alcance. Usar revisión adicional cuando el umbral de negocio lo requiera. Responsable de riesgo: Gerencia de Datos y Operaciones. Tratamiento R11. Estado abierto y sin verificar; 0 retests.
Referencias	- https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html - https://api-security.owasp.org/editions/2023/en/0xa5-broken-function-level-authorization/

Procedimiento detallado

- Justificación de severidad técnica** PR:L por soporte autenticado. C:H corresponde a exposición del catálogo financiero bajo la función no autorizada. I/A:N por exportación de lectura. El volumen canario de 20 filas no es una extracción real ni el universo empresarial asumido. CVSS representa la consecuencia técnica acotada del guion y no sustituye el riesgo empresarial.
- Actor y precondiciones del guion** U05 soporte-consulta. Sesión U05 válida; Conocimiento del endpoint incluido en la documentación de guion; Dataset canario de 20 filas.
- Paso documental 1 (no ejecutado)** Representar consulta legítima de un caso asignado por U05.
- Paso documental 2 (no ejecutado)** Invocar en el guion la función exportar con la misma sesión, sin elevar rol.

5. **Paso documental 3 (no ejecutado)** Contar 20 filas canario y comparar permisos y alcance; no ejecutar extracción masiva ni estimar extrapolación como volumen observado.
6. **E11A · transcripción sintética completa** El tamaño mostrado es solo la totalidad del dataset canario; no son 50.000 clientes extraídos.

```
Sujeto: soporte-consulta
Permiso funcional exportar: no
Endpoint ilustrado: clientes/exportar
Respuesta: archivo canario / 20 filas ficticias
Campos: customer_canary_id, cartera_canaria, saldo_ficticio
PII real: ninguna
```

7. **E11B · transcripción sintética completa** La limitación de frecuencia no sustituye el permiso funcional ni el ámbito autorizado.

```
Soporte-consulta → caso asignado: permitido
Soporte-consulta → exportar catálogo: debe denegarse
Analista-exportación → cartera autorizada: permitido con finalidad
Analista-exportación → cartera ajena: debe denegarse
```

8. Estos extractos se construyeron para el modelo. No son respuestas capturadas de una infraestructura real.

SIMULACIÓN · EVIDENCIA SINTÉTICA · NO EJECUTADO

F11 · Exportación de clientes por un rol de consulta

Extractos abreviados. Transcripciones completas en el informe; no son capturas de un sistema real.

E11A · Respuesta de exportación sintética

Rol consulta: exportación indebida
Datos: 20 clientes ficticios

El tamaño mostrado es solo la totalidad del dataset canario; no son 50.000 clientes extraídos.

E11B · Matriz de autorización funcional

Meta: limitar función y ámbito
Caso asignado: acceso permitido

La limitación de frecuencia no sustituye el permiso funcional ni el ámbito autorizado.

Banco Lumbre ficticio | extractos ilustrativos | Véase la transcripción A/B y los límites de la ficha

Figura 11. SIMULACIÓN · E11A: función no autorizada responde al rol consulta; E11B: consulta individual y función exportar son permisos distintos. Evidencia sintética no ejecutada.

9. **Resultado definido en el modelo** Un rol de consulta recibe 20 filas sintéticas mediante una función que no le corresponde.
10. **Controles actuales definidos** Sesión interna requerida; Control visual del botón; Consulta normal de casos asignados. No se les atribuye una eficacia real ni rebaja automática del índice.
11. **Límites del resultado** Solo dataset canario; No exportación de PII; No cientos de miles de registros; No acceso anónimo; No duplicar el impacto de F01: cambia actor, permiso funcional y tratamiento.
12. **Contención propuesta** Restringir el endpoint a roles aprobados y limitarlo a la cartera de cada sujeto mientras se define el flujo gobernado.
13. **Prevención y dependencias** Pruebas de funciones no visibles, recertificación del rol exportación y alertas por cambios de volumen o cartera; comprobar que todos los formatos aplican la misma política. Dependencias: R10 trazabilidad protegida; Catálogo de permisos y finalidades; Política de datos mínimos de soporte. Responsable técnico: Operaciones / Datos / Backoffice.
14. **Retest prospectivo: control positivo** PENDIENTE; no ejecutado. Analista autorizado exporta el conjunto mínimo de su cartera y deja un evento íntegro.

15. **Retest prospectivo: control negativo** Soporte-consulta no invoca exportar; parámetros, filtros y formatos no amplían filas ni columnas autorizadas.
16. **Criterio de cierre y regresión** Permiso funcional, ámbito y trazabilidad acreditados por matriz de actores y exportaciones canario. CSV, XLSX y cualquier futura exportación conservan controles equivalentes. La meta residual se reevaluará tras implementar y probar; aquí no se declara corregido.
17. **Activos afectados**
 - operaciones.bancolumbre.example
 - datos.bancolumbre.example

F12 Script almacenado en notas de backoffice		Media 5.4
CWE	CWE-79	
CVSS 3.1	5.4 CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N	
Descripción (incl. causa raíz)	SIMULACIÓN: condición definida en el guion; sin verificación contra un sistema real. Nombre completo: Notas internas se renderizan como HTML y permiten script almacenado en backoffice. El modelo guarda notas de soporte y las incorpora a un contexto HTML ejecutable sin codificación ni sanitización apropiadas. Una nota canario provoca un marcador visible cuando otro operador abre el caso. El marcador no transmite datos ni realiza una acción financiera. Causa raíz: El sistema usa renderizado HTML para contenido que debería ser texto plano. No hay una política de sanitización para las pocas etiquetas permitidas y la CSP del escenario permite el contexto empleado.	
Impacto de seguridad	Podría manipular la interfaz o realizar acciones disponibles en el contexto del usuario. El alcance financiero requiere validar autorizaciones y step-up; no se afirma que el marcador permita aprobar pagos ni exportar información. Riesgo de negocio: inherente y actual 9/25 (Moderado), P=3, I=3. Residual objetivo 3/25, pendiente. Prioridad P2. Límite: Sólo marcador visual en la sesión de un operador. Cookies HttpOnly y step-up conservan barreras sobre pagos en el modelo. I3 refleja manipulación operativa condicionada; no se demuestra exfiltración ni una operación financiera.	
Dominio afectado	Nota de caso / ficha de soporte de operaciones.bancolumbre.example	
Remediación	Renderizar como texto mediante APIs seguras y codificación contextual. Si se requiere formato limitado, sanitizar con política estricta y librería mantenida, sin manejar HTML arbitrario. Endurecer CSP y revisar otros sinks de la misma nota como capas complementarias. Responsable de riesgo: Gerencia de Aplicaciones Internas. Tratamiento R12. Estado abierto y sin verificar; 0 retests.	
Referencias	• https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html	

Procedimiento detallado

1. **Justificación de severidad técnica** UI:R porque otro operador abre la nota. S:C por ejecución en el contexto de navegador del lector. C:L/I:L son efectos razonables acotados de contenido activo, no fraude ni robo de cookies demostrado. A:N por

marcador sin indisponibilidad. CVSS representa la consecuencia técnica acotada del guion y no sustituye el riesgo empresarial.

2. **Actor y precondiciones del guion** Operador canario con permiso de añadir una nota; lector U04. Permiso de añadir nota al caso canario; Otro operador consulta el caso; Renderizador vulnerable definido en el modelo.
3. **Paso documental 1 (no ejecutado)** Representar una nota normal de soporte como control positivo.
4. **Paso documental 2 (no ejecutado)** Insertar un marcador canario no exfiltrante en el campo que el guion trata como HTML ejecutable.
5. **Paso documental 3 (no ejecutado)** Abrir el caso con U04 y observar la aparición del marcador en la narrativa; retirar la nota canario sin realizar acciones de negocio.
6. **E12A • transcripción sintética completa** Un marcador ejecutable ilustra XSS; no es prueba de robo de sesión ni fraude.

```
Caso: CASE-CANARIO-001
Autor de nota: operador-canario
Lector: operador-aprobador
Tratamiento: HTML sin codificación contextual
Marcador ilustrado: SIMULACION_XSS_NOTA
Conexión externa / envío de datos: ninguno
```

7. **E12B • transcripción sintética completa** HttpOnly limita lectura directa de cookie, pero no constituye reparación de XSS ni prueba de inmunidad de otras acciones.

```
Nota de texto ordinaria: renderizada
Marcador sintético: ejecutable en ficha vulnerable
Cookie de sesión: HttpOnly en el modelo
Pago sensible: step-up separado, no realizado
Objetivo: nota como texto, sin ejecución
```

8. Estos extractos se construyeron para el modelo. No son respuestas capturadas de una infraestructura real.

SIMULACIÓN • EVIDENCIA SINTÉTICA • NO EJECUTADO

F12 • Script almacenado en notas de backoffice

Extractos abreviados. Transcripciones completas en el informe; no son capturas de un sistema real.

E12A • Renderizado sintético

Notas: HTML sin codificación
Sin conexión externa ni envío

Un marcador ejecutable ilustra XSS; no es prueba de robo de sesión ni fraude.

E12B • Control de contraste

Marcador: ejecutable en el modelo
Cookie HttpOnly; pago con step-up

HttpOnly limita lectura directa de cookie, pero no constituye reparación de XSS ni prueba de inmunidad de otras acciones.

Banco Lumbre ficticio | extractos ilustrativos | Véase la transcripción A/B y los límites de la ficha

Figura 12. SIMULACIÓN • E12A: nota almacenada alcanza contexto ejecutable; E12B: controles sensibles permanecen fuera del efecto probado. Evidencia sintética no ejecutada.

9. **Resultado definido en el modelo** Ejecución de marcador visual en el contexto del lector de una nota canario.
10. **Controles actuales definidos** Acceso a caso requiere sesión; Cookie HttpOnly; Step-up separado para operación sensible definido como control de contraste. No se les atribuye una eficacia real ni rebaja automática del índice.
11. **Límites del resultado** Sin exfiltración; Sin robo de cookies; Sin transferencia o aprobación; Sin persistencia fuera de la nota; Sin atribuir impacto a otras superficies HTML no revisadas.
12. **Contención propuesta** Desactivar renderizado de HTML en notas y revisar registros del mismo tipo para retirar marcadores canario.

- 13. Prevención y dependencias** Pruebas de salida por contexto y revisión de componentes compartidos, vista previa, historial y notificaciones; no usar CSP como sustituto de tratamiento seguro del contenido. Dependencias: Decisión de producto sobre texto vs formato permitido; Inventario de sinks de la nota. Responsable técnico: Desarrollo de Backoffice / Seguridad de Aplicaciones.
- 14. Retest prospectivo: control positivo** PENDIENTE; no ejecutado. Notas de texto y formato permitido permanecen legibles y accesibles.
- 15. Retest prospectivo: control negativo** Marcadores se presentan como datos, no se ejecutan, tampoco en historial o vista previa.
- 16. Criterio de cierre y regresión** Codificación o sanitización verificadas en todos los consumidores de la nota; sin solicitudes externas ni acciones de negocio. Cambios de componente y exportación no restituyen renderizado ejecutable. La meta residual se reevaluará tras implementar y probar; aquí no se declara corregido.
- 17. Activos afectados**
 - operaciones.bancolumbre.example

13 Narrativa de ataque y límites de encadenamiento

Las cadenas siguientes distinguen condiciones, permisos iniciales y límites. El mapa de dependencias no demuestra una explotación integral.

C01 • De soporte a autorización de pagos

F04 permite modelar cambio de un factor MFA sin verificación independiente. Ese cambio no equivale a login: la autenticación primaria y otras barreras permanecen requeridas y su satisfacción no se representa. Si una vía adicional permitiera acceso a una cuenta con rol de preparador, F02 permitiría al mismo actor completar la aprobación dentro del modelo. No se afirma apropiación de cuenta, acceso universal de soporte ni liquidación de fondos.

Límite: Cadena condicional, no ejecutada, con autenticación primaria como requisito adicional no demostrado. Las dos fichas tienen controles y evidencias independientes.

C02 • Delegación corporativa hacia rol financiero

F06 incorpora una cuenta canario al grupo de autorizadores. La sincronización de A03 convierte ese grupo en rol de A04. Si se revoca después la cuenta o el grupo y persiste una familia refresh en las condiciones de F03, la exposición continúa hasta que se valide el estado en cada renovación.

Límite: No representa compromiso del dominio, membresía Domain Admin ni DCSync. La regla de mapeo de grupo a rol es un supuesto explícito del caso.

C03 • Frontera de integración y trazabilidad

F05 ilustra una solicitud saliente no aprobada. F08 muestra que un punto de origen de integración asumido alcanza puertos internos fuera de la matriz de flujos. F10 requiere por separado la identidad svc-pagos con permisos de escritura. No hay una cadena probada que transforme SSRF en credencial, modificación de datos o alteración de eventos.

Límite: Es un mapa de dependencias y agravantes, no una explotación end-to-end. No sumar impactos independientes como si fueran tres pérdidas distintas.

14 Referencias, glosario y límites de la entrega

Referencias de riesgo

RB01 • NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments. [Fuente oficial](#). septiembre 2012, final. Evaluación por escenarios, factores de verosimilitud e impacto; escalas locales y registro de incertidumbre. No prescribe nuestra matriz 5×5.

RB02 • NIST IR 8286A Rev. 1, Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. [Fuente oficial](#). diciembre 2025, final. Conexión entre apetito, tolerancia, objetivos empresariales y registros de riesgo. La edición 2021 fue reemplazada.

RB03 • NIST IR 8286B-upd1, Prioritizing Cybersecurity Risk for Enterprise Risk Management. [Fuente oficial](#). febrero 2025, actualización final. Priorización por objetivos, tratamiento, propietarios, costes de respuesta y seguimiento. No valida los plazos ficticios del caso.

RB04 • FIRST CVSS v4.0 User Guide. [Fuente oficial](#). versión 4.0, consulta 2026-10-07. CVSS Base describe severidad técnica y no constituye por sí solo una evaluación de riesgo empresarial.

RB05 • Financial Stability Board, Principles for an Effective Risk Appetite Framework. [Fuente oficial](#). 18 noviembre 2013, final. Diferenciar capacidad, apetito, límites y perfil; responsabilidades del directorio y alta dirección. No demuestra capacidad financiera de Banco Lumbré.

RB06 • BCBS, Principles for operational resilience. [Fuente oficial](#). 31 marzo 2021, publicación vigente. Operaciones críticas, tolerancia a la disrupción, dependencias y gobierno de resiliencia. Usamos la publicación final de 2021, no el módulo consolidado de 2026 que la web identifica como borrador.

Referencias técnicas

S01 • API1:2023 Broken Object Level Authorization. [Fuente oficial](#). Distinción de autorización por objeto; comprobar sujeto, objeto y acción, sin usar ID opaco como reparación.

S02 • Authorization Cheat Sheet. [Fuente oficial](#). Denegación por defecto, privilegio mínimo y verificación de permisos por solicitud.

S03 • Transaction Authorization Cheat Sheet. [Fuente oficial](#). Autorización aplicada en servidor y vinculada a datos específicos de transacción, separada de autenticación de inicio de sesión.

S04 • Session Management Cheat Sheet. [Fuente oficial](#). Ciclo de sesión, invalidación, renovación por cambios de privilegio y trazabilidad sin secretos.

S05 • Multifactor Authentication Cheat Sheet. [Fuente oficial](#). Recuperación y cambio de factores como operaciones sensibles, verificación y notificación independientes.

S06 • Server Side Request Forgery Prevention Cheat Sheet. [Fuente oficial](#). Política de destinos y defensas de aplicación y red adaptadas al caso de uso de llamadas salientes.

S07 • Delegation of Control in AD DS on Windows Server. [Fuente oficial](#). Delegación de tareas y modificación de membresías con alcance de OU y herencia; no equivale necesariamente a administración del dominio.

S08 • Secure use reference. [Fuente oficial](#). Permisos mínimos, control de secretos en salidas y uso de identidad de corta duración para workflows cuando sea aplicable.

S09 • Network Segmentation Cheat Sheet. [Fuente oficial](#). Fronteras de red y limitación de movimientos por flujos explícitos como capa complementaria a autenticación.

S10 • SQL Injection Prevention Cheat Sheet. [Fuente oficial](#). Parametrización, listas permitidas para elementos no parametrizables y privilegio mínimo de datos.

- S11 • Logging Cheat Sheet.** [Fuente oficial](#). Protección de eventos frente a acceso y modificación no autorizados, trazabilidad y exclusión de valores sensibles.
- S12 • API5:2023 Broken Function Level Authorization.** [Fuente oficial](#). Separar permisos de invocación de función del acceso a objetos y de la visibilidad de la interfaz.
- S13 • Cross Site Scripting Prevention Cheat Sheet.** [Fuente oficial](#). Salida segura según contexto, APIs seguras y sanitización de HTML permitido; CSP es defensa complementaria.
- S14 • Common Vulnerability Scoring System v3.1 Specification Document.** [Fuente oficial](#). Puntaje base y vector técnicos, diferenciados de priorización organizacional, pérdidas monetarias y riesgo empresarial.
- S15 • Special-Use Domain Names.** [Fuente oficial](#). Espacio .example reservado para documentación; los dominios del ejercicio no se presentan como destinos reales.

Glosario

Término	Uso en la muestra
CVSS	Severidad técnica derivada de un vector; no probabilidad ni pérdida empresarial
IRN	Índice ordinal $P \times I$, 1–25, definido para el escenario
P / I	Plausibilidad relativa e impacto máximo entre cuatro dimensiones
BOLA / BFLA	Autorización a nivel de objeto / a nivel de función
MFA / IAM	Autenticación multifactor / gobierno de identidades y acceso
Maker-checker	Preparador y aprobador distintos, con permisos válidos
RTO / RPO	Objetivo de tiempo de recuperación / punto recuperable; no pruebas ejecutadas
KRI / KPI	Indicador de exposición / indicador de ejecución, con denominador y fuente
Residual objetivo	Meta condicionada a implementación y retest; no reducción ya observada
T0	Aprobación hipotética del plan que iniciaría los SLA; no fecha efectiva aquí

Limitaciones de entrega y lectura

Las cuatro salidas son generadas por report-gen 0.21.2 desde la misma fuente. La comprobación de contenido y hashes acredita integridad de exportación, no pruebas bancarias. Word conserva campos de índice: los números de página se actualizan al abrirlo con Ctrl+A y F9. La paginación puede diferir de PDF. El HTML es autónomo; sus filtros son opciones de lectura y no permisos. Markdown omite el gráfico de severidad del generador, pero conserva las figuras sintéticas y las tablas.

Muestra pública de metodología y capacidad de comunicación; no acredita experiencia laboral bancaria ni una certificación de cumplimiento.

Compatibilidad de lectura: el HTML portátil original de report-gen 0.21.2 puede presentar desbordamiento de la barra de filtros en una pantalla de 320 px. Para ese ancho, se recomienda la lectura PDF o un visor de escritorio. El archivo HTML conserva los recursos y controles originales del generador; no se alteró su plantilla. La validación visual de Word se realiza mediante LibreOffice; no equivale a una prueba de Microsoft Word nativo.