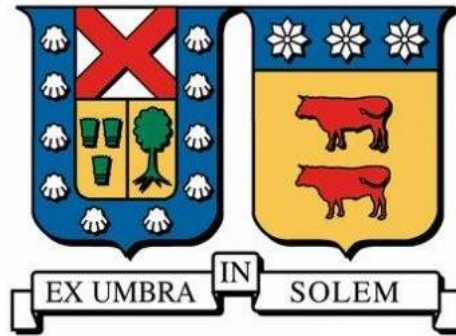




**UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA DEPARTAMENTO DE
INDUSTRIAS**

**DISEÑO DE UN MODELO DE ANÁLISIS DE DATOS FORENSES PARA DETECTAR
ANOMALÍAS Y FORTALECER EL CONTROL DEL PROCESO DE
ABASTECIMIENTO EN UNA OPERACIÓN MINERA CHILENA.**

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL INDUSTRIAL

AUTOR

RENATO ALEJANDRO SANTIS PONCE

PROFESOR GUÍA

ESTEBAN SALGADO VALENZUELA

SANTIAGO, 2026



CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título ☐ Tesis de Postgrado

Título del trabajo:

Diseño de un modelo de análisis de datos forense para detectar anomalías y fortalecer el control del proceso de abastecimiento en una operación minera chilena

Nombre del candidato(a):

Renato Alejandro Santis Ponce

Carrera / Grado:

Ingeniería Civil Industrial

Campus: Vitacura **Departamento:** Industrial

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Esteban Salgado, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

☒ El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por (**marcar una opción**):

☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 08/07/2026

Firma: 

Estudiante o Candidato(a):



Fecha: 08-07-2026 Firma: _____

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

Índice

1. AGRADECIMIENTOS	6
2. PROBLEMA DE INVESTIGACIÓN.....	7
3. OBJETIVOS.....	12
3.1. OBJETIVO GENERAL.....	12
3.2. OBJETIVOS ESPECÍFICOS	12
4. MARCO TEÓRICO	13
4.1. RELEVANCIA DEL ABASTECIMIENTO COMO FUNCIÓN CRÍTICA EN LA OPERACIÓN MINERA	13
4.2. EL PROCESO DE ABASTECIMIENTO BAJO EL ENFOQUE PROCURE-TO-PAY (P2P).....	13
4.2.1. <i>El proceso de abastecimiento</i>	14
4.2.2. <i>Perspectiva Procure-to-Pay (P2P) y trazabilidad documental-transaccional</i>	14
4.2.3. <i>Importancia del proceso para identificar anomalías y fortalecer el control</i>	16
4.3. RIESGOS, DESVIACIONES E IRREGULARIDADES EN EL PROCESO DE ABASTECIMIENTO P2P.....	16
4.4. CONTROL INTERNO, COMPLIANCE Y GESTIÓN DE TERCEROS	18
4.5. AUDITORÍA FORENSE APLICADA AL PROCESO DE ABASTECIMIENTO	20
4.6. ANÁLISIS DE DATOS FORENSES Y DETECCIÓN DE ANOMALÍAS.....	21
4.6.1. <i>Qué se entiende por análisis de datos forenses</i>	22
4.6.2. <i>Diferencia entre analítica descriptiva, diagnóstica y orientada a anomalías</i>	22
4.6.3. <i>Detección de anomalías y principales pruebas analíticas</i>	23
4.6.4. <i>Utilidad de la analítica en el monitoreo continuo</i>	23
5. METODOLOGÍA.....	26
5.1. DISEÑO Y ENFOQUE DE LA INVESTIGACIÓN	26
5.2. IMPLEMENTACIÓN DEL MODELO MEDIANTE LENGUAJE PYTHON	27
5.3. SIMULACIÓN DEL MODELO MEDIANTE DATOS SINTÉTICOS GENERADOS CON APOYO DE INTELIGENCIA ARTIFICIAL.....	29
6. RESULTADOS Y DISCUSIÓN	31
6.1. DISEÑO DEL MODELO DE ANÁLISIS DE DATOS FORENSES.....	31
6.1.1. <i>Pruebas de consistencia</i>	31
6.1.2. <i>Pruebas de duplicidad</i>	39
6.1.3. <i>Pruebas de secuencia</i>	46
6.1.4. <i>Pruebas de relación</i>	53
6.1.5. <i>Pruebas de temporalidad</i>	60
6.2. IMPLEMENTACIÓN DEL MODELO MEDIANTE LENGUAJE PYTHON	67
6.2.1. <i>Propósito de la implementación computacional del modelo</i>	67
6.2.2. <i>Arquitectura general del script</i>	68
6.2.3. <i>Bibliotecas utilizadas y su función dentro del modelo</i>	69
6.2.4. <i>Lectura, clasificación y homologación de las fuentes de datos</i>	70
6.2.5. <i>Interacción del script con el usuario</i>	72
6.2.6. <i>Lógica de ejecución de las pruebas</i>	73
6.2.7. <i>Generación de alertas y trazabilidad de los resultados</i>	74
6.2.8. <i>Salida del modelo y estructura del archivo Excel</i>	75
6.2.9. <i>Requerimientos de ejecución del modelo</i>	76
6.3. SIMULACIÓN DEL MODELO MEDIANTE DATOS SINTÉTICOS GENERADOS CON APOYO DE INTELIGENCIA ARTIFICIAL.....	77
6.3.1. <i>Propósito de la simulación del modelo</i>	77
6.3.2. <i>Generación de la base sintética con apoyo de inteligencia artificial</i>	78
6.3.3. <i>Archivos sintéticos generados para representar el flujo P2P</i>	80
6.3.4. <i>Ejecución del modelo sobre la base sintética</i>	81
6.3.5. <i>Resultados generales de la ejecución</i>	82
6.3.6. <i>Matriz de alertas, trazabilidad y resumen de situaciones observadas</i>	86
6.4. LIMITACIONES DE LOS RESULTADOS.	87
7. CONCLUSIÓN	91
8. REFERENCIAS	95

9.	APÉNDICE	101
9.1.	APÉNDICE A: LISTADO DE ANEXOS INCORPORADOS EN LA INVESTIGACIÓN.....	101
9.2.	APÉNDICE B: LISTADO DE FIGURAS INCORPORADAS EN LA INVESTIGACIÓN.	101
9.3.	APÉNDICE C: LISTADO DE TABLAS INCORPORADAS EN LA INVESTIGACIÓN.	101

1. Agradecimientos

Quiero agradecer, en primer lugar, a mis padres, el motor de mi vida. Gracias por creer en mí incluso cuando yo dudaba, por apostar por mis capacidades sin reservas y por sostenerme durante cada crisis universitaria. Me permitieron caer, pero jamás me dejaron solo en el camino. Todo lo que soy lleva algo de ustedes.

A mi mejor amiga, Isidora, por acompañarme durante estos cinco años, compartir largas tardes de estudio y recordarme que también había una vida para disfrutar. A Ignacia, Valentina, Sofía, Sebastián y Claudio, por hacer de la universidad una etapa más alegre y enseñarme que no todo era estudiar. A mis compañeros de generación y, especialmente, a Sophie Barsom, mi cómplice y apoyo fundamental en este proceso.

A toda mi familia, en especial a mi tío Rusio, por regalarme su tiempo, su espacio y su confianza, y a mi hermana Josefa, porque, aun en la distancia, siempre estuvo cerca de mi corazón.

Finalmente, quiero agradecerme a mí mismo. Por la disciplina, la fortaleza y la determinación, por no rendirme, incluso cuando el camino se volvió difícil. Lo lograste, Renato. Gracias por seguir adelante y creer en ti.

2. Problema de investigación

El problema de investigación se origina en la necesidad de analizar cómo la industria minera chilena, sector estratégico para el país, puede enfrentar brechas de control interno en el proceso de abastecimiento de bienes y servicios provistos por terceros, proceso cuya existencia es crítica debido a la implicancia en la continuidad operacional y, al mismo tiempo, la red extensa de relaciones con proveedores, contratistas y subcontratistas que debe ser adecuadamente controlada. Cuando la trazabilidad de datos y los mecanismos de monitoreo no se desarrollan al mismo ritmo que la escala operativa del abastecimiento, se incrementa la exposición a irregularidades, desviaciones y riesgos que pueden afectar la eficiencia, la integridad y la confiabilidad del proceso.

La relevancia de esta problemática se comprende, en primer lugar, por la importancia económica y productiva de la minería en Chile. De acuerdo con la Sociedad Nacional de Minería (SONAMI, 2025), en 2024 el PIB¹ minero representó aproximadamente un 11,7% del PIB nacional, generó alrededor de 286 mil empleos directos y concentró cerca del 25% de la formación bruta de capital fijo del país. Esta importancia también se proyecta hacia los próximos años, dado que la cartera de inversión minera para el período 2025-2034 asciende a US\$104.549 millones, mientras que las proyecciones de producción de cobre anticipan volúmenes cercanos a 5,97 millones de toneladas hacia 2027 y una participación chilena de 27,3% en la producción mundial de cobre al año 2034 (Comisión Chilena del Cobre [COCHILCO], 2025a, 2025b). En este contexto, la estabilidad y el control de los procesos que sostienen la operación minera adquieren especial relevancia, no solo para la continuidad de las compañías, sino también para el desempeño de una actividad con impacto significativo en la economía nacional.

Dentro de esa lógica, el abastecimiento cumple una función esencial. En minería, abastecer no significa únicamente comprar materiales o insumos físicos, sino también contratar repuestos, equipos, transporte, ingeniería, mantenimiento, servicios especializados y apoyo operativo. Por ello, la competitividad y continuidad de una operación minera dependen en gran medida del ecosistema de

¹**Producto Interno Bruto (PIB):** indicador macroeconómico que mide el valor total de los bienes y servicios finales producidos en un país durante un período determinado. Se utiliza para estimar el tamaño y desempeño de una economía.

proveedores que permite sostener el funcionamiento de las faenas (SONAMI, 2025). La magnitud de este proceso se refleja en que, durante 2023, 26 operaciones mineras equivalentes al 96% de la producción de cobre de Chile informaron un gasto por US\$23.147 millones en bienes y servicios (COCHILCO, 2024). A ello se suma la existencia de 8.428 empresas vinculadas al suministro de máquinas, equipos, tecnologías y servicios para la minería, lo que evidencia un universo amplio de relaciones comerciales asociadas a la actividad (Subsecretaría de Relaciones Económicas Internacionales [SUBREI] & ProChile, 2024).

Esta amplitud del ecosistema proveedor genera un volumen significativo de interacciones, documentos y registros transaccionales. Cada relación con terceros puede involucrar solicitudes, órdenes de compra, contratos, anexos, recepciones, hojas de entrada de servicio, certificaciones, estados de pago, facturas, respaldos documentales y registros contables. En términos operativos, una sola faena minera puede procesar más de 100 mil documentos anuales vinculados a contratistas y cumplimiento normativo, antecedente que, sin constituir una estadística oficial representativa de toda la industria, permite dimensionar la escala documental que puede alcanzar una operación minera y la dificultad de sostener controles exhaustivos mediante revisión manual individual (trendTIC, 2026). Por ello, la trazabilidad no constituye solo una práctica deseable, sino una condición necesaria para controlar adecuadamente el flujo de abastecimiento.

Sin embargo, la existencia de datos no garantiza por sí sola un control efectivo. La problemática de esta investigación no radica en la participación de terceros, ya que esta es inherente al modelo operativo de la minería, sino en que el proceso de abastecimiento no puede seguir siendo gestionado mediante controles fragmentados, revisiones manuales y validaciones no siempre integradas entre las distintas etapas del flujo.

La relevancia de esta brecha se refuerza al considerar la evidencia internacional sobre fraude, compras y controles internos. A nivel global, una organización típica pierde aproximadamente 5% de sus ingresos anuales por fraude, y más de la mitad de los fraudes ocupacionales se explica por ausencia

de controles internos o por anulación de controles existentes (Association of Certified Fraud Examiners [ACFE], 2024). Esta evidencia resulta pertinente para el problema planteado, porque sitúa al control interno como un factor crítico para prevenir o detectar oportunamente situaciones irregulares. En la misma línea, PwC (2024a) identifica al fraude en compras como uno de los delitos económicos más disruptivos y advierte que una proporción relevante de organizaciones no cuenta con programas robustos de gestión del riesgo de terceros o no utiliza analítica de datos de manera intensiva para identificar fraude en abastecimiento. Esta información no permite afirmar que toda operación minera presente fraude, pero sí sustenta que un proceso intensivo en terceros, documentación y pagos requiere mecanismos de control proporcionales a su complejidad.

En Chile, esta necesidad de prevención y control también se relaciona con un entorno regulatorio más exigente. La Ley N° 21.595 sistematizó los delitos económicos y reforzó la importancia de los mecanismos corporativos de prevención, supervisión y trazabilidad frente a conductas con potencial responsabilidad para personas naturales y jurídicas (Biblioteca del Congreso Nacional de Chile, 2023). A su vez, la Norma de Carácter General N° 461 exige reportar información sobre gobierno corporativo, gestión de riesgos, modelo de negocios y gestión de proveedores, incorporando una lógica de transparencia, rendición de cuentas y monitoreo sobre terceros (Comisión para el Mercado Financiero [CMF], 2021). Bajo esta perspectiva, el abastecimiento deja de ser solo un proceso administrativo y se transforma en un ámbito de exposición regulatoria y eventualmente penal.

Esta preocupación adquiere mayor concreción cuando se observan antecedentes públicos recientes en la industria minera chilena. La judicialización de un presunto fraude interno en Minera Los Pelambres, filial de Antofagasta Minerals, asociado a adjudicación irregular de licitaciones, compras spot² dirigidas y adquisición de materiales innecesarios o sobrevalorados por al menos \$8.203 millones, ilustra cómo una falla de control en abastecimiento puede alcanzar una alta materialidad económica y generar cuestionamientos sobre la integridad organizacional (Cárdenas, 2025). Al tratarse de una causa

²**Compra spot:** adquisición puntual de un bien o servicio realizada para atender una necesidad urgente o excepcional, que no sigue la conducta regular del proceso de abastecimiento ni forma parte de la planificación habitual de compras.

en curso, este antecedente debe entenderse como una señal pública de riesgo y no como un hecho judicialmente concluido. Su utilidad para esta investigación radica en que permite observar cómo los procesos de compras, licitaciones, validación y pago pueden convertirse en espacios sensibles cuando existen debilidades de control, segregación de funciones, trazabilidad o monitoreo.

En este marco, la investigación se orienta por cuatro interrogantes centrales:

- ¿Cuáles son las principales brechas de trazabilidad, integración de datos y control presentes en el proceso de abastecimiento de bienes y servicios prestados por terceros en una operación minera chilena?
- ¿Qué anomalías y señales de alerta pueden presentarse en las distintas etapas del proceso, desde la solicitud y emisión de la orden de compra hasta la recepción, certificación, facturación y pago?
- ¿Qué variables y cruces de información permiten identificar de manera más efectiva dichas anomalías dentro del proceso de abastecimiento minero?
- ¿Cómo puede el análisis de datos forenses contribuir al fortalecimiento del control del proceso de abastecimiento en una operación minera chilena?

Frente a esta situación, la presente investigación propone abordar el proceso de abastecimiento desde un enfoque de análisis de datos forenses orientado a la prevención y al fortalecimiento del control. En lugar de limitarse a controles manuales basados en muestras o revisiones posteriores a la ocurrencia de una desviación, el estudio se enfocará en trabajar sobre los datos generados a lo largo del flujo operativo, incluyendo solicitudes, órdenes de compra, recepciones, certificaciones de servicio, facturas y pagos. A partir de esa información, se buscará definir variables, cruces, pruebas analíticas e indicadores capaces de detectar inconsistencias, desviaciones o patrones atípicos relevantes para la gestión del riesgo. De este modo, la tesis no busca probar judicialmente un ilícito, sino diseñar un modelo aplicado que permita transformar un proceso tradicionalmente reactivo en uno más preventivo, trazable y susceptible

de automatización. Con ello, se espera aportar una herramienta de fortalecimiento del control del abastecimiento minero, útil para auditoría interna, compliance operacional y gestión de riesgos, y, al mismo tiempo, contribuir al conocimiento aplicado sobre el uso de analítica forense de datos en procesos intensivos en terceros, alta materialidad económica y elevada exposición al riesgo.

Para efectos de esta investigación, la operación minera considerada corresponde a una faena minera chilena en la cual las áreas usuarias generan solicitudes de requerimiento de bienes o servicios que ingresan al proceso formal de abastecimiento. Dicho proceso será analizado bajo un enfoque Procure-to-Pay, considerando la lógica de un sistema ERP tipo SAP, sin que el modelo quede limitado exclusivamente a dicha plataforma.

3. Objetivos

3.1. Objetivo general

Diseñar un modelo de análisis de datos forenses aplicado al proceso de abastecimiento de bienes y servicios de terceros en una operación minera chilena, con el fin de identificar anomalías y señales de alerta, y fortalecer la trazabilidad y el control del proceso.

3.2. Objetivos específicos

- Analizar el proceso de abastecimiento de bienes y servicios de terceros en una operación minera chilena, identificando sus etapas, actores, registros y puntos de control relevantes para la trazabilidad del flujo.
- Identificar las principales brechas de trazabilidad, integración de datos y control presentes en las etapas del proceso de abastecimiento.
- Definir las variables, criterios de análisis y cruces de información que permitan detectar anomalías y señales de alerta en el proceso de abastecimiento minero.
- Diseñar pruebas analíticas e indicadores forenses orientados a detectar inconsistencias, desvíos y patrones atípicos en las distintas etapas del proceso de abastecimiento.
- Integrar las variables, cruces de información, pruebas analíticas e indicadores definidos en una propuesta de modelo de análisis de datos forenses, incorporando una estructura de reporte de alertas orientada al fortalecimiento de la trazabilidad y el control del proceso de abastecimiento.
- Simular la aplicación del modelo de análisis de datos forenses en un escenario representativo del proceso de abastecimiento, con el fin de evaluar preliminarmente su utilidad para la detección de anomalías y señales de alerta.

4. Marco teórico

4.1. Relevancia del abastecimiento como función crítica en la operación minera

El abastecimiento en una operación minera debe comprenderse como una función crítica para la continuidad operacional y no solo como una actividad administrativa de compra. Su importancia radica en que permite disponer oportunamente de bienes y servicios necesarios para sostener el funcionamiento de la faena, conectando las necesidades de las áreas usuarias con el mercado proveedor.

La criticidad de este proceso se explica por la alta dependencia que la minería mantiene respecto de proveedores y contratistas. COCHILCO (2024) reportó que, durante 2023, una muestra de 26 operaciones productoras de cobre, representativa del 96% de la producción nacional, informó US\$23.147 millones en compras de insumos para la operación. A su vez, el Consejo Minero (2026) señaló que, en 2024, las remuneraciones a trabajadores y los pagos a proveedores de insumos y servicios alcanzaron US\$30.488 millones, equivalentes al 59% de las principales partidas de distribución de flujos de la gran minería. Estos antecedentes permiten observar que una parte sustantiva del funcionamiento minero se sostiene mediante relaciones con terceros, tanto en términos económicos como operacionales.

Desde una perspectiva organizacional, el abastecimiento opera como una función transversal dentro de la compañía (Lagos, 2023). Por ello, su gestión requiere trazabilidad, coordinación y control tanto entre las áreas internas como en la relación con los proveedores, ya que cualquier quiebre en este proceso puede afectar la continuidad operacional y debilitar la consistencia del flujo de abastecimiento.

4.2. El proceso de abastecimiento bajo el enfoque Procure-to-Pay (P2P)

Una vez reconocida la relevancia del abastecimiento para la continuidad operacional minera, corresponde precisar qué se entiende por este proceso y cómo se estructura dentro de la organización. Esta definición es necesaria porque el abastecimiento no constituye una compra aislada, sino un conjunto de actividades que vincula la necesidad interna con la gestión del proveedor y con los controles que permiten respaldar la operación del requerimiento.

4.2.1.El proceso de abastecimiento

El proceso de abastecimiento se define como el conjunto secuencial de actividades mediante las cuales una organización identifica una necesidad, gestiona la compra o contratación requerida para satisfacer dicha necesidad, formaliza el vínculo con un proveedor, verifica la recepción del bien o la conformidad del servicio y habilita el pago correspondiente. Esta definición permite diferenciar el abastecimiento de una simple compra aislada, ya que incorpora decisiones, autorizaciones, registros, responsabilidades y controles que deben operar de manera coordinada. En esta línea, ChileCompra (2022) plantea que los procedimientos de abastecimiento poseen tanto una dimensión operativa, vinculada con la disponibilidad de bienes y servicios, como una dimensión de control, asociada a la justificación de la necesidad, la formalización de la adquisición y la conservación de evidencia para su revisión posterior. Desde esta perspectiva, el abastecimiento conecta la necesidad del usuario interno con la respuesta del mercado proveedor y con el reconocimiento contable y financiero de la transacción.

4.2.2.Perspectiva Procure-to-Pay (P2P) y trazabilidad documental-transaccional

Una forma útil de estudiar el abastecimiento es mediante el enfoque Procure-to-Pay (P2P), también denominado Purchase-to-Pay. SAP (2026) describe este enfoque como la integración entre los sistemas de compras³ y cuentas por pagar⁴, con el propósito de mejorar la eficiencia, controlar el gasto y mantener visibilidad sobre el ciclo completo de adquisición. De manera complementaria, Oracle (s. f.) presenta el P2P como un proceso integrado que normalmente comprende requerimiento, orden de compra, recepción y cuentas por pagar. En términos prácticos, esta mirada desplaza el foco desde la compra como hecho puntual hacia una secuencia lógica de punta a punta, permitiendo así observar el abastecimiento como una cadena documental y transaccional

Para efectos de esta investigación, el ciclo P2P se estructura en cinco etapas principales, cada una de estas etapas cumple una función específica y, al mismo tiempo, incorpora puntos de control

³**Sistema de compras:** herramienta o módulo utilizado por una organización para gestionar las actividades asociadas a la adquisición de bienes y servicios, incluyendo solicitudes, órdenes de compra, aprobaciones, proveedores, condiciones comerciales y seguimiento del proceso de compra.

⁴**Sistema de cuentas por pagar:** herramienta o módulo contable-financiero utilizado para registrar, validar y administrar las obligaciones de pago de una organización frente a sus proveedores, considerando facturas, vencimientos, aprobaciones, registros contables y ejecución o programación de pagos.

esperados. A continuación, las cinco etapas principales del ciclo P2P:

- La solicitud de pedido o SolPed: Corresponde al inicio del ciclo. Su función es formalizar una necesidad interna, dejando evidencia de qué se requiere, quién lo solicita, con qué propósito y bajo qué imputación presupuestaria o centro de costo.
- La orden de compra (OC): Formaliza la adquisición o contratación frente al proveedor. En ella se establecen condiciones comerciales y operativas, tales como descripción del bien o servicio, precio, cantidad, plazos, moneda, condiciones de pago e imputación contable.
- La hoja de entrada de servicios (HES): Acredita que el servicio fue efectivamente ejecutado o aceptado por el área responsable. En el caso de bienes, esta función puede cumplirse mediante una hoja de entrada de mercaderías u otro registro de recepción. La Asociación Chilena de Seguridad (2026) muestra que, para procesar pagos a proveedores, se exige la existencia de OC y HES o HEM, según corresponda, lo que permite entender la recepción o conformidad como una evidencia de realidad operacional antes del pago.
- La facturación: representa el cobro formal del proveedor y, en el contexto chileno, normalmente se materializa mediante documentos tributarios electrónicos. Desde la lógica P2P, la factura no basta por sí sola para justificar el pago, sino que debe estar vinculada con la OC y con la recepción o conformidad correspondiente.
- El pago: Corresponde al cierre del ciclo P2P. En esta etapa, la organización transforma una obligación documentada en una salida efectiva de fondos. Su control esperado es que el pago se ejecute solo cuando exista consistencia entre la necesidad, la orden de compra, la conformidad del bien o servicio, la factura y los registros contables.

Adicionalmente, la efectividad de este ciclo depende también de la correcta distribución de roles

y responsabilidades. El usuario interno formula la necesidad, el área de compras gestiona la adquisición, el responsable operativo valida la recepción o conformidad, cuentas por pagar revisa la documentación y registra la obligación, tesorería ejecuta el pago y el proveedor entrega el bien o servicio y emite la factura correspondiente. Asimismo, la auditora Deloitte (s. f.) advierte que la segregación de funciones es necesaria para evitar la acumulación de permisos incompatibles en los sistemas, siendo esta una característica propia del ciclo P2P.

4.2.3. Importancia del proceso para identificar anomalías y fortalecer el control

Ahora bien, la relevancia del proceso de abastecimiento no es únicamente operativa, si no también tiene una importancia directa para la detección de anomalías, porque cada etapa del ciclo P2P genera evidencia que puede ser contrastada. Cuando la secuencia documental y transaccional funciona correctamente, es posible reconstruir el recorrido de una adquisición desde la necesidad inicial hasta el pago. En cambio, cuando se observa brechas de consistencias entre las etapas, aparecen quiebres de trazabilidad que pueden transformarse en señales de alerta.

4.3. Riesgos, desviaciones e irregularidades en el proceso de abastecimiento P2P

El análisis del ciclo P2P permite entender que los riesgos del abastecimiento no dependen solo de una decisión de compra, sino de la forma en que las distintas etapas del proceso se conectan y se controlan. Cuando esa conexión se debilita, pueden generarse espacios de discrecionalidad, pérdida de respaldo o baja capacidad de verificación. En minería, estos riesgos adquieren especial relevancia por la participación intensiva de terceros y por el impacto que una falla en el abastecimiento puede tener sobre la continuidad operacional. Por ello, resulta necesario estudiar las desviaciones e irregularidades que pueden presentarse en el proceso, considerando tanto la trazabilidad documental como los registros transaccionales que deja cada operación. Esta mirada es coherente con el U.S. Department of Justice (2024), que destaca la importancia de identificar riesgos, gestionar terceros y utilizar datos para verificar el funcionamiento efectivo de los controles. Asimismo, la ACFE (2024) advierte que muchos fraudes ocupacionales son detectados por denuncias, lo que refuerza la necesidad de complementar los controles

tradicionales con procedimientos analíticos más oportunos y alineados con los riesgos propios del ciclo.

Dentro del flujo P2P, las principales debilidades suelen concentrarse en aquellos puntos donde existe mayor discrecionalidad, evidencia insuficiente, baja segregación de funciones o controles susceptibles de ser eludidos. Estas alertas pueden ordenarse según la etapa del proceso en que se originan:

- Etapa de requerimiento y adjudicación: Pueden presentarse especificaciones diseñadas para favorecer a un proveedor, restricciones artificiales a la competencia, compras directas sin justificación suficiente, uso inadecuado de urgencias, proveedores no homologados o fraccionamiento de requerimientos para evitar umbrales de aprobación.
- Etapa de ejecución, recepción o conformidad: Pueden observarse recepciones o HES sin respaldo suficiente, conformidades técnicas emitidas de forma tardía, servicios aceptados sin evidencia operacional, diferencias entre el alcance contratado y lo efectivamente ejecutado, o validaciones documentales que no permiten acreditar adecuadamente la prestación del bien o servicio.
- Etapa de facturación y pago: Pueden identificarse facturas duplicadas, facturas sin referencia clara a la orden de compra o recepción correspondiente, pagos indebidos, pagos acelerados sin justificación, inconsistencias entre OC, HES, factura y pago, o modificaciones riesgosas en datos maestros del proveedor, especialmente cuentas bancarias, condiciones de pago o datos de identificación.

Asimismo, la corrupción, la colusión y los conflictos de interés deben comprenderse como riesgos transversales del abastecimiento, más que como eventos asociados a una sola etapa. Por su parte, el conflicto de interés puede afectar la objetividad del proceso cuando un colaborador participa en la selección, evaluación, recepción o pago de un proveedor con el cual mantiene vínculos personales, económicos o funcionales no declarados. En estos casos, el riesgo no se agota en la adjudicación, sino que puede extenderse al ciclo completo.

Adicionalmente, las irregularidades documentales y transaccionales son relevantes porque conectan los riesgos del abastecimiento con evidencia verificable. A diferencia de riesgos más conductuales, muchas desviaciones del P2P dejan huellas en los datos. La ACFE (s. f.) propone pruebas analíticas orientadas a revisar facturas que no cumplen con el three-way match⁵, identificar duplicidades, analizar discrepancias entre condiciones de pago y datos maestros, o detectar pagos aprobados en condiciones anómalas. De esta manera, las debilidades de control pueden transformarse en señales observables.

Por ello, las red flags⁶ cumplen un rol central como puente entre la comprensión conceptual del riesgo y el diseño de pruebas analíticas. La literatura reciente ha destacado el uso de análisis estadístico, aprendizaje automático, análisis de redes y process mining para identificar patrones de colusión, favoritismo y comportamiento anómalo, aunque su efectividad depende de la calidad, disponibilidad y trazabilidad de los datos (Lyra et al., 2022; Santos et al., 2025). Por ello, el estudio de riesgos, desviaciones e irregularidades en el proceso de abastecimiento permite fundamentar la necesidad de un modelo de análisis de datos forenses orientado a detectar anomalías y fortalecer el control del flujo P2P en una operación minera chilena.

4.4. Control interno, compliance y gestión de terceros

Las desviaciones e irregularidades que pueden presentarse en el proceso de abastecimiento no dependen únicamente de errores transaccionales aislados, sino también de la forma en que la organización gobierna, supervisa y controla su relación con terceros. Por ello, el análisis de riesgos del ciclo P2P debe complementarse con una revisión del control interno, compliance y la gestión de proveedores, ya que estos elementos permiten establecer criterios, responsabilidades y mecanismos de monitoreo para prevenir, detectar y responder frente a debilidades del proceso. En esta línea, COSO (2013) plantea que el control interno debe entenderse como un proceso integrado a la gestión

⁵**Three-way match:** control de cuentas por pagar que consiste en comparar tres elementos antes de autorizar un pago: la orden de compra, la recepción o conformidad del bien o servicio, y la factura del proveedor. Su objetivo es verificar que lo facturado corresponda a lo solicitado, autorizado y efectivamente recibido o ejecutado.

⁶**Red flags:** señales de alerta que indican condiciones inusuales, inconsistencias o patrones atípicos que pueden revelar errores, debilidades de control, incumplimientos o posibles irregularidades. No prueban por sí solas la existencia de fraude, pero justifican una revisión más profunda.

organizacional, orientado a entregar una seguridad razonable sobre el cumplimiento de los objetivos del negocio. Esta mirada resulta especialmente relevante en abastecimiento, donde la calidad de los controles condiciona directamente la exposición a errores, desviaciones y conductas impropias.

Bajo esa misma lógica, el cumplimiento no puede reducirse al acatamiento formal de normas externas, sino que debe comprenderse como una capacidad organizacional para traducir obligaciones legales, regulatorias y éticas en políticas, procedimientos, controles y prácticas que funcionen efectivamente en la operación. En este sentido, la International Organization for Standardization (ISO, 2021) señala en la ISO 37301 que un sistema de gestión de compliance⁷ debe desarrollarse, de modo que sea receptivo a la realidad de la organización. Complementariamente, la ISO (2025) sostiene en la ISO 37302 que la sola existencia de un sistema no basta, pues su efectividad debe ser evaluada mediante revisiones que permitan verificar si realmente funciona en la práctica. Desde esa mirada, elementos como la evaluación de riesgos, y la gestión de terceros no representan piezas aisladas, sino componentes de un sistema que debe demostrar efectividad real.

En el contexto chileno, esta exigencia adquiere especial relevancia, ya que la Biblioteca del Congreso Nacional de Chile (2009) muestra que la Ley N° 20.393 exige modelos de prevención estructurados sobre la identificación de riesgos, la definición de protocolos y procedimientos, la existencia de responsables, la supervisión del modelo y su actualización, donde posteriormente, la Biblioteca del Congreso Nacional de Chile (2023) evidencia que la Ley N° 21.595 amplió el catálogo de delitos por los cuales pueden responder penalmente las personas jurídicas y elevó el estándar preventivo exigible. En consecuencia, el compliance no debe entenderse como una dimensión periférica del control, sino como una necesidad de gobernanza que evidencia el funcionamiento efectivo.

Esta discusión adquiere una importancia particular en la industria minera chilena, donde la dependencia de proveedores y contratistas incrementa la criticidad del control sobre terceros. En este

⁷**Sistema de gestión de compliance:** conjunto de políticas, procedimientos, controles, responsabilidades y mecanismos de monitoreo que una organización implementa para prevenir, detectar y responder frente a riesgos de incumplimiento legal, regulatorio, ético o interno, promoviendo que sus actividades se desarrollen conforme a las obligaciones y estándares aplicables.

entorno, la gestión de terceros no puede limitarse a una revisión inicial del proveedor al momento de su incorporación, sino que debe abarcar todo el ciclo de relación. En esta línea, The Institute of Internal Auditors (IIA, 2018) sostiene que la debida diligencia de terceros debe aplicarse no solo al inicio del vínculo, sino también de forma periódica y proporcional al nivel de riesgo, con el objeto de verificar que el tercero continúe cumpliendo los estándares definidos por la organización y que no incorpore riesgos inaceptables. El mismo instituto subraya que las políticas y procedimientos de gestión de terceros deben contemplar criterios de revisión, escalamiento y tratamiento de señales de alerta, y que el contrato constituye un control relevante en la medida en que comunica al tercero las expectativas de la organización, su apetito de riesgo y sus exigencias mínimas de comportamiento y control. Esta necesidad de gestión continua también se observa en evidencia reciente.

4.5. Auditoría forense aplicada al proceso de abastecimiento

A partir del rol que cumplen el control interno, el compliance y la gestión de terceros en el proceso de abastecimiento, la auditoría forense adquiere relevancia cuando es necesario ir más allá de la existencia formal de controles y examinar cómo operó realmente una transacción. En el ciclo P2P, las desviaciones no siempre se presentan como hechos evidentes, sino como quiebres de trazabilidad, inconsistencias documentales, aprobaciones atípicas o patrones que requieren ser reconstruidos y contrastados con evidencia. Por ello, la perspectiva forense permite analizar el proceso con mayor profundidad, identificando señales que pueden anticipar, explicar o evidenciar situaciones irregulares. La Association of Certified Fraud Examiners (ACFE, 2024) reconoce el fraude ocupacional como un fenómeno persistente y de alto impacto para las organizaciones, lo que justifica contar con enfoques capaces de revisar no solo el hecho consumado, sino también las condiciones que lo hacen posible.

Esta aproximación se diferencia de otros enfoques de auditoría, mientras la auditoría financiera se orienta principalmente a evaluar riesgos de incorrección material en los estados financieros, y la auditoría interna entrega aseguramiento y asesoría sobre gobierno, gestión de riesgos y control, la auditoría forense profundiza en la explicación de cómo pudo ocurrir una irregularidad y qué soportes

permiten sustentar sus hallazgos (International Auditing and Assurance Standards Board [IAASB], 2025; The Institute of Internal Auditors [IIA], 2024). Los estudios aplicados en auditoría forense muestran, además, que el análisis integrado de soportes, registros y secuencias operativas puede revelar desviaciones que una revisión convencional no capta con la misma profundidad (Castellanos Polo et al., 2022).

Asimismo, el aporte más relevante de la auditoría forense en este ámbito radica en su capacidad para reconstruir la trazabilidad documental y transaccional de las operaciones, examinando no solo la existencia de soportes, sino también la coherencia de su secuencia, la consistencia entre documentos y registros, y la integridad de la evidencia digital que los respalda. En el proceso de abastecimiento, ello supone revisar de manera articulada el flujo operativo. En este punto, la evidencia digital y documental deja de ser un simple respaldo operativo y pasa a convertirse en un insumo clave para reconstruir hechos y reconocer patrones de comportamiento anómalos. Esta aproximación permite identificar comportamientos que, observados de manera aislada, podrían parecer administrativos, pero que en conjunto revelan desviaciones relevantes.

4.6. Análisis de datos forenses y detección de anomalías

En el contexto actual de gestión de riesgos, control interno y cumplimiento, el análisis de datos forenses se ha consolidado como una capacidad técnica relevante para identificar desviaciones que no siempre son visibles mediante revisiones manuales o pruebas tradicionales. Esta necesidad es especialmente importante en procesos intensivos en transacciones y terceros, como el abastecimiento, donde el volumen de datos, la multiplicidad de actores y la secuencia documental aumentan la exposición a errores, irregularidades y eventos de fraude. En este escenario, la evidencia internacional también refuerza la relevancia del tema, la Association of Certified Fraud Examiners reportó en su edición 2024, basada en 1.921 casos reales investigados en 138 países y territorios, que más de la mitad de los fraudes ocupacionales analizados estuvo asociada a la ausencia o vulneración de controles internos, mientras que el 43% de los casos fue detectado a través de denuncias (ACFE, 2024). Estos antecedentes muestran que

la detección oportuna sigue siendo un desafío central para las organizaciones y que la analítica de datos puede transformarse en un soporte técnico concreto para fortalecer la trazabilidad, el monitoreo y la respuesta ante señales de riesgo.

4.6.1. Qué se entiende por análisis de datos forenses

El análisis de datos forenses puede definirse como el uso sistemático de técnicas analíticas para examinar grandes volúmenes de datos, con el propósito de identificar patrones, relaciones, excepciones y anomalías relevantes para la auditoría, la investigación y la gestión del riesgo. Nigrini (2020) explica que su valor radica en la posibilidad de aplicar pruebas estructuradas sobre poblaciones completas de datos y no solo sobre muestras limitadas, lo que permite detectar comportamientos atípicos que justifican una revisión posterior. En la misma línea, Vona (2017) sostiene que la analítica forense no debe entenderse únicamente como una herramienta para buscar fraude, sino como una forma de traducir escenarios de riesgo en pruebas concretas que permitan ubicar transacciones o registros que requieren validación adicional.

Esta precisión es importante porque una anomalía no equivale, por sí sola, a la existencia de fraude. Más bien, corresponde a una desviación respecto del comportamiento esperado del proceso o de su lógica de control. Por ello, el análisis de datos forenses cumple una función de detección y focalización.

4.6.2. Diferencia entre analítica descriptiva, diagnóstica y orientada a anomalías

No toda explotación de datos persigue el mismo objetivo. En la literatura sobre fraude y analítica se distinguen distintos niveles de análisis que conviene separar para evitar confusiones conceptuales. Baesens, Van Vlasselaer y Verbeke (2015) diferencian enfoques descriptivos, predictivos y relacionales, mientras que Rezaee y Wang (2019) subrayan que la analítica aplicada al ámbito forense debe responder a finalidades concretas de revisión, prevención y apoyo a la investigación.

Para efectos de esta tesis, resulta útil distinguir tres niveles. La analítica descriptiva muestra qué

ocurrió, resumiendo volúmenes, frecuencias, distribuciones o concentraciones dentro del proceso. La analítica diagnóstica busca explicar por qué ocurrió una determinada situación, relacionando variables, secuencias o condiciones que ayudan a comprender la desviación observada. Finalmente, la analítica orientada a anomalías se enfoca en localizar registros o comportamientos que se apartan del patrón esperado y que, precisamente por ello, deben ser examinados con mayor detalle. En ese sentido, Kuenkaikaew y Vasarhelyi (2013) señalan que el valor de la analítica aumenta cuando las transacciones pueden compararse con modelos o comportamientos esperados para detectar excepciones de forma temprana. Así, mientras la analítica descriptiva entrega contexto y la diagnóstica aporta explicación, la analítica orientada a anomalías cumple una función más directa de detección de red flags (Baesens et al., 2015; Kuenkaikaew & Vasarhelyi, 2013; Rezaee & Wang, 2019).

4.6.3. Detección de anomalías y principales pruebas analíticas

En los sistemas transaccionales, las anomalías suelen aparecer como desviaciones respecto de la lógica normal del proceso, de sus reglas de negocio o de sus controles esperados. Desde esta perspectiva, la detección no depende del azar ni de la simple revisión casual de documentos, sino de examinar grandes volúmenes de registros bajo criterios definidos de control. Nigrini (2020) destaca que la analítica forense adquiere valor cuando organiza pruebas sistemáticas capaces de identificar excepciones dentro de poblaciones completas. En términos similares, el IIA (2011) señala que el análisis de datos permite aplicar pruebas más extensas y eficientes, incluso mediante comparaciones simples.

4.6.4. Utilidad de la analítica en el monitoreo continuo

Otro aporte relevante del análisis de datos forenses es su capacidad para apoyar esquemas de monitoreo continuo. El IIA (2011) ya advertía que la analítica mejora la cobertura y eficiencia del aseguramiento al permitir revisar grandes volúmenes de transacciones y controles con mayor oportunidad. Esta lógica se profundiza cuando la revisión deja de ser exclusivamente retrospectiva y se aproxima a una observación más permanente del proceso. En esa línea, Kuenkaikaew y Vasarhelyi (2013) plantean que una auditoría con orientación predictiva puede comparar transacciones con modelos

normativos o esperados antes o muy cerca de su ejecución, lo que permite identificar excepciones con mayor anticipación.

De forma complementaria, GTAG 3 del Institute of Internal Auditors define la auditoría continua como una combinación de evaluaciones permanentes de riesgos y controles habilitadas por tecnología, y distingue este enfoque del monitoreo continuo, que corresponde a una función de gestión destinada a verificar si los controles internos operan efectivamente (The Institute of Internal Auditors, 2015). Bajo esta perspectiva, la utilidad de la analítica no radica en reemplazar el criterio del auditor o del área de compliance, sino en mejorar la oportunidad, cobertura y focalización del análisis. Sin embargo, su uso también exige cautela. Appelbaum, Kogan y Vasarhelyi (2017) advierten que el uso intensivo de analítica y big data en auditoría plantea desafíos asociados a la interpretación de la evidencia, la calidad de los datos y la pertinencia de los procedimientos aplicados. Por ello, las alertas generadas por la analítica deben entenderse como señales de revisión y no como prueba concluyente. En un proceso de abastecimiento, esta capacidad resulta especialmente valiosa porque permite detectar desviaciones de forma más temprana, disminuir la dependencia de revisiones ex post y fortalecer la respuesta frente a eventos que pueden afectar la integridad del proceso.

A partir de los elementos desarrollados en este capítulo, la Figura 01 sintetiza la lógica conceptual del modelo analítico-forense propuesto. En ella se observa cómo una necesidad operacional ingresa al ciclo de abastecimiento bajo un enfoque Procure-to-Pay, generando documentos, registros transaccionales y evidencia que permiten reconstruir el recorrido de la operación. Posteriormente, esa información puede ser consolidada, integrada y analizada mediante pruebas forenses orientadas a identificar patrones, desviaciones y señales de alerta. De este modo, el modelo no busca concluir por sí mismo la existencia de una irregularidad, sino transformar los datos del proceso en alertas trazables que permitan priorizar revisiones, distinguir situaciones justificadas y fortalecer el control interno, el compliance operacional y la gestión de terceros en el abastecimiento minero.

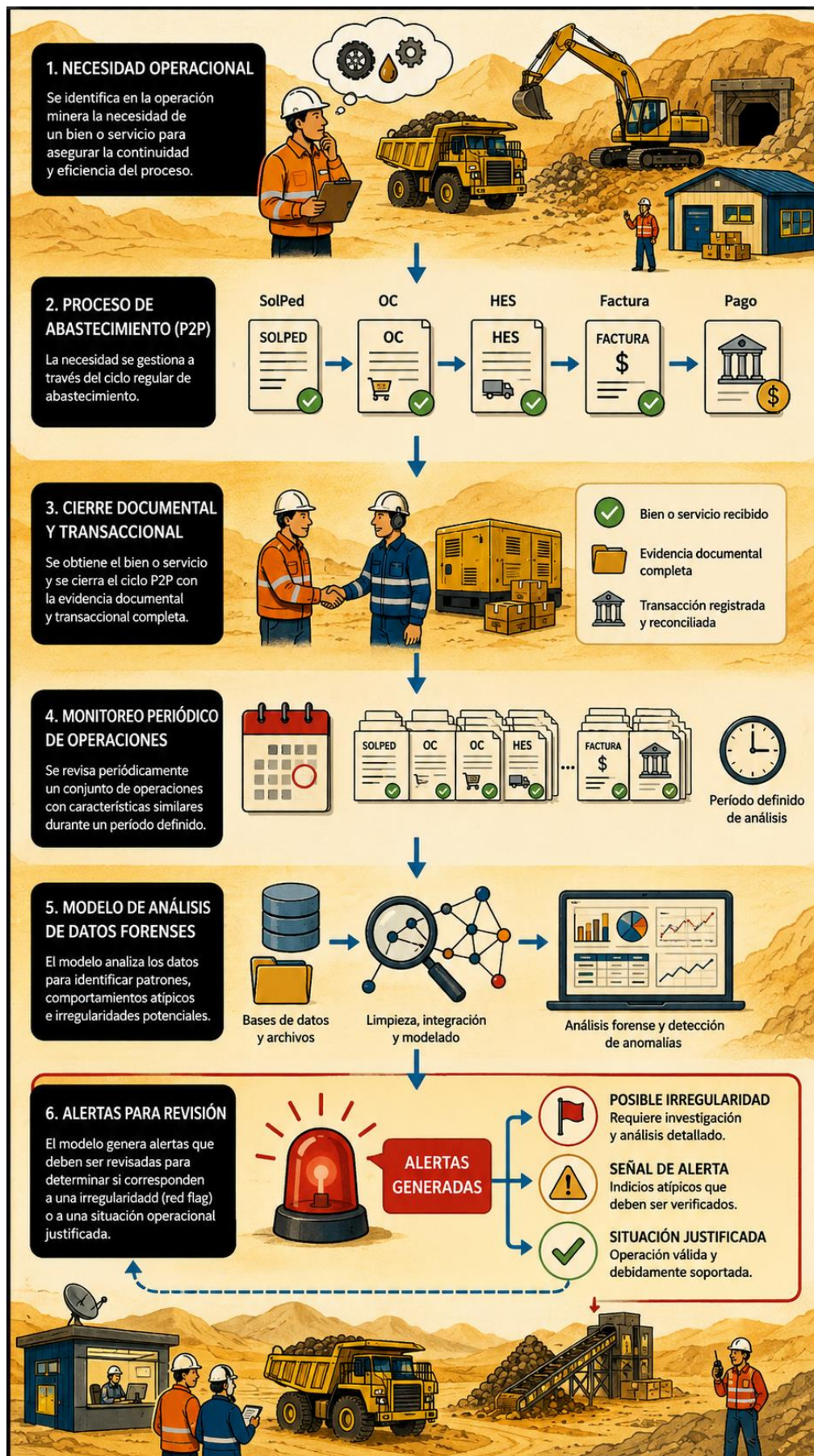


Figura 01: Modelo conceptual del flujo analítico-forense aplicado al proceso de abastecimiento P2P.

5. Metodología

La metodología de esta investigación se construye a partir de la necesidad de traducir el análisis conceptual del proceso de abastecimiento minero en un procedimiento aplicado de revisión, simulación e interpretación de datos. De esta manera, la metodología permite establecer el camino mediante el cual los riesgos y señales de alerta identificados en el proceso Procure-to-Pay serán transformados en procedimientos de análisis orientados a detectar anomalías y apoyar el fortalecimiento del control interno.

5.1. Diseño y enfoque de la investigación

La presente investigación tendrá un carácter aplicado y propositivo, ya que se orienta al diseño de una herramienta metodológica de análisis de datos forenses para identificar anomalías, señales de alerta y patrones atípicos en el proceso de abastecimiento de una operación minera chilena. El modelo se construirá sobre la lógica operacional del proceso Procure-to-Pay, la cual será utilizada como base para organizar las pruebas analíticas del modelo. De esta forma, cada prueba se vinculará con una etapa del proceso, con los documentos que la respaldan, con los usuarios que intervienen y con los controles que deberían operar para asegurar consistencia documental, trazabilidad transaccional y adecuada segregación de funciones.

El propósito del modelo no será determinar la existencia de fraude ni emitir conclusiones sobre responsabilidades específicas, sino identificar registros, relaciones o condiciones que se aparten del comportamiento esperado del proceso. En este sentido, las anomalías detectadas serán entendidas como señales de alerta que requieren análisis posterior y juicio profesional. Esta precisión es relevante porque el enfoque forense de datos no reemplaza la investigación ni la validación de antecedentes, sino que permite focalizar la atención en aquellos casos que presentan mayor riesgo, inconsistencia o debilidad de control.

El componente central del diseño será la elaboración de un catálogo de pruebas analíticas forenses. En el cual cada prueba será documentada según su objetivo, categoría, fuente de datos

requerida, variables utilizadas, regla de análisis, criterio de alerta y resultado esperado. Esta documentación permitirá que el modelo sea comprensible, trazable y replicable, evitando que las alertas se generen como resultados aislados sin explicación metodológica. Para efectos de esta investigación, las pruebas se organizarán en cinco categorías principales:

1. **Duplicidad:** Identificar registros repetidos, exactos o similares, asociados a facturas, pagos, órdenes de compra, proveedores, cuentas bancarias u otros campos críticos del proceso.
2. **Secuencia:** Verificar que las etapas del flujo sigan el orden esperado entre solicitud de pedido, orden de compra, recepción o HES, facturación y pago.
3. **Temporalidad:** Detectar registros creados, aprobados o procesados en condiciones inusuales.
4. **Consistencia:** Revisar la coherencia entre documentos, datos maestros y registros transaccionales, considerando proveedor, monto, moneda, centro de costo, cuenta bancaria, OC, HES, factura y pago.
5. **Relacional:** Identificar vínculos, concentraciones o coincidencias relevantes entre usuarios, proveedores, documentos, cuentas bancarias, datos maestros y roles del proceso.

Esta clasificación facilitará la interpretación de los resultados, ya que cada alerta podrá asociarse a una lógica específica de control.

5.2. Implementación del modelo mediante lenguaje Python

Una vez definido el diseño general del modelo y el catálogo de pruebas analíticas forenses, el siguiente paso metodológico consistirá en trasladar esta estructura a un procedimiento técnico ejecutable mediante lenguaje Python. Esta etapa permitirá que las pruebas diseñadas dejen de ser únicamente criterios metodológicos y puedan aplicarse sobre archivos estructurados, con el propósito de procesar información, reconstruir relaciones entre documentos, identificar desviaciones y generar resultados

trazables para su revisión posterior.

El modelo será desarrollado en Python debido a su capacidad para procesar bases de datos, recorrer carpetas de información, reconocer archivos disponibles, estandarizar campos, cruzar registros y aplicar reglas lógicas sobre grandes volúmenes de datos. El procedimiento considerará como entrada una carpeta que contendrá los archivos asociados al proceso de abastecimiento, tales como solicitudes de pedido, órdenes de compra, HES o registros de recepción, facturas, pagos, maestros de proveedores, usuarios y cuentas bancarias. A partir de estos insumos, el modelo deberá validar la estructura de la información, reconocer las variables necesarias para cada prueba, homologar formatos y construir las relaciones documentales que permitan seguir el recorrido de una operación dentro del flujo Procure-to-Pay.

La implementación se diseñará con una lógica interactiva, de modo que el usuario pueda seleccionar si desea ejecutar una prueba específica, una categoría completa de pruebas o la totalidad del catálogo analítico. Esta funcionalidad permitirá ajustar el alcance del análisis según la disponibilidad de información, el objetivo de revisión y el tipo de anomalía que se desee observar. De esta manera, el modelo no operará como una herramienta rígida, sino como una estructura flexible que podrá adaptarse a distintos escenarios de análisis dentro del proceso de abastecimiento.

Durante la ejecución, cada alerta generada deberá conservar trazabilidad hacia la información de origen. Esto significa que el resultado no solo indicará la existencia de una desviación, sino también el archivo del cual proviene, el registro asociado, la prueba aplicada, la categoría de análisis y las observaciones derivadas del cruce de información. Los resultados serán documentados en un archivo Excel consolidado, que funcionará como salida principal del modelo y permitirá revisar las alertas de manera ordenada. Además, esta salida incorpora métricas de desempeño de cada ejecución, tales como cantidad de registros procesados, número de pruebas aplicadas, alertas generadas por categoría, proporción de alertas sobre el total analizado y distribución de desviaciones según tipo de prueba o etapa del proceso.

5.3. Simulación del modelo mediante datos sintéticos generados con apoyo de inteligencia artificial

Una vez implementado el modelo en Python, se realizará una simulación utilizando una base de datos sintética y representativa del proceso de abastecimiento. Esta base será construida con apoyo de herramientas de inteligencia artificial⁸ y bajo criterios definidos por el investigador, tomando como referencia un prototipo realista de datos del proceso Procure-to-Pay observado a partir de la experiencia laboral del investigador en contextos organizacionales vinculados al abastecimiento. En este sentido, la base sintética simulará la estructura y lógica de extracción de información desde un sistema ERP tipo SAP, incorporando registros ficticios, pero organizados bajo una lógica coherente con las etapas habituales del proceso de abastecimiento.

La inteligencia artificial será utilizada como apoyo para crear proveedores, usuarios, fechas, montos, descripciones de bienes o servicios y relaciones entre documentos, sin embargo, la estructura de la base, las variables requeridas y las anomalías incorporadas serán definidas metodológicamente por la investigación. De esta forma, la base sintética no corresponderá a información real ni confidencial de una organización específica, sino a una representación controlada y anonimizada, construida sobre reglas de negocio, relaciones documentales y criterios de trazabilidad propios de un flujo de abastecimiento real.

La base sintética estará compuesta por archivos asociados a las principales etapas del proceso de abastecimiento, donde cada archivo deberá contener variables suficientes para permitir la trazabilidad entre documentos y la aplicación de las pruebas analíticas definidas en el catálogo del modelo.

La simulación considerará registros normales y registros con anomalías incorporadas de manera controlada, con el fin de observar si el modelo logra identificar duplicidades, alteraciones de secuencia, temporalidades inusuales, inconsistencias documentales o relaciones atípicas entre usuarios, proveedores y documentos. Las alertas generadas serán registradas como resultados observados de la base sintética,

⁸**Inteligencia artificial:** La inteligencia artificial se entiende como el conjunto de sistemas computacionales capaces de procesar datos, identificar patrones y ejecutar tareas que normalmente requieren intervención o razonamiento humano.

permitiendo revisar si cada desviación detectada conserva trazabilidad hacia el registro original y si entrega información útil para una revisión posterior.

Esta etapa no buscará demostrar la existencia de fraude ni medir efectividad estadística sobre datos reales, sino verificar preliminarmente la viabilidad del modelo, el orden de sus resultados y su capacidad para documentar alertas de manera trazable e interpretable dentro de un escenario controlado.

6. Resultados y discusión

Esta sección presenta la forma en que el análisis conceptual del proceso de abastecimiento se transforma en un modelo aplicado de revisión forense de datos. El desarrollo parte de la premisa de que las brechas de trazabilidad, las inconsistencias documentales y las señales de alerta del flujo Procure-to-Pay pueden ser traducidas en pruebas analíticas concretas, capaces de orientar una revisión más ordenada y focalizada. En este sentido, la sección comienza con la presentación del catálogo de pruebas diseñado para el modelo, continúa con la explicación de su implementación mediante un script dinámico en Python y posteriormente aborda su simulación sobre una base sintética representativa del proceso con el fin de evaluar la viabilidad del modelo. Finalmente, se incorporan las limitaciones de la investigación, con el propósito de precisar el alcance de los resultados y evitar que las alertas generadas sean interpretadas como evidencia concluyente de irregularidad.

6.1. Diseño del modelo de análisis de datos forenses

El modelo de análisis de datos forenses se diseñó sobre la base de un catálogo compuesto por cinco categorías de pruebas. Estas categorías corresponden a consistencia, duplicidad, secuencia, temporalidad y relaciones, cada una integrada por veinte pruebas aplicables al proceso de abastecimiento Procure-to-Pay. De esta forma, el modelo permite transformar las señales de alerta identificadas conceptualmente en reglas concretas de análisis.

A continuación, se desarrolla cada una de estas categorías, detallando la finalidad de las pruebas, los requerimientos técnicos para su aplicación y el tipo de alerta que cada una busca identificar dentro del flujo Procure-to-Pay.

6.1.1. Pruebas de consistencia

Las pruebas de consistencia tienen como finalidad revisar si los datos registrados en las distintas etapas del proceso de abastecimiento mantienen coherencia entre sí. Su foco está en comprobar que los campos críticos de una misma operación conserven correspondencia a medida que la transacción avanza en el flujo. Cuando estos datos no coinciden, se generan brechas que dificultan reconstruir

adecuadamente la operación y debilitan la trazabilidad documental y transaccional del proceso.

Estas brechas son relevantes porque una operación puede contar formalmente con documentos asociados, pero presentar diferencias internas que afectan su confiabilidad. Si estas inconsistencias no son identificadas y revisadas oportunamente, evidencian un quiebre de trazabilidad y control, al dificultar la conciliación entre documentos, registros contables y pagos asociados al proceso de abastecimiento. En casos más sensibles, la reiteración de estas inconsistencias puede evidenciar fallas de control o uso inadecuado de datos maestros, que faciliten eventuales irregularidades dentro del proceso.

Por esta razón, las pruebas de consistencia permiten focalizar la revisión en operaciones donde los documentos existen, pero sus datos no mantienen plena coherencia entre sí. Su utilidad radica en identificar casos que requieren validación documental, explicación operativa o análisis de control, sin que la alerta constituya por sí misma una conclusión de fraude o irregularidad. A continuación, se presentan veinte pruebas de consistencia consideradas en el catálogo:

- **CON-01. Consistencia entre SolPed y OC vinculada:** identifica órdenes de compra asociadas a una solicitud de pedido cuyos datos principales no coinciden con el requerimiento inicial, como descripción, material, grupo de artículos, cantidad o solicitante.
- **CON-02. Consistencia de centro de costo entre SolPed y OC:** detecta operaciones en que el centro de costo, centro gestor, elemento PEP o tipo de imputación de la orden de compra difiere de lo registrado en la solicitud de pedido.
- **CON-03. Consistencia entre proveedor sugerido o fijo y proveedor adjudicado:** identifica casos en que el proveedor sugerido, deseado o fijo en la solicitud de pedido no coincide con el proveedor finalmente registrado en la orden de compra.

- **CON-04. Consistencia de cantidad y unidad de medida entre SolPed y OC:** detecta diferencias entre la cantidad solicitada y la cantidad comprada, o cambios en la unidad de medida utilizada entre la solicitud de pedido y la orden de compra.
- **CON-05. Consistencia de valor estimado entre SolPed y OC:** identifica diferencias relevantes entre el valor estimado en la solicitud de pedido y el valor finalmente comprometido en la orden de compra.
- **CON-06. Consistencia entre OC y contrato marco:** identifica órdenes de compra asociadas a contratos marco cuyos datos no coinciden con las condiciones contractuales esperadas, como proveedor, servicio, material, precio, moneda o período de vigencia.
- **CON-07. Consistencia de material, servicio o grupo de artículos entre OC y HES:** detecta hojas de entrada de servicios cuyos datos de material, servicio, descripción o grupo de artículos no coinciden con lo establecido en la orden de compra.
- **CON-08. Consistencia de cantidad o valor entre OC y HES:** identifica casos en que la cantidad o el valor registrado en la HES no guarda correspondencia con lo autorizado en la orden de compra.
- **CON-09. Consistencia entre HES y factura:** detecta facturas cuyos datos principales no coinciden con la HES que debería respaldar la recepción o conformidad del servicio, considerando proveedor, monto, moneda, OC o referencia documental.
- **CON-10. Consistencia de proveedor entre OC, HES, factura y pago:** identifica operaciones en que el proveedor registrado cambia entre la orden de compra, la HES, la factura o el pago.

- **CON-11. Consistencia de moneda entre OC, factura y pago:** detecta operaciones en que la moneda registrada en la orden de compra, la factura o el pago no coincide, sin que exista una conversión o justificación clara.
- **CON-12. Consistencia entre monto facturado y monto pagado:** identifica facturas cuyo monto pagado no coincide con el importe registrado, considerando posibles descuentos, retenciones, notas de crédito o pagos parciales.
- **CON-13. Consistencia entre receptor de pago y proveedor facturado:** detecta casos en que el receptor del pago difiere del proveedor registrado en la factura o en la orden de compra.
- **CON-14. Consistencia de cuenta bancaria entre pago y maestro de proveedores:** identifica pagos realizados a cuentas bancarias que no coinciden con las cuentas registradas o vigentes del proveedor en el maestro de datos.
- **CON-15. Consistencia de condiciones y vía de pago:** detecta diferencias entre las condiciones de pago, vía de pago, vencimiento o forma de pago registradas en el maestro de proveedores, la orden de compra, la factura y el pago.
- **CON-16. Consistencia de sociedad, centro y organización de compras:** identifica operaciones en que la sociedad, centro, organización de compras, grupo de compras o centro de beneficio no mantiene coherencia entre las distintas etapas del proceso.
- **CON-17. Consistencia de imputación contable:** detecta diferencias entre la imputación definida en la compra y la clasificación contable registrada posteriormente en la factura o el pago, considerando centro de costo, elemento PEP, cuenta de mayor o cuenta contraparte.
- **CON-18. Consistencia entre estado documental y procesamiento posterior:**

identifica documentos bloqueados, anulados, incompletos, borrados o no liberados que igualmente presentan avances posteriores, como HES, factura o pago.

- **CON-19. Consistencia de datos fiscales del proveedor:** detecta diferencias entre la identificación fiscal, RUT, razón social o código de proveedor registrado en el maestro y los datos utilizados en la OC, factura o pago.
- **CON-20. Consistencia entre documento de compensación, factura y pago:** identifica facturas marcadas como compensadas o pagadas cuyo documento de compensación no coincide con el registro de pago, el proveedor, el monto o el estado contable esperado.

Una vez descrita la finalidad de cada prueba y su implicancia dentro del flujo Procure-to-Pay, la siguiente tabla presenta los elementos técnicos necesarios para su aplicación. Para ello, cada prueba se organiza según el código asignado, las fuentes de datos requeridas, las variables principales que permiten realizar el cruce, la regla de análisis que define la validación de consistencia y el resultado esperado que debería entregar el modelo.

Tabla 01: *Requerimientos técnicos de las pruebas de consistencia.*

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
CON-01	SolPed, OC	Solicitud de pedido, posición SolPed, documento de compra, posición OC, ID único, texto breve, material, grupo de artículos, cantidad solicitada, cantidad pedida, solicitante, autor, proveedor, monto.	Vincular la SolPed con la OC mediante pedido/posición o ID único y comparar si los datos principales del requerimiento se mantienen consistentes entre ambos documentos.	Listado de órdenes de compra cuyos datos principales no coinciden con la solicitud de pedido relacionada, indicando SolPed, OC, proveedor, solicitante, campos inconsistentes y monto asociado.
CON-02	SolPed, OC, maestro de centros de costo	Solicitud de pedido, documento de compra, centro, centro gestor, centro de costo, elemento PEP, tipo de imputación, solicitante, grupo de compras, monto.	Comparar la imputación organizacional registrada en la SolPed con la imputación informada en la OC, considerando centro de costo, centro gestor, centro, elemento PEP o tipo de imputación.	Operaciones en que la compra fue imputada a una unidad distinta de la registrada en el requerimiento inicial, con identificación de SolPed, OC, área afectada, monto y diferencia de imputación.
CON-03	SolPed, OC, maestro de proveedores	Proveedor deseado, proveedor fijo, proveedor sugerido, proveedor OC, nombre	Comparar el proveedor sugerido, deseado o fijo en la SolPed con el proveedor finalmente registrado en la	Casos en que el proveedor adjudicado difiere del proveedor previsto en la solicitud, permitiendo revisar

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
		de proveedor, código proveedor, RUT/ID fiscal, documento de compra, solicitud de pedido.	OC.	cambios de proveedor, autorización y respaldo documental.
CON-04	SolPed, OC	Solicitud de pedido, posición SolPed, documento de compra, posición OC, cantidad solicitada, cantidad pedida, unidad de medida, material, texto breve, grupo de artículos.	Comparar cantidad y unidad de medida entre la SolPed y la OC vinculada, validando si la compra mantiene el alcance del requerimiento inicial.	Operaciones con diferencias de cantidad o unidad de medida entre lo solicitado y lo comprado, indicando variación, material, proveedor y documento asociado.
CON-05	SolPed, OC	Precio de valoración, valor total SolPed, precio neto OC, valor neto de orden, moneda, cantidad, proveedor, solicitante, centro de costo.	Calcular la variación entre el valor estimado en la SolPed y el valor comprometido en la OC, considerando monto, moneda y cantidad.	Solicitudes que derivan en órdenes de compra con diferencias relevantes de valor, permitiendo revisar desviaciones presupuestarias o cambios de alcance.
CON-06	OC, contratos, acuerdos marco, maestro de proveedores	Documento de compra, contrato marco, posición contrato, proveedor, material, service code, texto breve, precio, moneda, fecha inicio vigencia, fecha fin vigencia.	Cruzar la OC con el contrato marco o acuerdo asociado y comparar proveedor, ítems, condiciones comerciales, moneda y período de vigencia.	Órdenes de compra asociadas a contratos cuyas condiciones no coinciden con la operación, identificando contrato, OC, proveedor y campo inconsistente.
CON-07	OC, HES	Documento de compra, posición, hoja de entrada, texto breve OC, denominación HES, material, service code, grupo de artículos, proveedor, centro.	Comparar material, servicio, descripción o grupo de artículos entre la OC y la HES relacionada.	HES asociadas a órdenes de compra con diferencias en servicio, material o clasificación, permitiendo revisar si la conformidad corresponde a lo contratado.
CON-08	OC, HES	Documento de compra, posición, hoja de entrada, cantidad de pedido, cantidad HES, valor neto de orden, valor bruto pedido, valor HES, moneda, proveedor.	Comparar la cantidad y el valor registrado en la HES contra la cantidad, valor y saldo autorizado en la OC.	Recepciones o conformidades con cantidades o valores que no guardan correspondencia con la OC, indicando diferencia, proveedor, HES y documento de compra.
CON-09	HES, Facturas, OC	Hoja de entrada, documento de compra, posición, número de factura, referencia, proveedor, monto HES, monto factura, moneda, fecha factura.	Vincular la factura con la HES y la OC asociada, comparando proveedor, monto, moneda y referencias documentales.	Facturas cuyos datos no coinciden con la HES que respalda la conformidad, permitiendo revisar diferencias antes de validar el pago.
CON-10	OC, HES, Facturas, Pagos, maestro de proveedores	Proveedor OC, proveedor HES, proveedor factura, receptor de pago, código proveedor, nombre, RUT/ID fiscal, documento de compra, factura, documento de compensación.	Comparar el proveedor y su identificación fiscal a lo largo de las etapas OC, HES, factura y pago.	Operaciones donde el proveedor cambia entre etapas del flujo, indicando documento afectado, proveedor original, proveedor posterior y monto relacionado.
CON-11	OC, Facturas, Pagos, tipos de cambio si	Moneda OC, moneda documento factura,	Comparar la moneda registrada en OC, factura	Operaciones con diferencias de moneda no trazables entre

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
	aplica	moneda local, moneda de pago, importe factura, importe pago, tipo de cambio, documento de compra, documento de compensación.	y pago, verificando si las diferencias cuentan con conversión o registro equivalente.	compra, facturación y pago, permitiendo revisar valoración, conversión y condiciones comerciales.
CON-12	Facturas, Pagos, notas de crédito, retenciones si aplica	Número de factura, referencia, proveedor, importe factura, importe pago, moneda, documento de compensación, retención, descuento, nota de crédito, estado de compensación.	Sumar los pagos asociados a una factura y compararlos con el monto exigible, considerando descuentos, retenciones, notas de crédito o pagos parciales.	Facturas con pagos superiores, inferiores o no conciliados con el importe registrado, indicando diferencia monetaria, proveedor y documento de compensación.
CON-13	Facturas, Pagos, maestro de proveedores, maestro de receptores de pago	Proveedor factura, receptor de pago, RUT/ID fiscal, nombre proveedor, cuenta bancaria, titular de cuenta, documento de compensación, importe pagado.	Comparar el receptor de pago con el proveedor registrado en la factura y validar si existe relación autorizada en maestro o documentación de respaldo.	Pagos dirigidos a receptores distintos del proveedor facturado, permitiendo revisar cesiones, mandatos, configuraciones especiales o excepciones documentadas.
CON-14	Pagos, maestro de proveedores, maestro de cuentas bancarias, logs de modificación	Proveedor, receptor de pago, cuenta bancaria, IBAN, SWIFT/BIC, clave de banco, titular de cuenta, fecha de modificación, usuario modificador, fecha de pago.	Normalizar los datos bancarios del pago y compararlos con las cuentas registradas o vigentes del proveedor en el maestro.	Pagos efectuados a cuentas bancarias no registradas, no vigentes o modificadas recientemente, con detalle de proveedor, cuenta, fecha de pago y usuario modificador.
CON-15	Maestro de proveedores, OC, Facturas, Pagos, workflow/liberaciones	Condiciones de pago, vía de pago, forma de pago, fecha de vencimiento, vencimiento neto, bloqueo de pago, fecha pago, proveedor, documento de compra, factura.	Comparar condiciones, vía y forma de pago entre maestro de proveedores, OC, factura y pago, verificando cambios o excepciones.	Operaciones con condiciones o vías de pago inconsistentes, indicando proveedor, documento, condición original, condición aplicada y fecha de pago.
CON-16	SolPed, OC, HES, Facturas, Pagos, maestro organizacional	Sociedad, centro, organización de compras, grupo de compras, centro de beneficio, división, centro de costo, documento de compra, factura, pago.	Comparar sociedad, centro, organización de compras y centro de beneficio a través de las etapas vinculadas del proceso.	Operaciones registradas con estructuras organizacionales inconsistentes, permitiendo revisar unidad responsable, imputación y trazabilidad del gasto.
CON-17	OC, Facturas, Pagos, maestro de cuentas, centros de costo	Tipo de imputación, centro de costo, elemento PEP, cuenta de mayor, cuenta contraparte, grupo de artículos, documento de compra, factura, pago.	Comparar la imputación definida en la OC con la clasificación contable registrada en la factura y el pago.	Casos con diferencias de cuenta, centro de costo, elemento PEP o tipo de imputación, permitiendo revisar clasificación contable y trazabilidad financiera.
CON-18	SolPed, OC, HES, Facturas, Pagos, workflow/liberaciones, logs de modificación	Estado de liberación, indicador de bloqueo, indicador de borrado, datos incompletos, factura final, bloqueo de pago, anulado con, fecha de estado, usuario	Identificar documentos con estado restrictivo y verificar si presentan etapas posteriores, como HES, factura o pago.	Operaciones que avanzaron pese a presentar documentos bloqueados, anulados, incompletos, borrados o no liberados, con detalle del estado y etapa posterior observada.

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
		modificador.		
CON-19	Maestro de proveedores, OC, Facturas, Pagos	Código proveedor, RUT/ID fiscal, razón social, nombre proveedor, receptor de pago, documento de compra, referencia factura, documento de compensación.	Comparar la identificación fiscal y razón social del proveedor en el maestro contra los datos utilizados en OC, factura y pago.	Transacciones con diferencias en RUT, razón social o código de proveedor, permitiendo revisar errores de identificación o inconsistencias del maestro de terceros.
CON-20	Facturas, Pagos, partidas abiertas/compensada	Número de factura, referencia, documento de compensación, fecha compensación, estado de partida, importe factura, importe pago, proveedor, ejercicio compensación.	Vincular factura y pago mediante documento de compensación, verificando coherencia entre estado contable, proveedor, monto y registro de pago.	Facturas marcadas como compensadas o pagadas con diferencias en documento de compensación, monto, proveedor o estado contable, permitiendo revisar el cierre financiero de la operación.

Una vez definidos los requerimientos técnicos para la aplicación de las pruebas de consistencia, las alertas generadas pueden ordenarse según su nivel de criticidad. Para efectos de este catálogo, las pruebas de consistencia pueden agruparse en tres niveles de criticidad:

- Criticidad alta: Corresponde a alertas que afectan campos sensibles vinculados con el proveedor, el receptor de pago, la cuenta bancaria, el monto pagado, el estado documental o el cierre financiero de la operación. En este nivel se consideran las pruebas CON-09, CON-10, CON-12, CON-13, CON-14, CON-15, CON-18 y CON-20.
- Criticidad media: Corresponde a alertas que afectan la coherencia operativa, contractual, presupuestaria o contable de la operación, pero que no necesariamente se ubican en la etapa inmediata del desembolso. En este nivel se consideran las pruebas CON-05, CON-06, CON-07, CON-08, CON-11, CON-16, CON-17 y CON-19.
- Criticidad baja: Corresponde a alertas ubicadas principalmente en el origen del requerimiento o en campos iniciales de la operación, donde la inconsistencia afecta la trazabilidad del proceso, pero no necesariamente implica por sí misma una obligación registrada o una salida inmediata de fondos. En este nivel se

consideran las pruebas CON-01, CON-02, CON-03 y CON-04.

Esta clasificación debe entenderse como una criticidad base⁹ y no como una calificación definitiva. De esta manera, la criticidad permite orientar la revisión de los resultados y priorizar aquellos casos que requieren mayor análisis documental, operativo o de control.

6.1.2. Pruebas de duplicidad

Las pruebas de duplicidad tienen como finalidad identificar situaciones en que un registro, documento u operación que debería ser único aparece más de una vez dentro del proceso de abastecimiento. Por ello, esta categoría se enfoca en revisar si los antecedentes del proceso permiten distinguir con claridad cuándo se trata de una operación real y distinta, y cuándo existe una posible repetición que debe ser revisada.

El riesgo asociado a este tipo de alertas surge cuando una misma operación puede ser tratada por el sistema como si correspondiera a más de una transacción válida. En ese escenario, la trazabilidad del proceso se debilita, porque deja de ser claro si el registro observado representa una nueva necesidad, una nueva obligación o un nuevo pago, o si corresponde a una repetición de algo ya registrado previamente. Esta falta de claridad puede generar efectos relevantes en el control del proceso, especialmente cuando la duplicidad no cuenta con una explicación documental suficiente.

Por esta razón, las pruebas de duplicidad permiten focalizar la revisión en operaciones donde la unicidad de los registros críticos no se observa con plena claridad. A continuación, se presentan veinte pruebas relacionadas con la categoría de duplicidad:

- **DUP-01. Factura duplicada exacta:** identifica facturas registradas más de una vez con coincidencia en sus datos principales, tales como proveedor, número de factura, tipo de documento, monto y moneda.

⁹**Criticidad base:** nivel inicial de prioridad asignado a una alerta según el tipo de quiebre detectado y la etapa del flujo Procure-to-Pay en que ocurre. Esta prioridad puede ajustarse según factores adicionales observados en la revisión, como monto, recurrencia, proveedor, respaldo documental, cercanía al pago, cambios en datos maestros o acumulación de alertas sobre una misma operación.

- **DUP-02. Factura duplicada por referencia normalizada:** detecta facturas que podrían corresponder al mismo documento, aunque hayan sido registradas con diferencias menores de formato en su referencia o número de factura.
- **DUP-03. Factura similar por proveedor, monto y fecha cercana:** identifica facturas del mismo proveedor que presentan montos iguales o muy similares y fechas próximas entre sí, aunque sus referencias documentales no sean idénticas.
- **DUP-04. Factura con referencia similar entre proveedores distintos:** identifica facturas de proveedores diferentes que presentan referencias, montos, fechas o descripciones similares.
- **DUP-05. Misma factura asociada a más de una orden de compra:** identifica facturas que aparecen vinculadas a dos o más órdenes de compra dentro del proceso.
- **DUP-06. Misma factura asociada a más de una HES:** detecta facturas que aparecen relacionadas con más de una hoja de entrada de servicios.
- **DUP-07. Pago duplicado exacto:** identifica pagos repetidos con coincidencia en proveedor, receptor de pago, monto, moneda, fecha y cuenta bancaria.
- **DUP-08. Misma factura pagada más de una vez:** detecta facturas que presentan más de un pago asociado o cuya suma pagada supera el monto originalmente registrado.
- **DUP-09. Pagos similares en una ventana temporal corta:** identifica pagos realizados al mismo proveedor, por montos iguales o cercanos y en fechas próximas.

- **DUP-10. Documento de compensación¹⁰ con facturas repetidas:** detecta documentos de compensación que contienen una misma referencia de factura más de una vez dentro del grupo de partidas liquidadas.
- **DUP-11. Orden de compra duplicada exacta o similar:** identifica órdenes de compra emitidas con características muy similares en proveedor, descripción, monto, cantidad o fecha.
- **DUP-12. Posiciones duplicadas dentro de una misma orden de compra:** detecta ítems repetidos dentro de una misma OC, considerando material, servicio, descripción, cantidad o precio.
- **DUP-13. Solicitud de pedido duplicada exacta o similar:** identifica solicitudes de pedido creadas con requerimientos, cantidades, valores o descripciones similares dentro de un período cercano.
- **DUP-14. Solicitudes de pedido similares que derivan en múltiples órdenes de compra:** detecta solicitudes parecidas que terminan generando más de una orden de compra.
- **DUP-15. HES duplicada exacta:** identifica hojas de entrada de servicios repetidas para una misma orden de compra, proveedor, período, descripción o monto.
- **DUP-16. HES similar por período, proveedor y monto:** detecta hojas de entrada de servicios que presentan similitudes relevantes en proveedor, período, descripción y valor.
- **DUP-17. Glosas de servicios similares facturadas por proveedores distintos:**

¹⁰**Documento de compensación:** documento contable que muestra que una factura o deuda pendiente fue cerrada, normalmente porque ya fue pagada o compensada en el sistema.

identifica facturas u órdenes de compra de distintos proveedores cuyas descripciones de servicio son altamente similares, especialmente cuando también presentan montos o fechas cercanas.

- **DUP-18. Proveedor duplicado por identificación fiscal¹¹:** detecta proveedores registrados con más de un código maestro utilizando una misma identificación fiscal.
- **DUP-19. Proveedor duplicado por razón social o nombre similar:** identifica proveedores con nombres o razones sociales altamente parecidas, aunque tengan códigos de proveedor distintos.
- **DUP-20. Cuenta bancaria o receptor de pago duplicado en proveedores distintos:** detecta proveedores diferentes que comparten una misma cuenta bancaria, titular o receptor de pago.

Una vez descrita la finalidad de cada prueba y su implicancia dentro del flujo Procure-to-Pay, la siguiente tabla presenta los elementos técnicos necesarios para su aplicación. Para ello, cada prueba se organiza según el código asignado, las fuentes de datos requeridas, las variables principales que permiten realizar el cruce, la regla de análisis que define la validación de consistencia y el resultado esperado que debería entregar el modelo.

Tabla 02: Requerimientos técnicos de las pruebas de duplicidad.

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
DUP-01	Facturas	Nº documento, referencia, Nº factura, tipo de documento, proveedor, nombre proveedor, Nº identificación fiscal, importe en moneda documento, moneda documento, sociedad, fecha de documento.	Agrupar las facturas por proveedor, identificación fiscal, referencia o número de factura, tipo de documento, monto, moneda y sociedad, identificando combinaciones repetidas.	Listado de facturas con coincidencia exacta en sus datos principales, indicando proveedor, documento SAP, referencia, monto, moneda y sociedad asociada.
DUP-02	Facturas	Referencia, Nº factura, referencia normalizada, proveedor, Nº	Normalizar la referencia o número de factura eliminando espacios,	Facturas que podrían corresponder al mismo documento aunque hayan sido

¹¹**Identificación fiscal:** número que identifica tributariamente a una persona o empresa. En Chile, corresponde normalmente al RUT.

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
		identificación fiscal, importe en moneda documento, moneda documento, sociedad, fecha de documento.	guiones, puntos, ceros iniciales y diferencias de formato, para luego comparar proveedor, monto, moneda y sociedad.	registradas con formatos distintos, permitiendo revisar posibles duplicidades no detectadas por coincidencia exacta.
DUP-03	Facturas	Proveedor, nombre proveedor, N° identificación fiscal, referencia, N° factura, importe en moneda documento, moneda documento, fecha de documento, fecha de emisión, fecha de recepción.	Comparar facturas del mismo proveedor con montos iguales o similares y fechas cercanas, aun cuando la referencia o número de factura sea distinto.	Casos de facturas similares por proveedor, monto y fecha, permitiendo revisar si corresponden a obligaciones distintas o a una posible repetición del registro.
DUP-04	Facturas, maestro de proveedores	Referencia, N° factura, tipo de documento, proveedor, nombre proveedor, N° identificación fiscal, descripción o texto disponible, importe, moneda, fecha de documento.	Normalizar referencias y comparar facturas de proveedores distintos que presenten folios, montos, fechas o descripciones similares.	Facturas registradas bajo proveedores diferentes con características documentales o económicas similares, permitiendo validar si corresponden a operaciones independientes o a una posible repetición.
DUP-05	Facturas, OC	Referencia, N° factura, proveedor, N° identificación fiscal, documento de compra, posición OC, importe factura, moneda, fecha de documento.	Agrupar facturas por proveedor, referencia normalizada, monto y moneda, y contar la cantidad de órdenes de compra distintas asociadas a la misma factura.	Facturas vinculadas a más de una orden de compra, indicando proveedor, referencia, monto, OC asociadas y documentos relacionados para revisión de trazabilidad.
DUP-06	Facturas, HES, OC	Referencia, N° factura, proveedor, N° identificación fiscal, hoja de entrada, documento de compra, posición, importe factura, moneda, fecha de documento.	Agrupar facturas por proveedor, referencia normalizada, monto y moneda, y contar la cantidad de HES distintas asociadas a la misma factura.	Facturas asociadas a más de una HES, permitiendo revisar si existe una prestación consolidada, una doble conformidad o una relación documental no suficientemente clara.
DUP-07	Pagos	N° documento, documento de compensación, proveedor, receptor de pago, N° identificación fiscal, importe en moneda de pago, moneda de pago, fecha de pago, fecha compensación, cuenta bancaria, IBAN, titular de cuenta.	Agrupar pagos por proveedor, receptor de pago, monto, moneda, fecha de pago y cuenta bancaria, identificando combinaciones repetidas.	Pagos con coincidencia exacta en sus datos principales, indicando proveedor, receptor, monto, fecha, cuenta bancaria y documento de compensación asociado.
DUP-08	Facturas, Pagos	N° documento factura, referencia, N° factura, proveedor, importe factura, moneda, documento de compensación, importe pagado, fecha de pago, estado de partida, anulado con, motivo de anulación.	Vincular facturas con pagos mediante referencia, proveedor, documento financiero o documento de compensación, y comparar el total pagado contra el monto de la factura.	Facturas con más de un pago asociado o con pagos acumulados superiores al importe registrado, excluyendo casos con reversa, anulación o ajuste documentado cuando corresponda.

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
DUP-09	Pagos	Proveedor, receptor de pago, N° identificación fiscal, importe en moneda de pago, moneda de pago, fecha de pago, fecha valor, documento de compensación, cuenta bancaria, IBAN, titular de cuenta.	Comparar pagos del mismo proveedor o receptor dentro de una ventana temporal definida, considerando montos iguales o cercanos y la misma cuenta bancaria.	Pagos similares realizados en fechas próximas, permitiendo revisar si corresponden a obligaciones distintas, pagos parciales justificados o posibles reprocesamientos.
DUP-10	Facturas, Pagos	Documento de compensación, ejercicio compensación, posición compensación, proveedor, referencia, N° factura, importe factura, moneda, fecha compensación, estado de partida.	Agrupar las partidas por documento de compensación y verificar si una misma referencia de factura aparece más de una vez dentro del mismo grupo de pago.	Documentos de compensación que contienen facturas repetidas, indicando proveedor, referencia, monto, posición de compensación y fecha de cierre contable.
DUP-11	OC	Documento de compra, posición, proveedor, nombre proveedor, texto breve, material, grupo de artículos, cantidad de pedido, precio neto, valor neto de orden, moneda, centro de costo, fecha creación.	Normalizar descripciones de compra y agrupar órdenes por proveedor, texto o material, cantidad, precio, monto, moneda, centro de costo y fechas cercanas.	Órdenes de compra iguales o altamente similares, permitiendo revisar posibles dobles compromisos comerciales asociados a una misma necesidad.
DUP-12	OC	Documento de compra, posición, material, N° material proveedor, texto breve, PO Item Text, service code, cantidad de pedido, unidad de medida, precio neto, valor neto de orden, tipo de posición.	Comparar posiciones dentro de una misma OC por material o servicio, descripción, cantidad, unidad de medida, precio y valor asociado.	Posiciones repetidas dentro de una misma orden de compra, indicando documento, posiciones afectadas, material o servicio, cantidad, precio y valor comprometido.
DUP-13	SolPed	Solicitud de pedido, posición SolPed, texto breve, material, categoría material, grupo de artículos, solicitante, autor, cantidad solicitada, precio de valoración, valor total, moneda, centro, fecha de solicitud.	Normalizar descripciones del requerimiento y agrupar solicitudes por solicitante, material o servicio, cantidad, valor, moneda, centro y fechas cercanas.	Solicitudes de pedido exactas o similares, permitiendo revisar si una misma necesidad fue ingresada más de una vez desde el origen del proceso.
DUP-14	SolPed, OC	Solicitud de pedido, posición SolPed, pedido, posición pedido, documento de compra, posición OC, solicitante, proveedor, texto breve, material, cantidad solicitada, cantidad comprada, valor total, valor OC, centro.	Identificar SolPed similares y verificar si derivaron en órdenes de compra distintas, comparando requerimiento, solicitante, proveedor, cantidad, valor y centro.	Solicitudes equivalentes que generaron múltiples órdenes de compra, permitiendo revisar posibles dobles compras originadas en la etapa de requerimiento.
DUP-15	HES	Hoja de entrada, documento de compra,	Agrupar HES por OC, posición, proveedor,	HES con coincidencia exacta en sus datos principales,

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
		posición, proveedor, nombre proveedor, texto breve, denominación, período, fecha documento, valor bruto pedido, valor neto de orden, moneda, autor, centro, sociedad.	período, descripción normalizada, monto y moneda, identificando combinaciones repetidas.	permitiendo revisar posibles dobles conformidades de servicio asociadas a una misma operación.
DUP-16	HES	Hoja de entrada, documento de compra, posición, proveedor, texto breve, denominación, período, fin, fecha de referencia, valor bruto pedido, valor neto de orden, moneda, autor.	Comparar HES del mismo proveedor con períodos coincidentes o superpuestos, descripciones similares y montos iguales o cercanos.	HES similares por proveedor, período y monto, permitiendo revisar si corresponden a prestaciones distintas o a una posible doble aceptación del servicio.
DUP-17	Facturas, OC, HES, maestro de proveedores	Proveedor, nombre proveedor, N° identificación fiscal, referencia factura, documento de compra, hoja de entrada, texto breve, descripción de servicio, grupo de artículos, monto, moneda, fecha documento.	Aplicar comparación aproximada de textos sobre glosas, descripciones o denominaciones de servicios entre proveedores distintos, considerando además montos y fechas cercanas.	Servicios con glosas altamente similares registrados bajo proveedores diferentes, permitiendo revisar si corresponden a prestaciones independientes o a una posible duplicidad de cobro.
DUP-18	Maestro de proveedores, Facturas, Pagos	Código proveedor, nombre proveedor, razón social, N° identificación fiscal, sociedad, estado proveedor, receptor de pago, documentos facturados, pagos asociados.	Normalizar la identificación fiscal y agrupar proveedores por RUT o ID fiscal, contando la cantidad de códigos maestros asociados al mismo identificador.	Proveedores con una misma identificación fiscal y más de un código maestro, permitiendo revisar duplicidades del maestro y operaciones asociadas a cada registro.
DUP-19	Maestro de proveedores, Facturas, Pagos	Código proveedor, nombre proveedor, razón social, nombre normalizado, N° identificación fiscal, receptor de pago, dirección, correo, teléfono, cuenta bancaria, sociedad.	Aplicar similitud textual sobre nombres o razones sociales y cruzar coincidencias con datos de contacto, identificación fiscal o información bancaria.	Proveedores con nombres altamente similares o datos relacionados, permitiendo revisar si corresponden al mismo tercero, a entidades vinculadas o a registros duplicados.
DUP-20	Maestro de proveedores, Pagos, Facturas, maestro de cuentas bancarias	Código proveedor, nombre proveedor, N° identificación fiscal, receptor de pago, cuenta bancaria, IBAN, SWIFT/BIC, código bancario, titular de cuenta, documento de compensación, fecha de pago, importe pagado.	Normalizar cuentas bancarias, IBAN, titulares y receptores de pago, y agrupar por estos campos para identificar proveedores distintos que comparten un mismo destino de pago.	Proveedores diferentes con cuenta bancaria, titular o receptor de pago coincidente, permitiendo revisar posibles relaciones no identificadas, errores de maestro o concentración de pagos en un mismo beneficiario.

Una vez definidos los requerimientos técnicos para la aplicación de las pruebas de duplicidad, las alertas generadas pueden ordenarse según su nivel de criticidad. Para efectos de este catálogo, las pruebas de duplicidad pueden agruparse en tres niveles de criticidad:

- Criticidad alta: corresponde a alertas que involucran pagos, documentos de compensación, cuentas bancarias, receptores de pago o registros maestros de proveedores, especialmente cuando la duplicidad se relaciona con una salida efectiva de fondos o con un destino de pago repetido. En este nivel se consideran las pruebas DUP-07, DUP-08, DUP-09, DUP-10, DUP-18 y DUP-20.
- Criticidad media-alta: corresponde a alertas que afectan documentos que pueden habilitar la generación, respaldo o procesamiento de una obligación dentro del flujo. En este nivel se consideran las pruebas DUP-01, DUP-02, DUP-03, DUP-04, DUP-05, DUP-06, DUP-11, DUP-15, DUP-16 y DUP-17.
- Criticidad media: corresponde a alertas ubicadas principalmente en el origen del requerimiento o en estructuras internas de compra que pueden afectar la trazabilidad, pero que no necesariamente implican una obligación financiera inmediata. En este nivel se consideran las pruebas DUP-12, DUP-13, DUP-14 y DUP-19.

Esta clasificación debe entenderse como una criticidad base y no como una calificación definitiva. De esta manera, la criticidad permite orientar la revisión de los resultados y priorizar aquellos casos que requieren mayor análisis documental, operativo o de control.

6.1.3. Pruebas de secuencia

Las pruebas de secuencia tienen como finalidad identificar quiebres en el orden lógico del proceso de abastecimiento dentro del flujo Procure-to-Pay. En este tipo de proceso, cada etapa debería avanzar de manera ordenada. Primero se registra una solicitud de pedido, luego se emite una orden de compra, posteriormente se acredita la recepción del bien o la conformidad del servicio mediante una HES, después se registra la factura y finalmente se ejecuta el pago. Por ello, esta categoría permite revisar si el recorrido de una operación mantiene una relación ordenada y verificable entre sus documentos.

Cuando el orden lógico del flujo se interrumpe, puede generar que el proceso avance sobre antecedentes incompletos, aprobaciones tardías o registros incorporados después de que la operación ya ocurrió, provocando que la organización quede más expuesta a validar compras, servicios, facturas o pagos sin contar con una secuencia documental clara, lo que dificulta revisar la legitimidad del proceso, y confirmar que cada etapa fue respaldada antes de continuar con la siguiente.

Por esta razón, las pruebas de secuencia permiten focalizar la revisión en operaciones donde el flujo aparece alterado y donde resulta necesario verificar el respaldo documental y la justificación de eventuales excepciones. A continuación, se describen veinte pruebas de secuencia consideradas en el catálogo:

- **SEC-01. Orden de compra creada antes de la solicitud de pedido:** identifica operaciones en que la orden de compra fue creada antes de existir la solicitud de pedido que debía originar el requerimiento.
- **SEC-02. Orden de compra creada antes de la liberación de la solicitud de pedido:** identifica casos en que la orden de compra fue emitida cuando la solicitud de pedido aún no se encontraba aprobada o liberada.
- **SEC-03. Recepción o HES registrada antes de la liberación de la orden de compra:** identifica operaciones en que la recepción del bien o la conformidad del servicio fue registrada antes de que la orden de compra estuviera aprobada.
- **SEC-04. Recepción o HES registrada antes de la creación de la orden de compra:** identifica casos en que la recepción o HES fue registrada antes de que existiera la orden de compra relacionada.
- **SEC-05. Recepción o HES registrada con orden de compra no habilitada:** identifica recepciones o HES asociadas a órdenes de compra que, al momento del registro, se encontraban bloqueadas, incompletas, eliminadas o con un estado

no válido.

- **SEC-06. Prestación del servicio iniciada antes de la vigencia del contrato:** identifica servicios cuyo período de ejecución comenzó antes de que existiera una vigencia contractual o comercial aplicable.
- **SEC-07. HES aceptada antes del término del período de servicio:** identifica HES aprobadas o aceptadas antes de que finalizara el período de prestación informado.
- **SEC-08. Factura emitida antes de la creación de la orden de compra:** identifica facturas cuya fecha de emisión es anterior a la fecha de creación de la orden de compra relacionada.
- **SEC-09. Factura registrada antes de la recepción o HES:** identifica facturas contabilizadas antes de que exista una recepción del bien o una HES asociada.
- **SEC-10. Factura registrada antes de la aceptación o liberación de la HES:** identifica facturas ingresadas antes de que la HES estuviera aceptada o liberada.
- **SEC-11. Factura contabilizada antes de su fecha de emisión:** identifica facturas cuya fecha de contabilización es anterior a la fecha de emisión del documento.
- **SEC-12. Factura contabilizada antes de su recepción formal:** identifica facturas registradas contablemente antes de la fecha en que fueron recibidas por la compañía o ingresadas al canal definido.
- **SEC-13. Factura registrada contra OC o HES anulada, bloqueada o eliminada previamente:** identifica facturas asociadas a órdenes de compra o HES que ya presentaban una condición no válida antes del registro de la factura.

- **SEC-14. Referencia OC/HES incorporada o modificada después del registro de la factura:** identifica facturas cuya referencia a orden de compra, posición o HES fue agregada o modificada después de su contabilización inicial.
- **SEC-15. Pago ejecutado antes del registro contable de la factura:** identifica pagos cuya fecha de pago o compensación es anterior al registro contable de la factura asociada.
- **SEC-16. Pago ejecutado antes del desbloqueo o aprobación de la factura:** identifica pagos realizados cuando la factura aún mantenía bloqueo de pago o no contaba con aprobación registrada.
- **SEC-17. Pago ejecutado antes del vencimiento neto sin autorización trazable:** identifica pagos realizados antes de la fecha de vencimiento definida por las condiciones de pago, sin evidencia de autorización o excepción.
- **SEC-18. Documento de compensación anterior a las facturas compensadas:** identifica documentos de compensación cuya fecha es anterior a la emisión, registro o contabilización de las facturas vinculadas.
- **SEC-19. Anulación o reversa posterior al pago sin regularización financiera:** identifica documentos anulados o reversados después del pago, sin una nota de crédito, reversa de pago, compensación inversa o ajuste financiero asociado.
- **SEC-20. Modificación de datos maestros sensibles entre factura y pago:** identifica cambios en datos maestros del proveedor, receptor de pago o cuenta bancaria realizados después del registro de la factura y antes del pago.

Una vez descrita la finalidad de cada prueba y su implicancia dentro del flujo Procure-to-Pay, la siguiente tabla presenta los elementos técnicos necesarios para su aplicación. Para ello, cada prueba se organiza según el código asignado, las fuentes de datos requeridas, las variables principales que permiten

realizar el cruce, la regla de análisis que define la validación y el resultado esperado que debería entregar el modelo.

Tabla 03: *Requerimientos técnicos de las pruebas de secuencia.*

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
SEC-01	SolPed, OC	Solicitud de pedido, posición SolPed, documento de compra, posición OC, fecha de solicitud, fecha de creación OC, solicitante, autor, proveedor, monto, centro de costo.	Vincular la SolPed con la OC mediante pedido/posición o ID único y comparar si la fecha de creación de la OC es anterior a la fecha de solicitud.	Listado de órdenes de compra creadas antes de la SolPed, indicando diferencia de días, proveedor, solicitante, usuario creador, monto y centro de costo.
SEC-02	SolPed, OC, workflow ¹² /liberaciones	Solicitud de pedido, estado de liberación, fecha de liberación SolPed, fecha final de liberación, documento de compra, fecha de creación OC, grupo y estrategia de liberación.	Comparar la fecha de creación de la OC con la fecha de liberación final de la SolPed, verificando si la OC fue creada antes de que el requerimiento estuviera aprobado.	Casos en que la compra avanzó antes de la aprobación formal del requerimiento interno, con identificación de SolPed, OC, usuario responsable y fecha de liberación pendiente o posterior.
SEC-03	OC, HES/recepción, workflow/liberaciones OC	Documento de compra, posición, estado de liberación OC, indicador de liberación, fecha de liberación OC, hoja de entrada, fecha de creación HES, fecha documento HES, proveedor.	Comparar la fecha de registro de la HES o recepción con la fecha de liberación de la OC, identificando recepciones registradas antes de la aprobación formal de la compra.	Operaciones donde se registró recepción o conformidad antes de completar la liberación de la OC, con detalle de proveedor, documento, usuario y diferencia temporal.
SEC-04	OC, HES/recepción	Documento de compra, posición, hoja de entrada, fecha de creación OC, fecha documento OC, fecha creación HES, fecha documento HES, proveedor, centro.	Vincular la HES o recepción con la OC y verificar si la fecha de la HES es anterior a la fecha de creación de la orden de compra.	HES o recepciones registradas antes de existir la OC relacionada, permitiendo identificar posibles formalizaciones posteriores del respaldo comercial.
SEC-05	OC, HES/recepción, logs de modificación	Documento de compra, posición, indicador de borrado, indicador de bloqueo, datos incompletos, estado OC, fecha de bloqueo, fecha de desbloqueo, fecha HES, usuario modificador.	Evaluar el estado de la OC vigente al momento de registrar la HES o recepción, identificando si existían bloqueos, datos incompletos, eliminación o condiciones no habilitantes.	Operaciones donde la recepción o conformidad fue registrada sobre una OC que no estaba plenamente habilitada para respaldar el flujo.
SEC-06	OC, HES, contratos, acuerdos marco	Documento de compra, contrato marco, posición contrato, fecha creación OC, fecha liberación OC, inicio de vigencia contractual, fin de vigencia contractual, período del servicio, fecha inicio HES.	Comparar la fecha de inicio del servicio con la fecha de creación/liberación de la OC y con el inicio de vigencia del contrato o acuerdo marco.	Servicios cuyo período de ejecución comienza antes de la formalización comercial o contractual, con identificación de contrato, OC, proveedor y período observado.
SEC-07	HES, workflow/aprobación	Hoja de entrada, período del servicio,	Comparar la fecha de aceptación o liberación de	HES aceptadas antes de la finalización del servicio

¹²**Workflow:** flujo de trabajo configurado en un sistema ERP para ordenar, automatizar y registrar pasos de revisión o aprobación dentro de un proceso.

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
	es HES	fecha inicio, fecha fin, fecha de aceptación HES, fecha de liberación HES, estado HES, usuario aprobador, proveedor.	la HES con la fecha de término del período de servicio declarado.	informado, permitiendo revisar conformidades otorgadas de forma anticipada.
SEC-08	OC, Facturas	Documento de compra, posición, proveedor, número de factura, referencia, fecha de emisión factura, fecha documento factura, fecha creación OC.	Relacionar la factura con la OC y verificar si la fecha de emisión o documento de factura es anterior a la fecha de creación de la orden de compra.	Facturas emitidas antes de la existencia de la OC relacionada, con detalle de proveedor, factura, OC y diferencia de días.
SEC-09	Facturas, OC, HES/recepción	Número de documento factura, documento de compra, hoja de entrada, fecha contabilización factura, fecha registro factura, fecha HES, fecha recepción, proveedor, importe.	Comparar la fecha de registro o contabilización de la factura con la fecha de HES o recepción asociada.	Facturas registradas antes de contar con recepción o conformidad previa, identificando el documento afectado, proveedor, importe y fecha de respaldo posterior.
SEC-10	Facturas, HES, workflow/aprobaciones HES	Número de documento factura, hoja de entrada, fecha contabilización factura, estado HES, fecha aceptación HES, fecha liberación HES, usuario aprobador.	Comparar la fecha de contabilización de la factura con la fecha de aceptación o liberación de la HES.	Facturas procesadas antes de completar la validación formal del servicio, con identificación de factura, HES, aprobador y fechas relevantes.
SEC-11	Facturas	Número de documento, número de factura, referencia, fecha de emisión, fecha documento, fecha contabilización, proveedor, usuario registrador.	Comparar la fecha de contabilización con la fecha de emisión o fecha documento de la factura.	Facturas con registro contable anterior a su emisión documental, permitiendo revisar inconsistencias de captura o integridad temporal.
SEC-12	Facturas, mesa de entrada/AP, DTE o registro documental	Número de documento, fecha de recepción, fecha de entrada, fecha de registro, fecha contabilización, canal de recepción, usuario registrador, proveedor.	Comparar la fecha de contabilización de la factura con la fecha de recepción formal o ingreso al canal definido.	Facturas contabilizadas antes de su recepción formal por la compañía, con detalle del canal, usuario, proveedor y diferencia temporal.
SEC-13	Facturas, OC, HES, logs de modificación	Número de factura, documento de compra, hoja de entrada, indicador de borrado OC/HES, bloqueo OC/HES, anulación, fecha de estado no válido, fecha contabilización factura.	Determinar si la OC o HES asociada a la factura presentaba anulación, bloqueo, eliminación o estado no válido antes o al momento de contabilizar la factura.	Facturas registradas sobre documentos de respaldo que no se encontraban válidos o habilitados, permitiendo revisar la continuidad del flujo.
SEC-14	Facturas, OC, HES, logs de modificación	Número de documento factura, documento de compra, posición, hoja de entrada, campo modificado, valor anterior, valor nuevo, fecha modificación, usuario modificador, fecha contabilización.	Revisar si las referencias a OC, posición u HES fueron agregadas o modificadas después de la contabilización inicial de la factura.	Facturas cuya trazabilidad documental fue ajustada posteriormente, con identificación del campo modificado, usuario, fecha del cambio y referencia incorporada.

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
SEC-15	Facturas, Pagos	Número de documento factura, documento de compensación, fecha contabilización factura, fecha registro factura, fecha pago, fecha compensación, proveedor, importe.	Relacionar factura y pago mediante documento de compensación y verificar si la fecha de pago o compensación es anterior al registro contable de la factura.	Pagos asociados a facturas registradas después del desembolso, con detalle de proveedor, importe, documento de compensación y diferencia temporal.
SEC-16	Facturas, Pagos, workflow/aprobaciones, bloqueos de pago	Número de factura, bloqueo de pago, fecha bloqueo, fecha desbloqueo, fecha aprobación, fecha pago, documento de compensación, usuario aprobador.	Comparar la fecha de pago con la fecha de aprobación, liberación o desbloqueo de la factura, verificando si existía bloqueo vigente al momento del desembolso.	Facturas pagadas antes de completar la validación o liberación de pago, indicando estado del bloqueo, aprobador, fecha de pago y documento compensado.
SEC-17	Facturas, Pagos, maestro proveedor, workflow de excepciones	Condiciones de pago, fecha vencimiento neto, fecha pago, vía de pago, proveedor, autorización de anticipo, usuario aprobador, motivo de excepción.	Comparar la fecha de pago con el vencimiento neto y verificar si existe autorización o motivo registrado para el pago anticipado.	Pagos realizados antes del vencimiento sin autorización trazable, permitiendo revisar excepciones, prioridad de pago y respaldo de aprobación.
SEC-18	Facturas, Pagos, partidas abiertas/compensadas	Documento de compensación, fecha compensación, número de documento factura, fecha emisión factura, fecha contabilización factura, ejercicio compensación, posición compensación.	Agrupar facturas por documento de compensación y comparar la fecha de compensación con las fechas de emisión, registro o contabilización de las facturas vinculadas.	Documentos de compensación con secuencia financiera inconsistente, identificando facturas compensadas, proveedor, importe y fecha de cierre.
SEC-19	Facturas, Pagos, notas de crédito, documentos de anulación, reversas	Número de factura, anulado con, ID de anulación, motivo de reversa, fecha anulación, fecha pago, documento de compensación, nota de crédito, reversa de pago.	Identificar facturas anuladas o reversadas después del pago y verificar si existe nota de crédito, reversa, compensación inversa o ajuste financiero posterior.	Operaciones pagadas y luego corregidas documentalmente sin regularización financiera trazable, con detalle de factura, pago, anulación y ajuste faltante.
SEC-20	Maestro de proveedores, maestro de cuentas bancarias, Facturas, Pagos, logs de modificación	Proveedor, receptor de pago, cuenta bancaria, IBAN, SWIFT/BIC, titular de cuenta, fecha modificación, usuario modificador, fecha factura, fecha pago.	Comparar la fecha de modificación de datos maestros sensibles con el intervalo entre el registro de la factura y la ejecución del pago.	Pagos precedidos por cambios sensibles en proveedor, receptor de pago o cuenta bancaria, requiriendo validación documental y aprobación independiente.

Una vez definidos los requerimientos técnicos para la aplicación de las pruebas de secuencia, las alertas generadas pueden ordenarse según su nivel de criticidad. Para efectos de este catálogo, las pruebas de secuencia pueden agruparse en tres niveles de criticidad:

- Criticidad alta: corresponde a alertas que se ubican en etapas cercanas al desembolso, al cierre financiero o a modificaciones sensibles del proveedor. En

este nivel se consideran las pruebas SEC-15, SEC-16, SEC-18, SEC-19 y SEC-20.

- Criticidad media-alta: corresponde a alertas que afectan documentos que habilitan la recepción, conformidad, facturación o reconocimiento de la obligación. En este nivel se consideran las pruebas SEC-03, SEC-04, SEC-05, SEC-06, SEC-07, SEC-08, SEC-09, SEC-10, SEC-13, SEC-14 y SEC-17.
- Criticidad media: corresponde a alertas ubicadas principalmente en el origen del requerimiento o en inconsistencias documentales internas que afectan la trazabilidad, pero que no necesariamente implican un desembolso inmediato. En este nivel se consideran las pruebas SEC-01, SEC-02, SEC-11 y SEC-12.

Esta clasificación debe entenderse como una criticidad base y no como una calificación definitiva. En la aplicación del modelo, el nivel de prioridad podría aumentar o disminuir según distintos aspectos del caso analizado. De esta manera, la criticidad permite orientar la revisión de los resultados.

6.1.4. Pruebas de relación

Las pruebas relacionales tienen como finalidad identificar vínculos, concentraciones y patrones recurrentes entre los usuarios, proveedores, documentos y roles que participan en el proceso de abastecimiento. En esta categoría, el análisis no se centra únicamente en revisar un documento o una etapa aislada, sino en observar las relaciones operativas y transaccionales que se forman entre los actores del flujo Procure-to-Pay. Por ello, estas pruebas permiten evaluar si las operaciones mantienen una separación razonable entre quienes solicitan, aprueban, compran, reciben, registran facturas y gestionan pagos.

Cuando estas relaciones no son advertidas oportunamente, el proceso puede perder independencia y quedar expuesto a brechas de control difíciles de detectar mediante una revisión documental tradicional. La recurrencia o concentración de relaciones entre actores, roles y proveedores

puede responder a condiciones operativas válidas, pero también puede reflejar falta de segregación de funciones, dependencia excesiva, baja rotación de controles o posibles conflictos de interés. En estos casos, el riesgo no está necesariamente en la existencia de la relación, sino en que esta opere sin revisión independiente o justificación suficiente.

Por esta razón, las pruebas relacionales permiten focalizar la revisión en aquellas operaciones donde los vínculos presenten una recurrencia o concentración que requiere análisis posterior. A continuación, se presentan veinte pruebas relacionales consideradas en el catálogo:

- **REL-01. Solicitante y aprobador de SolPed coincidentes:** identifica operaciones en que el usuario que crea o solicita la SolPed también participa en su aprobación o liberación.
- **REL-02. Solicitante y creador de orden de compra coincidentes:** identifica casos en que el usuario que origina el requerimiento también crea o gestiona la orden de compra asociada.
- **REL-03. Creador y aprobador de orden de compra coincidentes:** identifica órdenes de compra en que el usuario creador también participa como aprobador, liberador o responsable de autorización.
- **REL-04. Solicitante y aprobador de orden de compra coincidentes:** identifica operaciones en que el usuario que solicitó el requerimiento también interviene en la aprobación de la orden de compra.
- **REL-05. Creador de OC y autor de HES coincidentes:** identifica operaciones en que el usuario que crea la orden de compra también registra la HES o recepción del servicio.
- **REL-06. Autor y aprobador de HES coincidentes:** identifica hojas de entrada de servicio en que el usuario que registra la HES también participa en su

aceptación, aprobación o liberación.

- **REL-07. Solicitante y autor de HES coincidentes:** identifica casos en que el usuario que origina la necesidad también registra posteriormente la conformidad del servicio.
- **REL-08. Solicitante y aprobador de HES coincidentes:** identifica operaciones en que el solicitante original participa también como aprobador o aceptador de la HES.
- **REL-09. Aprobador de OC y aprobador de HES coincidentes:** identifica casos en que un mismo usuario aprueba tanto la orden de compra como la HES relacionada.
- **REL-10. Autor de HES y usuario de registro de factura coincidentes:** identifica operaciones en que el usuario que registra o valida la HES también interviene en el registro o tratamiento de la factura.
- **REL-11. Usuario de registro de factura y usuario de pago coincidentes:** identifica casos en que un mismo usuario registra o trata la factura y además participa en la compensación, liberación o gestión del pago.
- **REL-12. Usuario que modifica maestro de proveedor y participa en la operación P2P:** identifica casos en que un usuario modifica datos maestros de un proveedor y luego interviene en documentos asociados al mismo tercero, como SolPed, OC, HES, factura o pago.
- **REL-13. Concentración de HES creadas por usuario y proveedor:** identifica usuarios que crean o registran una proporción relevante de HES para un mismo proveedor.

- **REL-14. Concentración de HES aprobadas por usuario y proveedor:** identifica aprobadores que validan recurrentemente HES de un mismo proveedor.
- **REL-15. Dupla recurrente entre creador de HES y aprobador de HES:** identifica pares de usuarios que se repiten con alta frecuencia como creador y aprobador de HES para un mismo proveedor, contrato o centro de costo.
- **REL-16. Dupla recurrente entre solicitante y aprobador:** identifica pares de usuarios que se repiten de forma relevante entre quien solicita y quien aprueba requerimientos u órdenes de compra.
- **REL-17. Dupla recurrente entre solicitante y comprador:** identifica solicitantes y compradores que participan repetidamente en operaciones asociadas a un mismo proveedor, categoría o centro de costo.
- **REL-18. Tríada recurrente solicitante-comprador-aprobador:** identifica combinaciones repetitivas entre solicitante, comprador y aprobador asociadas a un mismo proveedor, contrato o grupo de artículos.
- **REL-19. Correlatividad de facturas emitidas por proveedor:** identifica facturas de un mismo proveedor cuyo número o folio presenta una secuencia muy continua, con pocos saltos entre documentos emitidos hacia la compañía.
- **REL-20. Dependencia financiera proveedor-cliente según secuencia de facturación:** identifica proveedores cuyas facturas emitidas a la compañía presentan alta continuidad numérica, frecuencia sostenida o baja dispersión de folios durante el período analizado.

Una vez descrita la finalidad de cada prueba y su implicancia dentro del flujo Procure-to-Pay, la siguiente tabla presenta los elementos técnicos necesarios para su aplicación. Para ello, cada prueba se organiza según el código asignado, las fuentes de datos requeridas, las variables principales que permiten

realizar el cruce, la regla de análisis que define la validación y el resultado esperado que debería entregar el modelo.

Tabla 04: *Requerimientos técnicos de las pruebas de relaciones.*

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
REL-01	SolPed, workflow/liberaciones, maestro de usuarios	Solicitud de pedido, autor, solicitante, usuario aprobador, estrategia de liberación, estado de liberación, fecha de solicitud, fecha de liberación.	Comparar el usuario creador o solicitante de la SolPed con el usuario que participa en su aprobación o liberación.	SolPed en que el solicitante y aprobador coinciden, permitiendo revisar posibles brechas de segregación entre creación y validación del requerimiento.
REL-02	SolPed, OC, maestro de usuarios	Solicitud de pedido, documento de compra, autor SolPed, solicitante, PO Creator, PO Creator Name, fecha de creación OC, proveedor, monto.	Vincular la SolPed con la OC asociada y comparar si el solicitante del requerimiento coincide con el creador de la orden de compra.	Operaciones donde la necesidad y la formalización comercial recaen en el mismo usuario, indicando concentración de funciones en el inicio del flujo P2P.
REL-03	OC, workflow/liberaciones OC, maestro de usuarios	Documento de compra, PO Creator, aprobador/liberador OC, estrategia de liberación, indicador de liberación, estado de liberación, valor neto, proveedor.	Comparar el usuario creador de la OC con el usuario que aprueba, libera o autoriza la misma orden de compra.	Órdenes de compra creadas y aprobadas por el mismo usuario, o con recurrencia del mismo patrón, para revisión de independencia en la autorización.
REL-04	SolPed, OC, workflow/liberaciones OC, maestro de usuarios	Solicitante, autor SolPed, documento de compra, aprobador OC, liberador OC, proveedor, centro de costo, grupo de compras, monto.	Vincular SolPed con OC y comparar el solicitante original con el aprobador o liberador de la orden de compra relacionada.	Operaciones donde quien originó la necesidad también interviene en la aprobación de la compra formal, permitiendo revisar independencia del control.
REL-05	OC, HES, maestro de usuarios	Documento de compra, posición, PO Creator, autor HES, hoja de entrada, proveedor, valor HES, fecha HES, centro.	Relacionar la OC con la HES y comparar el usuario creador de la orden de compra con el usuario autor de la hoja de entrada.	HES asociadas a OC creadas por el mismo usuario que registra la conformidad, permitiendo revisar concentración entre compra y recepción.
REL-06	HES, workflow/aprobaciones HES, maestro de usuarios	Hoja de entrada, autor HES, aprobador HES, indicador de aceptación, fecha creación HES, fecha aprobación HES, proveedor, monto.	Comparar el usuario que crea o registra la HES con el usuario que la aprueba, acepta o libera dentro del flujo de conformidad.	HES creadas y aprobadas por el mismo usuario, permitiendo revisar posibles debilidades en la segunda validación del servicio.
REL-07	SolPed, OC, HES, maestro de usuarios	Solicitante, autor SolPed, documento de compra, hoja de entrada, autor HES, proveedor, centro de costo, valor HES.	Vincular SolPed, OC y HES, y comparar el solicitante original con el usuario que registra la conformidad del servicio.	Operaciones donde quien solicita el bien o servicio también registra su recepción o conformidad, permitiendo revisar objetividad de la validación operacional.
REL-08	SolPed, OC, HES, workflow/aprobaciones HES, maestro de usuarios	Solicitante, aprobador HES, hoja de entrada, documento de compra, proveedor, monto, centro de costo, fecha aprobación HES.	Comparar el solicitante de la SolPed con el usuario que aprueba o acepta la HES relacionada.	Casos donde el solicitante participa en la aprobación de la conformidad, permitiendo revisar independencia entre requerimiento y aceptación del servicio.
REL-09	OC, HES, workflow/liberaciones OC, workflow/aprobación	Aprobador OC, aprobador HES, documento de compra, hoja de entrada,	Vincular OC con HES y comparar si el aprobador o liberador de la OC coincide con el aprobador	Operaciones donde la autorización comercial y la aceptación operacional recaen en un mismo usuario,

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
	es HES, maestro de usuarios	proveedor, monto OC, valor HES, fechas de aprobación.	o aceptador de la HES.	indicando concentración de control.
REL-10	HES, Factura, maestro de usuarios	Hoja de entrada, documento de compra, autor HES, número de documento factura, usuario registrador factura, código transacción, proveedor, importe.	Relacionar la factura con su HES u OC asociada y comparar el autor de HES con el usuario que registra o trata la factura.	Facturas cuyo registro o tratamiento se vincula al mismo usuario que registró la conformidad del servicio, permitiendo revisar independencia entre recepción y cuentas por pagar.
REL-11	Factura, Pagos, partidas compensadas, maestro de usuarios	Número de documento factura, usuario factura, documento de compensación, usuario pago, fecha contabilización, fecha pago, proveedor, importe.	Vincular factura y pago mediante documento de compensación, y comparar el usuario que registra o trata la factura con el usuario asociado al pago o compensación.	Casos donde el registro contable y la gestión del pago se concentran en un mismo usuario, permitiendo revisar separación entre AP y tesorería.
REL-12	Logs de modificación, maestro de proveedores, SolPed, OC, HES, Factura, Pagos	Usuario modificador, proveedor, campo modificado, fecha modificación, usuario transaccional, documento asociado, tipo de documento, fecha transacción.	Cruzar usuarios que modifican datos maestros de proveedor con usuarios que participan en documentos P2P del mismo proveedor dentro de una ventana definida.	Operaciones donde un usuario modifica datos maestros y participa en transacciones del mismo proveedor, permitiendo revisar independencia entre maestro y operación.
REL-13	HES, OC, maestro de proveedores, maestro de usuarios	Autor HES, proveedor, hoja de entrada, documento de compra, contrato marco, valor bruto, período, centro de costo.	Agrupar HES por usuario autor y proveedor, calculando frecuencia, monto acumulado y participación relativa dentro del período analizado.	Ranking de usuarios que concentran creación de HES para un mismo proveedor, permitiendo revisar dependencia operativa en la conformidad de servicios.
REL-14	HES, workflow/aprobaciones HES, OC, maestro de usuarios, maestro de proveedores	Aprobador HES, proveedor, hoja de entrada, contrato marco, centro de costo, monto aprobado, fecha aprobación, período.	Agrupar aprobaciones de HES por usuario aprobador y proveedor, calculando frecuencia, monto y participación sobre el total de HES del proveedor.	Aprobadores que concentran validaciones de HES para un mismo proveedor, permitiendo revisar rotación, independencia y suficiencia de la aprobación operacional.
REL-15	HES, workflow/aprobaciones HES, maestro de usuarios, maestro de proveedores	Autor HES, aprobador HES, proveedor, contrato marco, centro de costo, hoja de entrada, monto, período.	Construir pares autor-aprobador de HES y medir su recurrencia por proveedor, contrato, centro de costo o período.	Duplas recurrentes entre creador y aprobador de HES, permitiendo identificar circuitos operativos estables que requieren revisión de independencia.
REL-16	SolPed, OC, workflow/liberaciones, maestro de usuarios	Solicitante, aprobador SolPed, aprobador OC, proveedor, centro de costo, grupo de artículos, monto, fecha.	Construir pares solicitante-aprobador y calcular recurrencia, monto acumulado y concentración por proveedor, área o categoría de gasto.	Duplas recurrentes entre solicitantes y aprobadores, permitiendo revisar relaciones internas que concentran decisiones de requerimiento y autorización.
REL-17	SolPed, OC, maestro de usuarios, maestro de proveedores	Solicitante, PO Creator, grupo de compras, proveedor, documento de compra, grupo de artículos, valor neto, centro.	Construir pares solicitante-comprador y medir recurrencia por proveedor, grupo de artículos, centro de costo y período.	Relaciones recurrentes entre solicitantes y compradores, permitiendo identificar posibles circuitos internos de canalización de compras.
REL-18	SolPed, OC, workflow/liberaciones, maestro de usuarios,	Solicitante, PO Creator, aprobador OC, proveedor, contrato	Construir triadas solicitante-comprador-aprobador y medir su	Triadas internas recurrentes asociadas a proveedores o categorías específicas,

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
	maestro de proveedores	marco, grupo de artículos, centro de costo, monto.	repetición por proveedor, contrato, centro o categoría de gasto.	permitiendo revisar cadenas de decisión demasiado estables.
REL-19	Factura, maestro de proveedores, DTE o registro tributario disponible	Proveedor, RUT proveedor, número de factura, folio, fecha emisión, fecha recepción, importe, moneda, sociedad.	Ordenar las facturas de cada proveedor por fecha y número de factura, calculando saltos, continuidad y cercanía entre folios emitidos a la compañía.	Proveedores con facturas altamente correlativas o con baja dispersión de folios, permitiendo revisar continuidad de facturación y concentración comercial aparente.
REL-20	Factura, Pagos, maestro de proveedores, DTE o registro tributario disponible	Proveedor, número de factura, folio, fecha emisión, importe, frecuencia de facturación, monto acumulado, período, sociedad.	Analizar la continuidad numérica, frecuencia y monto de facturas emitidas por proveedor hacia la compañía durante el período revisado.	Proveedores con alta recurrencia y continuidad de facturación hacia la operación minera, generando una señal de posible dependencia comercial que requiere validación complementaria.

Una vez definidos los requerimientos técnicos para la aplicación de las pruebas relacionales, las alertas generadas pueden ordenarse según su nivel de criticidad. Para efectos de este catálogo, las pruebas relacionales pueden agruparse en tres niveles de criticidad:

- Criticidad alta: Corresponde a alertas que evidencian una posible falta de segregación de funciones en etapas críticas del flujo, especialmente cuando un mismo usuario participa en actividades que deberían mantenerse separadas, o cuando la relación detectada se produce cerca de la recepción, el registro de la factura, el pago o la modificación de datos maestros del proveedor. En este nivel se consideran las pruebas REL-03, REL-05, REL-06, REL-09, REL-10, REL-11 y REL-12.
- Criticidad media: Corresponde a alertas que reflejan relaciones recurrentes, duplas, tríadas o concentraciones relevantes entre usuarios, proveedores, áreas o roles del proceso, sin que necesariamente exista una misma persona controlando funciones incompatibles dentro de una operación puntual. En este nivel se consideran las pruebas REL-02, REL-04, REL-07, REL-08, REL-13, REL-14, REL-15, REL-16, REL-17 y REL-18.
- Criticidad baja: Corresponde a alertas ubicadas principalmente en etapas iniciales

del requerimiento o en análisis relacionales de carácter indirecto, donde la señal observada permite identificar patrones de concentración o continuidad, pero no implica por sí misma una validación operacional, una obligación registrada o una salida inmediata de fondos. En este nivel se consideran las pruebas REL-01, REL-19 y REL-20.

Esta clasificación debe entenderse como una criticidad base y no como una calificación definitiva. En la aplicación del modelo, el nivel de prioridad podría aumentar o disminuir según distintos aspectos del caso analizado. De esta manera, la criticidad permite orientar la revisión de los resultados y priorizar aquellos casos que requieren mayor análisis documental, operativo o de control.

6.1.5. Pruebas de temporalidad

Las pruebas de temporalidad revisan si los tiempos entre las etapas del proceso de abastecimiento son coherentes con el curso normal de una operación. En esta categoría no se analiza una fecha aislada, sino la relación entre los principales hitos del flujo. Su foco está en identificar operaciones que avanzan demasiado rápido, demasiado lento o fuera del momento lógico esperado según el tipo de compra, servicio o contrato.

El riesgo principal de estas pruebas es que la documentación no refleje el orden real de la operación. Cuando los tiempos no son razonables, puede ocurrir que una compra se haya formalizado después de iniciada la prestación, que una recepción se haya registrado sin una validación suficiente, que una factura se haya procesado antes de contar con respaldo completo o que un pago se haya ejecutado sin el tiempo necesario para revisar los antecedentes. En todos esos casos, el problema no es la fecha en sí misma, sino la pérdida de control sobre cuándo se autorizó, ejecutó, recepcionó, facturó o pagó la operación.

Por esta razón, las pruebas de temporalidad permiten detectar posibles regularizaciones posteriores, validaciones apresuradas, registros tardíos o pagos acelerados dentro del flujo Procure-to-

Pay. A continuación, se presentan veinte pruebas de temporalidad consideradas en el catálogo:

- **TEMP-01. SolPed creada con lead time mínimo antes de la OC:** identifica solicitudes de pedido creadas muy poco tiempo antes de la emisión de la orden de compra asociada.
- **TEMP-02. SolPed con lead time excesivo antes de la OC:** detecta solicitudes de pedido que permanecen abiertas durante un período prolongado antes de convertirse en orden de compra.
- **TEMP-03. SolPed de emergencia con demora elevada hasta la OC:** identifica solicitudes clasificadas como urgentes, spot o de emergencia que tardan demasiado en generar una orden de compra.
- **TEMP-04. OC emitida después del inicio del servicio:** detecta órdenes de compra cuya fecha de creación es posterior al inicio informado del servicio, período contractual o ejecución operacional.
- **TEMP-05. OC creada con lead time mínimo antes de la HES:** identifica operaciones en que la HES se registra muy poco tiempo después de la creación de la orden de compra.
- **TEMP-06. OC con lead time excesivo antes de la HES:** detecta órdenes de compra que tardan demasiado en generar una HES o recepción asociada.
- **TEMP-07. Lead time OC-HES incompatible con el tipo de contrato:** identifica operaciones cuyo tiempo entre la orden de compra y la HES no resulta razonable para el tipo de contratación registrado, sea contrato menor, contrato mayor o servicio spot.
- **TEMP-08. HES registrada antes del término del período del servicio:** detecta

hojas de entrada de servicio creadas o aceptadas antes de la fecha de término del período informado.

- **TEMP-09. HES registrada con atraso relevante respecto del período del servicio:** identifica conformidades registradas mucho después del término del período de prestación.
- **TEMP-10. HES modificada después de su aceptación:** detecta hojas de entrada de servicio que presentan modificaciones relevantes luego de haber sido aceptadas o liberadas.
- **TEMP-11. Factura emitida antes de la HES aceptada:** identifica facturas cuya fecha de emisión es anterior a la fecha de aceptación de la HES que debería respaldar el servicio.
- **TEMP-12. Factura registrada con lead time mínimo posterior a la HES:** detecta facturas ingresadas o contabilizadas inmediatamente después de la aceptación de la HES.
- **TEMP-13. Factura registrada con atraso excesivo desde su emisión o recepción:** identifica facturas cuya contabilización ocurre mucho después de su fecha de emisión o recepción.
- **TEMP-14. Factura contabilizada cerca del cierre contable:** detecta facturas registradas en fechas cercanas al cierre mensual o anual.
- **TEMP-15. Pago ejecutado con lead time mínimo desde el registro de la factura:** identifica pagos realizados muy poco tiempo después del registro o contabilización de la factura.
- **TEMP-16. Pago anticipado respecto del vencimiento neto:** detecta pagos

realizados antes de la fecha de vencimiento definida por las condiciones de pago.

- **TEMP-17. Pago tardío respecto del vencimiento neto:** identifica facturas pagadas con atraso relevante respecto de la fecha de vencimiento.
- **TEMP-18. Modificación de datos maestros poco antes de la factura o pago:** detecta cambios en datos críticos del proveedor, como cuenta bancaria, receptor de pago, condición de pago o vía de pago, realizados en una ventana cercana al registro de la factura o al desembolso.
- **TEMP-19. Regularización tardía de servicios spot o de emergencia:** identifica servicios clasificados como spot o de emergencia cuya documentación se completa mucho tiempo después de la ejecución, recepción, facturación o pago.
- **TEMP-20. Concentración temporal de HES, facturas o pagos en ventanas críticas:** detecta acumulaciones inusuales de HES, facturas o pagos en períodos específicos, como cierres mensuales, cierres anuales, campañas presupuestarias o ventanas de regularización.

Una vez descrita la finalidad de cada prueba y su implicancia dentro del flujo Procure-to-Pay, la siguiente tabla presenta los elementos técnicos necesarios para su aplicación. Para ello, cada prueba se organiza según el código asignado, las fuentes de datos requeridas, las variables principales que permiten realizar el cruce, la regla de análisis que define la validación temporal, el criterio de alerta y el resultado esperado que debería entregar el modelo.

Tabla 05: Requerimientos técnicos de las pruebas de temporalidad.

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
TEMP-01	SolPed, OC	Solicitud de pedido, posición SolPed, documento de compra, posición OC, fecha de solicitud, fecha de liberación, fecha de creación OC, solicitante, proveedor,	Vincular la SolPed con la OC y calcular el tiempo transcurrido entre la creación o liberación de la SolPed y la emisión de la OC.	Operaciones donde la OC fue creada en un lapso muy breve respecto de la SolPed, permitiendo revisar si el requerimiento fue generado como respaldo posterior de una compra ya gestionada.

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
		monto.		
TEMP-02	SolPed, OC	Solicitud de pedido, documento de compra, fecha de solicitud, fecha de liberación, fecha de creación OC, estado de liberación, centro, grupo de compras, monto.	Calcular los días transcurridos entre la SolPed y la OC, considerando la fecha de creación o liberación del requerimiento.	Solicitudes que permanecen abiertas por un periodo excesivo antes de convertirse en OC, permitiendo revisar vigencia del requerimiento y seguimiento del proceso.
TEMP-03	SolPed, OC, contratos	Solicitud de pedido, tipo de documento, indicador de emergencia, fecha de solicitud, fecha de OC, proveedor, grupo de compras, texto breve, monto.	Filtrar SolPed clasificadas como urgentes, spot o de emergencia y calcular el tiempo transcurrido hasta la creación de la OC.	Solicitudes urgentes que presentan demoras relevantes antes de formalizar la compra, permitiendo revisar si la urgencia declarada se encuentra debidamente justificada.
TEMP-04	OC, HES, contratos	Documento de compra, fecha creación OC, fecha documento OC, inicio período de validez, fecha inicio servicio, período HES, proveedor, tipo de contrato, monto.	Comparar la fecha de creación de la OC con la fecha de inicio del servicio, vigencia contractual o período informado en la HES.	Órdenes de compra emitidas después del inicio del servicio, permitiendo revisar posibles regularizaciones posteriores y existencia de autorización previa.
TEMP-05	OC, HES	Documento de compra, posición, hoja de entrada, fecha creación OC, fecha liberación OC, fecha creación HES, fecha documento HES, proveedor, monto.	Calcular el tiempo transcurrido entre la creación o liberación de la OC y la creación o aceptación de la HES.	HES registradas en un lapso muy breve desde la OC, permitiendo revisar si existió tiempo razonable para ejecutar y validar el servicio.
TEMP-06	OC, HES, historial de pedidos	Documento de compra, fecha creación OC, fecha de entrega, hoja de entrada, fecha creación HES, proveedor, centro, saldo pendiente, monto.	Calcular los días transcurridos entre la OC y la primera HES asociada, considerando la fecha de entrega o ejecución esperada.	Órdenes de compra con demora relevante hasta la recepción o conformidad, permitiendo revisar saldos abiertos, retrasos de ejecución o falta de seguimiento.
TEMP-07	OC, HES, contratos, maestro de tipos de contratación	Documento de compra, hoja de entrada, tipo de contrato, clase documento compras, fecha OC, fecha HES, proveedor, valor, grupo de artículos.	Clasificar las operaciones por tipo de contrato y comparar el tiempo OC-HES contra rangos esperados para cada modalidad.	Operaciones cuyo tiempo entre OC y HES no resulta coherente con la modalidad contractual declarada, permitiendo revisar clasificación y respaldo de la contratación.
TEMP-08	HES, OC, contratos	Hoja de entrada, documento de compra, fecha documento HES, fecha creación HES, período, fecha fin, fecha entrega, proveedor, texto breve.	Comparar la fecha de creación o aceptación de la HES con la fecha de término del período de servicio informado.	HES aceptadas antes del término del servicio, permitiendo revisar si la conformidad fue emitida antes de contar con evidencia completa de ejecución.
TEMP-09	HES, OC, contratos, respaldos operativos	Hoja de entrada, período, fecha fin, fecha creación HES, última modificación, autor, proveedor, documento de compra, monto.	Calcular los días transcurridos entre el término del período de servicio y la fecha de creación o aceptación de la HES.	HES registradas de forma tardía respecto del servicio, permitiendo revisar oportunidad de la conformidad y calidad del respaldo operativo.
TEMP-10	HES, logs de modificación, workflow de	Hoja de entrada, fecha de aceptación, última modificación, usuario	Identificar modificaciones en campos críticos de la HES después de su	HES aceptadas y posteriormente modificadas, permitiendo revisar motivo

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
	aceptación	modificador, monto, período, texto breve, indicador de aceptación, OC.	aceptación o liberación.	del cambio, autorización y soporte documental.
TEMP-11	Facturas, HES, OC	Número de documento, referencia factura, fecha de emisión, fecha documento factura, fecha registro, hoja de entrada, fecha aceptación HES, proveedor, monto.	Vincular la factura con la HES y comparar la fecha de emisión de la factura con la fecha de aceptación de la HES.	Facturas emitidas antes de la conformidad del servicio, permitiendo revisar si el cobro fue realizado antes de contar con respaldo aceptado.
TEMP-12	Facturas, HES, OC	Hoja de entrada, fecha aceptación HES, fecha registro factura, fecha contabilización, usuario, proveedor, monto, moneda.	Calcular el tiempo transcurrido entre la aceptación de la HES y el registro o contabilización de la factura.	Facturas registradas en un lapso mínimo posterior a la HES, permitiendo revisar si la validación documental fue suficiente antes del registro contable.
TEMP-13	Facturas, HES, OC	Número de documento, referencia, fecha emisión, fecha recepción, fecha registro, fecha contabilización, proveedor, importe, moneda.	Calcular los días transcurridos entre la emisión o recepción de la factura y su registro contable.	Facturas registradas tardíamente, permitiendo revisar gestión documental, oportunidad de contabilización y correcta imputación del período.
TEMP-14	Facturas, calendario contable, centros de costo	Número de documento, fecha contabilización, período contable, fecha documento, proveedor, centro de costo, importe, usuario.	Identificar facturas contabilizadas dentro de una ventana cercana al cierre mensual o anual.	Facturas registradas cerca del cierre contable, permitiendo revisar oportunidad del registro, respaldo documental e imputación temporal del gasto.
TEMP-15	Facturas, pagos, workflow de aprobación	Número de documento, referencia, fecha registro factura, fecha contabilización, fecha pago, documento de compensación, proveedor, importe.	Calcular el tiempo transcurrido entre el registro o contabilización de la factura y la fecha de pago o compensación.	Pagos ejecutados en un lapso mínimo desde el registro de la factura, permitiendo revisar si se completaron las validaciones previas al desembolso.
TEMP-16	Facturas, pagos, maestro de proveedores	Proveedor, condiciones de pago, vencimiento neto, fecha de vencimiento, fecha pago, vía de pago, importe, documento de compensación.	Comparar la fecha de pago con la fecha de vencimiento calculada según las condiciones de pago del proveedor o documento.	Pagos realizados antes del vencimiento esperado, permitiendo revisar autorización, excepción financiera o beneficio económico asociado.
TEMP-17	Facturas, pagos, maestro de proveedores	Proveedor, fecha vencimiento, vencimiento neto, fecha pago, condición de pago, importe, moneda, bloqueo de pago.	Calcular los días de atraso entre la fecha de vencimiento y la fecha efectiva de pago.	Facturas pagadas después del vencimiento, permitiendo revisar gestión de cuentas por pagar, bloqueos, disputas o retrasos no documentados.
TEMP-18	Maestro de proveedores, maestro de cuentas bancarias, logs de modificación, facturas, pagos	Código proveedor, cuenta bancaria, IBAN, receptor de pago, condición de pago, fecha modificación, usuario modificador, fecha factura, fecha pago.	Identificar modificaciones en datos críticos del proveedor dentro de una ventana previa al registro de factura o ejecución del pago.	Operaciones asociadas a datos maestros modificados poco antes de facturar o pagar, permitiendo validar autorización independiente del cambio.
TEMP-19	SolPed, OC, HES, facturas, pagos,	Tipo de contratación, indicador de	Filtrar servicios spot o de emergencia y calcular los	Servicios de emergencia documentados tardíamente,

Código	Fuentes de datos	Variables principales	Regla de análisis	Resultado esperado
	contratos, respaldos de emergencia	emergencia, fecha solicitud, fecha OC, período HES, fecha factura, fecha pago, proveedor, monto.	lapsos entre solicitud, formalización, recepción, facturación y pago.	permitiendo revisar si la excepción fue justificada y si existió trazabilidad suficiente.
TEMP-20	HES, facturas, pagos, calendario contable, calendario operativo	Fecha HES, fecha factura, fecha contabilización, fecha pago, proveedor, usuario, centro de costo, importe, período contable.	Medir concentración diaria o semanal de HES, facturas y pagos, comparándola con el comportamiento promedio o histórico del proceso.	Períodos con concentración inusual de registros, permitiendo revisar procesamiento masivo, presión de cierre o regularizaciones acumuladas.

Una vez definidos los requerimientos técnicos para la aplicación de las pruebas de temporalidad, las alertas generadas pueden ordenarse según su nivel de criticidad. Para efectos de este catálogo, las pruebas de temporalidad pueden agruparse en tres niveles de criticidad:

- Criticidad alta: corresponde a alertas que afectan etapas cercanas a la conformidad del servicio, la facturación, el desembolso o la modificación de datos sensibles del proveedor. En este nivel se consideran las pruebas TEMP-04, TEMP-08, TEMP-10, TEMP-11, TEMP-15, TEMP-18, TEMP-19 y TEMP-20.
- Criticidad media-alta: corresponde a alertas que afectan la oportunidad de los controles intermedios del proceso, especialmente entre la solicitud, la orden de compra, la HES, la factura y el vencimiento de pago. En este nivel se consideran las pruebas TEMP-01, TEMP-03, TEMP-05, TEMP-07, TEMP-09, TEMP-12, TEMP-14 y TEMP-16.
- Criticidad media: corresponde a alertas que afectan principalmente la eficiencia, oportunidad de gestión o seguimiento documental del proceso, sin que necesariamente impliquen una etapa inmediata de pago o un quiebre directo del respaldo previo. En este nivel se consideran las pruebas TEMP-02, TEMP-06, TEMP-13 y TEMP-17.

Esta clasificación debe entenderse como una criticidad base y no como una calificación definitiva. En la aplicación del modelo, el nivel de prioridad podría aumentar o disminuir según distintos

aspectos del caso analizado. De esta manera, la criticidad permite orientar la revisión de los resultados, priorizando no solo las alertas más cercanas al pago, sino también aquellas que se repiten con mayor frecuencia o muestran patrones temporales concentrados dentro del proceso.

6.2. Implementación del modelo mediante lenguaje Python

Una vez documentado el catálogo de pruebas analíticas forenses presentado en el apartado anterior, correspondió trasladar esa estructura conceptual a una herramienta computacional capaz de aplicarla de manera ordenada sobre archivos reales del proceso de abastecimiento. Esta sección describe cómo el modelo diseñado fue implementado mediante el lenguaje de programación Python, de modo que las pruebas dejaran de ser únicamente criterios metodológicos para convertirse en reglas ejecutables sobre la información del flujo Procure-to-Pay (P2P). El propósito de este apartado es explicar, qué hace la herramienta, cómo está organizada y por qué su funcionamiento contribuye a fortalecer el control del proceso de abastecimiento, sin transformar la explicación en un manual de programación.

Conviene precisar desde el inicio que la herramienta no busca probar la existencia de fraude ni emitir conclusiones de carácter judicial. Su finalidad es detectar anomalías, señales de alerta, inconsistencias relevantes que justifiquen una revisión posterior.

6.2.1. Propósito de la implementación computacional del modelo

El modelo conceptual describe qué se debe revisar y bajo qué criterios, pero por sí solo no permite procesar la gran cantidad de registros que genera el abastecimiento de una operación minera. Por esta razón fue necesario implementarlo en un lenguaje de programación que tradujera cada criterio en una instrucción que el computador pudiera ejecutar de forma ordenada, repetible y trazable. Se optó por Python porque permite procesar bases de datos, recorrer carpetas de información, leer distintos formatos de archivo, limpiar y estandarizar campos, homologar variables que provienen de fuentes diferentes, cruzar registros entre documentos y generar salidas estructuradas que pueden revisarse con posterioridad.

El resultado de este trabajo es el Modelo de Análisis de Datos Forense¹³, un programa que aplica el catálogo de pruebas sobre los archivos del proceso de abastecimiento.

La elección de un lenguaje de programación responde también a la necesidad de trazabilidad, al ejecutarse siempre con la misma lógica, la herramienta asegura que dos revisiones sobre los mismos archivos entreguen los mismos resultados, de modo que cada alerta pueda explicarse a partir de una regla conocida y reproducible, y no del criterio puntual de quien revisa.

La implementación se organizó en torno a las etapas del proceso Procure-to-Pay, de modo que la información que ingresa al modelo pueda asociarse al recorrido habitual de una operación de abastecimiento. Al estructurar la herramienta sobre esta secuencia, el modelo puede observar la coherencia entre las distintas etapas y reconstruir el vínculo entre los documentos que las respaldan.

6.2.2.Arquitectura general del script

El script¹⁴ fue desarrollado como un único archivo ejecutable, lo que facilita su uso en entornos como Spyder o la terminal sin requerir instalaciones complejas. Aunque está contenido en un solo archivo, internamente sigue una lógica modular. Se compone de aproximadamente seis mil novecientas líneas organizadas en trece capas funcionales, cada una responsable de una tarea distinta dentro del análisis. A ello se suman cien funciones de prueba, una por cada prueba del catálogo, y dos estructuras de apoyo que representan, respectivamente, una tabla leída desde un archivo y el resultado de ejecutar una prueba. Esta organización permite revisar, corregir o ampliar una parte del modelo sin afectar a las demás, y constituye evidencia de que la herramienta es una implementación técnica integral del modelo y no una prueba aislada.

Sin entrar en el detalle del código, conviene presentar una visión general de los bloques que componen la herramienta y de la función que cumple cada uno. La siguiente tabla resume los principales componentes del script, su función dentro del modelo, su aporte al análisis y un ejemplo aplicado al

¹³Ver Anexo 01.

¹⁴**Script:** archivo que contiene un conjunto de instrucciones escritas en un lenguaje de programación, en este caso Python, que el computador ejecuta de forma ordenada para realizar una tarea determinada.

proceso de abastecimiento.

Tabla 06: Componentes funcionales del script de análisis forense.

Componente del script	Función dentro del modelo	Aporte al análisis forense	Ejemplo aplicado al proceso P2P
Configuración general del modelo	Define el comportamiento base de la herramienta y los parámetros iniciales del análisis.	Asegura que todas las ejecuciones partan de criterios comunes y conocidos.	Establece cómo se interpretan montos, fechas y estados documentales antes de revisar.
Colores, umbrales y parámetros	Fija tolerancias, ventanas de tiempo y umbrales de similitud utilizados por las pruebas.	Hace explícitos los criterios numéricos que separan lo esperable de lo atípico.	Definir cuántos días de diferencia entre factura y pago se consideran relevantes.
Catálogo de pruebas analíticas	Almacena las cien pruebas con su código, categoría, fuente, variables, regla y criticidad.	Permite organizar la ejecución a partir de la estructura diseñada metodológicamente.	Disponer de la prueba que compara el proveedor entre OC, factura y pago.
Funciones de normalización	Limpian y estandarizan textos, montos, fechas, RUT y referencias documentales.	Permiten comparar datos que vienen escritos de maneras distintas.	Reconocer que “USD 1.000” y “1000 dólares” representan el mismo monto.
Lectura de archivos	Recorre la carpeta de entrada y extrae tablas desde distintos formatos.	Permite incorporar información aunque no venga en una única planilla.	Leer una OC en Excel y una factura contenida en un PDF.
Clasificación de fuentes P2P	Identifica a qué etapa o documento del proceso corresponde cada archivo.	Asocia cada tabla a la fuente que las pruebas requieren.	Reconocer que un archivo corresponde a HES y otro a pagos.
Homologación de columnas	Traduce los nombres de columnas de cada archivo a un nombre estándar del modelo.	Hace comparables archivos con encabezados diferentes.	Tratar “PO”, “Purchase Order” y “OC” como un mismo campo.
Construcción de la base P2P	Consolida las fuentes en estructuras ordenadas y comparables.	Permite cruzar documentos y seguir el recorrido de una operación.	Vincular una SolPed con su OC, su HES, su factura y su pago.
Ejecución de pruebas	Revisa qué información hay disponible y aplica las pruebas correspondientes.	Transforma las reglas del catálogo en revisiones efectivas sobre los datos.	Aplicar la prueba de secuencia para verificar el orden de las etapas.
Generación de alertas	Crea un registro trazable cada vez que se cumple el criterio de una prueba.	Convierte una desviación en una observación documentada y revisable.	Registrar una factura cuyo monto no coincide con el de la OC.
Métricas de ejecución	Cuantifica archivos, registros, pruebas y alertas de cada corrida.	Permite comprender el alcance real del análisis realizado.	Indicar cuántas pruebas se ejecutaron y cuántas quedaron sin datos.
Exportación a Excel	Consolida resultados y registros en un libro ordenado de varias hojas.	Entrega una salida auditable y filtrable para la revisión posterior.	Generar una hoja con la matriz de alertas y otra con el log de archivos.
Interacción con el usuario	Solicita los parámetros de la ejecución mediante preguntas en la terminal.	Permite ajustar el análisis sin modificar el código fuente.	Pedir la carpeta de entrada y qué pruebas se desean ejecutar.

6.2.3. Bibliotecas utilizadas y su función dentro del modelo

Para realizar estas tareas, el modelo se apoya en un conjunto de bibliotecas¹⁵ de Python. Algunas

¹⁵**Biblioteca de Python:** conjunto de funciones ya desarrolladas que un programa reutiliza para realizar tareas específicas sin necesidad de programarlas desde cero.

son necesarias para el funcionamiento principal y otras son opcionales y amplían sus capacidades, como la lectura de PDF o Word, el reconocimiento de texto en imágenes o la homologación aproximada de columnas. Una característica relevante del diseño es que el script funciona con o sin las bibliotecas opcionales, cuando alguna no está instalada, utiliza alternativas incluidas en la instalación estándar de Python, de modo que puede ejecutarse en distintos entornos sin perder su lógica esencial. La siguiente tabla describe las principales bibliotecas y su utilidad dentro del modelo.

Tabla 07: Bibliotecas de Python utilizadas en el modelo.

Biblioteca	Tipo de uso	Función dentro del script	Aporte al modelo forense
pandas	Requerida	Estructura, limpia, cruza y consolida los registros del flujo P2P en tablas.	Es la base que permite comparar y relacionar la información de las distintas fuentes.
numpy	Requerida	Apoya los cálculos numéricos y el manejo eficiente de valores.	Facilita comparaciones de montos y operaciones sobre grandes volúmenes de datos.
openpyxl	Requerida	Genera y da formato al archivo Excel final.	Entrega una salida ordenada, con color y auditable para la revisión.
pathlib	Requerida	Recorre carpetas y administra las rutas de los archivos.	Permite ubicar y leer los documentos de la carpeta de entrada.
argparse	Requerida	Gestiona los parámetros entregados al ejecutar el script.	Permite definir el análisis desde la terminal sin editar el código.
logging	Requerida	Registra eventos, advertencias y errores durante la ejecución.	Deja constancia de lo ocurrido en cada corrida, fortaleciendo la trazabilidad.
re y unicodedata	Requeridas	Reconocen patrones de texto, normalizan y eliminan acentos.	Estandarizan campos como RUT, folios y glosas para poder compararlos.
collections y datetime	Requeridas	Cuentan y agrupan registros, y manejan fechas y diferencias de tiempo.	Apoyan la detección de repeticiones y la revisión de plazos y lead times.
typing, json, warnings, sys y time	Requeridas	Documentan tipos, manejan datos estructurados, controlan avisos, interactúan con el sistema y miden tiempos.	Aportan orden, estabilidad y reporte del tiempo de ejecución de cada análisis.
pdfplumber y PyMuPDF (fitz)	Opcionales	Extraen tablas y texto desde documentos PDF.	Incorporan información cuando no viene en planillas Excel.
python-docx	Opcional	Lee y genera documentos de Word.	Permite incorporar tablas contenidas en archivos Word.
matplotlib	Opcional	Genera gráficos de apoyo.	Permite visualizar de forma simple la distribución de alertas.
rapidfuzz y unidecode	Opcionales	Miden la similitud aproximada entre textos y simplifican caracteres.	Apoyan la homologación de columnas y nombres parecidos.
pytesseract / PIL / easyocr	Opcionales	Reconocen texto contenido en imágenes (OCR).	Permiten leer respaldos escaneados cuando se requiere.

6.2.4. Lectura, clasificación y homologación de las fuentes de datos

Una característica relevante del modelo es que no depende de una única base rígida ni de un

formato completamente estandarizado. La herramienta está diseñada para revisar una carpeta de entrada¹⁶, identificar los archivos disponibles, leer distintas extensiones y reconocer su contenido. Esta flexibilidad es importante en auditoría forense, porque la información del abastecimiento rara vez se encuentra en una sola planilla, puede provenir de archivos Excel, reportes de sistemas ERP, documentos en PDF o Word, respaldos documentales, maestros de proveedores, registros de pagos o bitácoras con nombres de columnas diferentes.

En cuanto a la lectura, el script puede extraer tablas desde archivos Excel, archivos de texto separado (CSV, TSV y TXT), documentos PDF y documentos Word, y cuenta además con la posibilidad de reconocer texto contenido en imágenes mediante OCR cuando las bibliotecas correspondientes están disponibles. De este modo, la información puede incorporarse al análisis aunque su origen y formato sean diversos.

Una vez leídos los archivos, el modelo intenta clasificarlos según las fuentes del proceso P2P, combinando señales del nombre del archivo, del nombre de la hoja y de los nombres de las columnas. Entre las fuentes que reconoce se encuentran las solicitudes de pedido, las órdenes de compra, las hojas de entrada de servicio, las facturas, los pagos, los maestros de proveedores y de usuarios, las cuentas bancarias, los contratos, las bitácoras de modificación y las notas de crédito, entre otras. Esta clasificación es necesaria porque cada prueba requiere fuentes y variables específicas para ejecutarse.

El paso siguiente es la homologación¹⁷ de variables, que constituye uno de los principales desafíos resueltos por el modelo. El objetivo es reconocer las variables necesarias para las pruebas aunque los archivos no utilicen exactamente los mismos nombres de columnas. Para lograrlo, la herramienta normaliza el texto, elimina acentos, estandariza los nombres de las columnas y los compara contra diccionarios de sinónimos mediante coincidencias exactas, coincidencias por contención y coincidencias por similitud o fuzzy matching¹⁸. Adicionalmente, aplica reglas contextuales según la

¹⁶**Carpeta de entrada:** carpeta del computador en la que se ubican los archivos que el modelo leerá y analizará durante una ejecución.

¹⁷**Homologación:** proceso mediante el cual columnas o variables con nombres distintos, pero que representan lo mismo, se reconocen como equivalentes para poder compararlas y cruzarlas.

¹⁸**Fuzzy matching** (coincidencia aproximada): técnica que reconoce que dos textos son similares aunque no sean idénticos, lo que permite asociar nombres de columnas o de proveedores escritos de maneras distintas.

fuelle identificada, de modo que un mismo encabezado pueda interpretarse correctamente según el reporte del que proviene. Algunos ejemplos simples ilustran esta lógica:

- “OC”, “PO”, “Purchase Order” o “Purchasing Document” pueden representar una orden de compra.
- “HES”, “Entry Sheet” o “Service Entry Sheet” pueden representar una hoja de entrada de servicio.
- “Factura”, “Invoice”, “Folio” o “Reference” pueden representar un documento de facturación.
- “Documento de compensación”, “Clearing Document” o “Payment Document” pueden representar información asociada al pago.

Gracias a esta homologación, archivos heterogéneos se transforman en estructuras comparables y cruzables. Esto fortalece la trazabilidad, porque permite relacionar documentos del flujo P2P aunque la información provenga de sistemas y reportes distintos, y deja registro de cómo se interpretó cada columna para que la decisión pueda revisarse posteriormente.

6.2.5. Interacción del script con el usuario

El modelo es dinámico también en su relación con la persona que lo ejecuta, ya que conversa con ella mediante una serie de solicitudes en la terminal. De esta manera, el usuario no necesita modificar el código para definir los parámetros de la ejecución, basta con responder a las preguntas que la herramienta plantea. A modo ilustrativo, una ejecución típica solicita la carpeta de entrada, la carpeta de salida, el nombre del proyecto, el período analizado, la selección de pruebas y la activación del modo auditoría, para luego informar cuántos archivos fueron encontrados. La siguiente tabla explica cada una de estas solicitudes.

Tabla 08: *Parámetros de interacción para la ejecución del script.*

Solicitud del terminal	Qué significa	Qué debe ingresar el usuario	Efecto en la ejecución
Carpeta de entrada	Lugar donde se ubican los archivos que se desean analizar.	La ruta de la carpeta que contiene los documentos del proceso.	Define el conjunto de archivos que el modelo leerá y revisará.
Carpeta de salida	Lugar donde se guardarán los resultados del análisis.	La ruta de la carpeta donde se almacenará el informe.	Determina dónde se generará el archivo Excel de resultados.
Nombre del proyecto	Identificador del análisis que se está ejecutando.	Un nombre descriptivo de la revisión.	Permite reconocer y etiquetar la ejecución en los resultados.
Período analizado	Rango de tiempo al que corresponde la información.	El período de los datos, por ejemplo un rango de años.	Contextualiza temporalmente el análisis realizado.
Selección de pruebas	Conjunto de pruebas que se desea aplicar.	“todas”, una categoría, “alta criticidad” o códigos específicos como “CON-09, DUP-08”.	Ajusta el alcance del análisis al subconjunto elegido.

Esta forma de interacción hace que el modelo sea adaptable a distintos escenarios, es decir, una misma herramienta puede analizar un período acotado o extenso, ejecutar todo el catálogo o una sola categoría, y entregar un reporte liviano o uno que incluya las bases procesadas, según las necesidades de cada revisión.

6.2.6. Lógica de ejecución de las pruebas

El catálogo incorporado en el script contiene, para cada prueba, su código, su categoría, su nombre, la fuente requerida, las variables esperadas, la regla de análisis, el criterio de alerta y la criticidad base. A partir de esta información, la herramienta sigue una lógica clara para decidir qué pruebas puede ejecutar. Primero revisa qué fuentes y variables están disponibles tras la lectura y la homologación, si la información mínima requerida por una prueba está presente, la prueba se ejecuta, si falta una fuente o variable crítica, la prueba no se ejecuta o queda documentada como no aplicable.

Es importante interpretar correctamente los posibles resultados de este proceso. Una prueba ejecutada puede generar alertas o no generarlas, y el hecho de que no existan alertas no significa que la prueba haya fallado, sino que no se observaron desviaciones bajo la regla aplicada. A su vez, que una prueba no se ejecute¹⁹ debe entenderse como una limitación de disponibilidad de información y no como

¹⁹**Prueba no ejecutada:** prueba que no pudo aplicarse porque no estaba disponible alguna de las fuentes o variables que requiere; se documenta como tal y no equivale a la ausencia de riesgo.

ausencia de riesgo. Por último, cada alerta conserva el vínculo con la fuente, el documento, el campo o el registro que la originó, de modo que siempre pueda rastrearse su procedencia. Esta distinción permite defender metodológicamente el funcionamiento del modelo, ya que separa con claridad lo que se revisó, lo que no se pudo revisar y lo que efectivamente llamó la atención.

De manera complementaria, el recorrido operativo del modelo puede describirse en palabras para comprender el flujo completo sin necesidad de figuras. El usuario define la carpeta de entrada, el script identifica los archivos disponibles, se extraen las tablas o registros que contienen, las fuentes se clasifican según su relación con el proceso P2P, las columnas se normalizan y homologan, se construye una base de análisis o estructura relacional, se evalúan las pruebas que cuentan con la información necesaria, se documentan tanto las pruebas ejecutadas como las no ejecutadas, se generan alertas cuando se cumplen las condiciones definidas por cada prueba y, finalmente, los resultados se consolidan en un archivo Excel. Este recorrido se ejecuta de manera continua, y ninguna prueba que falle o que carezca de información detiene el proceso completo, lo que asegura que el modelo siempre entregue un resultado revisable.

6.2.7. Generación de alertas y trazabilidad de los resultados

Dentro del modelo, una alerta corresponde a una observación analítica generada cuando una operación cumple con la condición definida por una prueba. Cada alerta se construye de manera homogénea y conserva información suficiente para que pueda revisarse posteriormente sin necesidad de volver a ejecutar el modelo. Cuando la información está disponible, una alerta incluye el código de la prueba, su categoría, su nombre y su criticidad base, la situación observada y la regla que la originó, el documento involucrado, el proveedor, el o los usuarios, el monto, la moneda y la fecha asociada, la fuente de origen, el archivo y la hoja desde donde se obtuvo el dato, el campo evaluado y el valor observado en cada fuente comparada, y una recomendación preliminar de revisión.

Esta estructura es la que materializa la trazabilidad del modelo, ya que permite recorrer el camino que va desde una observación hasta el registro original que la motivó. De este modo, quien revise una alerta puede ubicar el documento de respaldo, comprender por qué se generó la observación y decidir,

con criterio propio, si corresponde profundizar en ella.

6.2.8. Salida del modelo y estructura del archivo Excel

La salida principal del modelo es un archivo Excel consolidado que debe entenderse como una herramienta de revisión y trazabilidad, y no solo como un archivo de resultados. El libro se organiza en varias hojas, cada una orientada a un aspecto distinto del análisis, de modo que cada observación pueda contrastarse con su origen. La siguiente tabla describe las principales hojas que puede contener y su utilidad para la revisión.

Tabla 09: Estructura del archivo Excel de salida del modelo.

Hoja del Excel	Contenido	Utilidad para la revisión
Portada y resumen ejecutivo	Datos generales de la ejecución y síntesis de los principales resultados.	Permite ubicar rápidamente el contexto y el alcance del análisis.
Métricas de ejecución	Indicadores de archivos, registros, pruebas y alertas de la corrida.	Ayuda a comprender las condiciones bajo las cuales se generaron los resultados.
Matriz de alertas	Listado detallado de todas las alertas con sus campos de trazabilidad.	Constituye el insumo central para revisar cada observación.
Hojas por categoría o prueba	Alertas organizadas según la prueba o categoría que las generó.	Facilita revisar un tipo específico de observación.
Pruebas no ejecutadas	Pruebas que no se aplicaron y el motivo correspondiente.	Hace visibles las limitaciones de información del análisis.
Diccionario u homologación de campos	Registro de cómo se interpretó cada columna de cada archivo.	Permite verificar la equivalencia de variables utilizada por el modelo.
Log de archivos y errores	Detalle de los archivos leídos, su clasificación y los errores de lectura.	Aporta trazabilidad sobre qué se procesó y qué presentó problemas.
Catálogo aplicado	Estructura del catálogo de pruebas utilizado en la ejecución.	Documenta las reglas bajo las cuales se realizó el análisis.
Bases procesadas (modo auditoría)	Volcado de las fuentes consolidadas cuando se activa el modo auditoría.	Refuerza la trazabilidad al conservar los respaldos procesados.

En conjunto, estas hojas permiten revisar de forma ordenada qué archivos fueron leídos, qué pruebas se ejecutaron y cuáles no, cuántas alertas se generaron, qué documentos están involucrados, qué categoría de riesgo o de control se ve afectada y qué trazabilidad existe hacia la fuente original, lo que convierte la salida del modelo en un material útil para la revisión posterior.

Las métricas de ejecución merecen una mención particular, porque permiten evaluar cada corrida del modelo y comprender su alcance real. Entre ellas se cuentan los archivos encontrados, las tablas extraídas, los registros procesados, las pruebas disponibles, seleccionadas, ejecutadas y no ejecutadas, las alertas generadas y su distribución por categoría y por criticidad, los errores de lectura, las

advertencias de homologación y el tiempo de ejecución. A ello se suma un log de ejecución²⁰, que registra los eventos, advertencias y errores ocurridos durante el análisis. En conjunto, estos elementos fortalecen la trazabilidad porque dejan constancia de las condiciones bajo las cuales se obtuvieron los resultados y permiten reconstruir lo sucedido en cada corrida, lo que resulta especialmente relevante al comparar o interpretar distintos análisis.

6.2.9. Requerimientos de ejecución del modelo

La ejecución del modelo no requiere conocimientos avanzados de programación, sino el cumplimiento de algunos pasos básicos. A continuación, se describe, de forma simple, lo que una persona necesita para utilizar la herramienta:

1. Contar con Python instalado en el computador.
2. Tener instaladas las bibliotecas necesarias para el funcionamiento del modelo.
3. Guardar el script en una carpeta de trabajo.
4. Preparar una carpeta de entrada con los archivos del proceso de abastecimiento.
5. Verificar que los archivos estén en formatos compatibles con la herramienta.
6. Ejecutar el script desde Spyder, la terminal u otro entorno equivalente.
7. Responder las solicitudes que la herramienta plantea en la terminal.
8. Revisar el archivo Excel generado con los resultados.
9. Validar las alertas contra los documentos originales.

Como se mencionó anteriormente, algunas bibliotecas son necesarias para el funcionamiento principal del modelo, mientras que otras son opcionales y amplían sus capacidades, como la lectura de

²⁰**Log de ejecución:** registro de los eventos, advertencias y errores ocurridos durante una corrida del modelo, utilizado para reconstruir.

PDF, Word o imágenes mediante OCR²¹, o la homologación aproximada de columnas. Dado que el script puede operar con alternativas estándar cuando las bibliotecas opcionales no están disponibles, su ejecución es posible en distintos entornos sin perder la lógica esencial del análisis.

6.3. Simulación del modelo mediante datos sintéticos generados con apoyo de inteligencia artificial

Una vez diseñado el catálogo de pruebas analíticas forenses e implementado el modelo mediante lenguaje Python, correspondió observar su comportamiento en un escenario controlado antes de proyectar su uso sobre datos reales. Para ello, y en línea con lo planteado en la sección 4.3 de la metodología, la simulación del modelo se realizó sobre una base de datos sintética²² generada con apoyo de inteligencia artificial.

6.3.1. Propósito de la simulación del modelo

La simulación se realizó con el objetivo de comprobar la credibilidad, la coherencia interna y la validez funcional preliminar²³ del modelo de análisis de datos forenses. Diseñar un catálogo de pruebas e implementarlo en una herramienta computacional no garantiza, por sí solo, que el modelo funcione de manera integrada, por ello fue necesario observar su comportamiento en un escenario controlado²⁴. De este modo, fue posible verificar si el modelo operaba de acuerdo con el diseño previsto.

Es importante precisar que la simulación no busca demostrar la existencia de fraude ni medir la efectividad estadística del modelo sobre datos reales. Su propósito es más acotado, verificar si el modelo es capaz de procesar archivos representativos del proceso de abastecimiento, reconocer fuentes y variables relevantes, ejecutar el catálogo de pruebas, generar alertas trazables, organizar los resultados de forma comprensible, permitir revisar la relación entre las anomalías incorporadas y las alertas

²¹**OCR** (reconocimiento óptico de caracteres): tecnología que permite extraer texto contenido en imágenes o documentos escaneados para incorporarlo al análisis.

²²**Datos sintéticos**: registros ficticios creados para representar un proceso realista de abastecimiento sin exponer información confidencial ni datos de personas o empresas reales.

²³**Validación funcional preliminar**: comprobación de que el modelo opera de acuerdo con su diseño en un escenario controlado; no equivale a una validación estadística ni definitiva sobre datos reales.

²⁴**Escenario controlado**: entorno de prueba en el que se conoce de antemano qué registros son normales y qué anomalías fueron incorporadas, lo que permite observar el comportamiento del modelo.

levantadas, y entregar una salida útil para auditoría forense, control interno y compliance operacional. En consecuencia, los resultados de esta sección deben leerse como una verificación de viabilidad operativa y una prueba de coherencia entre diseño, ejecución y resultado, y no como una validación definitiva del modelo.

6.3.2. Generación de la base sintética con apoyo de inteligencia artificial

La construcción de la base sintética se realizó con apoyo de inteligencia artificial, tomando como referencia la estructura documental y transaccional propia de un proceso de abastecimiento Procure-to-Pay. Para ello se consideraron campos, fuentes y relaciones observables en reportes de compras, recepción, facturación, pago, maestros y registros de control revisados en contexto profesional con la debida autorización, sin embargo, todos los datos utilizados en la simulación fueron generados de forma ficticia. En consecuencia, los proveedores, usuarios, montos, documentos, contratos, cuentas y registros incluidos en la base no corresponden a personas naturales ni jurídicas reales, sino a entidades simuladas con fines exclusivamente académicos, sin RUT válidos ni información confidencial.

La inteligencia artificial fue utilizada como apoyo para generar archivos representativos de cada etapa del proceso P2P, registros normales que reflejan una conducta regular y trazable, registros anómalos controlados, relaciones documentales entre la solicitud de pedido, la orden de compra, la hoja de entrada de servicio, la factura y el pago, así como maestros y archivos complementarios. El conjunto se diseñó con el propósito de reunir las estructuras suficientes para activar las cien pruebas del catálogo, de modo que la simulación no fuera una base aleatoria, sino un escenario controlado y trazable.

Con el fin de documentar de manera transparente cómo se solicitó la generación de la data, a continuación, se presenta un extracto resumido del prompt utilizado.

Tabla 10: *Extracto del prompt utilizado para generar datos sintéticos.*

«Actúa como ingeniero de datos senior experto en Python, auditoría forense, procesos Procure-to-Pay y generación de datos sintéticos. Estudia el script “Modelo de análisis de datos

forense.py” y genera una carpeta de simulación con datos transaccionales y documentales sintéticos, diseñada para ejecutar dicho script y activar las 100 pruebas del catálogo (CON-01 a CON-20, DUP-01 a DUP-20, SEC-01 a SEC-20, TEMP-01 a TEMP-20 y REL-01 a REL-20).

La carpeta debe representar transversalmente un proceso de abastecimiento P2P de una operación minera chilena e incluir al menos: SolPed, órdenes de compra, HES/recepciones, facturas, pagos, maestro de proveedores, maestro de usuarios, maestro de cuentas bancarias, contratos/acuerdos marco, workflow/liberaciones, logs de modificación, centros de costo, cuentas contables y notas de crédito/reversas.

La data debe combinar registros normales —con un flujo regular y trazable SolPed → OC → HES → Factura → Pago— y registros anómalos controlados diseñados para levantar alertas en cada prueba, acompañados de una matriz de anomalías esperadas que documente cada anomalía incorporada. Todos los datos deben ser completamente ficticios, sin nombres, proveedores ni RUT reales y sin información confidencial.»

La siguiente tabla resume las principales características que se pidieron y su aporte a la validación funcional del modelo.

Tabla 11: *Requerimientos de generación de la base sintética.*

Requerimiento solicitado	Propósito dentro de la simulación	Aporte a la validación funcional
Generación de archivos por etapa P2P	Representar el recorrido completo del proceso de abastecimiento.	Permite evaluar la lectura y clasificación de todas las fuentes.
Incorporación de registros normales	Reflejar una conducta regular y trazable del flujo.	Permite distinguir lo esperado de lo anómalo.
Incorporación de anomalías controladas	Activar las pruebas del catálogo de forma dirigida.	Permite observar si el modelo levanta las alertas previstas.
Compatibilidad con los nombres de columnas esperados	Facilitar la homologación de variables del script.	Permite que las pruebas encuentren los campos requeridos.
Inclusión de maestros y fuentes complementarias	Enriquecer la revisión con datos de control.	Permite ejecutar pruebas relacionales y de consistencia.
Registros suficientes para activar las 100 pruebas	Cubrir transversalmente todo el catálogo.	Permite una evaluación funcional integral del modelo.
Notas de crédito, reversas y logs de modificación	Representar ajustes y cambios posteriores al registro.	Permite probar temporalidad, secuencia y trazabilidad.
Uso de datos ficticios y no confidenciales	Resguardar la confidencialidad de la información.	Permite emplear la base con fines exclusivamente académicos.
Coherencia interna entre documentos	Mantener la trazabilidad documental del	Permite reconstruir la operación y cruzar

Requerimiento solicitado	Propósito dentro de la simulación	Aporte a la validación funcional
	flujo.	fuentes.
Matriz de anomalías esperadas	Documentar cada anomalía incorporada a la base.	Permite comparar lo esperado con lo efectivamente detectado.

6.3.3. Archivos sintéticos generados para representar el flujo P2P

Como resultado del proceso anterior se generaron quince archivos de entrada que representan las distintas fuentes del proceso de abastecimiento, además del archivo de salida producido posteriormente por el modelo, donde cada archivo se incorpora como anexo del informe. La siguiente tabla describe cada archivo, el documento o la fuente que representa y su función dentro de la simulación.

Tabla 12: Archivos sintéticos del flujo P2P utilizados en la simulación.

Archivo	Documento o fuente	Función dentro de la simulación
CDHDR_LogsModificacion_ChangeLog.docx ²⁵	Logs de modificación	Representa cambios en campos sensibles, datos maestros o ajustes documentales relevantes para consistencia, secuencia, temporalidad y relaciones.
FBL1N_Pagos_Payment.xlsx ²⁶	Pagos	Contiene registros de pago, compensación, importe, fechas y documentos financieros que cierran el ciclo P2P.
FK03_CuentasBancarias_BankMaster.pdf ²⁷	Maestro de cuentas bancarias	Simula cuentas, titulares y receptores de pago para pruebas sobre cuentas bancarias y cambios sensibles.
FS00_CuentasContables_GLAccount.xlsx ²⁸	Cuentas contables	Representa cuentas de mayor y clasificaciones contables para revisar imputación y consistencia financiera.
KS03_CentrosCosto_CostCenter.xlsx ²⁹	Centros de costo	Contiene centros de costo y unidades responsables para evaluar imputación y trazabilidad del gasto.
ME2N_OrdenesCompra_PurchaseOrder.xlsx ³⁰	Órdenes de compra	Representa la formalización comercial de compras y servicios, vinculando solicitudes, proveedores, montos y condiciones.
ME33K_Contratos_OutlineAgreement.docx ³¹	Contratos o acuerdos marco	Simula contratos y condiciones contractuales para validar coherencia entre contrato, OC y HES.
ME51N_SolPed_PurchaseRequisition.xlsx ³²	Solicitudes de pedido	Representa el origen del requerimiento interno dentro del flujo P2P.
MIRO_Facturas_Invoice.xlsx ³³	Facturas	Contiene documentos tributarios simulados, con referencias, montos, fechas y vínculos hacia OC y HES.

²⁵Ver anexo 02.

²⁶Ver anexo 03.

²⁷Ver anexo 04.

²⁸Ver anexo 05.

²⁹Ver anexo 06.

³⁰Ver anexo 07.

³¹Ver anexo 08.

³²Ver anexo 09.

³³Ver anexo 10.

Archivo	Documento o fuente	Función dentro de la simulación
ML84_HES_EntrySheet.xlsx ³⁴	Hojas de entrada de servicio	Representa la recepción o conformidad del servicio antes de la factura y el pago.
NC_Notas_de_Credito_Anulaciones_Reversas.xlsx ³⁵	Notas de crédito y reversas	Contiene documentos de regularización para revisar anulaciones, reversas y ajustes posteriores.
OX01_MaestroOrganizacional_EnterpriseStructure.xlsx ³⁶	Maestro organizacional	Representa sociedad, centro, organización y grupo de compras dentro de la estructura del gasto.
SU01_MaestroUsuarios_UserMaster.xlsx ³⁷	Maestro de usuarios	Contiene usuarios, roles y atributos requeridos para pruebas relacionales y de segregación de funciones.
Workflow_Releases_aprobaciones.pdf ³⁸	Workflow y aprobaciones	Simula liberaciones, aprobaciones, estados y flujos de control de documentos.
XK03_MaestroProveedores_VendorMaster.xlsx ³⁹	Maestro de proveedores	Contiene proveedores ficticios, datos fiscales y bancarios para pruebas de consistencia, duplicidad y relaciones.
Informe_Forense_P2P_sintetico.xlsx⁴⁰	Informe de salida del modelo	Corresponde al Excel generado por el script tras ejecutar el modelo sobre la base sintética.

En conjunto, estos archivos permiten reconstruir transversalmente el proceso de abastecimiento siguiendo el recorrido SolPed → OC → HES → Factura → Pago. Los archivos transaccionales aportan los documentos que avanzan a lo largo del flujo, mientras que los archivos maestros y complementarios enriquecen la revisión, ya que agregan información sobre proveedores, usuarios, cuentas bancarias, centros de costo, cuentas contables, contratos, workflow, logs de modificación y notas de crédito o reversas.

6.3.4. Ejecución del modelo sobre la base sintética

Una vez generada la carpeta de simulación⁴¹, esta fue utilizada como carpeta de entrada del script en Python. El procedimiento siguió un orden cronológico claro, en primer lugar se preparó la carpeta con los quince archivos sintéticos, luego se ejecutó el script Modelo de Análisis de Datos Forense, el modelo leyó y clasificó los archivos según su correspondencia con el proceso P2P, homologó las variables

³⁴Ver anexo 11.

³⁵Ver anexo 12.

³⁶Ver anexo 13.

³⁷Ver anexo 14.

³⁸Ver anexo 15.

³⁹Ver anexo 16.

⁴⁰Ver anexo 17.

⁴¹**Carpeta de simulación:** conjunto de archivos sintéticos utilizado como carpeta de entrada del modelo durante la ejecución.

equivalentes presentes en las distintas fuentes; evaluó la disponibilidad de fuentes y campos requeridos por cada prueba; ejecutó las pruebas aplicables; generó alertas cuando se cumplieron las reglas definidas y consolidó los resultados en el archivo ***Informe_Forense_P2P_sintetico.xlsx***.

El archivo Informe_Forense_P2P_sintetico.xlsx constituye la salida principal del modelo y funciona como un informe auditable, organizado en múltiples hojas que permiten recorrer los resultados desde una visión general hasta el detalle de cada alerta.

6.3.5. Resultados generales de la ejecución

Al ejecutar el modelo sobre la base sintética, este logró leer la carpeta de entrada, procesar las fuentes, ejecutar la totalidad del catálogo y generar una salida consolidada sin errores registrados. En concreto, se procesaron quince archivos, de los cuales se extrajeron quince tablas, con un total de 389 registros analizados. El modelo ejecutó las cien pruebas del catálogo de forma completa, sin pruebas parciales, sin pruebas no ejecutadas y sin pruebas con error, alcanzando un cien por ciento de pruebas efectivas. Como resultado, se levantaron 695 alertas, asociadas a un monto total alertado de \$396.110.000, y el proceso completo tomó 2,58 segundos. La siguiente tabla resume estas métricas principales.

Tabla 13: Métricas generales de ejecución del modelo.

Indicador	Valor
Archivos procesados	15
Tablas extraídas	15
Total de registros analizados	389
Pruebas del catálogo	100
Pruebas solicitadas	100
Pruebas ejecutadas (completas)	100
Pruebas parciales	0
Pruebas no ejecutadas	0
Pruebas con error	0
Porcentaje de pruebas efectivas	100%
Total de alertas levantadas	695
Monto total alertado	\$396.110.000
Errores registrados	0
Tiempo de ejecución	2,58 segundos

Estos resultados respaldan la viabilidad funcional de la implementación en un escenario

controlado: el modelo fue capaz de operar de acuerdo con el diseño previsto, recorriendo todas sus etapas y produciendo un informe consolidado. No obstante, conviene precisar que estas cifras no demuestran efectividad definitiva ni validan el modelo sobre la realidad operativa; corresponden a una validación funcional preliminar sobre una base sintética construida específicamente para ese propósito. La hoja de métricas del informe de salida presenta además el desglose de registros por fuente, como se aprecia en la siguiente figura.

El informe de salida organiza las 695 alertas levantadas según distintos criterios que facilitan su lectura. En cuanto a las categorías del catálogo, la distribución muestra que la mayor concentración de alertas se observa en la categoría de duplicidad, con 408 alertas. No obstante, esta concentración no implica que la duplicidad sea necesariamente el riesgo más importante en una operación real, refleja, más bien, las condiciones controladas incorporadas deliberadamente en la simulación. Las restantes categorías muestran que el modelo también es capaz de operar en otros frentes, consistencia, con 92 alertas, evidencia la capacidad de comparar campos críticos entre documentos; temporalidad, con 85, muestra la detección de lapsos, registros anticipados o tardíos; relacionales, con 76, refleja la identificación de vínculos, concentraciones y coincidencias entre usuarios y proveedores; y secuencia, con 34, da cuenta de la revisión del orden lógico del flujo P2P. A continuación, un grafico en barra con las distribución de alertas según categoría:

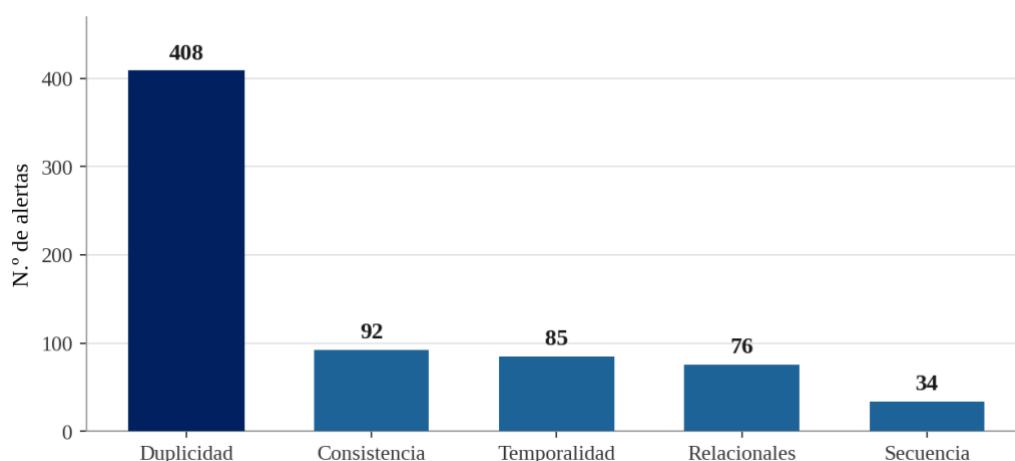


Figura 02. Distribución de alertas por categoría

Nota. Elaboración propia a partir del informe de salida del modelo (Anexo 17).

Respecto de la criticidad, la mayoría de las alertas se concentra en los niveles media-alta (322) y alta (259), mientras que las de criticidad media (96) y baja (18) son menos frecuentes. Esta distribución se explica, en parte, por el diseño de la base sintética, construida para activar pruebas de mayor sensibilidad vinculadas con pagos, facturación, datos maestros, duplicidades, cuentas bancarias, cambios de proveedor, condiciones de pago y quiebres de trazabilidad. A continuación, se muestra una distribución de criticidad en las alertas levantadas.

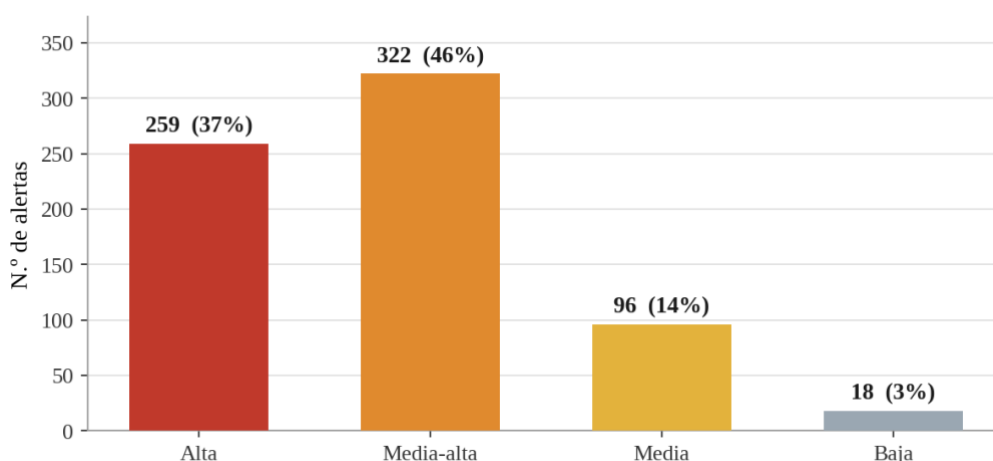


Figura 03. Distribución de alertas por criticidad base
Nota. Elaboración propia a partir del informe de salida del modelo (Anexo 17).

En cuanto a las etapas del proceso, las mayores concentraciones se ubican en facturas (221), en el tramo OC→HES (122) y en pagos (117), seguidas por OC→Facturas (74) y Facturas→Pagos (44). Estas etapas son especialmente sensibles porque se ubican cerca de la conformidad del servicio, la generación de la obligación, el registro contable y el desembolso. La simulación permitió observar, en consecuencia, que el modelo logra capturar alertas en puntos críticos del flujo P2P, particularmente en aquellos tramos donde la trazabilidad documental y financiera resulta más relevante para el control interno.

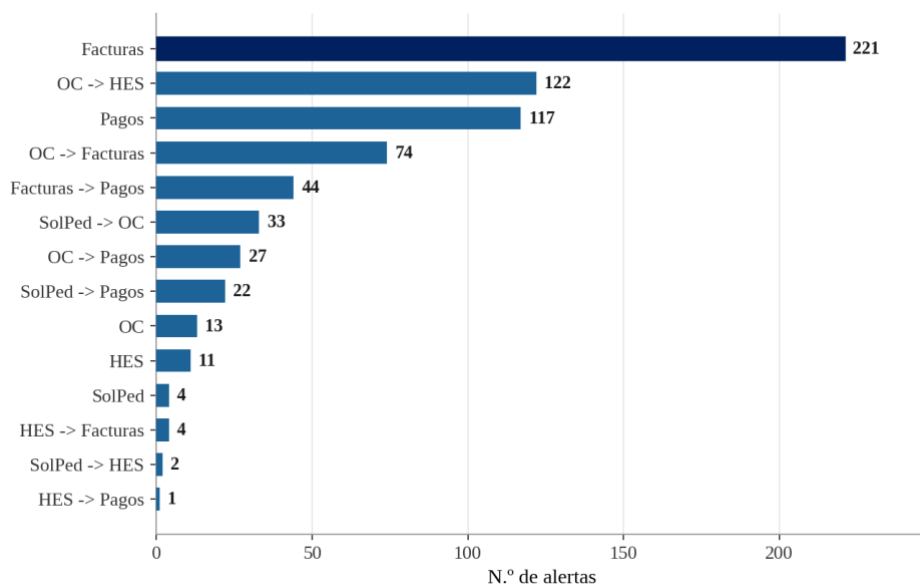


Figura 04. Distribución de alertas por etapa del proceso P2P
Nota. Elaboración propia a partir del informe de salida del modelo (Anexo 17).

Por último, la agrupación por proveedor muestra que un proveedor ficticio concentra 248 alertas, seguido por otro con 87 y por el resto del listado con cantidades menores. Como todos los proveedores son simulados, este ranking no debe interpretarse como una afirmación sobre empresas reales; su utilidad es demostrar que el modelo es capaz de identificar focos de revisión asociados a terceros específicos. En un escenario real, un ranking de esta naturaleza podría ayudar a priorizar la revisión de proveedores, contratos, cuentas bancarias o documentos con mayor acumulación de señales, mientras que en la simulación su valor radica en mostrar que el informe de salida permite agrupar alertas y facilitar su revisión.

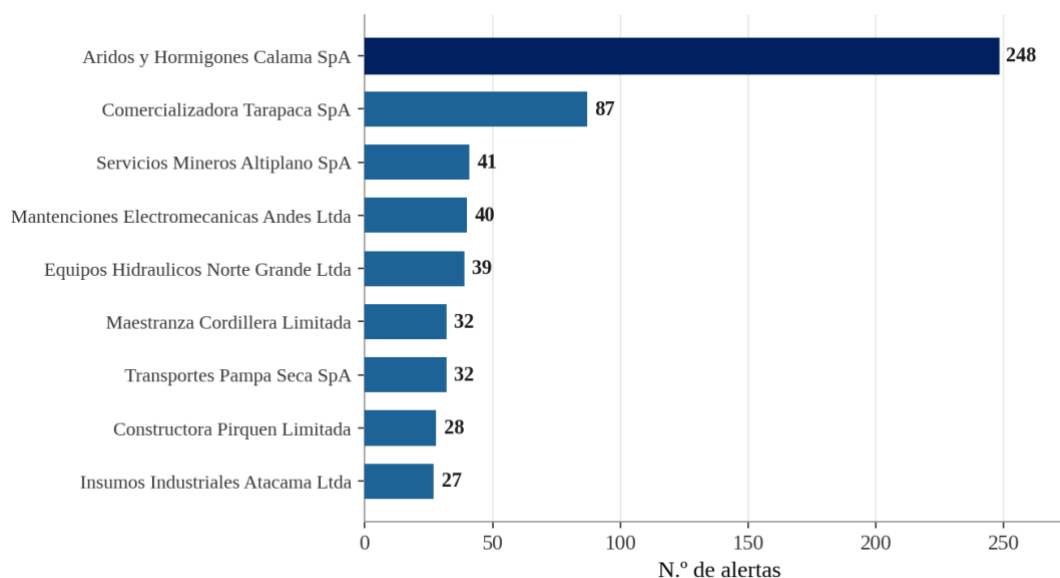


Figura 06. Proveedores ficticios con mayor número de alertas

Nota. Elaboración propia a partir del informe de salida del modelo (Anexo 17). Los nombres corresponden a entidades simuladas.

6.3.6. Matriz de alertas, trazabilidad y resumen de situaciones observadas

La hoja Matriz alertas es el componente que sostiene la trazabilidad⁴² del modelo, ya que contiene el detalle de cada alerta⁴³ levantada. Para cada observación, la matriz registra hasta treinta y un campos, entre ellos el identificador de la alerta, el código y la categoría de la prueba, su nombre y criticidad base, la situación observada, la etapa P2P y los documentos involucrados (SolPed, OC, HES, factura y pago o compensación), el proveedor, el identificador fiscal y los usuarios, las fuentes comparadas con sus campos y valores, la diferencia detectada, las fechas, el monto y la moneda, el archivo y la hoja de origen, el método y la confianza de vinculación, las variables cruzadas y la referencia a la matriz de anomalías esperadas. Esta estructura es clave porque permite saber no solo que existe una alerta, sino también qué documento, campo, valor y fuente la originaron.

A modo de ejemplo, la siguiente tabla resume una alerta de pago duplicado exacto levantada por la prueba DUP-07, utilizando proveedores ficticios. El registro muestra cómo la matriz conserva la información necesaria para que un revisor pueda ubicar el documento de respaldo y comprender el

⁴²**Trazabilidad:** posibilidad de recorrer el camino que va desde una alerta hasta el documento, campo, valor y fuente que la originaron.

⁴³**Alerta:** observación generada por el modelo cuando una operación cumple la condición de una prueba; constituye una señal de revisión y no una conclusión de irregularidad.

motivo de la alerta.

Tabla 14: Ejemplo de alerta trazable generada por el modelo.

Campo de la matriz	Valor registrado
ID de alerta	ALERTA-000302-DUP-07
Código de prueba	DUP-07
Categoría	Duplicidad
Nombre de la prueba	Pago duplicado exacto
Criticidad base	Alta
Etapas P2P	Pagos
Situación observada	Pago duplicado exacto (proveedor, monto, fecha y cuenta), con 2 ocurrencias.
Pago / compensación	2000007015
Proveedor (ficticio)	Suministros de Faena Quebrada SpA
Campo evaluado (Fuente A)	proveedor + importe_pago + fecha_pago + cuenta_bancaria
Valor observado	suministros de faena quebrada spa 6.100.000 07-05-2025 99001122
Registros coincidentes (Fuente B)	2 ocurrencias
Monto	\$6.100.000
Archivo origen	FBL1N_Pagos_Payment.xlsx
Método de vinculación	agrupación por clave compuesta
Confianza de vinculación	alta
Referencia a matriz esperada	DUP-07

Complementariamente, la hoja Resumen situaciones observadas presenta una síntesis agregada por prueba, que reúne el código, la categoría, el nombre y la criticidad de la prueba, la etapa P2P, el número de alertas, el período observado, los proveedores y usuarios destacados y una descripción agregada de la situación. Esta hoja facilita transformar la matriz detallada en una lectura ejecutiva, ya que permite pasar desde una revisión transaccional, registro por registro, hacia una lectura más resumida, útil para la elaboración de reportes de auditoría o de compliance.

El detalle completo de las alertas levantadas por cada una de las pruebas ejecutadas puede observarse en el archivo “**Informe_Forense_P2P_sintetico**”, incorporado como **Anexo 17**. Dicho archivo permite revisar individualmente los resultados generados por el modelo, incluyendo la prueba aplicada, la categoría correspondiente, la criticidad base, la situación observada y los antecedentes de trazabilidad asociados a cada alerta, constituyendo así el principal respaldo operativo de la simulación realizada.

6.4. Limitaciones de los resultados.

Los resultados de los apartados anteriores deben interpretarse dentro del alcance metodológico

de esta investigación. El modelo fue diseñado, implementado y simulado para observar su viabilidad funcional, su capacidad de estructurar pruebas analíticas y su utilidad preliminar para generar alertas trazables en el proceso Procure-to-Pay; no constituyen, por tanto, una validación definitiva ni evidencia concluyente de fraude, error o incumplimiento, sino una verificación controlada de su funcionamiento.

- En primer lugar, el modelo detecta anomalías, no fraude, es decir, identifica inconsistencias, duplicidades, quiebres de secuencia, temporalidades atípicas y relaciones relevantes que justifican una revisión posterior, pero no prueba irregularidades ni determina responsabilidades. Cada alerta es una señal de revisión; una alerta no equivale a fraude, la criticidad no equivale a culpabilidad y una anomalía no supone automáticamente un incumplimiento. Toda observación requiere revisión documental, análisis de contexto y juicio profesional.
- En segundo lugar, la simulación se realizó sobre una base sintética construida para representar un flujo Procure-to-Pay y activar el catálogo. Por ello, los resultados no representan la distribución real de riesgos de una operación minera ni permiten estimar tasas reales de fraude, error o incumplimiento. Como la base se preparó de forma controlada, con las fuentes, los campos y las relaciones necesarias, la ejecución completa de las cien pruebas refleja ese diseño. En un escenario real podrían faltar fuentes o variables, de modo que algunas pruebas se ejecutarían parcialmente o no se ejecutarían, lo que debe leerse como una limitación de disponibilidad de información y no como ausencia de riesgo.
- En tercer lugar, la utilidad del modelo depende de la calidad, la completitud, la consistencia y la trazabilidad de los archivos de entrada. Campos incompletos, formatos inconsistentes, documentos faltantes, maestros desactualizados o relaciones no trazables entre las etapas del flujo limitan su capacidad de reconstruir la operación y de levantar alertas confiables. La sola existencia de datos no garantiza un control efectivo: deben

estar integrados, disponibles y bien estructurados.

- En cuarto lugar, aunque el script incorpora normalización, sinónimos y coincidencia aproximada para homologar variables con nombres distintos, no puede aplicarse de forma automática a cualquier organización. Cada empresa tiene distintos sistemas ERP, nombres de columnas y formas de registrar aprobaciones, pagos o documentos, por lo que, antes de usarlo en una operación real, se requiere una etapa de adaptación, parametrización y prueba de homologación que considere su estructura de datos, sus maestros, sus reglas de negocio y sus umbrales de materialidad. Del mismo modo, los umbrales de monto, tiempo o similitud pueden requerir ajustes según el contexto: un pago anticipado puede ser riesgoso en un caso y estar justificado por contrato en otro.
- En quinto lugar, el modelo apoya la revisión, pero no reemplaza los controles preventivos, la segregación de funciones, la auditoría interna, el compliance ni el criterio profesional; su valor está en mejorar la cobertura, la oportunidad y la focalización de la revisión, mientras que la decisión final sobre cada alerta corresponde a una evaluación humana. Además, la investigación no mide sensibilidad, especificidad ni tasas de falsos positivos o negativos sobre datos reales: la simulación verifica el funcionamiento operativo, pero no permite afirmar niveles de efectividad o capacidad de detección en entornos reales.
- Por último, el modelo fue concebido como una base para fortalecer el control y avanzar hacia el monitoreo continuo, pero la tesis no implementa un sistema de ese tipo en producción, lo que exigiría integrarlo con sistemas reales, automatizar cargas periódicas, definir responsables y flujos de tratamiento de alertas y medir su efectividad en el tiempo. Su alcance es, además, acotado ya que se enfoca en el proceso de abastecimiento bajo una lógica Procure-to-Pay de una operación minera chilena, por lo que no abarca todos los procesos de una compañía, ni todos los riesgos corporativos, ni todos los

módulos de un ERP.

Estas limitaciones no invalidan el modelo, sino que delimitan su alcance. Su aporte radica en ofrecer una estructura analítica, trazable y adaptable, capaz de transformar los riesgos del abastecimiento en pruebas concretas y alertas revisables; debe entenderse como una herramienta de apoyo para fortalecer el control y orientar las revisiones, y no como una solución cerrada o definitiva.

7. Conclusión

La pregunta que orientó esta investigación fue de qué manera el análisis de datos forenses puede contribuir al fortalecimiento del control del proceso de abastecimiento en una operación minera chilena. La conclusión central que permite extraer el trabajo es que ese aporte no radica en la capacidad de probar fraude de forma automática, sino en la posibilidad de transformar datos dispersos y fragmentados del flujo Procure-to-Pay en alertas trazables, interpretables y priorizables. Dicho de otro modo, el valor del análisis de datos forenses no está en sustituir el criterio humano por un veredicto técnico, sino en convertir la trazabilidad del proceso en una capacidad concreta de control, capaz de orientar dónde, por qué y con qué prioridad debe dirigirse la revisión.

Para sostener esta conclusión conviene volver sobre el problema que dio origen al estudio. El abastecimiento minero no constituye una simple sucesión de compras, sino un proceso de alta materialidad económica, fuerte dependencia de terceros, elevado volumen documental y exposición permanente a riesgos de control. La investigación evidencia que, en un proceso con estas características, las revisiones manuales o basadas en muestras aisladas resultan estructuralmente insuficientes, no por una ausencia de controles definidos, sino porque la información que permitiría activarlos suele encontrarse dispersa entre distintos sistemas, reportes y documentos. De ahí que la verdadera condición crítica para prevenir, detectar y revisar anomalías no sea únicamente la existencia de controles, sino la trazabilidad documental y transaccional que conecta la solicitud de pedido, la orden de compra, la recepción, la factura y el pago.

Desde una perspectiva metodológica, el enfoque Procure-to-Pay fue la decisión que permitió que ese problema se volviera analizable. Al concebir el abastecimiento como un flujo de punta a punta, en el que cada etapa genera evidencia susceptible de ser cruzada con las demás, los riesgos dejaron de ser nociones abstractas para convertirse en relaciones observables entre documentos, usuarios, proveedores y registros. Sobre esa base se construyó lo que constituye el principal aporte metodológico de la investigación, un catálogo de cien pruebas analíticas organizadas en cinco categorías. El valor de este catálogo no reside en su extensión, sino en que opera como el puente que traduce el riesgo en regla. En

ese sentido, el modelo no solo identifica anomalías, sino que documenta por qué una situación merece ser revisada, lo que lo hace reproducible y defendible.

La implementación del catálogo mediante lenguaje Python permite concluir algo que trasciende su dimensión técnica. Su relevancia no está en el código en sí mismo, sino en que hizo replicable, ordenado y auditable un procedimiento de revisión que, de otro modo, dependería del esfuerzo manual y del criterio puntual de quien lo ejecuta. Al traducir las reglas del catálogo en una herramienta capaz de leer archivos heterogéneos, clasificar fuentes, homologar variables, reconstruir relaciones entre documentos y generar un informe de salida con alertas y trazabilidad, la programación introdujo una propiedad que el propio diagnóstico del problema reclamaba, la reproducibilidad. Cada ejecución deja constancia de lo que se revisó, bajo qué reglas y con qué resultado, de manera que la cobertura, la oportunidad y la auditabilidad de la revisión dejan de depender de la memoria o la disponibilidad de un analista.

La simulación con datos sintéticos cumplió, en este marco, una función epistemológica precisa. Los resultados obtenidos sugieren que el modelo es funcionalmente viable, en tanto logró leer la información, ejecutar la totalidad del catálogo y producir una salida consolidada y trazable en un escenario controlado. No obstante, la investigación es explícita en que esta simulación no constituye una validación estadística ni una prueba sobre datos reales, su aporte consiste en comprobar la coherencia interna entre el diseño y la implementación, y en confirmar que el modelo genera alertas interpretables y vinculadas a su origen documental.

Es precisamente en este punto donde la investigación da un paso que refuerza su validez práctica. Además del escenario sintético, el modelo fue aplicado de manera preliminar en el contexto laboral del investigador, sobre un flujo real de abastecimiento correspondiente a una investigación en curso. Por razones de confidencialidad no se revelan el nombre de la organización, sus proveedores o usuarios, ni montos específicos o datos identificables, el análisis se limita a describir las situaciones observadas y su relevancia para el control. El propósito de esta aplicación no fue emitir conclusiones sobre el caso, sino

verificar si las categorías analíticas diseñadas conservaban su utilidad al enfrentarse a información real y no preparada deliberadamente para activar las pruebas.

Los resultados de esa aplicación preliminar sugieren que sí. El modelo logró captar señales relevantes e irregularidades potenciales dentro del flujo, entre ellas una concentración de roles en un mismo usuario, que figuraba simultáneamente como solicitante y aprobador en distintas etapas del proceso, lo que apunta a una posible brecha de segregación de funciones y relaciones entre ese usuario y un proveedor adjudicado de forma directa, que configuran la señal de un eventual conflicto de interés. Adicionalmente, la ausencia de hojas de entrada de servicio respecto de facturas ya registradas, que evidencia un quiebre de trazabilidad entre la recepción y la facturación.

La convergencia de estos elementos permite concluir que la investigación respondió a su pregunta y cumplió sus objetivos.

El aporte de la investigación puede leerse en dos planos complementarios. En lo académico, el trabajo contribuye al articular en un modelo aplicado disciplinas que suelen abordarse por separado (auditoría forense, analítica de datos, control interno, compliance y gestión del abastecimiento minero), ofreciendo una forma ordenada de traducir riesgos en pruebas y señales. En lo práctico, el modelo entrega una herramienta capaz de apoyar a la auditoría interna, al compliance operacional, a la gestión de terceros y a la revisión de riesgos del proceso P2P, al focalizar la atención en las operaciones que más la requieren y dotar a esas funciones de información más estructurada y accionable.

Estas conclusiones deben interpretarse, sin embargo, dentro de límites claros. El modelo detecta anomalías y señales de alerta, pero no determina fraude ni responsabilidades, su rendimiento depende de la calidad, la completitud y la disponibilidad de los datos, requiere parametrización y adaptación según las particularidades de cada operación, y la simulación sintética, por su naturaleza, no reemplaza una validación sobre datos reales. Por sobre todo, la interpretación final de cada alerta exige juicio profesional, revisión documental y conocimiento del contexto.

Hacia el futuro, los resultados sugieren una línea natural de evolución. El modelo puede avanzar desde una herramienta de revisión hacia un esquema de monitoreo continuo, integrarse con los sistemas ERP de la operación, incorporar tableros de alertas para el seguimiento de las observaciones, parametrizar sus umbrales según criterios de materialidad y validarse progresivamente sobre datos reales. En esa trayectoria, la aplicación preliminar ya realizada en un contexto laboral constituye un primer indicio del potencial del modelo para insertarse en la práctica efectiva del control.

En definitiva, la investigación permite concluir que el análisis de datos forenses puede fortalecer el control del abastecimiento minero al convertir la trazabilidad del proceso en una capacidad concreta de prevención y revisión. En procesos intensivos en terceros, documentos y pagos, la prevención no depende solo de contar con controles definidos, sino de disponer de información conectada, revisable y accionable y es justamente esa conexión la que el modelo contribuye a construir.

8. Referencias

- Sociedad Nacional de Minería. (2025). Cadenas de valor mineras en Chile: Desafíos, oportunidades y miradas para el futuro. <https://www.sonami.cl/v2/wp-content/uploads/2025/11/Estudio-Cadenas-Valor-Mineria-V1.pdf>
- Comisión Chilena del Cobre. (2025a). Informe cartera de proyectos de inversión minera 2025–2034. <https://www.cochilco.cl/web/informe-cartera-de-proyectos-de-inversion-minera-2025-2034/>
- Comisión Chilena del Cobre. (2025b). Informe proyección de la producción de cobre en Chile. Periodo 2025–2034. <https://www.cochilco.cl/web/informe-proyeccion-de-la-produccion-de-cobre-en-chile-periodo-2025-2034/>
- Comisión Chilena del Cobre. (2024). Participación de proveedores en operaciones y proyectos: Gasto 2023. <https://www.cochilco.cl/web/download/918/2024/12831/participacion-de-proveedores-en-operaciones-y-proyectos-gasto-2023.pdf>
- Subsecretaría de Relaciones Económicas Internacionales & ProChile. (2024). Reporte de exportaciones: Proveedores de la minería chilena. <https://www.subrei.gob.cl/estudios-y-documentos/documentos/detalle-otras-fichas-y-reportes/reporte-de-exportaciones-proveedores-de-la-miner%C3%ADa-chilena>
- TrendTIC. (2026, 30 de enero). Compliance con IA en minería: Automatización permite ahorros de hasta US\$2,5 millones y más de 100 mil documentos por faena. <https://www.trendtic.cl/2026/01/compliance-con-ia-en-mineria-automatizacion-permite-ahorros-de-hasta-us25-millones-y-mas-de-100-mil-documentos-por-faena/>
- Association of Certified Fraud Examiners. (2024). Occupational fraud 2024: A report to the nations.

<https://www.acfe.com/-/media/files/acfe/pdfs/rtn/2024/2024-report-to-the-nations.pdf>

PwC. (2024). Global economic crime survey 2024.

<https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html>

Biblioteca del Congreso Nacional de Chile. (2023). Ley N° 21.595: Ley de delitos económicos.

<https://www.bcn.cl/leychile/navegar?idNorma=1195119>

Comisión para el Mercado Financiero. (2021). Norma de Carácter General N° 461.

https://www.cmfcile.cl/normativa/ncg_461_2021.pdf

Cárdenas, L. (2025, 1 de diciembre). El fraude interno que denuncia Minera Los Pelambres con más de \$8.000 millones en perjuicios. La Tercera. <https://www.latercera.com/pulso/noticia/el-fraude-interno-que-denuncia-minera-los-pelambres-con-mas-de-8000-millones-en-perjuicios/>

Consejo Minero. (2026). Cifras actualizadas de la minería: Marzo 2026. <https://consejominero.cl/wp-content/uploads/2026/04/20260420-CAM-marzo-2.pdf>

Lagos, J. (2023). Nuevo modelo de gestión de abastecimiento para una compañía minera [Tesis de magíster, Universidad de Chile]. Repositorio Académico Universidad de Chile. <https://repositorio.uchile.cl/bitstream/handle/2250/198708/Nuevo-modelo-de-gestion-de-abastecimiento-para-una-compania-minera.pdf>

ChileCompra. (2022). Manual de procedimiento de abastecimiento: Dirección de Compras y Contratación Pública. <https://www.chilecompra.cl/wp-content/uploads/2022/08/Manual-de-Abastecimiento-Direccion-de-Compras-y-Contratacion-Publica.pdf>

SAP. (2026). ¿Qué es procure-to-pay (P2P): La guía completa?

<https://www.sap.com/latinamerica/resources/what-is-procure-to-pay>

Oracle. (s. f.). The procure-to-pay business process in a WMS integration.

https://docs.oracle.com/cd/G17334_01/fscm92pbr52/eng/fscm/fstp/TheProcure-to-PayBusinessProcessinaWMSIntegration-c9fc5e.html

Asociación Chilena de Seguridad. (2026). Procedimiento de pago a proveedores nacionales.

<https://www.achs.cl/docs/librariesprovider2/nosotros-documentos/procedimiento-pago-a-proveedores.pdf>

Deloitte. (s. f.). Gestión de accesos y segregación de funciones.

<https://www.deloitte.com/es/es/services/consulting/services/gestion-de-accesos.html>

U.S. Department of Justice. (2024). Evaluation of corporate compliance programs.

<https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl>

Association of Certified Fraud Examiners. (s. f.). Anti-fraud data analytics tests.

<https://www.acfe.com/fraud-resources/fraud-risk-tools---coso/anti-fraud-data-analytics-tests>

Lyra, M. S., Damásio, B., Pinheiro, F. L., & Bacao, F. (2022). Fraud, corruption, and collusion in public procurement activities: A systematic literature review on data-driven methods.

Applied Network Science, 7, Article 83. <https://doi.org/10.1007/s41109-022-00523-6>

Santos, E. S. dos, Santos, M. M. dos, Castro, M., & Carvalho, J. T. (2025). Detection of fraud in public procurement using data-driven methods: A systematic mapping study. EPJ Data

Science, 14, Article 50. <https://doi.org/10.1140/epjds/s13688-025-00569-3>

Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control—Integrated framework: Executive summary.

https://www.sechistorical.org/collection/papers/2010/2013_0501_COSOInternal.pdf

International Organization for Standardization. (2021). Compliance management systems—Requirements with guidance for use (ISO Standard No. 37301:2021).

<https://www.iso.org/standard/75080.html>

International Organization for Standardization. (2025). Compliance management systems—Guidance for the evaluation of effectiveness (ISO Standard No. 37302:2025).

<https://www.iso.org/standard/37302>

Biblioteca del Congreso Nacional de Chile. (2009). Ley N° 20.393: Establece la responsabilidad penal de las personas jurídicas en los delitos que indica.

<https://www.bcn.cl/leychile/navegar?idNorma=1008668>

The Institute of Internal Auditors. (2018). Auditing third-party risk management.

<https://www.theiia.org/globalassets/documents/content/articles/guidance/practice-guides/practice-guide-auditing-third-party-risk-management.pdf>

International Auditing and Assurance Standards Board. (2025). ISA 240 (Revised), The auditor's responsibilities relating to fraud in an audit of financial statements.

<https://www.iaasb.org/publications/isa-240-revised-auditor-s-responsibilities-relating-fraud-audit-financial-statements>

The Institute of Internal Auditors. (2024). Global internal audit standards.

<https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/>

Castellanos Polo, O. C., Velásquez Ochoa, J. A., Arboleda Posada, G. I., & Suaza Arcila, J. O.

(2022). La auditoría forense: ¿Un instrumento esencial de control interno en las entidades públicas? *Administración & Desarrollo*, 52(1), 95–112.

<https://doi.org/10.22431/25005227.vol52n1.6>

Nigrini, M. J. (2020). *Forensic analytics: Methods and techniques for forensic accounting investigations* (2nd ed.). John Wiley & Sons.

Vona, L. W. (2017). *Fraud data analytics methodology: The fraud scenario approach to uncovering fraud in core business systems*. John Wiley & Sons.

Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). *Fraud analytics using descriptive, predictive, and social network techniques: A guide to data science for fraud detection*. John Wiley & Sons.

Rezaee, Z., & Wang, J. (2019). Relevance of big data to forensic accounting practice and education. *Managerial Auditing Journal*, 34(3), 268–288. <https://doi.org/10.1108/MAJ-08-2017-1633>

Kuenkaikaew, S., & Vasarhelyi, M. A. (2013). The predictive audit framework. *The International Journal of Digital Accounting Research*, 13, 37–71. https://doi.org/10.4192/1577-8517-v13_2

The Institute of Internal Auditors. (2011). *GTAG 16: Data analysis technologies*.

<https://www.theiia.org/en/content/guidance/recommended/supplemental/gtags/gtag-data-analysis-technologies/>

The Institute of Internal Auditors. (2015). GTAG 3: Continuous auditing: Coordinating continuous auditing and monitoring to provide continuous assurance (2nd ed.).

<https://www.theiia.org/globalassets/documents/content/articles/guidance/gtag/gtag-3-continuous-auditing/gtag-3-continuous-auditing-2nd-edition.pdf>

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory*, 36(4), 1–27.

<https://doi.org/10.2308/ajpt-51684>

9. Apéndice

9.1. Apéndice A: Listado de anexos incorporados en la investigación

Anexo	Nombre correspondiente
Anexo 01	Modelo de Análisis de Datos Forense.py
Anexo 02	CDHDR_LogsModificacion_ChangeLog.docx
Anexo 03	FBL1N_Pagos_Payment.xlsx
Anexo 04	FK03_CuentasBancarias_BankMaster.pdf
Anexo 05	FS00_CuentasContables_GLAccount.xlsx
Anexo 06	KS03_CentrosCosto_CostCenter.xlsx
Anexo 07	ME2N_OrdenesCompra_PurchaseOrder.xlsx
Anexo 08	ME33K_Contratos_OutlineAgreement.docx
Anexo 09	ME51N_SolPed_PurchaseRequisition.xlsx
Anexo 10	MIRO_Facturas_Invoice.xlsx
Anexo 11	ML84_HES_EntrySheet.xlsx
Anexo 12	NC_Notas_de_Credito_Anulaciones_Reversas.xlsx
Anexo 13	OX01_MaestroOrganizacional_EnterpriseStructure.xlsx
Anexo 14	SU01_MaestroUsuarios_UserMaster.xlsx
Anexo 15	Workflow_Releases_aprobaciones.pdf
Anexo 16	XK03_MaestroProveedores_VendorMaster.xlsx
Anexo 17	Informe_Forense_P2P_sintetico.xlsx

9.2. Apéndice B: Listado de figuras incorporadas en la investigación.

Figura	Nombre correspondiente
Figura 01	Modelo conceptual del flujo analítico-forense aplicado al proceso de abastecimiento P2P
Figura 02	Distribución de alertas por categoría
Figura 03	Distribución de alertas por criticidad base
Figura 04	Distribución de alertas por etapa del proceso P2P
Figura 05	Proveedores ficticios con mayor número de alertas

9.3. Apéndice C: Listado de tablas incorporadas en la investigación.

Tabla	Nombre correspondiente
Tabla 01	Requerimientos técnicos de las pruebas de consistencia
Tabla 02	Requerimientos técnicos de las pruebas de duplicidad
Tabla 03	Requerimientos técnicos de las pruebas de secuencia
Tabla 04	Requerimientos técnicos de las pruebas relacionales
Tabla 05	Requerimientos técnicos de las pruebas de temporalidad
Tabla 06	Componentes funcionales del script de análisis forense
Tabla 07	Bibliotecas de Python utilizadas en el modelo
Tabla 08	Parámetros de interacción para la ejecución del script

Tabla	Nombre correspondiente
Tabla 09	Categorías analíticas ejecutadas por el modelo
Tabla 10	Estructura del archivo Excel de salida del modelo
Tabla 11	Extracto del prompt utilizado para generar datos sintéticos
Tabla 12	Requerimientos de generación de la base sintética
Tabla 13	Archivos sintéticos del flujo P2P utilizados en la simulación
Tabla 14	Hojas del informe de salida generado por el modelo
Tabla 15	Métricas generales de ejecución del modelo
Tabla 16	Ejemplo de alerta trazable generada por el modelo