Diseño de un Modelo de Continuidad del Negocio y Aseguramiento de la Información para Laminados de Occidente S.A. basado en una Arquitectura de Migración a Microsoft Azure

Jose Julian Delgado Diaz

Especialización en Seguridad Informática, Universidad Piloto de Colombia

Investigación 2

Ingeniera: Helen Nahir. Barbosa Hurtado

2 de diciembre de 2025

Contenido

Resumen 11

Abstract 13

Introducción 15

Planteamiento del Problema 15

Formulación del Problema 16

Justificación 17

Objetivos 19

Objetivo General 19

Objetivos Específicos 19

Hipótesis 21

Hipótesis Nula 21

Alcance y Limitaciones del Proyecto 22

Marco Teórico 24

Gestión de la Continuidad del Negocio y Resiliencia Organizacional 24

Marco Normativo y Estándares de Referencia 25

El Ecosistema ISO 22301 e ISO/TS 22317 25

NIST SP 800-34 Rev. 1: Planificación de Contingencia para TI 26

ISO/IEC 27001:2022 y Seguridad de la Información 26

Gestión de Riesgos de Seguridad de la Información (ISO/IEC 27005) 26

Zero Trust Security 27

Metodologías de Análisis y Métricas de Recuperación 29

Análisis de Impacto al Negocio (BIA) y Evaluación Multidimensional 29

Definición Técnica de Métricas de Continuidad (MTPD, RTO, RPO) 29

Computación en la Nube y Azure Well-Architected Framework....30
Pilar de Fiabilidad (Reliability) y Continuidad en Azure....32
Arquitectura de Alta Disponibilidad y Recuperación Ante Desastres....33
Zonas de Disponibilidad y Replicación Geográfica....35
Trabajos y Estudios Previos Sobre Continuidad en la Nube....36
Sistemas de Control Industrial y Convergencia IT/OT....40
Marco Referencial....42
Misión:....43
Visión:....44
Estructura Organizacional....44
Descripción de Áreas Clave para el Modelo de Continuidad....45
Bases Legales....47
Protección de Datos Personales (Habeas Data)....47
Normativa sobre Ciberseguridad y Delitos Informáticos....48
Validez Jurídica de la Información Digital....48
Diseño Metodológico de la Investigación....49
Enfoque y Tipo de Investigación....49
Diseño de la Investigación....50
Población y Muestra....51
Técnicas e Instrumentos de Recolección de la Información....53
Revisión Documental....53
Entrevistas Semiestructuradas....53
Levantamiento Técnico de la Infraestructura de TI....54
Análisis de Impacto al Negocio (BIA)....55
Matriz de Riesgos....56

Revisión de Marcos de Referencia y Buenas Prácticas 57
Procedimiento y Fases del Estudio 58
Fase 1 – Caracterización de la Organización y de la Infraestructura Tecnológica 58
Fase 2 – Análisis de Riesgos y Análisis de Impacto al Negocio (BIA) 60
Fase 3 – Diseño del Modelo de Continuidad del Negocio y Aseguramiento de la Información 61
Fase 4 – Diseño y Validación de la Arquitectura de Referencia en Microsoft Azure 62
Técnicas de Análisis de la Información 64
Análisis Cualitativo 64
Análisis Cuantitativo de Riesgos y Continuidad 65
Análisis Comparativo AS-IS vs TO-BE de RTO/RPO 66
Triangulación de Fuentes 67
Matriz de Relación entre Objetivos, Actividades, Instrumentos y Entregables 68
Variables e Indicadores del Estudio 71
Variable Independiente: 71
Variables Dependientes Principales: 71
Resultados 74
Diagnóstico AS-IS de la Infraestructura Tecnológica de Laminados de Occidente S.A. 74
Servidores y Aplicaciones Críticas 77
Obsolescencia, Falta de Redundancia y Concentración de Servicios 78
Resultados del Análisis de Impacto al Negocio (BIA) 80
Enfoque Metodológico y Normativo 80
Definición de Parámetros y Escalas Utilizadas 81
Tabla 5. (continuación) 82
Mapeo de Dependencias Críticas 82

Periodo Máximo Tolerable de Interrupción (MTPD) 83
Objetivo de Tiempo de Recuperación (RTO) 84
Objetivo de Punto de Recuperación (RPO) 84
Análisis del BIA Detallado por Dimensiones 87
MES/SCADA Ignition 7.8.5 87
ERP SIESA Gcuno 8 (Aplicación + Base de Datos) 88
Priorización de Servicios y Brechas de Continuidad 90
Definición de Parámetros Ideales para la Arquitectura en Azure (TO-BE) 90
Matriz de Resultados del BIA y Requisitos de Recuperación 91
Análisis de Brecha (Gap Analysis): AS-IS vs. Necesidad del Negocio 92
Gestión y Valoración de Riesgos de Seguridad y Continuidad 93
Enfoque metodológico: ISO/IEC 27005 93
Fase 1: Identificación y Clasificación de Activos 94
Fase 2: Identificación de Amenazas y Vulnerabilidades 95
Fase 3: Escalas de Valoración del Riesgo 96
Fase 4: Estrategia de Tratamiento y Riesgo Residual 100
Conclusión del Análisis de Riesgos 101
Diseño de la Arquitectura de Referencia en Microsoft Azure (TO-BE) 101
Estrategia de Regiones y Alta Disponibilidad 104
Especificación de Componentes de Infraestructura 104
Arquitectura de Seguridad y Segmentación (Zero Trust) 105
Conectividad Híbrida y Protección de Flujos OT 106
Validación de la Arquitectura frente a Metas de Continuidad 107
Conclusión del Diseño Arquitectónico y Cumplimiento del Objetivo 108
Plan de Migración Gradual y Transición de Servicios Críticos 109

Estrategia de Migración: Rehosting y Replatforming 109
Fases de Ejecución y Cronograma Lógico 110
Gestión de Riesgos de Transición y Plan de Retorno (Rollback) 111
Estructura de Gobierno y Asignación de Responsabilidades 112
Cronograma Maestro de Implementación (Horizonte 1 Año) 113
Pruebas de Aceptación y Validación (Go/No-Go) 115
Lineamientos de Monitoreo, Capacitación y Mejora Continua del Modelo 115
Estrategia de Observabilidad y Monitoreo Proactivo 116
Plan de Capacitación y Gestión del Cambio 117
Ciclo de Mejora Continua y Mantenimiento del Modelo (PDCA) 118
Conclusión del Modelo de Gobierno 119
Validación de Hipótesis y Respuesta a la Pregunta de Investigación 119
Respuesta a la Formulación del Problema 119
Contraste y Validación de Hipótesis 120
Discusión 123
Síntesis interpretativa de los resultados 123
Comparación con teorías y marcos de referencia 124
Explicación de hallazgos relevantes 126
Implicaciones para la gestión de TI y la continuidad del negocio 127
Conclusiones 128
Referencias 130
Anexos 135
Anexo A: Guía de entrevista semiestructurada – Gerente General 135
Anexo B: Guía de entrevista semiestructurada – Jefe de Planta / Producción (MES/SCADA). 138
Anexo C: Guía de entrevista semiestructurada – Jefe de Logística y Distribución. 140

Anexo D: Guía de entrevista semiestructurada – Responsable de Tecnología / Sistemas. 142

Anexo E: Guía de entrevista semiestructurada – Usuario clave ERP (Administración y Finanzas). 144

Anexo F: Guía de entrevista semiestructurada – Usuario clave ERP (Área Comercial). 146

Lista de Figuras

Figura 1. Principios Zero Trust.....28

Figura 2. Pilares del Marco de Buena Arquitectura (Well-Architected Framework) para la Industria.....32

Figura 3. Costo promedio de una brecha de datos según la duración del ciclo de vida del incidente 39

Figura 4. Costo promedio de una brecha de datos por industria (Comparativo 2024-2025).....41

Figura 5. Estructura Organizacional de Laminados de Occidente S.A.....45

Figura 6. Esquema AS-IS de la infraestructura tecnológica de Laminados de Occidente S.A. ...75

Figura 7. Arquitectura de Referencia TO-BE propuesta en Microsoft Azure para los servicios críticos de Laminados de Occidente S.A.....103

Lista de Tablas.

Tabla 1. Matriz de relación entre objetivos específicos, actividades, técnicas e instrumentos y entregables. 69

Tabla 2. Variables e indicadores del estudio 72

Tabla 3. Servidores y aplicaciones críticas de Laminados de Occidente S.A. (escenario AS-IS) 77

Tabla 4. Principales problemas identificados en la infraestructura AS-IS 78

Tabla 5. Criterios de Evaluación de Impacto Multidimensional 81

Tabla 6. Relación Procesos - Servicios TI - Infraestructura (AS-IS). 82

Tabla 7. Resumen del BIA para servicios críticos (escenario AS-IS) 86

Tabla 8. Matriz de Resultados del BIA y Definición de Requisitos (RTO/RPO). 91

Tabla 9. Análisis de Brecha de Continuidad (Gap Analysis) 92

Tabla 10. Inventario y Clasificación de Activos Críticos de Información (AS-IS) 95

Tabla 11. Diccionario de Amenazas y Vulnerabilidades Identificadas 96

Tabla 12. Escala de Probabilidad de Ocurrencia del Riesgo 97

Tabla 13. Matriz de Evaluación de Riesgos (Mapa de Calor 5x5) 98

Tabla 14. Niveles de Clasificación y Directrices de Tratamiento del Riesgo 98

Tabla 15. Matriz de Riesgos Inherente y Priorización (Escenario AS-IS) 99

Tabla 16. Plan de Tratamiento y Proyección de Riesgo Residual 100

Tabla 17. Especificación de Componentes de Infraestructura y Servicios Azure (TO-BE) 105

Tabla 18. Matriz de Controles de Seguridad y Segmentación de Red 106

Tabla 19. Estrategia de Conectividad Híbrida IT/OT 107

Tabla 20. Mecanismos de Resiliencia y Alineación con Metas de Recuperación 107

Tabla 21. Definición de Estrategias de Migración por Servicio 110

Tabla 22. Plan Detallado de Migración Gradual y Ventanas de Riesgo 111

Tabla 23. Matriz de Riesgos de Transición y Protocolos de Rollback 112

Tabla 24. Matriz de Responsabilidades para la Migración (Modelo RACI) 113

Tabla 25. Cronograma de Ejecución del Proyecto de Migración y Continuidad.....114

Tabla 26. Matriz de Monitoreo y Alertas para Servicios Críticos (TO-BE).....116

Tabla 27. Plan de Desarrollo de Competencias y Capacitación.....117

Tabla 28. Calendario de Actividades de Mantenimiento y Mejora Continua.....118

Resumen

Laminados de Occidente S.A. es una empresa colombiana dedicada a la fabricación de tubos colapsibles y envases laminados para los sectores farmacéutico, cosmético e industrial. Su operación depende de sistemas de información críticos, especialmente el ERP Siesa y el sistema SCADA de planta, los cuales hoy se ejecutan sobre una infraestructura local envejecida, sin redundancia ni mecanismos formales de continuidad del negocio. Esta situación expone a la organización a riesgos de indisponibilidad, pérdida de datos y fallas en cadena que podrían afectar la producción, la trazabilidad y el cumplimiento de requisitos regulatorios.

Con el objetivo de fortalecer la resiliencia operativa de Laminados de Occidente S.A. ante su futura migración a Microsoft Azure, este trabajo estructura un modelo de continuidad del negocio y seguridad de la información. Bajo un enfoque descriptivo y aplicado, la propuesta articula marcos de referencia clave (ISO 22301, ISO/IEC 27001, NIST SP 800-34 y el Azure Well-Architected Framework) con la realidad tecnológica de la empresa. A partir de un diagnóstico técnico de la situación actual, se determinaron las vulnerabilidades de los servicios críticos, sus interdependencias y las brechas de seguridad que deben ser mitigadas en el entorno de nube.

Con estos resultados se definen principios de continuidad (resiliencia, redundancia, alta disponibilidad y automatización), así como objetivos de recuperación (RTO, RPO) y acuerdos de nivel de servicio (SLA) acordes con la realidad operativa de Laminados de Occidente S.A.Sobre esta base, se propone una arquitectura de referencia en Microsoft Azure, basada en regiones y zonas de disponibilidad, que incorpora mecanismos de respaldo, replicación geográfica, control de acceso y monitoreo centralizado.

El resultado es un modelo integral de continuidad y aseguramiento de la información que no pretende implementar la migración, sino dejar trazada una hoja de ruta técnica y de gobernanza. Este modelo busca reducir la exposición a fallas operativas, mejorar los tiempos de recuperación y sentar las bases para una modernización tecnológica planificada, alineada con buenas prácticas internacionales y con las necesidades reales de la organización.

Palabras Clave: Continuidad del negocio, Aseguramiento de la información, Migración a la nube, Microsoft Azure, Resiliencia operativa, Recuperación ante desastres

Abstract

Laminados de Occidente S.A. is a Colombian company dedicated to the manufacture of collapsible tubes and laminated packaging for the pharmaceutical, cosmetic, and industrial sectors. Its operations rely on critical information systems, specifically the Siesa ERP and the plant SCADA system, which currently run on aging on-premises infrastructure lacking redundancy or formal business continuity mechanisms. This scenario exposes the organization to risks of unavailability, data loss, and cascading failures that could impact production, traceability, and compliance with regulatory requirements.

With the objective of strengthening the operational resilience of Laminados de Occidente S.A. ahead of its future migration to Microsoft Azure, this work structures a business continuity and information security model. Adopting a descriptive and applied approach, the proposal articulates key frameworks (ISO 22301, ISO/IEC 27001, NIST SP 800-34, and the Azure Well-Architected Framework) with the company's technological reality. Based on a technical diagnosis of the current situation, the vulnerabilities of critical services, their interdependencies, and the security gaps that must be mitigated in the cloud environment were determined.

From these results, continuity principles (resilience, redundancy, high availability, and automation) are defined, alongside recovery objectives (RTO, RPO) and service level agreements (SLA) aligned with Laminados de Occidente S.A.' operational reality. On this basis, a reference architecture in Microsoft Azure is proposed, designed across regions and availability zones, incorporating backup mechanisms, geographic replication, access control, and centralized monitoring.

The outcome is a comprehensive business continuity and information assurance model that does not aim to implement the migration, but rather to establish a technical and governance

roadmap. This model seeks to reduce exposure to operational failures, improve recovery times, and lay the foundations for a planned technological modernization, aligned with international best practices and the organization's specific needs.

Keywords: Business continuity, Information assurance, Cloud migration, Microsoft Azure, Operational resilience, Disaster recovery.

Introducción

Planteamiento del Problema

Laminados de Occidente S.A. ha crecido, y ese crecimiento se nota en planta, en pedidos y en decisiones que dependen cada vez más de los sistemas de información. El punto es que la tecnología que los sostiene no avanzó al mismo ritmo. Hoy conviven servidores viejos, sistemas operativos fuera de soporte y copias de seguridad que no siempre se prueban. Si un equipo crítico falla en el momento menos oportuno, la empresa puede perder horas valiosas de producción y, peor aún, datos que son la base de su trazabilidad y de sus decisiones diarias.

No es un problema aislado ni solo técnico es un riesgo de continuidad del negocio. La operación depende de que el ERP (Siesa) y sus piezas asociadas estén disponibles, que la información fluya y que, si algo se rompe, exista un plan claro para seguir operando o recuperarse sin dramas. La experiencia muestra que las organizaciones que no diseñan su continuidad terminan reaccionando tarde y a mayor costo, con impactos en productividad y en reputación. De ahí la necesidad de pasar de apagar incendios a diseñar la resiliencia, fijar objetivos de recuperación (RTO/RPO), ordenar responsabilidades y definir cómo se protege y recupera la información.

En ese camino, la computación en la nube no se plantea como una moda sino como un medio para ganar estabilidad y capacidad de respuesta. Microsoft documenta de forma abierta la diferencia entre continuidad, alta disponibilidad y recuperación ante desastres, y cómo aterrizarlas en arquitecturas confiables (Microsoft, 2025). La idea no es mover servidores a Azure sin más, sino diseñar una solución con redundancia, pruebas y monitoreo que se ajuste a lo que Laminados de Occidente S.A. realmente necesita, y que respalde su día a día en planta.

Además, el tema no se resuelve solo con adquisición de productos, también exige marco conceptual y de gobierno. La ISO 22301 da el lenguaje y el esqueleto para gestionar la continuidad del negocio como un sistema que se planifica, se opera y se mejora de forma continua (ISO, 2019). Y el NIST SP 800-34 Rev.1 explica, con guías prácticas, cómo estructurar planes de contingencia de TI que conectan prevención, respuesta y recuperación (NIST, 2010). Con estas referencias como base, el proyecto se enfoca en diseñar (no implementar) un modelo de continuidad para Laminados de Occidente S.A., alineado con buenas prácticas y con la realidad de su operación.

Formulación del Problema

¿Cómo el diseño de un modelo de continuidad del negocio y aseguramiento de la información, basado en la migración de los servicios críticos de TI de Laminados de Occidente S.A. a Microsoft Azure, puede fortalecer la continuidad operativa, la protección de la información y la recuperación oportuna de los sistemas y datos críticos ante fallas de infraestructura?

Justificación

Laminados de Occidente S.A. se encuentra en un punto en el que su crecimiento industrial no se refleja del todo en su infraestructura tecnológica. La empresa opera con sistemas que ya cumplieron su ciclo de vida útil, con servidores locales que no ofrecen redundancia, copias de seguridad poco confiables y una gestión de información que depende demasiado de la intervención manual. Todo esto ha hecho evidente la necesidad de diseñar una estrategia de continuidad de negocio que garantice la estabilidad operativa y la protección de los datos críticos ante cualquier eventualidad.

En este escenario, la nube se convierte en una oportunidad para modernizar la infraestructura sin detener la producción. Sin embargo, trasladar los servicios a la nube sin un diseño estructurado podría generar más riesgos que beneficios. Por eso, este trabajo se centra en diseñar un modelo de continuidad del negocio y aseguramiento de la información, como paso previo a cualquier migración. Este diseño servirá como una hoja de ruta técnica y estratégica que oriente a la empresa en cómo proteger su operación y mantener sus servicios disponibles incluso frente a fallos inesperados.

La importancia del proyecto radica en que aborda un problema real de sostenibilidad tecnológica. De acuerdo con IBM (2024), la alta disponibilidad se define como la capacidad de un sistema para permanecer accesible incluso ante el fallo de uno o más componentes. Este concepto no se limita a evitar caídas del sistema, sino que constituye un proceso continuo de planificación, supervisión y mejora que debe integrarse en la cultura organizacional. Asimismo, la norma ISO 22301 (International Organization for Standardization [ISO], 2019) subraya que la continuidad del negocio no debe depender de acciones reactivas, sino de una planificación basada en riesgos, que anticipe escenarios críticos y establezca procedimientos claros de

recuperación. Esto resulta especialmente relevante en entornos industriales como el de Laminados de Occidente S.A., donde los tiempos de parada no solo afectan la productividad, sino también la seguridad y la trazabilidad de los productos.

Por otra parte, el diseño de un modelo de continuidad no solo beneficia a la empresa internamente; también fortalece su reputación ante clientes y aliados, al demostrar que cuenta con políticas de resiliencia y recuperación acordes con las buenas prácticas internacionales. Como detallan los estudios de impacto económico publicados en Microsoft Learn (Forrester Consulting, 2024), las organizaciones que integran mecanismos de continuidad y resiliencia (como Azure Site Recovery) logran reducir hasta un 80% el tiempo de inactividad no planificado, mitigando drásticamente el impacto operativo de los incidentes críticos gracias a la automatización y la replicación geográfica. Este proyecto no busca desarrollar infraestructura, sino diseñar conocimiento aplicado, un esquema sostenible y adaptable a las condiciones reales de la empresa.

El proyecto se justifica porque atiende una necesidad prioritaria de Laminados de Occidente S.A., garantizar la continuidad de sus operaciones a través de un diseño sólido, escalable y alineado con estándares internacionales, permitiendo que la organización avance hacia la nube de manera planificada y segura. Además, aporta un valor académico al integrar principios de seguridad informática, resiliencia organizacional y gobernanza tecnológica en un caso real del contexto empresarial colombiano.

Objetivos

El diseño de un modelo de continuidad requiere mirar más allá de la tecnología. Es necesario comprender cómo funcionan los procesos, qué servicios son críticos, cómo se manejan los datos y qué impacto tendría una interrupción prolongada. A partir de ese análisis se podrán definir las estrategias más adecuadas para proteger la información, reducir tiempos de recuperación y planificar el crecimiento tecnológico con base en buenas prácticas y estándares internacionales.

Con esto, el proyecto busca aportar una solución práctica, pensada desde la realidad de la empresa, que sirva como guía para futuras decisiones de inversión tecnológica y que refuerce la seguridad de sus operaciones diarias.

Objetivo General

Diseñar un modelo de continuidad del negocio y aseguramiento de la información para Laminados de Occidente S.A., orientado a la migración de sus servicios críticos hacia Microsoft Azure, bajo los principios de disponibilidad, resiliencia y gobernanza tecnológica.

Objetivos Específicos

1. Analizar la situación actual de la infraestructura tecnológica de Laminados de Occidente S.A., identificando sus principales riesgos y vulnerabilidades para establecer la línea base del modelo de continuidad.

2. Definir los componentes, políticas y niveles de servicio (RTO, RPO) que fundamentarán los requisitos de disponibilidad y resiliencia del nuevo modelo en la nube.
3. Diseñar una arquitectura de referencia en la nube de Microsoft Azure como núcleo tecnológico del modelo, integrando medidas de seguridad, respaldo y recuperación ante desastres.
4. Proponer un plan de migración gradual de los servicios críticos hacia Azure, asegurando la continuidad operativa durante la transición
5. Establecer lineamientos de monitoreo, capacitación y gobernanza tecnológica para garantizar la sostenibilidad y mejora continua del modelo diseñado.

Hipótesis

El diseño de un modelo de continuidad del negocio y aseguramiento de la información para Laminados de Occidente S.A., orientado a la migración de sus servicios críticos hacia Microsoft Azure y basado en los principios de disponibilidad, resiliencia y gobernanza tecnológica, permite mejorar los niveles de disponibilidad de los servicios, reducir los tiempos de recuperación (RTO/RPO) y disminuir la exposición a fallas operativas y pérdidas de información frente al esquema de infraestructura local actual.

Hipótesis Nula

El diseño de un modelo de continuidad del negocio y aseguramiento de la información para Laminados de Occidente S.A., orientado a la migración de sus servicios críticos hacia Microsoft Azure y basado en los principios de disponibilidad, resiliencia y gobernanza tecnológica, no tendrá efecto significativo en los niveles de disponibilidad de los servicios, ni en los tiempos de recuperación (RTO/RPO), ni en la exposición a fallas operativas y pérdidas de información frente al esquema de infraestructura local actual.

Alcance y Limitaciones del Proyecto

El presente proyecto se centra exclusivamente en el diseño del modelo de continuidad del negocio y aseguramiento de la información para Laminados de Occidente S.A., con miras a una futura migración de sus servicios críticos hacia la nube de Microsoft Azure. Esto significa que el trabajo no incluye la ejecución técnica de la migración ni la adquisición o configuración real de servidores, redes o licencias. Lo que se busca es dejar trazado un modelo sólido y viable que sirva de guía cuando la empresa decida ponerlo en práctica.

El alcance del proyecto cubre todo el proceso de análisis, diseño y propuesta: desde el diagnóstico de la infraestructura actual hasta la formulación de la arquitectura recomendada en la nube, con sus políticas de respaldo, continuidad y recuperación ante desastres. También se incluirán lineamientos para la seguridad de la información, el control de accesos, la gestión de riesgos y la definición de niveles de servicio (RTO, RPO y SLA) que aseguren la disponibilidad de los sistemas.

Este diseño se basará en buenas prácticas internacionales, especialmente las establecidas en la norma ISO 22301 (ISO, 2019)sobre gestión de la continuidad del negocio y la ISO 27001 (ISO, 2022) sobre seguridad de la información, además del Azure Well-Architected Framework (Microsoft, 2025), que orienta el diseño de infraestructuras resilientes en la nube. Todo se adaptará a las condiciones reales de Laminados de Occidente S.A., priorizando el equilibrio entre costo, funcionalidad y sostenibilidad.

En cuanto a sus limitaciones, el proyecto no aborda pruebas de rendimiento, simulaciones de carga ni configuraciones específicas dentro de Azure, ya que eso requeriría recursos técnicos y financieros fuera del alcance académico. Tampoco contempla la implementación de políticas de

respaldo o monitoreo en producción, pues esas acciones deben realizarse una vez la empresa apruebe el plan y cuente con los medios necesarios.

Es importante aclarar que los resultados esperados se enfocan en la planificación estratégica y técnica, no en resultados operativos inmediatos. El valor del trabajo radica en dejar un modelo integral, argumentado y documentado, que permita a la organización avanzar hacia la continuidad y la modernización tecnológica con una base segura y sustentada.

Marco Teórico

El diseño de un modelo de continuidad del negocio y aseguramiento de la información para una organización del sector manufacturero, como lo es Laminados de Occidente S.A., trasciende la simple actualización tecnológica para convertirse en un imperativo estratégico de resiliencia organizacional. Este capítulo establece los fundamentos teóricos y normativos que sustentan dicha transformación, articulando tres ejes conceptuales críticos: la convergencia de sistemas de información corporativos y de control industrial (IT/OT) esenciales para la producción ; la gestión formal de la continuidad basada en la norma ISO 22301 y la especificación técnica ISO/TS 22317 (ISO, 2021) para el Análisis de Impacto al Negocio (BIA), y la arquitectura de nube moderna regida por el pilar de Fiabilidad (Reliability) del Azure Well-Architected Framework (Microsoft, 2025).

A través de esta integración teórica, se busca fundamentar cómo la migración de servicios críticos específicamente el ERP Siesa y el sistema MES/SCADA hacia Microsoft Azure no solo mitiga los riesgos de obsolescencia de la infraestructura local actual, sino que habilita capacidades avanzadas de recuperación ante desastres alineadas con las exigentes normativas de disponibilidad de los sectores farmacéutico y cosmético que atiende la organización.

Gestión de la Continuidad del Negocio y Resiliencia Organizacional

La gestión de la continuidad del negocio (BCM) ha evolucionado de ser una práctica centrada meramente en la recuperación tecnológica ante desastres (Disaster Recovery), hacia un enfoque holístico de resiliencia organizacional. Según la norma ISO 22300:2021, la resiliencia es la capacidad de una organización para absorber y adaptarse en un entorno cambiante. En el

contexto de empresas del sector manufacturero como Laminados de Occidente S.A., esto implica no solo la restauración de servidores, sino la preservación de la cadena de valor operativa frente a interrupciones.

El enfoque moderno de BCM busca trascender la reacción ante fallos para integrar la prevención y la adaptabilidad en el diseño mismo de los procesos. Como señalan IBM (2025) y otros referentes de la industria, la resiliencia cibernética articula la seguridad de la información con la continuidad operativa, garantizando que la organización pueda resistir incidentes, recuperarse rápidamente y aprender de ellos para minimizar impactos futuros.

Marco Normativo y Estándares de Referencia

Para garantizar que el modelo de continuidad propuesto cumpla con estándares de calidad y auditoría internacional, esta investigación se fundamenta en la integración de tres marcos normativos clave:

El Ecosistema ISO 22301 e ISO/TS 22317

La norma ISO 22301:2019 establece los requisitos para planificar, establecer e implementar un Sistema de Gestión de Continuidad del Negocio (SGCN). Este estándar exige que la organización comprenda sus necesidades y obligaciones, y establezca una capacidad de recuperación definida. Sin embargo, para la ejecución técnica, la referencia indispensable es la especificación técnica ISO/TS 22317:2015. Esta guía detalla la metodología para realizar el Análisis de Impacto al Negocio (BIA), proporcionando las directrices necesarias para identificar procesos críticos y priorizar su recuperación basándose en evidencia y no en intuición.

NIST SP 800-34 Rev. 1: Planificación de Contingencia para TI

Mientras que la ISO 22301 ofrece la visión estratégica, la guía NIST SP 800-34 Rev. 1 (2010) proporciona el marco táctico para los sistemas de información. Este estándar desarrollado por el National Institute of Standards and Technology de Estados Unidos. estructura la planificación de contingencia en fases técnicas concretas: identificación de recursos, selección de estrategias de recuperación y pruebas de validación. Su aplicación es fundamental para traducir los requisitos del negocio en configuraciones técnicas de servidores y redes.

ISO/IEC 27001:2022 y Seguridad de la Información

La continuidad no puede existir sin seguridad. La norma ISO/IEC 27001:2022 define los controles para garantizar la confidencialidad, integridad y disponibilidad de la información. En el diseño propuesto, este marco se complementa con el modelo de *Zero Trust* (Confianza Cero), que asume que ninguna entidad dentro o fuera de la red es confiable por defecto, exigiendo verificación explícita y privilegios mínimos, un enfoque crítico al migrar servicios locales a un entorno de nube pública.

Gestión de Riesgos de Seguridad de la Información (ISO/IEC 27005)

Mientras que la norma ISO/IEC 27001 establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), la norma ISO/IEC 27005:2018 proporciona las directrices para la gestión del riesgo de seguridad de la información. Este estándar es el "motor" que permite identificar por qué y cómo proteger los activos.

En el contexto de esta investigación, la ISO/IEC 27005 fundamenta el enfoque de análisis de riesgos mediante la relación causal de tres elementos:

- **Activo:** Cualquier cosa que tiene valor para la organización y que requiere protección.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede dañar un sistema o una organización.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Esta norma se alinea con los principios generales de la **ISO 31000** (Gestión del Riesgo), pero los especializa para el entorno tecnológico, permitiendo valorar el riesgo no solo por su impacto financiero, sino por la pérdida de confidencialidad, integridad y disponibilidad de la información.

Zero Trust Security

El modelo de Zero Trust Security surge como un enfoque moderno que rompe con la idea tradicional de “confiar dentro de la red”. En un entorno Zero Trust, nada ni nadie se considera confiable por defecto. Cada acceso, dispositivo o usuario debe autenticarse y verificarse continuamente, sin importar si está dentro o fuera de la red corporativa. Microsoft (Microsoft, 2025) explica que este enfoque se basa en tres principios: verificar explícitamente, aplicar el menor privilegio posible y asumir la posibilidad de una brecha.

El modelo de *Zero Trust* (Confianza Cero) fundamenta la seguridad de la arquitectura propuesta. De acuerdo con la publicación especial **NIST SP 800-207**, Zero Trust no es una tecnología única, sino un "conjunto en evolución de paradigmas de ciberseguridad que mueven las defensas de perímetros estáticos basados en red hacia el enfoque en usuarios, activos y recursos" (Rose et al., 2020, p. 4).

En el contexto de Azure, **Microsoft (2025)** operacionaliza este estándar bajo tres principios de diseño: 1) Verificar explícitamente cada solicitud de acceso; 2) Utilizar el acceso de privilegios mínimos (JIT/JEA); y 3) Asumir la brecha, segmentando las redes y cifrando los datos de extremo a extremo.

Figura 1.
Principios Zero Trust

Nota: Tomado de *El papel fundamental de Confianza Cero en la seguridad de nuestro mundo*, por Microsoft, 2021, Microsoft News Center Latinoamérica. https://news.microsoft.com/es-xl/el-papel-fundamental-de-confianza-cero-en-la-seguridad-de-nuestro-mundo/. Derechos de autor 2021 por Microsoft.

Para un entorno en la nube como Azure, Zero Trust se integra con los servicios de identidad, control de acceso y monitoreo, asegurando que cada componente del sistema cumpla políticas consistentes de seguridad. Si se combina con la ISO 27001, se obtiene un marco fuerte y actualizado: la norma da la estructura de gestión, y Zero Trust aporta la capa práctica de defensa en entornos distribuidos. En el caso de Laminados de Occidente S.A., esta combinación resulta esencial para proteger los servicios críticos una vez estén migrados, garantizando que la seguridad no dependa únicamente del perímetro de red.

Metodologías de Análisis y Métricas de Recuperación

La efectividad de una estrategia de continuidad radica en la precisión de sus métricas. No es posible diseñar una arquitectura tecnológica eficiente sin antes definir, mediante un Análisis de Impacto al Negocio (BIA), los parámetros temporales que delimitan la tolerancia de la organización.

Análisis de Impacto al Negocio (BIA) y Evaluación Multidimensional

El BIA es el proceso analítico que permite correlacionar los procesos de negocio con los recursos tecnológicos que los soportan. Según la ISO/TS 22317, el impacto de una interrupción no es unidimensional; debe evaluarse a través de diversas categorías para comprender la magnitud real del daño. Las dimensiones de impacto más comúnmente utilizadas en la práctica del BIA incluyen:

- **Operacional:** Se refiere a la incapacidad de producir bienes, prestar servicios o realizar funciones internas críticas, afectando la cadena de valor.
- **Financiera:** Abarca las pérdidas monetarias directas (caída de ingresos, multas) e indirectas (costos de recuperación, pérdida de cuota de mercado futura).
- **Legal y Regulatoria:** Considera el incumplimiento de leyes, normativas sectoriales u obligaciones contractuales que pueden derivar en sanciones o litigios.
- **Reputacional:** Evalúa el daño a la imagen de marca, la pérdida de confianza de los clientes, inversores y partes interesadas, que puede ser más devastadora a largo plazo que el impacto financiero inmediato.

Definición Técnica de Métricas de Continuidad (MTPD, RTO, RPO)

El Análisis de Impacto al Negocio (BIA) tiene como fin último establecer los parámetros temporales de recuperación. De acuerdo con la norma **ISO 22300:2021**, que establece el

vocabulario para la seguridad y resiliencia, se definen los siguientes conceptos rectores para la estrategia de continuidad:

- **Periodo Máximo Tolerable de Interrupción (MTPD):** Se define como el "lapso de tiempo después del cual la viabilidad de la organización se ve irreparablemente amenazada si no se reanuda la entrega del producto o servicio" (ISO, 2025). Este parámetro representa el punto de no retorno para la operación de Laminados de Occidente S.A.
- **Objetivo de Tiempo de Recuperación (RTO):** La norma lo define como el "período de tiempo después de un incidente dentro del cual se debe reanudar el producto o servicio, o se deben recuperar los recursos de las actividades" (ISO, 2025). En términos operativos, el RTO debe ser siempre menor que el MTPD para garantizar un margen de seguridad.
- **Objetivo de Punto de Recuperación (RPO):** Se refiere al "punto en el tiempo al que deben restaurarse los datos para permitir que la actividad se reanude" (ISO, 2025). Este indicador determina la pérdida máxima de datos aceptable (ej. transacciones del ERP o históricos del SCADA) entre el último respaldo exitoso y el momento de la interrupción.

Computación en la Nube y Azure Well-Architected Framework

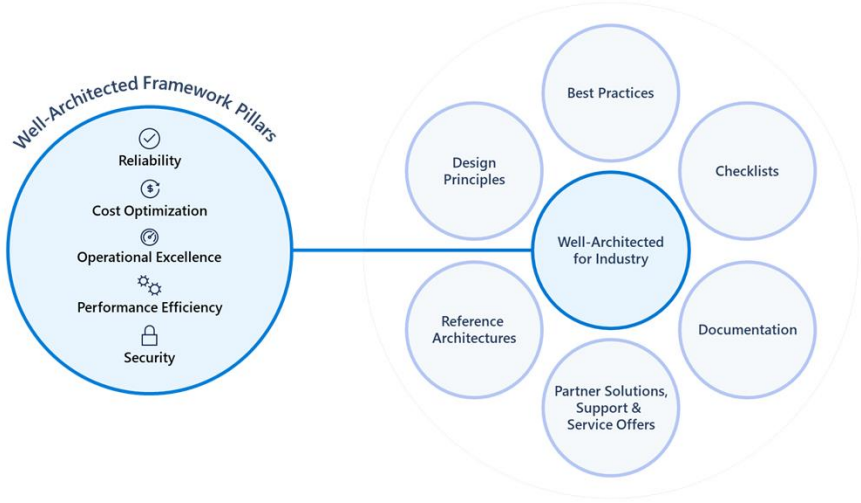
En los últimos años, la nube dejó de ser una novedad para convertirse en una necesidad. Hoy casi todas las empresas, grandes o pequeñas, buscan aprovecharla para reducir costos, mejorar su seguridad y tener más control sobre su información. La computación en la nube es, en palabras simples, un modelo que permite acceder a recursos informáticos (como almacenamiento, servidores o bases de datos) a través de internet, sin tener que mantener físicamente los equipos en la empresa.

Antes, todo dependía del hardware local: si un servidor se dañaba, había que reemplazarlo, configurarlo y esperar que todo volviera a la normalidad. En la nube, esas tareas se automatizan y se escalan con facilidad. Según IBM (2024), este enfoque ofrece ventajas como la disponibilidad continua, la flexibilidad y la capacidad de pagar solo por lo que se usa. Esto es clave para organizaciones como Laminados de Occidente S.A., que necesita estabilidad sin asumir los costos de una infraestructura propia (Microsoft, 2025).

Dentro del ecosistema de Microsoft, la nube se llama Azure, y no se trata solo de alojar máquinas virtuales, sino de construir soluciones completas. Para que esas soluciones funcionen bien, Microsoft creó una guía llamada Azure Well-Architected Framework. Este marco ayuda a diseñar arquitecturas que sean seguras, confiables, eficientes y sostenibles. Lo interesante es que no impone reglas rígidas, sino que enseña a evaluar y mejorar continuamente las decisiones de diseño.

El Well-Architected Framework se basa en cinco pilares fundamentales: fiabilidad, seguridad, eficiencia del rendimiento, optimización de costos y excelencia operativa, como se evidencia en la figura 2. En el caso de esta investigación, el más importante es el de confiabilidad, porque está directamente ligado a la continuidad del negocio. Este pilar aborda cómo mantener un servicio disponible, cómo reaccionar ante fallos y cómo reducir al mínimo los tiempos de inactividad. En otras palabras, traduce la teoría de continuidad en acciones concretas dentro del entorno de Azure.

Figura 2.
Pilares del Marco de Buena Arquitectura (Well-Architected Framework) para la Industria



Nota: Tomado de *Microsoft Cloud for Industry Well-Architected Framework overview*, por Microsoft, 2025, Microsoft Learn. https://learn.microsoft.com/en-us/industry/well-architected/overview. Derechos de autor 2025 por Microsoft.

Pilar de Fiabilidad (Reliability) y Continuidad en Azure

El pilar de fiabilidad es el corazón del diseño cuando se busca garantizar la continuidad. Microsoft (2025) lo define como la capacidad de un sistema para resistir fallas y seguir funcionando de forma estable. Dicho de manera sencilla, un sistema confiable no es el que nunca se cae, sino el que está preparado para levantarse rápido y sin perder información.

Para lograrlo, Azure recomienda tres estrategias básicas: eliminar los puntos únicos de falla, usar redundancia en diferentes zonas y automatizar los procesos de recuperación. Esto se traduce en prácticas concretas como distribuir los servicios entre varias regiones, replicar los datos en tiempo real y usar herramientas de monitoreo que detecten problemas antes de que afecten al usuario.

Además, Azure ofrece acuerdos de nivel de servicio (SLA) que definen el porcentaje mínimo de disponibilidad que un cliente puede esperar. Por ejemplo, muchos de sus servicios

garantizan una disponibilidad mensual del 99,9 %, y otros más críticos alcanzan el 99,99 %. Aunque la diferencia parezca mínima, esos decimales representan horas menos de inactividad al año, lo cual puede ser vital para empresas manufactureras como Laminados de Occidente S.A., donde cada minuto de parada afecta la producción.

El pilar de fiabilidad también promueve la automatización. En lugar de depender de que alguien esté pendiente para reiniciar un servicio o conmutar un servidor, las configuraciones de Azure permiten que eso ocurra de forma automática. Así, cuando un componente falla, otro asume su carga en segundos. Este tipo de diseño es el que se busca en el proyecto: una infraestructura que mantenga operativos los servicios críticos y asegure que la empresa siga funcionando, aun ante imprevistos.

La computación en la nube no solo cambia la forma de trabajar con tecnología, sino la forma de pensar la continuidad. Diseñar bajo el enfoque del Azure Well-Architected Framework permite que la empresa tenga un plan claro y adaptable, con medidas reales de fiabilidad y recuperación. Esto representa un paso firme hacia la modernización tecnológica que Laminados de Occidente S.A. necesita para su crecimiento.

Arquitectura de Alta Disponibilidad y Recuperación Ante Desastres

Cuando se habla de mantener un servicio activo las 24 horas, todos los días del año, el concepto clave es la alta disponibilidad. Este término no se refiere solo a tener buenos servidores, sino a construir una arquitectura que pueda soportar fallos sin que el usuario lo note. En la práctica, significa que, si un componente del sistema deja de funcionar, otro toma su lugar de inmediato y el servicio sigue operativo.

En los entornos tradicionales, lograr eso era costoso y complejo. Requería duplicar servidores, redes y almacenamiento físico, algo que solo grandes compañías podían permitirse. Hoy, la nube cambió ese panorama: los proveedores ofrecen infraestructura distribuida y automatizada, lo que permite construir sistemas con disponibilidad constante sin tener que invertir en equipos propios. Microsoft (Microsoft, 2025) explica que la alta disponibilidad se logra cuando los componentes críticos de un servicio se encuentran replicados y distribuidos de tal manera que un fallo local no interrumpe el funcionamiento global del sistema.

En este punto entra en juego la recuperación ante desastres (Disaster Recovery), que complementa la alta disponibilidad. Mientras la primera busca que el sistema no se detenga, la segunda se enfoca en cómo volver a la normalidad si ocurre una falla mayor, como un apagón general, una pérdida de datos o un ataque cibernético. Ambas estrategias trabajan juntas: la alta disponibilidad mantiene el servicio en marcha, y la recuperación ante desastres asegura que, si toda falla, exista una copia lista para restaurar.

Diseñar este tipo de arquitecturas requiere planificar con cuidado. No se trata solo de copiar archivos o clonar servidores. Hay que definir prioridades, identificar qué servicios son realmente críticos y decidir con qué frecuencia se deben replicar los datos. Azure Architecture Center (Microsoft, 2025) ofrece lineamientos claros para implementar planes de recuperación por niveles, con opciones que van desde replicaciones dentro de la misma región hasta copias en regiones completamente distintas, dependiendo del nivel de riesgo que se quiera cubrir.

En el caso de Laminados de Occidente S.A., una empresa con sistemas de producción e información centralizados, diseñar una arquitectura de alta disponibilidad es fundamental. No solo por la seguridad de los datos, sino porque una interrupción podría detener procesos de manufactura, retrasar entregas o afectar la comunicación interna. La arquitectura de referencia

diseñada establece un entorno de nube resiliente, capaz de asegurar la continuidad operativa y una recuperación eficiente ante incidentes críticos.

Zonas de Disponibilidad y Replicación Geográfica

Dentro del entorno de Microsoft Azure, los conceptos de zonas de disponibilidad y replicación geográfica son esenciales para asegurar la continuidad de los servicios. Las zonas de disponibilidad son, en términos sencillos, centros de datos físicamente separados dentro de una misma región, cada uno con energía, red y refrigeración independientes. Si una zona sufre una falla, las otras siguen operando. Al distribuir los recursos entre zonas, se evita que un problema local afecte todo el sistema.

La replicación geográfica lleva esta idea un paso más allá: consiste en duplicar los datos y servicios en otra región geográfica, incluso en otro país, para garantizar que un desastre de gran escala no interrumpa la operación. Microsoft (2025) detalla que Azure ofrece distintas opciones de replicación (como la replicación local, regional y geográfica) que se adaptan a las necesidades de disponibilidad y recuperación de cada organización.

Estas herramientas permiten aplicar estrategias conocidas como activo-pasivo o activo-activo. En un esquema activo-pasivo, una instancia principal atiende el servicio mientras otra permanece en espera, lista para activarse si la principal falla. En cambio, en el modelo activo-activo, varias instancias trabajan al mismo tiempo, compartiendo la carga y brindando una mayor tolerancia a fallos. La elección entre una u otra depende del presupuesto, la criticidad del servicio y el nivel de riesgo aceptable.

Implementar estas prácticas no solo garantiza que los sistemas de Laminados de Occidente S.A. sean más resistentes, sino que también se alinea con los estándares internacionales de continuidad, como la ISO 22301, que exige disponer de medidas de respaldo y

recuperación efectivas. En el entorno actual, donde los datos son el activo más valioso, diseñar con alta disponibilidad y replicación no es un lujo, sino una necesidad para asegurar la estabilidad del negocio.

Para garantizar la resiliencia de la arquitectura propuesta, se adoptan conceptos nativos de la nube definidos por el proveedor. Según la documentación oficial de arquitectura de Microsoft (2025), las Zonas de Disponibilidad son ubicaciones físicas separadas dentro de una misma región de Azure, cada una equipada con alimentación, refrigeración y redes independientes. Este diseño garantiza que, si una zona se ve afectada por un fallo local, los servicios replicados en otras zonas permanezcan operativos, ofreciendo una latencia de ida y vuelta inferior a 2 milisegundos.

Complementariamente, la estrategia incorpora la Replicación Geográfica. Microsoft define este mecanismo como la capacidad de replicar recursos de forma asíncrona en una región secundaria emparejada, situada a cientos de kilómetros de distancia, para proteger la carga de trabajo ante desastres regionales o cortes masivos. Esta combinación permite a Laminados de Occidente S.A. cumplir con los principios de Alta Disponibilidad y Recuperación ante Desastres (BCDR) exigidos por el modelo de responsabilidad compartida en la nube.

Trabajos y Estudios Previos Sobre Continuidad en la Nube

En los últimos años, el tema de la continuidad del negocio en la nube ha pasado de ser un interés técnico para convertirse en una prioridad para casi todas las organizaciones. Cada vez más empresas confían en servicios en línea para manejar información sensible o procesos críticos, lo que las obliga a pensar en cómo seguir funcionando si algo falla. Por eso, distintos

estudios y experiencias han buscado entender cuáles son las mejores prácticas para mantener la operación estable en entornos de nube.

Uno de los aportes más reconocidos en esta línea es el trabajo de “High availability in clouds: systematic review and research challenges” (Endo et al., 2016), quienes analizaron diferentes estrategias de alta disponibilidad dentro de plataformas en la nube. Su estudio resalta que la clave no está en evitar las fallas (porque eso es imposible), sino en reducir su impacto y garantizar una recuperación rápida. Para ellos, la automatización y la redundancia son las dos herramientas más efectivas para lograrlo. Estas ideas son totalmente aplicables a la realidad de una empresa como Laminados de Occidente S.A., que necesita asegurar la continuidad de sus procesos productivos sin depender de infraestructura física.

Otros autores, como Rahman et al. (2020), han analizado estrategias en las que la infraestructura local se complementa con servicios en la nube. Su investigación muestra que, cuando las copias de seguridad se distribuyen entre distintos entornos, la recuperación ante desastres es más eficiente. Esto reduce la posibilidad de perder información y ofrece a las empresas una forma más controlada de migrar sus sistemas, algo muy útil para organizaciones que aún están en transición tecnológica.

Nascimento et al. (2024) abordaron la continuidad desde un enfoque más actual: las aplicaciones nativas en la nube. Ellos explican que, gracias al uso de contenedores y orquestadores como Kubernetes, es posible que los sistemas se ajusten de manera automática ante picos de carga o fallas en un nodo. Este tipo de diseño hace que la nube sea más que un simple lugar de almacenamiento: la convierte en un entorno adaptable, donde la resiliencia se construye en cada capa del servicio.

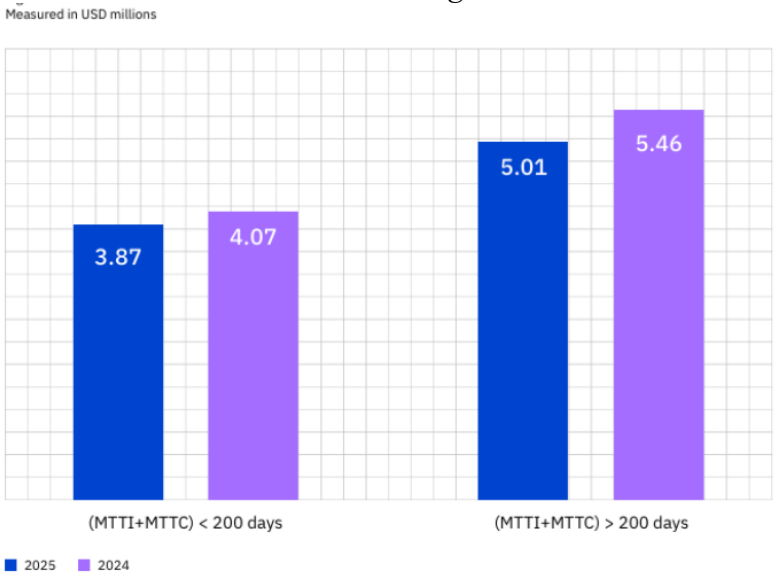
Los fabricantes de tecnología también han contribuido con investigaciones aplicadas. Microsoft (2025), a través de su guía de diseño confiable, demuestra que los proyectos que incluyen estrategias de recuperación desde la fase inicial logran reducir sus tiempos de inactividad y sus costos de mantenimiento. De igual forma, IBM (2025) enfatiza que la continuidad del negocio no depende únicamente de la tecnología, sino también de la preparación de las personas y de la claridad de los procesos. Un sistema puede tener todos los respaldos del mundo, pero si el equipo no sabe cómo actuar frente a una emergencia, el resultado será el mismo: una parada no planificada.

La definición de tiempos de recuperación (RTO) estrictos para Laminados de Occidente S.A. no responde únicamente a criterios operativos, sino a una necesidad financiera crítica validada por la industria. Según el análisis del ciclo de vida de incidentes presentado en el *Cost of a Data Breach Report 2025* de IBM (2025), existe una correlación directa entre el tiempo de contención y el impacto económico.

Como se evidencia en la Figura 3, las organizaciones que carecen de mecanismos ágiles de continuidad y cuyos incidentes se extienden por más de 200 días enfrentan costos promedio de USD 5.01 millones. En contraste, aquellas capaces de contener el evento en un ciclo menor a 200 días reducen este impacto a USD 3.87 millones, logrando un ahorro superior al 22%. Esta diferencia justifica la inversión en la arquitectura de respaldo y recuperación de Microsoft Azure propuesta está diseñada específicamente para minimizar los tiempos de inactividad y mantener a la organización dentro del umbral de recuperación rentable

Figura 3.

Costo promedio de una brecha de datos según la duración del ciclo de vida del incidente



Nota: Tomado de *Cost of a Data Breach Report 2025* (Figura 12, p. 19), por IBM, 2025. https://www.ibm.com/reports/data-breach. Derechos de autor 2025 por IBM.

A partir de estos estudios, se puede afirmar que la continuidad en la nube no es un simple proyecto técnico, sino un proceso de madurez organizacional. Las empresas más exitosas no se limitan a hacer copias o a contratar un servicio en la nube: diseñan estructuras con redundancia, políticas claras y roles definidos. Justamente, el propósito de este trabajo es seguir esa misma línea, adaptando los principios identificados por los investigadores al contexto de Laminados de Occidente S.A., una empresa que necesita garantizar la estabilidad de sus servicios sin depender del hardware local.

Con base en estos antecedentes, el diseño que aquí se propone buscará unir las recomendaciones técnicas con la realidad operativa de la organización. La idea no es copiar modelos externos, sino construir una propuesta realista, sostenible y alineada con las capacidades

actuales de la empresa, que le permita mantener su operación sin interrupciones incluso ante fallas graves o eventos inesperados.

Sistemas de Control Industrial y Convergencia IT/OT

Los sistemas de ejecución de manufactura (MES) actúan como el puente crítico entre la planificación empresarial (ERP) y el control de planta. De conformidad con la norma ANSI/ISA-95, que establece el estándar internacional para la integración de sistemas, el MES se ubica en el Nivel 3, gestionando los flujos de trabajo, la trazabilidad y la calidad en tiempo real para alinear la producción con el negocio (International Society of Automation, 2010)

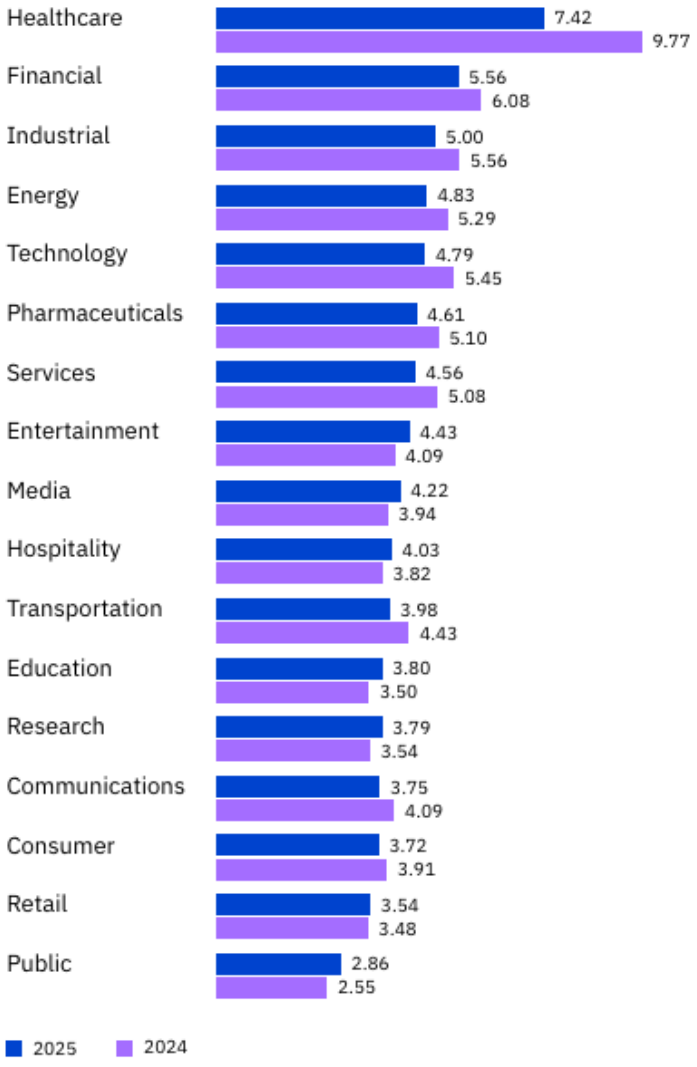
El sistema SCADA permite la supervisión y adquisición de datos de los procesos industriales, interactuando directamente con los PLCs en los Niveles 1 y 2, tal como define el marco de referencia de seguridad para sistemas de control industrial del NIST (2023).

La inversión en una arquitectura de nube resiliente para Laminados de Occidente S.A. se justifica por el alto nivel de exposición financiera del sector manufacturero. Según el Cost of a Data Breach Report 2025 de IBM (2025), el sector industrial se posiciona como el tercero más castigado económicamente, solo por detrás de salud y finanzas.

Como se evidencia en la Figura 4, el costo promedio de una brecha de datos en el sector industrial se mantiene en niveles críticos, registrando USD 5.00 millones en 2025 y habiendo alcanzado picos de USD 5.56 millones en el periodo anterior. Estas cifras demuestran que la interrupción de las operaciones de planta y la cadena de suministro genera pérdidas millonarias, validando la inversión en una arquitectura de alta disponibilidad en Azure como una medida de contención de costos. Por tanto, mitigar este riesgo mediante la alta disponibilidad de Azure no es un gasto operativo, sino una medida de protección de activos críticos.

Figura 4.

Costo promedio de una brecha de datos por industria (Comparativo 2024-2025)



Nota: Tomado de *Cost of a Data Breach Report 2025* (Figura 3, p. 13), por IBM, 2025. https://www.ibm.com/reports/data-breach. Derechos de autor 2025 por IBM.

Marco Referencial

Laminados de Occidente S.A., conocida comercialmente como Laminados de Occidente S.A., es una empresa colombiana dedicada a la fabricación de tubos colapsibles de aluminio y laminados para la industria farmacéutica, cosmética e industrial. Desde su fundación en 1950, la compañía se ha consolidado como un proveedor líder de envases primarios de alta calidad, exportando actualmente a varios países de América y operando bajo un sistema de gestión certificado en ISO 9001:2015 (Laminados de Occidente S.A., 2025)

Su misión declara el compromiso de fabricar y comercializar tubos colapsibles de alta calidad para el envasado y preservación de productos farmacéuticos, cosméticos e industriales, atendiendo los requisitos de los clientes, así como las exigencias ocupacionales, ambientales y legales aplicables. Esta orientación hacia mercados regulados y de alto valor agregado convierte a la continuidad operativa y a la integridad de la información en elementos estratégicos para la organización.

Laminados de Occidente S.A. tiene su sede y planta principal en Palmira, Valle del Cauca, en la dirección Carrera 99 No. 99-99, desde donde atiende el mercado nacional y las exportaciones regionales. La empresa pertenece al sector manufacturero, clasificada en la categoría de fabricación de otros productos elaborados de metal, con especialización en envases metálicos y laminados.

Laminados de Occidente S.A. participa en la cadena de valor de envases y empaques como fabricante de tubos colapsibles de aluminio y tubos laminados tipo ABL, diseñados para actuar como envase primario de productos semisólidos y líquidos: cremas, geles, ungüentos, tintes, óleos, adhesivos, siliconas y otros productos farmacéuticos, cosméticos e industriales.

Sus principales clientes son compañías de los sectores:

- **Farmacéutico**: laboratorios que requieren envases primarios con alta hermeticidad, barrera a la luz y compatibilidad con principios activos.
- **Cosmético y cuidado personal**: fabricantes de cremas, tratamientos capilares, tintes y productos dermatológicos.
- **Industrial**: productores de siliconas, adhesivos, óleos y otros compuestos que requieren envases de dosificación precisa y resistentes.

Esta combinación de sectores implica atender requisitos técnicos y de calidad muy exigentes, tanto por los estándares de la industria como por las regulaciones sanitarias y ambientales que aplican a los envases que entran en contacto directo con productos farmacéuticos y cosméticos.

Misión:

"Fabricar y comercializar tubos colapsibles de alta calidad para el envasado y preservación de productos farmacéuticos, cosméticos e industriales. Atendiendo los requisitos de nuestros clientes, los ocupacionales y ambientales aplicables. Fortaleciendo la competencia y habilidades de nuestro recurso humano, con responsabilidad y compromiso hacia la mejora y sostenibilidad de la empresa y de todos nuestros grupos de interés." (Laminados de Occidente S.A., 2025).

Visión:

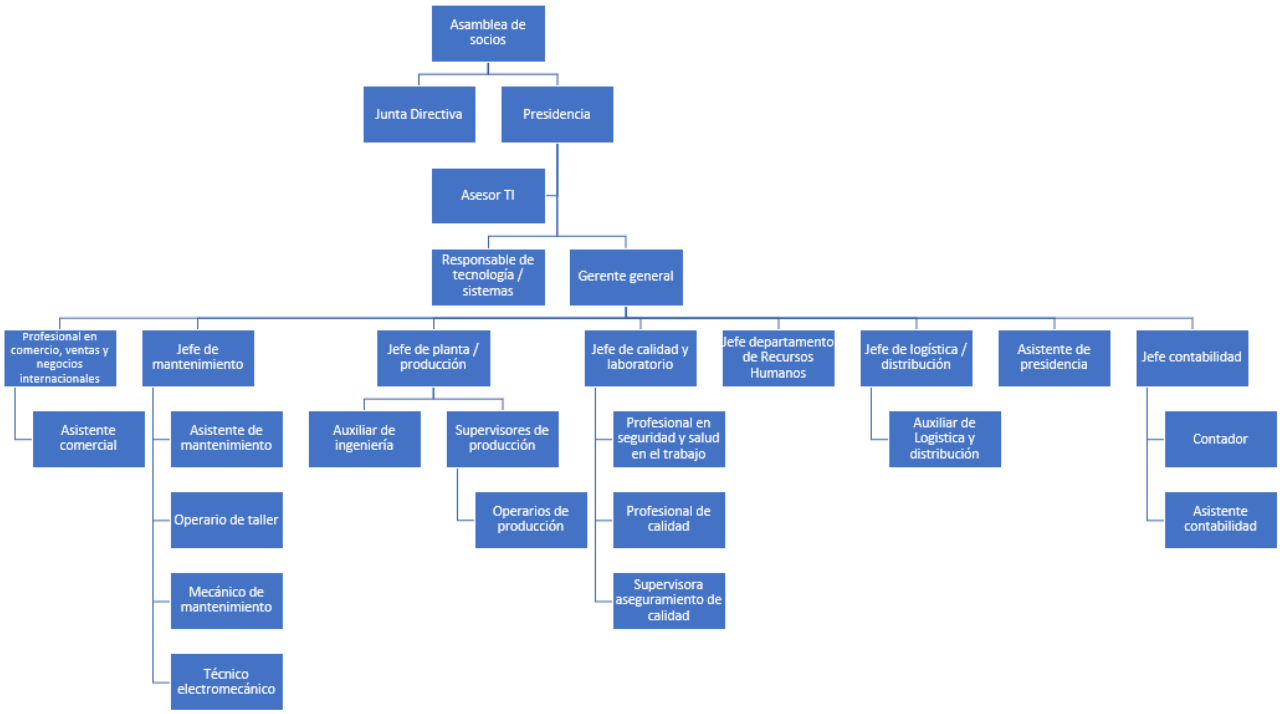
"En 2030 Industrias de Envases S. A., espera mantener el reconocimiento a nivel nacional como una empresa productora de tubos colapsibles de excelente calidad y servicio que, mediante la transformación digital, optimización de recursos, integración de tecnologías avanzadas, procesos innovadores y amigables con el medio ambiente, logre obtener un crecimiento anual en las ventas para el beneficio de las partes interesadas" (Laminados de Occidente S.A., 2025)

Estructura Organizacional

La estructura organizacional de Laminados de Occidente S.A. responde a un modelo jerárquico funcional, diseñado para soportar la operación de manufactura continua y la comercialización de envases en mercados regulados. Esta estructura permite una clara delimitación de responsabilidades, aspecto fundamental para la gobernanza de TI y la asignación de roles en el modelo de continuidad del negocio propuesto.

Como se aprecia en la Figura 5, la organización está encabezada por la Asamblea de Socios y la Junta Directiva, quienes definen el rumbo estratégico, delegando la ejecución en la Gerencia General. De esta gerencia se desprenden las áreas misionales y de apoyo que fueron objeto de análisis en el diseño metodológico de esta investigación, dada su dependencia crítica de los sistemas de información ERP Siesa y MES/SCADA.

Figura 5.
Estructura Organizacional de Laminados de Occidente S.A.



Nota: El organigrama ilustra las líneas de reporte y las áreas funcionales clave. Se destacan las jefaturas de Planta, Logística y Contabilidad como principales usuarios de los sistemas críticos, y el área de Tecnología como responsable de la infraestructura. Fuente: Elaboración propia a partir de documentación interna (2025).

Descripción de Áreas Clave para el Modelo de Continuidad

Para efectos del diseño de la arquitectura de migración a Microsoft Azure y el plan de continuidad (BCP), se han identificado las siguientes áreas como críticas, basándose en la "Población y Muestra" definida en el capítulo metodológico:

- **Gerencia General:** Representa el nivel de decisión estratégico. Es el "Dueño del Riesgo" principal y quien debe aprobar las inversiones necesarias para la modernización tecnológica hacia la nube y las políticas de gobierno de TI.

- **Responsable de Tecnología / Sistemas:** Ubicado bajo la supervisión directa de la Gerencia General y apoyado por una Asesoría TI externa. Este rol es el eje central de la investigación, encargado de administrar la infraestructura actual (AS-IS), ejecutar la migración propuesta (TO-BE) y gestionar los servicios de Azure (backup, replicación, seguridad).

- **Jefe de Planta / Producción:** Lidera el "corazón" operativo de la empresa. De esta área depende el sistema **MES/SCADA Ignition**, identificado en el BIA como el activo de mayor criticidad operativa. Su personal (supervisores y operarios) requiere disponibilidad inmediata de los datos de producción para garantizar la trazabilidad exigida por los clientes farmacéuticos.

- **Jefe de Logística / Distribución:** Gestiona la cadena de suministro y los inventarios. Su operación depende transaccionalmente del **ERP Siesa**. Una interrupción en esta área afecta directamente los compromisos de entrega y la facturación, lo que justifica los estrictos RTO (Objetivos de Tiempo de Recuperación) planteados en el diseño.

- **Jefe de Contabilidad y Área Comercial:** Representados en el organigrama por las jefaturas administrativas y los profesionales en ventas. Son los usuarios intensivos del ERP para la gestión financiera, facturación y servicio al cliente. Su inclusión en el análisis de riesgos permitió identificar el impacto financiero y reputacional ante fallas de infraestructura.

Esta estructura evidencia que, aunque el área de TI es un departamento de soporte, tiene una responsabilidad transversal sobre la continuidad de todas las áreas misionales (Producción,

Logística y Comercial), validando la necesidad de transitar desde una infraestructura local y aislada hacia un modelo de nube resiliente y centralizado.

Bases Legales

El presente proyecto se fundamenta en la normativa vigente en Colombia respecto a la protección de datos, la seguridad de la información y el comercio electrónico, así como en los estándares internacionales que rigen la continuidad del negocio y la gestión de riesgos tecnológicos. A continuación, se detallan los instrumentos jurídicos y técnicos que blindan la propuesta de migración hacia Microsoft Azure.

Protección de Datos Personales (Habeas Data)

La migración de la infraestructura de Laminados de Occidente S.A. a la nube implica el tratamiento de información sensible de empleados, clientes y proveedores. Por ello, el proyecto se alinea estrictamente con la Ley 1581 de 2012 (Ley General de Protección de Datos Personales), la cual obliga a las organizaciones a garantizar la seguridad, confidencialidad e integridad de los datos bajo su custodia. (Congreso de la República de Colombia, 2012).

En este contexto, Laminados de Occidente S.A. actúa como "Responsable del Tratamiento", mientras que Microsoft Azure funge como "Encargado". Para cumplir con el principio de seguridad exigido por el artículo 4 de dicha ley, la arquitectura propuesta implementa controles técnicos como el cifrado de datos en reposo y en tránsito, asegurando que la información no sea adulterada, perdida o consultada por personal no autorizado. Asimismo, se observa el Decreto 1377 de 2013, que reglamenta la ley mencionada, exigiendo la implementación de mecanismos internos efectivos para demostrar la responsabilidad (Accountability) en el manejo de la información.

Normativa sobre Ciberseguridad y Delitos Informáticos

Para proteger a la organización frente a amenazas digitales, la estrategia de seguridad se enmarca en la Ley 1273 de 2009, la cual modificó el Código Penal colombiano creando el bien jurídico tutelado de "la protección de la información y de los datos". (Congreso de la República de Colombia, 2009)

La implementación de controles de acceso robustos (Zero Trust) y autenticación multifactor (MFA) en la nueva plataforma busca prevenir conductas tipificadas en esta ley, tales como:

- **Acceso abusivo a un sistema informático (Art. 269A):** Protegiendo los sistemas contra intrusiones externas.
- **Obstaculización ilegítima de sistema informático (Art. 269B):** Mitigando riesgos de ataques de Denegación de Servicio (DDoS) mediante la resiliencia de la nube.
- **Daño Informático (Art. 269D):** Garantizando la integridad de los datos operativos mediante copias de seguridad inmutables.

Validez Jurídica de la Información Digital

Dado que Laminados de Occidente S.A. maneja información operativa y comercial crítica, el proyecto se ampara en la Ley 527 de 1999, que define y reglamenta el acceso y uso de los mensajes de datos y el comercio electrónico en Colombia. (Congreso de la República de Colombia, 1999)

Esta norma otorga plena validez jurídica y probatoria a la información digital, siempre que se garantice su autenticidad, integridad y disponibilidad. La arquitectura en Azure asegura el cumplimiento de estos requisitos a través de logs de auditoría inalterables y sistemas de

trazabilidad que permiten verificar el origen y la conservación de los mensajes de datos generados por los sistemas de manufactura (MES) y administrativos (ERP)

Diseño Metodológico de la Investigación

Desde el enfoque metodológico adoptado en este trabajo, cada uno de los objetivos específicos se entiende como un entregable concreto dentro del proyecto. En particular, el análisis de la infraestructura tecnológica actual (Objetivo 1) se materializa en un diagnóstico detallado y en una matriz de riesgos asociada a los servidores y aplicaciones críticas; la definición de componentes, políticas y niveles de servicio (Objetivo 2) se refleja en el Análisis de Impacto al Negocio (BIA) y en la tabla de requisitos de continuidad (RTO, RPO, SLA); el diseño de la arquitectura de referencia en Microsoft Azure (Objetivo 3) se concreta en los diagramas y la descripción técnica de la solución propuesta; el plan de migración gradual (Objetivo 4) se presenta como una hoja de ruta por fases para la transición de los servicios críticos hacia la nube y para finalizar, los lineamientos de monitoreo, capacitación y mejora continua (Objetivo 5) constituyen la propuesta de gobernanza y sostenibilidad del modelo de continuidad del negocio y aseguramiento de la información para Laminados de Occidente S.A.

Enfoque y Tipo de Investigación

La presente investigación se desarrolla bajo un enfoque mixto, que combina elementos cualitativos y cuantitativos. El componente cualitativo permite comprender, desde la perspectiva de los actores de Laminados de Occidente S.A., cómo se perciben los riesgos asociados a la continuidad del negocio y al aseguramiento de la información; mientras que el componente cuantitativo facilita la valoración de dichos riesgos mediante matrices y escalas de impacto y

probabilidad, así como la definición de objetivos de recuperación (RTO y RPO) y niveles de servicio (SLA).

En cuanto a su naturaleza, el estudio se clasifica como una investigación aplicada, dado que busca ofrecer una solución concreta a un problema real de la organización que es la ausencia de un modelo formal de continuidad del negocio y de aseguramiento de la información para sus servicios críticos, en el contexto de una futura migración hacia Microsoft Azure.

Por su propósito, se trata de una investigación descriptiva y explicativa. Es descriptiva porque caracteriza el entorno tecnológico actual de Laminados de Occidente S.A., identifica sus sistemas críticos, sus dependencias y sus vulnerabilidades frente a incidentes que comprometan la disponibilidad y la integridad de la información. Es explicativa porque analiza la relación entre dichos riesgos y la arquitectura tecnológica existente, y propone un modelo de continuidad y una arquitectura de referencia en la nube que permita mitigar las causas identificadas.

El diseño es no experimental y de tipo estudio de caso, ya que no se manipulan variables en un entorno controlado, sino que se observa la situación real de la empresa y se construye una propuesta metodológica y arquitectónica específica para Laminados de Occidente S.A.

Diseño de la Investigación

El estudio se estructura como un estudio de caso único centrado en Laminados de Occidente S.A., que se desarrolla en cuatro grandes etapas:

1. Caracterización de la organización y de su entorno tecnológico actual.
2. Análisis de riesgos y desarrollo del Análisis de Impacto al Negocio (BIA).
3. Diseño del modelo de continuidad del negocio y de aseguramiento de la información.

4. Formulación de la arquitectura de referencia en Microsoft Azure y validación frente a marcos de buenas prácticas.

Cada etapa se articula con los objetivos específicos de la investigación y produce entregables concretos (matrices, diagramas, tablas de requisitos y lineamientos), que posteriormente son integrados en un modelo general de continuidad y seguridad.

Población y Muestra

La población de la investigación está conformada por los procesos y servicios de TI de Laminados de Occidente S.A. que inciden en la continuidad de la operación productiva y administrativa de la organización. Esta población incluye:

- Los sistemas de información críticos (principalmente el ERP Siesa y los sistemas complementarios asociados a producción, inventarios y facturación).
- La infraestructura tecnológica sobre la cual se soportan dichos sistemas (servidores, bases de datos, servidores de archivos y servicios de red).
- Los actores clave involucrados en la gestión de la información y de la operación (directivos, responsables de procesos y personal de TI).

Para efectos de la investigación se definió una muestra intencional, seleccionada con base en la criticidad de los procesos y en el rol de los participantes:

- **Procesos y sistemas incluidos en la muestra:**
    - Proceso de producción de envases y tubos colapsibles.
    - Proceso de gestión de inventarios y materias primas.
    - Proceso de facturación y despacho de productos.

- Sistema ERP Siesa y su base de datos principal.
- Sistema SCADA de planta, incluyendo el servidor de aplicación, base de datos de históricos
- Servidor de archivos asociado a documentación operativa y técnica crítica.

En el caso del sistema SCADA, se incluye dentro del análisis de criticidad, del BIA y de la matriz de riesgos por su impacto directo sobre la continuidad de la producción; no obstante, el diseño de arquitectura en Microsoft Azure se orienta principalmente a los componentes de registro, respaldo y explotación de datos, manteniendo las funciones de control en tiempo real sobre la infraestructura local o de borde de la planta.

- **Actores participantes:**
  - Gerente general de Laminados de Occidente S.A.
  - Jefe de planta / producción.
  - Jefe de logística / distribución.
  - Responsable de tecnología / sistemas.
  - Dos usuarios clave del ERP Siesa (área administrativa y área comercial).

En total, se trabajó con una muestra de seis (6) informantes clave, quienes aportaron información para el BIA, la identificación de riesgos y la definición de prioridades de recuperación. Las guías de entrevista utilizadas con cada uno de estos actores se presentan en los Anexos A al F, donde se detalla el conjunto de preguntas aplicadas y las orientaciones para la recolección de la información.

Técnicas e Instrumentos de Recolección de la Información

Para la recolección de la información se utilizaron las siguientes técnicas e instrumentos:

Revisión Documental

Se llevó a cabo un análisis de documentos internos de la organización, entre los que se incluyen:

- Organigrama y descripción general de la empresa.
- Diagramas de red y de infraestructura tecnológica disponibles.
- Listado de servidores, aplicaciones y bases de datos.
- Procedimientos internos relacionados con copias de seguridad, manejo de incidentes y soporte.

Esta revisión permitió comprender la estructura actual de la plataforma tecnológica y su relación con los procesos misionales.

Entrevistas Semiestructuradas

Se aplicaron entrevistas semiestructuradas a seis informantes clave (ver Anexos A al F), correspondientes al gerente general, jefe de planta, jefe de logística, responsable de tecnología y dos usuarios clave del ERP. Las entrevistas se orientaron a:

- Identificar los procesos críticos para la continuidad del negocio.
- Establecer la dependencia de dichos procesos frente a sistemas de información y recursos tecnológicos.
- Levantar percepciones sobre incidentes pasados, tiempos de recuperación reales y principales puntos débiles de la infraestructura actual.
- Identificar requerimientos y expectativas frente a una futura migración a la nube.

Las entrevistas se guiaron por un cuestionario base, pero permitieron profundizar en los temas que surgieron durante la conversación.

Las guías completas utilizadas en estas entrevistas se incluyen en los Anexos A al F:

- Anexo A: Guía de entrevista semiestructurada – Gerente General.
- Anexo B: Guía de entrevista semiestructurada – Jefe de Planta / Producción (MES/SCADA).
- Anexo C: Guía de entrevista semiestructurada – Jefe de Logística y Distribución.
- Anexo D: Guía de entrevista semiestructurada – Responsable de Tecnología / Sistemas.
- Anexo E: Guía de entrevista semiestructurada – Usuario clave ERP (Administración y Finanzas).
- Anexo F: Guía de entrevista semiestructurada – Usuario clave ERP (Área Comercial).

Estos instrumentos sirvieron como base para el levantamiento de información cualitativa que posteriormente se integró al diagnóstico del entorno tecnológico, al Análisis de Impacto al Negocio (BIA) y a la construcción de la matriz de riesgos.

Levantamiento Técnico de la Infraestructura de TI

Además de la revisión documental y de las entrevistas, se realizó un levantamiento técnico detallado de la infraestructura de servidores sobre la cual se ejecutan las aplicaciones críticas de Laminados de Occidente S.A. Este ejercicio tuvo como finalidad identificar, con precisión, las características de hardware y software que condicionan la continuidad del negocio.

Para ello se recopiló información de cada servidor relevante, incluyendo nombre lógico, rol principal, modelo y generación del equipo, tipo y cantidad de procesadores, memoria RAM instalada, tipo y capacidad de los discos, presencia o no de arreglos de redundancia (RAID) y versión del sistema operativo. De manera particular, se documentaron los servidores que alojan el ERP SIESA Gcuno 8 y su base de datos en SQL Server 2014, el servidor del MES/SCADA Ignition 7.8.5, el servidor de reportes y archivos, y el controlador de dominio.

Este levantamiento permitió evidenciar que varios de los equipos corresponden a modelos HP ProLiant de generaciones antiguas, con sistemas operativos como Windows Server 2012 / 2012 R2 y discos únicos sin RAID. La combinación de aplicaciones críticas y bases de datos en un mismo host, junto con la ausencia de redundancia de almacenamiento y la obsolescencia de las plataformas, se consolidó como un insumo clave para el análisis de riesgos, el BIA y la justificación de la migración hacia una arquitectura más resiliente en la nube.

Análisis de Impacto al Negocio (BIA)

Con base en la información obtenida de las entrevistas y del levantamiento técnico, se diseñó y aplicó un formato de Análisis de Impacto al Negocio (BIA) adaptado a la realidad de Laminados de Occidente S.A. Este instrumento permitió valorar, de manera estructurada, las consecuencias que tendría la interrupción de los servicios críticos sobre los procesos misionales.

El formato de BIA incluyó, entre otros, los siguientes campos: nombre del servicio o aplicación, procesos de negocio que depende de él, principales dependencias tecnológicas (servidores, bases de datos, red OT/IT, PLC), nivel de impacto ante una interrupción (en una escala de 1 a 5), Periodo Máximo Tolerable de Interrupción (MTPD), Objetivo de Tiempo de Recuperación (RTO) y Objetivo de Punto de Recuperación (RPO) en el escenario actual (AS-IS).

A través de sesiones de trabajo con el responsable de tecnología y los dueños de proceso, se diligenció el BIA para los servicios identificados como más críticos: el MES/SCADA Ignition, el ERP SIESA (aplicación y base de datos) y el servicio de reportes/BI. Este ejercicio permitió establecer, por ejemplo, que el sistema MES/SCADA presenta un impacto máximo (5), con un MTPD cercano a las 4 horas, mientras que el ERP se ubica en un nivel de impacto alto, con un MTPD estimado entre 8 y 12 horas. Los resultados consolidados del BIA se emplearon posteriormente como base para definir los requerimientos de continuidad en el diseño de la arquitectura objetivo en Microsoft Azure.

Matriz de Riesgos

Complementario al BIA, se construyó una matriz de riesgos orientada a identificar y priorizar las amenazas que afectan la continuidad de los servicios críticos. Para su elaboración se adoptó la metodología propuesta por la norma **ISO/IEC 27005**, estructurando el análisis en tres pasos:

1. **Identificación de activos:** Inventario de servidores y servicios críticos.
2. **Modelado de amenazas y vulnerabilidades:** Asociación de amenazas (ej. fallo de hardware, ransomware) con las debilidades técnicas específicas de la infraestructura actual (ej. obsolescencia, falta de parches, ausencia de RAID).
3. **Valoración del riesgo:** Cálculo del nivel de riesgo inherente mediante una escala cualitativa-semicuantitativa que combina la probabilidad de ocurrencia de la amenaza con el impacto global identificado previamente en el BIA.

Esta alineación metodológica asegura que la valoración no dependa de percepciones subjetivas, sino de un análisis estructurado de las vulnerabilidades técnicas reales diagnosticadas en la fase de levantamiento.

La matriz de riesgos no solo permitió priorizar los escenarios más críticos a tratar, sino que también orientó la definición de tratamientos propuestos, tales como la migración de bases de datos a servicios gestionados en Azure, la implementación de mecanismos de redundancia zonal y regional, el uso de soluciones de respaldo en la nube y el fortalecimiento de la seguridad de red bajo principios de Zero Trust.

Revisión de Marcos de Referencia y Buenas Prácticas

Como parte de las técnicas de recolección de información, se realizó una revisión dirigida de normas, marcos de referencia y documentación técnica especializada en continuidad del negocio y arquitecturas en la nube. Este ejercicio bibliográfico se centró en estándares como ISO 22301 (gestión de continuidad del negocio) (ISO, 2019) e ISO/IEC 27001 (ISO, 2022), en guías del NIST relacionadas con recuperación ante desastres (NIST, 2010) y en la documentación oficial de Microsoft sobre el Azure Well-Architected Framework, en particular el pilar de Reliability (Microsoft, 2025).

También se consultaron referencias sobre estrategias de alta disponibilidad, recuperación ante desastres (BCDR) y arquitecturas multirregión en Microsoft Azure, así como los acuerdos de nivel de servicio (SLA) asociados a máquinas virtuales, bases de datos administradas, servicios de backup y replicación. Esta revisión sirvió para contextualizar los hallazgos de la infraestructura actual de Laminados de Occidente S.A. frente a buenas prácticas internacionalmente reconocidas y para fundamentar las decisiones de diseño de la arquitectura objetivo, en términos de RTO, RPO, disponibilidad esperada y mecanismos de protección de la información.

La información obtenida de estos marcos de referencia no se trató como un simple marco teórico aislado, sino que se integró como un insumo práctico para validar el modelo propuesto y

para asegurar que las recomendaciones de migración a Azure resultaran coherentes con los requisitos de continuidad del negocio y con las exigencias de los sectores farmacéutico y cosmético a los que la empresa presta servicios.

Procedimiento y Fases del Estudio

El desarrollo de la investigación no se llevó a cabo como un conjunto de actividades aisladas, sino organizado en fases sucesivas que permitieron ir pasando del diagnóstico de la situación actual al diseño del modelo de continuidad del negocio y de la arquitectura objetivo en la nube. Cada fase se conectó directamente con uno o varios objetivos específicos y dio lugar a entregables concretos para la organización.

A continuación, se describen las fases consideradas en el estudio.

Fase 1 – Caracterización de la Organización y de la Infraestructura Tecnológica

En la primera fase se buscó comprender el contexto organizacional y tecnológico de Laminados de Occidente S.A. El propósito fue disponer de una visión clara de los procesos misionales, de los sistemas de información que los soportan y del estado actual de la infraestructura sobre la cual funcionan.

En esta fase se realizaron, entre otras, las siguientes actividades:

- Inventario Automatizado de Hardware y Software: Ejecución de scripts de auditoría (basados en PowerShell) y revisión manual de las consolas de administración para recopilar la configuración exacta de los servidores físicos (CPU, RAM, Discos), versiones de firmware y niveles de parcheo del sistema operativo.

- Análisis de Rendimiento: Recolección de contadores de rendimiento durante ventanas de operación pico para determinar el consumo real de recursos (IOPS de disco, uso de memoria y ancho de banda de red), dato clave para el dimensionamiento correcto (Rightsizing) en Azure.
- Mapeo de Dependencias de Red: Revisión de las tablas de enrutamiento en el firewall perimetral y diagramación lógica de las conexiones entre la red administrativa (IT) y la red de control industrial (OT), identificando puertos abiertos y flujos de datos críticos.
- Revisión de Políticas de Backup Actuales: Auditoría física de los medios de almacenamiento de copias de seguridad y verificación de los logs de tareas programadas para determinar la tasa de éxito real de los respaldos locales.
- Revisión de documentos internos relacionados con la estructura organizacional, descripción de procesos y lineamientos de TI.
- Levantamiento de información sobre los sistemas de información en uso, identificando aquellos considerados críticos para la operación (ERP SIESA Gcuno 8, MES/SCADA Ignition 7.8.5, servicios de reportes y servidor de dominio).
- Levantamiento técnico detallado de los servidores que alojan estas aplicaciones, registrando modelo de hardware, capacidades, versiones de sistema operativo y motor de base de datos, así como la presencia o ausencia de mecanismos de redundancia.

El resultado de esta fase fue un diagnóstico inicial AS-IS de la plataforma tecnológica de Laminados de Occidente S.A., que dejó en evidencia la existencia de servidores antiguos, sistemas operativos fuera de soporte, discos únicos sin RAID y una alta dependencia de infraestructura local sin alternativas de alta disponibilidad ni sitio alterno.

Fase 2 – Análisis de Riesgos y Análisis de Impacto al Negocio (BIA)

Con la información de la fase anterior, la segunda fase se centró en valorar el riesgo y el impacto que tendría la interrupción de los servicios críticos sobre la operación del negocio.

En esta fase se llevaron a cabo las siguientes acciones:

- Aplicación de entrevistas semiestructuradas a informantes clave (gerencia, producción, logística, tecnología y usuarios del ERP), con el fin de identificar procesos críticos, incidentes de indisponibilidad y percepciones sobre tiempos de tolerancia a fallas.
- Diligenciamiento del formato de BIA para los servicios ERP SIESA, MES/SCADA Ignite y reportes/BI, estimando el impacto de su indisponibilidad, el Periodo Máximo Tolerable de Interrupción (MTPD), y los valores de RTO y RPO en el escenario actual.
- Construcción de una matriz de riesgos, relacionando activos críticos (servidores, aplicaciones, respaldos, red) con amenazas, vulnerabilidades, probabilidad de ocurrencia, impacto y nivel de riesgo resultante, así como posibles tratamientos.
- Talleres de Calibración de Impacto: Realización de sesiones de trabajo con la Gerencia General para definir y validar las escalas de impacto financiero (en SMMLV), reputacional y legal, alineadas con la norma ISO/TS 22317.
- Ejecución de Entrevistas Semiestructuradas: Aplicación de los instrumentos de recolección de información a los dueños de los procesos de Producción, Logística y Finanzas para estimar los tiempos de inactividad máximos tolerables (MTPD) basados en escenarios reales de falla.
- Cálculo de Brechas de Recuperación: Comparación cuantitativa entre el RTO requerido por el negocio (obtenido en las entrevistas) y el RTO real estimado técnicamente (basado en la infraestructura obsoleta), documentando el "Gap de Continuidad".

- Valoración de Riesgos con Matriz de Calor: Mapeo de amenazas específicas (ej. fallo de disco único, ransomware) contra las vulnerabilidades detectadas, calculando el riesgo inherente mediante la fórmula Probabilidad x Impacto, siguiendo las directrices de la norma ISO/IEC 27005.

Esta fase produjo como entregables un cuadro BIA consolidado y una matriz de riesgos priorizada, que permitieron justificar la necesidad de mejorar los mecanismos de continuidad y orientaron las decisiones posteriores de diseño en la nube.

Fase 3 – Diseño del Modelo de Continuidad del Negocio y Aseguramiento de la Información

A partir de los resultados del diagnóstico y del BIA, la tercera fase estuvo orientada a definir el modelo de continuidad del negocio y el esquema de aseguramiento de la información para Laminados de Occidente S.A., sin entrar todavía en la tecnología específica de la nube.
En esta fase se desarrollaron las siguientes actividades:

- Definición de principios de continuidad para la organización, tales como resiliencia, redundancia, priorización de servicios, automatización de recuperación y protección de la información.
- Establecimiento de requisitos de continuidad para los servicios críticos, a partir de los valores de impacto, MTPD, RTO y RPO identificados en el BIA.
- Identificación de controles y prácticas de aseguramiento de la información alineados con normas como ISO 22301 e ISO/IEC 27001, considerando aspectos de disponibilidad, integridad y confidencialidad de los datos.
- Elaboración de un modelo conceptual que relaciona procesos de negocio, servicios de TI, amenazas, medidas de continuidad y actividades de respuesta ante incidentes.

- Selección de Servicios y SKUs en Azure: Definición de los componentes de infraestructura como servicio (IaaS) y plataforma como servicio (PaaS), seleccionando las familias de máquinas virtuales y niveles de servicio de base de datos (Business Critical) que cumplen con los SLA requeridos.
- Diseño de Red y Seguridad (Landing Zone): Definición de la topología de red virtual (VNet), segmentación de subredes, reglas de Grupos de Seguridad de Red (NSG) y configuración de la VPN Site-to-Site para la conectividad híbrida segura.
- Estrategia de Resiliencia y Recuperación: Configuración teórica de los grupos de disponibilidad (Availability Sets), políticas de Azure Backup (frecuencia y retención) y planes de replicación de Azure Site Recovery entre la región principal (East US) y la región de contingencia.
- Estimación de Costos Operativos: Uso de la calculadora oficial de precios de Azure para proyectar el costo mensual de la solución (TCO), validando la viabilidad económica frente al presupuesto de TI de la organización.

Al cierre de esta fase se obtuvo un modelo de continuidad y aseguramiento de la información adaptado a la realidad de Laminados de Occidente S.A., que sirve como puente entre el análisis de la situación actual y la propuesta de arquitectura en Microsoft Azure.

Fase 4 – Diseño y Validación de la Arquitectura de Referencia en Microsoft Azure

La cuarta fase se enfocó en traducir el modelo de continuidad y los requisitos de servicio en una arquitectura de referencia TO-BE soportada por la nube de Microsoft Azure, teniendo en cuenta el pilar de Reliability del Azure Well-Architected Framework.

Las actividades principales de esta fase fueron:

- Selección de servicios de Azure apropiados para soportar las aplicaciones críticas (máquinas virtuales para componentes legados, Azure SQL Managed Instance para la base de datos del ERP, Azure Backup, Azure Site Recovery, servicios de red y seguridad, entre otros).
- Diseño de una arquitectura multizona y multirregión (por ejemplo, región principal East US y región secundaria Central US), definiendo cómo se implementan la redundancia, la replicación de datos y los mecanismos de conmutación por desastre (DR).
- Estimación de los RTO y RPO TO-BE, tomando como referencia las capacidades y SLA publicados por Microsoft para los servicios seleccionados y comparándolos con los valores AS-IS obtenidos en el BIA.
- Validación de la arquitectura propuesta frente a los objetivos específicos del proyecto, los riesgos identificados y las recomendaciones de los marcos de referencia revisados, verificando que la solución contribuya efectivamente a mejorar la continuidad del negocio y el aseguramiento de la información.
- Análisis de Estrategias de Migración: Evaluación de cada carga de trabajo para determinar la estrategia adecuada (Rehost, Refactor, Replatform), priorizando la estabilidad del ERP y el sistema SCADA.
- Diseño de Pruebas de Concepto (PoC): Definición de protocolos de prueba para validar la latencia de la aplicación y la integridad de los datos antes de la migración definitiva.
- Elaboración del Plan de Retorno (Rollback): Documentación de los procedimientos técnicos paso a paso para revertir la operación al entorno on-premise en caso de fallos críticos durante la ventana de migración.

- Definición de Métricas de Monitoreo: Selección de los indicadores clave de rendimiento (KPI) y configuración de alertas en Azure Monitor para supervisar proactivamente la salud de los servicios migrados.

Como resultado, se obtuvo una arquitectura de referencia en Microsoft Azure que responde a las necesidades de continuidad de Laminados de Occidente S.A., junto con criterios para una migración gradual que permita mantener la operación activa durante el proceso de transición.

Técnicas de Análisis de la Información

La información recopilada a través de los diferentes instrumentos (entrevistas semiestructuradas, revisión documental, levantamiento técnico de infraestructura, BIA y matriz de riesgos) se sometió a un proceso de análisis que combinó enfoques cualitativos y cuantitativos. El objetivo fue no solo describir la situación actual de Laminados de Occidente S.A., sino también contrastarla con los requerimientos de continuidad del negocio y con las capacidades de la solución propuesta en Microsoft Azure.

Análisis Cualitativo

En primer lugar, se realizó un análisis cualitativo de contenido sobre la información obtenida en las entrevistas y en los documentos internos de la organización. Para ello, se agruparon las respuestas de los diferentes informantes en categorías temáticas, tales como:

- Procesos de negocio considerados críticos.
- Dependencia de los procesos frente al ERP SIESA y al MES/SCADA Ignition.
- Experiencias previas de fallas e indisponibilidad de sistemas.

- Percepciones sobre tiempos aceptables de interrupción y pérdida de información.
- Riesgos percibidos en relación con la infraestructura actual y con la seguridad de la información.

Esta clasificación permitió identificar patrones recurrentes y puntos de convergencia entre las distintas áreas (gerencia, producción, logística, tecnología, administración y comercial), así como posibles divergencias entre la percepción de riesgo y la realidad técnica observada en el levantamiento de infraestructura.

Adicionalmente, se analizaron documentos internos y registros disponibles (por ejemplo, inventarios de servidores, reportes de incidentes, lineamientos de TI), con el fin de complementar y contrastar lo expresado en las entrevistas. Este cruce de información permitió construir una visión más completa del contexto organizacional y tecnológico de Laminados de Occidente S.A., que sirvió como base para la formulación del modelo de continuidad del negocio.

Análisis Cuantitativo de Riesgos y Continuidad

En paralelo al análisis cualitativo, se aplicaron técnicas de análisis cuantitativo sobre los datos estructurados derivados del BIA y de la matriz de riesgos. En el caso del Análisis de Impacto al Negocio (BIA), se normalizaron los valores de impacto (en una escala de 1 a 5) y se sistematizaron los tiempos estimados de MTPD, RTO y RPO para cada servicio crítico (ERP, MES/SCADA y reportes). Estos datos permitieron:

- Comparar el nivel de criticidad relativa entre los diferentes servicios.
- Identificar qué aplicaciones presentan brechas más significativas entre la tolerancia del negocio y las capacidades actuales de recuperación.
- Establecer prioridades en términos de inversión y esfuerzos de continuidad.

En cuanto a la matriz de riesgos, se asignaron valores de probabilidad e impacto a cada combinación activo–amenaza–vulnerabilidad, utilizando escalas sencillas (por ejemplo: baja, media, alta) apoyadas en valores numéricos. A partir de estos valores se calculó un nivel de riesgo resultante, que permitió clasificar los escenarios en riesgos moderados, altos o críticos.

Este análisis cuantitativo evidenció, entre otros aspectos, que los servidores que soportan el ERP y el MES/SCADA (al estar montados sobre hardware obsoleto, con sistemas operativos fuera de soporte y sin redundancia de discos) concentran un nivel de riesgo crítico para la continuidad del negocio. Asimismo, se identificó como factor de riesgo relevante la dependencia de respaldos locales sin replicación automática fuera del sitio.

Análisis Comparativo AS-IS vs TO-BE de RTO/RPO

Con el fin de valorar el impacto potencial de la migración hacia la nube, se realizó un análisis comparativo entre la situación actual (AS-IS) y el escenario propuesto en Microsoft Azure (TO-BE) en términos de RTO y RPO para los servicios críticos.

Para ello, se partió de los valores de RTO y RPO actuales estimados en el BIA y se contrastaron con los tiempos de recuperación y pérdida de datos que es posible alcanzar utilizando servicios de Azure tales como:

- Máquinas virtuales distribuidas en Zonas de Disponibilidad.
- Azure SQL Managed Instance con opciones de alta disponibilidad y restauración a un punto en el tiempo.
- Azure Backup con almacenamiento georredundante.
- Azure Site Recovery para replicación y recuperación ante desastres entre regiones.

En este análisis se tuvieron en cuenta los SLA publicados por Microsoft para estos servicios, así como las características de las arquitecturas multizona y multirregión. A partir de esa información se elaboraron cuadros comparativos donde, por ejemplo, el MES/SCADA y el ERP pasan de RTO de varias horas (6–12 h) y RPO de medio día o más, a objetivos de recuperación del orden de minutos en el escenario TO-BE.

Este ejercicio permitió demostrar, de manera cuantitativa, la mejora en continuidad que aporta la arquitectura propuesta en la nube y sirvió para comprobar que los nuevos valores de RTO y RPO se alinean mejor con los MTPD definidos por el negocio.

Triangulación de Fuentes

Los resultados de los análisis cualitativo y cuantitativo se integraron mediante un proceso de triangulación de fuentes. Esto implicó contrastar:

- Lo expresado por los distintos actores en las entrevistas.
- Los hallazgos del diagnóstico técnico y del inventario de servidores y aplicaciones.
- Los valores obtenidos en el BIA y en la matriz de riesgos.
- Las recomendaciones y buenas prácticas extraídas de los marcos de referencia revisados (normas de continuidad del negocio y documentación oficial de Azure).

Esta triangulación permitió verificar la coherencia interna de los resultados, reducir sesgos derivados de una única fuente de información y fortalecer la validez del modelo de continuidad del negocio y de la arquitectura en Microsoft Azure propuesta para Laminados de Occidente S.A.

Matriz de Relación entre Objetivos, Actividades, Instrumentos y Entregables

Con el fin de asegurar la coherencia entre los objetivos planteados en el capítulo 1, el diseño metodológico y los resultados que se presentan en capítulos posteriores, se construyó una matriz que relaciona cada objetivo específico con las actividades principales realizadas, las técnicas e instrumentos de recolección de información empleados y los productos o entregables obtenidos. Esta matriz permite verificar que todos los objetivos específicos se encuentran efectivamente desarrollados en el cuerpo del trabajo y que cada uno de ellos se traduce en resultados concretos para la organización. A continuación, se presenta la matriz de relación:

Tabla 1.
Matriz de relación entre objetivos específicos, actividades, técnicas e instrumentos y entregables.

Objetivo específico	Actividades principales	Técnicas / instrumentos	Productos / entregables
1. Analizar la situación actual de la infraestructura tecnológica de Laminados de Occidente S.A.S., identificando sus principales riesgos y vulnerabilidades.	Revisión de la documentación disponible sobre la plataforma de TI y los procesos misionales; levantamiento técnico de servidores y aplicaciones críticas (ERP SIESA, MES/SCADA Ignition, reportes y dominio); entrevistas con el responsable de tecnología y con los líderes de proceso para complementar la información.	Revisión documental de lineamientos e inventarios de TI; levantamiento técnico de infraestructura (servidores, sistemas operativos, bases de datos, almacenamiento); entrevistas semiestructuradas a responsables clave (ver Anexos 1 a 6).	Diagnóstico AS-IS de la infraestructura tecnológica; inventario de servidores y aplicaciones críticas con sus principales características; identificación preliminar de riesgos y vulnerabilidades asociados a obsolescencia, falta de redundancia y dependencia de infraestructura local.
2. Definir los componentes, políticas y niveles de servicio (RTO, RPO, SLA) necesarios para asegurar la continuidad del negocio.	Realización de sesiones de trabajo con el responsable de TI y dueños de proceso; aplicación del formato de Análisis de Impacto al Negocio (BIA) para los servicios críticos; estimación de MTPD, RTO y RPO en el escenario actual; contraste de estos valores con las necesidades del negocio y con las capacidades de las soluciones en la nube.	Formato de BIA adaptado a la realidad de Laminados de Occidente S.A.; entrevistas semiestructuradas para levantar percepciones de impacto y tiempos de tolerancia; revisión de documentación técnica y SLA de servicios Azure relacionados con continuidad y disponibilidad.	Cuadro BIA consolidado para el ERP, el MES/SCADA y el servicio de reportes/BI; tabla de requisitos de continuidad y niveles de servicio (MTPD, RTO, RPO, SLA) para los servicios críticos; identificación de brechas entre la situación actual y los requerimientos deseados.
3. Diseñar una arquitectura de referencia en la nube de Microsoft Azure que integre medidas de seguridad, respaldo y recuperación ante desastres.	Selección de servicios de Azure adecuados a los requisitos de continuidad y seguridad definidos; diseño de una arquitectura multi-zona y multi-región (East US / Central US) para soportar el ERP y el MES/SCADA; definición de mecanismos de respaldo, alta disponibilidad y recuperación ante desastres; incorporación de controles de seguridad y gobernanza.	Revisión del Azure Well-Architected Framework (pilar Reliability) y de la documentación oficial de Azure sobre alta disponibilidad y BCDR; análisis de opciones técnicas con el responsable de TI; contraste con los riesgos identificados en la matriz de riesgos.	Arquitectura TO-BE en Microsoft Azure para los servicios críticos de Laminados de Occidente S.A.; diagramas de red y de componentes (ERP, MES/SCADA, bases de datos, backup, Site Recovery, seguridad de red); descripción técnica de los servicios de Azure utilizados y de su contribución a la continuidad del negocio y al aseguramiento de la información.

Tabla 1 (continuación)

Objetivo específico	Actividades principales	Técnicas / instrumentos	Productos / entregables
4. Proponer un plan de migración gradual que permita mantener la operación activa durante el proceso de transición.	Identificación de dependencias entre aplicaciones y servidores en el entorno actual; definición de oleadas o fases de migración (por servicio o por componente); análisis de riesgos asociados a la transición; formulación de criterios de ejecución, monitoreo y reversa para cada fase de migración.	Revisión del diagnóstico AS-IS y de la arquitectura TO-BE; entrevistas con responsables de tecnología y líderes de procesos para validar restricciones operativas; análisis de escenarios de migración (lift-and-shift, modernización parcial, coexistencia temporal).	Plan de migración por fases de los servicios críticos hacia Microsoft Azure, con secuencia de actividades y dependencias; propuesta de cronograma de alto nivel; identificación de riesgos de transición y medidas de mitigación para mantener la operación activa durante el cambio.
5. Establecer lineamientos de monitoreo, capacitación y mejora continua que fortalezcan la cultura de seguridad y resiliencia organizacional.	Identificación de indicadores clave de continuidad y seguridad; revisión de capacidades de monitoreo y registro disponibles en Azure (logs, alertas, paneles); definición de roles y responsabilidades para la operación del modelo; propuesta de actividades básicas de capacitación y de un ciclo de revisión periódica del modelo.	Revisión de marcos de referencia (ISO 22301, ISO/IEC 27001 y Azure Well-Architected Framework); entrevistas con el responsable de TI y con la gerencia para entender expectativas de gobernanza; análisis de las herramientas de monitoreo y logging en Azure.	Lineamientos de monitoreo y operación del modelo de continuidad (qué se debe supervisar, con qué herramientas y con qué frecuencia); propuesta de plan básico de capacitación para el personal involucrado; esquema de mejora continua que incluye pruebas periódicas de recuperación, revisión de indicadores y actualización del modelo de continuidad del negocio.

Nota: Tabla diseñada para asegurar la coherencia entre los objetivos planteados en el capítulo 1, el diseño metodológico y los resultados. Fuente: Elaboración propia

Variables e Indicadores del Estudio

Aunque el presente trabajo tiene un enfoque aplicado y de diseño arquitectónico, resulta pertinente explicitar las variables de estudio y los indicadores utilizados para valorar los efectos del modelo propuesto sobre la continuidad del negocio de Laminados de Occidente S.A. Esto contribuye a dar mayor transparencia a la lógica de análisis y a la forma en que se contrastan la situación actual (AS-IS) y el escenario objetivo (TO-BE).

En coherencia con el objetivo general y los objetivos específicos, se consideran las siguientes variables:

Variable Independiente:

Modelo de continuidad del negocio y arquitectura de referencia en Microsoft Azure diseñada para los servicios críticos de Laminados de Occidente S.A. Esta variable se operacionaliza a través de las decisiones de diseño (uso de servicios gestionados, redundancia zonal y regional, mecanismos de backup y recuperación ante desastres, segmentación de redes, controles de seguridad y lineamientos de operación).

Variables Dependientes Principales:

1. Nivel de continuidad operativa esperada para los servicios críticos (ERP, MES/SCADA, reportes y dominio).
2. Niveles de servicio de recuperación definidos para dichos servicios:
   - Recovery Time Objective (RTO).
   - Recovery Point Objective (RPO).
3. Nivel de riesgo tecnológico residual asociado a la indisponibilidad de los servicios críticos.

4. Grado de alineación con marcos de referencia en continuidad y seguridad (ISO 22301, ISO/IEC 27001, NIST SP 800-34, Azure Well-Architected, entre otros).

Para efectos de análisis, cada variable se relaciona con uno o más indicadores cualitativos y cuantitativos, resumidos en la Tabla 2

Tabla 2.
Variables e indicadores del estudio

Variable	Tipo	Indicadores principales	Fuente de información	Método de obtención
Modelo de continuidad y arquitectura TO-BE en Azure	Independiente	a) Presencia de redundancia zonal y regional. b) Uso de servicios gestionados para datos críticos. c) Existencia de mecanismos formales de backup y DR. d) Lineamientos de monitoreo y mejora continua.	Diseño arquitectónico, documentación técnica de Azure, marcos de referencia utilizados.	Revisión documental, análisis de arquitectura, triangulación con entrevistas a personal de TI.
Nivel de continuidad operativa esperada	Dependiente	a) Valores de RTO y RPO definidos para cada servicio crítico en el escenario TO-BE. b) Comparación de dichos valores con el MTPD del negocio.	BIA, comparativo AS-IS vs TO-BE, entrevistas a informantes clave.	Análisis de BIA, elaboración de matrices comparativas, juicio experto.
Niveles de servicio de recuperación (RTO, RPO)	Dependiente	a) RTO AS-IS y TO-BE por servicio. b) RPO AS-IS y TO-BE por servicio. c) Brecha de mejora (reducción de tiempo de recuperación y de pérdida de datos).	Levantamiento de la infraestructura actual, BIA, diseño arquitectónico TO-BE.	Estimación semicuantitativa, matrices de comparación, apoyo en documentación de capacidades de la plataforma.
Riesgo tecnológico residual	Dependiente	a) Clasificación de riesgo (bajo, moderado, alto, crítico) para cada activo crítico antes y después del modelo propuesto. b) Número de puntos únicos de falla identificados. c) Presencia de controles de mitigación.	Matriz de riesgos, entrevistas, documentación de arquitectura.	Análisis de matrices 5×5 de probabilidad e impacto, triangulación de fuentes.

Tabla 2. (continuación)

Variable	Tipo	Indicadores principales	Fuente de información	Método de obtención
Alineación con marcos de referencia	Dependiente	a) Correspondencia entre componentes del modelo y requisitos de ISO 22301 (continuidad). b) Correspondencia con controles de ISO/IEC 27001 (seguridad de la información). c) Alineación con el pilar de fiabilidad del Azure Well-Architected Framework.	Marco teórico, diseño del modelo, documentación de Microsoft y normas internacionales.	Análisis de correspondencia (gap analysis), revisión cruzada de requerimientos y componentes del modelo.

Nota: Tabla diseñada para efectos de análisis, cada variable se relaciona con uno o más indicadores cualitativos y cuantitativos Fuente: Elaboración propia

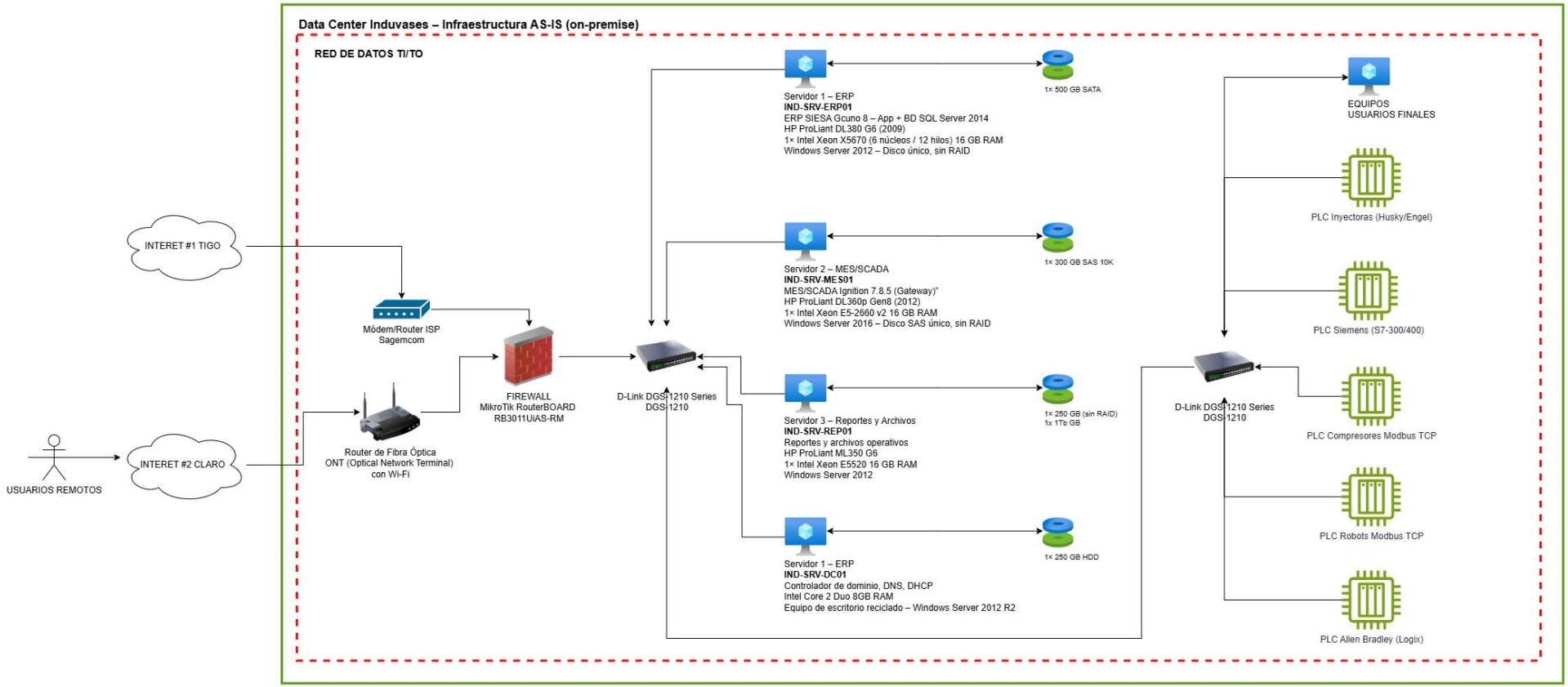
Resultados

En este capítulo se presentan los principales resultados obtenidos a partir de la aplicación de las técnicas e instrumentos descritos en el capítulo metodológico. Primero se expone el diagnóstico de la infraestructura tecnológica actual (AS-IS) de Laminados de Occidente S.A., para luego avanzar hacia el análisis de impacto al negocio (BIA), la matriz de riesgos y el contraste entre la situación actual y la arquitectura objetivo, propuesta en Microsoft Azure.

Diagnóstico AS-IS de la Infraestructura Tecnológica de Laminados de Occidente S.A.

El punto de partida del estudio fue comprender en qué condiciones se encuentran hoy los servicios tecnológicos que sostienen los procesos críticos de Laminados de Occidente S.A., en particular el ERP SIESA Gcuno 8, el sistema MES/SCADA Ignition 7.8.5 y los servicios de reportes y directorio activo. Para ello se realizó un levantamiento técnico de los servidores, complementado con entrevistas al responsable de tecnología y a los líderes de proceso. El análisis evidenció que la organización depende de una infraestructura local basada en servidores físicos antiguos, con sistemas operativos en versiones cercanas o ya fuera de soporte, sin mecanismos de redundancia de discos y con una fuerte concentración de cargas críticas en pocos equipos. En la Figura 6 se presenta un esquema simplificado de la arquitectura AS-IS de Laminados de Occidente S.A., donde se observa la concentración de servicios críticos (ERP, MES/SCADA, reportes y servicios de dominio) en un conjunto reducido de servidores físicos ubicados en la sede de la organización. Como se ha descrito, estos equipos operan sin redundancia de discos, con sistemas operativos y motores de base de datos en versiones obsoletas o próximas al fin de soporte, y sin un sitio alterno de recuperación, lo que explica los niveles de riesgo y las brechas de continuidad identificados en los apartados anteriores.

Figura 6.
Esquema AS-IS de la infraestructura tecnológica de Laminados de Occidente S.A. S.A.



Nota: El diagrama ilustra la infraestructura tecnológica actual de Laminados de Occidente S.A. Fuente: Elaboración propia a partir del levantamiento de infraestructura (2025).

En la Figura 6 se aprecia, además, la forma en que se estructura la red de Laminados de Occidente S.A. En el extremo izquierdo se representan dos enlaces de Internet suministrados por operadores distintos (Tigo y Claro), que convergen en un módem/router del proveedor y en un router de fibra óptica. Ambos dispositivos alimentan un único firewall MikroTik RB3011UiAS-RM, desde el cual el tráfico se dirige a un switch de distribución D-Link DGS-1210 que actúa como punto central de conexión para los servidores y para la red de planta.

En la parte derecha del esquema se ubican los cuatro servidores físicos identificados en la Tabla 3 (IND-SRV-ERP01, IND-SRV-MES01, IND-SRV-REP01 e IND-SRV-DC01), conectados a dicho switch central, así como los controladores lógicos programables (PLC) que gobiernan inyectoras, compresores, robots y líneas de producción basadas en plataformas Siemens y Allen-Bradley. La red de control industrial (OT) y la red corporativa (TI) comparten, en la práctica, la misma infraestructura de conmutación, sin una segmentación lógica formal más allá del firewall perimetral.

El diagrama también ilustra la presencia de usuarios remotos que acceden a los servicios corporativos a través de los enlaces de Internet disponibles. Esta configuración refuerza la existencia de puntos únicos de falla (firewall, switch principal) y de un acoplamiento estrecho entre TI y OT, elementos que explican el riesgo elevado de propagación de incidentes y la clasificación de “alto” o “crítico” asociada a la debilidad de los controles de segmentación en la matriz de riesgos presentada más adelante.

Servidores y Aplicaciones Críticas

En la Tabla 3 se presenta una síntesis de los servidores que alojan las aplicaciones más relevantes para la operación de Laminados de Occidente S.A., junto con sus principales características de hardware y software.

Tabla 3.
Servidores y aplicaciones críticas de Laminados de Occidente S.A. (escenario AS-IS)

Nombre del servidor	Rol / Aplicación principal	Modelo HP / Año aprox.	CPU	RAM	Almacenamiento	Sistema operativo
IND-SRV-ERP01	ERP SIESA Gcuno 8 (aplicación + base de datos SQL 2014)	HP ProLiant DL380 G6 (2009)	1× Intel Xeon X5670 (6 núcleos / 12 hilos)	16 GB	1× 500 GB SATA (sin RAID)	Windows Server 2012
IND-SRV-MES01	MES/SCADA Ignition 7.8.5 (Ignition Gateway)	HP ProLiant DL360p Gen8 (2012)	1× Intel Xeon E5-2660 v2 (10c / 20t)	16 GB	1× 300 GB SAS 10K (sin RAID)	Windows Server 2016
IND-SRV-REP01	Servidor de reportes y archivos	HP ProLiant ML350 G6	1× Intel Xeon E5520 (4c / 8t)	16 GB	1× 250 GB (sin RAID) 1x 1Tb GB	Windows Server 2012 R2
IND-SRV-DC01	Controlador de dominio, DNS y DHCP	Equipo de escritorio reciclado	Intel Core 2 Duo	8 GB	1× 250 GB HDD	Windows Server 2012 R2

Nota: En la Tabla 3 se presenta una síntesis de los servidores que alojan las aplicaciones más relevantes para la operación de Laminados de Occidente S.A. Fuente: Elaboración propia a partir del levantamiento de infraestructura (2025)

En el caso del ERP, la aplicación SIESA Gcuno 8 y la base de datos SQL Server 2014 se ejecutan en el mismo servidor (IND-SRV-ERP01), lo que implica que la carga transaccional y el motor de base de datos compiten por los mismos recursos de CPU, memoria y disco. El sistema MES/SCADA se soporta en la plataforma Ignition 7.8.5, una versión antigua que requiere Java 8 y que se ejecuta sobre Windows Server 2016 en el servidor IND-SRV-MES01.

El servidor IND-SRV-REP01 agrupa funciones de reportes y almacenamiento de archivos, mientras que el IND-SRV-DC01 cumple roles de infraestructura básica (directorio activo, DNS, DHCP), pero está montado sobre un equipo que no fue diseñado originalmente como servidor corporativo.

Obsolescencia, Falta de Redundancia y Concentración de Servicios

Del análisis de la infraestructura se desprenden varios hallazgos que afectan directamente la continuidad del negocio y el aseguramiento de la información. En la Tabla 4 se resumen los principales problemas identificados por servidor.

Tabla 4.
Principales problemas identificados en la infraestructura AS-IS

Activo / Servidor	Tipo de problema principal	Descripción del problema	Riesgo asociado para la continuidad del negocio
IND-SRV-ERP01	Obsolescencia y concentración de cargas	Servidor HP ProLiant DL380 G6 (2009) con Windows Server 2012 y SQL Server 2014, ambos en versiones cercanas o fuera de soporte. Aplicación ERP y base de datos comparten el mismo host. No existe RAID ni servidor en espejo.	Alta probabilidad de caída completa del ERP ante falla de hardware o disco; tiempos de recuperación prolongados; riesgo de pérdida de datos y dificultades para cumplir requerimientos de auditoría y trazabilidad.
IND-SRV-MES01	Falta de alta disponibilidad en sistema crítico	Versión antigua de Ignition (7.8.5) sin esquema de redundancia de gateway; único disco SAS sin RAID; dependencia directa de este servidor para la supervisión y registro de producción.	Interrupción del sistema MES/SCADA implica pérdida de visibilidad sobre producción, riesgos en la calidad y en la seguridad del proceso; tiempos de recuperación estimados entre 6 y 12 horas en incidentes graves.
IND-SRV-REP01	Infraestructura obsoleta y sin respaldo robusto	Servidor HP ProLiant ML350 G6 con Windows Server 2012 R2 y un solo disco sin redundancia. Aloja reportes y archivos operativos.	Aunque su impacto es menor en tiempo real, la pérdida de este servidor puede afectar la disponibilidad de reportes históricos y documentación de soporte para auditorías y análisis.

Tabla 4. (continuación)

Activo / Servidor	Tipo de problema principal	Descripción del problema	Riesgo asociado para la continuidad del negocio
IND-SRV-DC01	Hardware inadecuado y riesgo global de infraestructura	Controlador de dominio, DNS y DHCP montado sobre un equipo de escritorio reciclado, con recursos limitados y sin discos redundantes.	Falla de este equipo puede dejar indisponibles servicios básicos de autenticación y resolución de nombres, afectando al resto de servidores y estaciones de trabajo de la organización.

Nota: Tabla diseñada para evaluar los principales problemas identificados por servidor. Fuente: Elaboración propia a partir del levantamiento de infraestructura (2025)

A estos problemas se suma el hecho de que los respaldos se realizan de manera local, con copias diarias en el mismo entorno y copias semanales en medios extraíbles gestionados manualmente. No existe, en el escenario actual, una solución de backup automatizado y georredundante, ni procedimientos sistemáticos de prueba de restauración.

De manera general, el diagnóstico AS-IS muestra una infraestructura:

- Monolítica y centralizada, apoyada en pocos servidores físicos.
- Con sistemas operativos y motores de base de datos en versiones obsoletas o próximas al fin de soporte.
- Sin redundancia de discos ni esquemas de alta disponibilidad para las aplicaciones críticas.
- Dependiente de respaldos locales que no garantizan protección adecuada frente a desastres mayores o incidentes de seguridad.

Estos hallazgos se convierten en insumo directo para el Análisis de Impacto al Negocio (BIA) y la matriz de riesgos que se presentan en los apartados siguientes, y justifican la

necesidad de migrar los servicios críticos hacia una arquitectura más resiliente en la nube de Microsoft Azure.

Resultados del Análisis de Impacto al Negocio (BIA)

El Análisis de Impacto al Negocio (Business Impact Analysis, BIA) se desarrolló con el propósito de determinar el efecto que tendría la interrupción de los servicios tecnológicos críticos sobre los procesos misionales de Laminados de Occidente S.A., y de esta manera establecer los tiempos máximos tolerables de interrupción (MTPD), así como los objetivos de tiempo de recuperación (RTO) y de punto de recuperación (RPO) en el escenario actual.

El BIA se diseñó tomando como referencia los lineamientos de la norma ISO 22301 (gestión de continuidad del negocio) y la guía específica para BIA recogida en ISO/TS 22317, adaptando sus principios al contexto de una organización manufacturera de envases y tubos colapsibles. El BIA constituye uno de los principales entregables asociados al Objetivo específico 2, al proporcionar una base cuantitativa y cualitativa para definir los niveles de servicio de continuidad requeridos por el negocio.

Enfoque Metodológico y Normativo

Para garantizar la validez de los resultados, el BIA se desarrolló siguiendo los lineamientos de la especificación técnica ISO/TS 22317:2015 (Directrices para el análisis del impacto empresarial). El procedimiento se estructuró en cuatro etapas secuenciales:

1. **Contextualización y priorización:** Identificación de productos y servicios prioritarios (envases para sectores farmacéutico y cosmético) y los procesos que los soportan.

2. **Definición de criterios de impacto:** Establecimiento de escalas parametrizadas para evaluar el daño en dimensiones financiera, operativa, legal y reputacional.
3. **Evaluación de dependencias:** Mapeo de la relación entre procesos de negocio y los activos tecnológicos actuales (Servidores y Aplicaciones identificados en el diagnóstico AS-IS).
4. **Determinación de requisitos de continuidad:** Cálculo del Período Máximo Tolerable de Interrupción (MTPD) y definición de los objetivos de recuperación (RTO y RPO) requeridos

Definición de Parámetros y Escalas Utilizadas

Con el fin de mitigar la subjetividad en la evaluación del riesgo, se definieron escalas de valoración ajustadas a la realidad de una empresa de manufactura industrial. En la tabla 5 se evidencian los hallazgos cualitativos de las entrevistas en niveles de criticidad estandarizados.

Tabla 5.
Criterios de Evaluación de Impacto Multidimensional

Nivel	Valor	Impacto Financiero (Estimado por evento)	Impacto Operativo (Producción/Logística)	Impacto Regulatorio y Legal	Impacto Reputacional
Bajo	1	< 10 SMMLV	Interrupción menor (< 2 horas). Recuperable con horas extra.	Sin incumplimiento legal. Observación menor interna.	Quejas aisladas sin escalamiento.
Moderado	2	10 - 50 SMMLV	Retrasos en procesos de soporte. No afecta la línea de producción principal.	Observaciones en auditorías internas de calidad.	Reclamos formales de clientes no estratégicos.

Tabla 5. (continuación)

Nivel	Valor	Impacto Financiero (Estimado por evento)	Impacto Operativo (Producción/Logística)	Impacto Regulatorio y Legal	Impacto Reputacional
Alto	3	50 - 100 SMMLV	**Parada parcial de planta.** Afectación de despachos del día. Retrasos en facturación.	Posible incumplimiento contractual leve. Hallazgos en auditoría ISO 9001.	Quejas de clientes recurrentes. Tensión comercial.
Muy Alto	4	100 - 300 SMMLV	**Parada total de turno.** Incumplimiento de entregas críticas (JIT). Pérdida de trazabilidad de lotes.	Riesgo de sanciones regulatorias. Hallazgos mayores en auditorías de clientes farmacéuticos.	Pérdida de confianza de clientes clave. Riesgo de devolución de lotes.
Crítico	5	> 300 SMMLV	**Parada operativa > 24h.** Pérdida masiva de materia prima o producto en proceso. Cese de flujo de caja.	Demandas legales. Cierre temporal por entes de control sanitario/ambiental.	Daño irreversible a la imagen corporativa. Pérdida de contratos estratégicos.

Nota: La tabla 5 permite traducir los hallazgos cualitativos de las entrevistas en niveles de criticidad estandarizados. Fuente: elaboración propia.

Mapeo de Dependencias Críticas

Antes de cuantificar el impacto, fue necesario establecer la dependencia técnica de los procesos misionales frente a la infraestructura obsoleta identificada en el diagnóstico, ver tabla 6.

Tabla 6.
Relación Procesos - Servicios TI - Infraestructura (AS-IS).

Proceso de Negocio Crítico	Servicio TI de Soporte	Activo Tecnológico (Hardware AS-IS)	Dependencia de Datos (Info Crítica)	Criticidad Inherente
Producción y Calidad (Control de piso, Trazabilidad)	Sistema MES / SCADA (Ignition)	**IND-SRV-MES01** (HP ProLiant Gen8)	Variables de proceso, recetas, alarmas, históricos de lotes.	**CRÍTICA**
Logística, Facturación y Finanzas (Pedidos, Despachos, Cierre)	ERP SIESA (App + BD)	**IND-SRV-ERP01** (HP ProLiant G6)	Inventarios, Pedidos, Facturas, Cartera, Contabilidad.	**MUY ALTA**

Tabla 6. (continuación)

Proceso de Negocio Crítico	Servicio TI de Soporte	Activo Tecnológico (Hardware AS-IS)	Dependencia de Datos (Info Crítica)	Criticidad Inherente
Auditoría y Estrategia (Análisis histórico)	Servicios de Archivos y Reportes	**IND-SRV-REP01** (HP ProLiant G6)	Informes de gestión, evidencias de auditoría, planos.	**MEDIA/ALTA**

Nota: La tabla 6 evidencia la dependencia técnica de los procesos misionales frente a la infraestructura. Fuente: elaboración propia.

Periodo Máximo Tolerable de Interrupción (MTPD)

El MTPD se definió como el tiempo máximo durante el cual Laminados de Occidente S.A. puede tolerar la interrupción de un servicio antes de que las consecuencias se consideren inaceptables. Se trabajó con rangos de tiempo, orientativamente:

- Menos de 4 horas
- Entre 4 y 8 horas
- Entre 8 y 12 horas
- Entre 12 y 24 horas
- Más de 24 horas

Estos rangos se establecieron considerando la naturaleza de los procesos industriales de la empresa (turnos de producción, ventanas de despacho, cierres de facturación) y las definiciones de “tiempo máximo de parada” y “punto de no retorno” presentes en la documentación de continuidad del negocio.

Objetivo de Tiempo de Recuperación (RTO)

El RTO AS-IS se entendió como el tiempo que, en la práctica, la organización tarda hoy en recuperar un servicio después de una interrupción grave, considerando:

- Incidentes históricos reportados por el responsable de TI.
- Capacidades reales de restauración sobre servidores físicos antiguos.
- Ausencia de alta disponibilidad y de servidores en espejo.

Los valores se expresaron también en rangos (por ejemplo, 6–12 h; 8–12 h; 24–48 h), lo que refleja la variabilidad observada en la experiencia de recuperación.

Objetivo de Punto de Recuperación (RPO)

El RPO AS-IS se definió como la cantidad máxima de datos que la organización puede perder (en términos de tiempo no respaldado) sin que la situación sea considerada inmanejable. En el escenario actual, se tuvieron en cuenta:

- La frecuencia de las copias de seguridad.
- El hecho de que los respaldos son mayoritariamente locales y manuales.
- La capacidad real de reconstruir información a partir de soportes físicos.

Los rangos utilizados (por ejemplo, "≥ 6–12 horas", "≥ 12 horas", "≥ 24 horas") reflejan el hecho de que, en algunos casos, podrían perderse registros de medio día o más.

Estas escalas, definidas con anterioridad a la valoración, permitieron que el BIA fuese consistente, trazable y comparable entre servicios, evitando que los valores respondieran únicamente a percepciones aisladas o subjetivas.

Resultados del BIA

Aplicando la metodología y las escalas descritas, se elaboró el BIA para los servicios tecnológicos identificados como más críticos para Laminados de Occidente S.A. La Tabla 7 presenta una síntesis de los resultados para el escenario actual (AS-IS).

Tabla 7.

Resumen del BIA para servicios críticos (escenario AS-IS)

Servicio / Aplicación	Procesos de negocio afectados principales	Impacto económico (1–5)	Impacto operativo (1–5)	Impacto regulatorio / de cumplimiento (1–5)	Impacto reputacional (1–5)	Impacto global (1–5)	MTPD estimado	RTO (AS-IS)	RPO (AS-IS)	Comentario síntesis
MES/SCADA Ignition 7.8.5	Producción, control de calidad en línea, seguridad del proceso, trazabilidad de variables de planta	**4 – Muy alto**: paradas de línea, desperdicio de material, pérdida de eficiencia y posibles incumplimientos de volúmenes	**5 – Crítico**: pérdida de visibilidad sobre la operación, dificultad para reaccionar ante alarmas, riesgo de paradas no controladas	**4 – Muy alto**: riesgo de no poder demostrar condiciones de operación ante auditorías de clientes o entes reguladores (parámetros de proceso, registros)	**4 – Muy alto**: percepción de inestabilidad operativa por parte de clientes industriales, sobre todo farmacéuticos/cosméticos	**5 – Crítico**	4 h	6–12 h	≥ 12 h	Sistema esencial para supervisión y registro de planta. Cualquier interrupción prolongada compromete la continuidad productiva y la capacidad de demostrar cómo se fabricó cada lote.
ERP SIESA Gcuno 8 (App + BD SQL 2014)	Gestión de pedidos, inventarios, facturación, cartera, contabilidad, despacho	**5 – Crítico**: afecta el registro de ventas, facturación y flujo de caja; riesgo de errores en inventarios y costos	**4 – Muy alto**: detiene o ralentiza procesos administrativos clave (pedidos, despachos, cierres)	**4 – Muy alto**: dificultad para cumplir requisitos de trazabilidad documental, cierres contables y soportes fiscales/tributarios	**4 – Muy alto**: incumplimientos en tiempos de entrega o errores en facturación que afectan la confianza de clientes y aliados	**4 – Muy alto**	8–12 h	8–12 h	≥ 6–12 h	Soporta el "cerebro administrativo" de la empresa. Una caída extensa tiene efectos directos en dinero, contratos y credibilidad, aunque la planta pueda seguir operando algunas horas.
Reportes / BI y archivos operativos (IND-SRV-REP01)	Análisis de información, reportería gerencial, soportes para auditorías, documentación de procesos	**3 – Alto**: retrasa análisis y decisiones, pero no detiene de inmediato ventas ni producción	**2 – Moderado**: dificulta la consulta de información histórica; afecta la eficiencia, pero no el día a día de forma inmediata	**3 – Alto**: riesgo de no disponer a tiempo de reportes y evidencias requeridos en auditorías de calidad o de clientes	**2 – Moderado**: menor visibilidad hacia clientes, pero impacto reputacional diferido (se manifiesta en auditorías, no en operación diaria)	**3 – Alto**	24 h	24–48 h	≥ 24 h	Servicio de soporte. Su caída no paraliza la operación en tiempo real, pero limita la capacidad de analizar, demostrar y documentar adecuadamente lo que se hace.

Nota: Resultados Consolidados del Análisis de Impacto al Negocio (BIA). Fuente: Elaboración propia.

Análisis del BIA Detallado por Dimensiones

MES/SCADA Ignition 7.8.5

- **Impacto económico (4/5 – Muy alto).** Una caída del MES/SCADA no solo detiene o frena la producción, sino que incrementa el desperdicio (material fuera de especificación, reprocesos) y obliga a trabajar "a ciegas" en términos de eficiencia. Se estima que la sumatoria de horas improductivas y material desperdiciado en un turno ubica este impacto en el rango de 100 a 300 SMMLV, validando su clasificación como Nivel 4 según los criterios metodológicos establecidos.
- **Impacto operativo (5/5 – Crítico).** Aquí es donde el MES/SCADA "pega más fuerte". Sin Ignition, la planta pierde visibilidad en tiempo real de variables, alarmas y eventos. Se reduce la capacidad de reacción ante desviaciones y se incrementa el riesgo de paradas no planificadas. Operar sin el sistema durante varias horas implica degradar los controles y fiarse de apuntes manuales, lo que es muy frágil para una operación industrial.
- **Impacto regulatorio (4/5 – Muy alto).** Para clientes de sectores farmacéutico y cosmético, la capacidad de demostrar en qué condiciones se fabricó un lote es clave. La falta de registros históricos confiables (temperaturas, tiempos, alarmas, etc.) puede comprometer auditorías, investigaciones de calidad o cumplimiento de buenas prácticas.
- **Impacto reputacional (4/5 – Muy alto).** Aunque muchos clientes no "vean" directamente el SCADA, sí perciben sus consecuencias: incumplimientos, reprocesos, devoluciones o dificultad para explicar incidentes. Si se vuelve recurrente, la reputación de la planta como proveedor confiable se erosiona.

Conclusión: El MES/SCADA combina un impacto operativo crítico con impactos altos en las demás dimensiones. De ahí que el impacto global se clasifique como 5 (Crítico) y se justifique un MTPD de 4 horas, muy por debajo de los RTO reales que hoy se manejan (6–12 h).

ERP SIESA Gcuno 8 (Aplicación + Base de Datos)

- **Impacto económico (5/5 – Crítico).** El ERP está directamente ligado al flujo de dinero: registro de ventas, facturación, cartera, costos, inventarios. Si no se pueden facturar pedidos o si hay errores en registros contables, las consecuencias económicas son inmediatas y acumulativas. Dado el volumen de facturación diario de Laminados de Occidente S.A., una interrupción superior a 24 horas generaría un lucro cesante y costos asociados que superan el umbral de 300 SMMLV, situando este riesgo en la categoría máxima (Crítico) de la escala.
- **Impacto operativo (4/5 – Muy alto).** Aunque la planta puede seguir operando unas horas sin ERP (si las órdenes ya están liberadas), la gestión de pedidos, despachos, inventarios y cierres se ve seriamente afectada. Un turno completo sin ERP se traduce en desorden administrativo y carga extra de trabajo para "ponerse al día".
- **Impacto regulatorio (4/5 – Muy alto).** El ERP es fuente principal de trazabilidad documental para facturación, impuestos, reportes financieros y otros aspectos que pueden estar sujetos a revisión de autoridades o auditorías externas. La pérdida de datos o inconsistencias puede derivar en observaciones graves o sanciones.
- **Impacto reputacional (4/5 – Muy alto).** Errores en facturación, faltantes de inventario, entregas incompletas o fechas incumplidas afectan directamente la relación con los

clientes. A diferencia del MES/SCADA, aquí la afectación se ve rápido en el contacto administrativo y comercial.

Conclusión: El ERP presenta un perfil de impacto muy alto en las cuatro dimensiones, con especial peso económico. No se lo califica como 5 global solo porque la planta puede seguir produciendo unas horas sin él, pero su impacto global 4 (Muy alto) y un MTPD de 8–12 h dejan claro que no soporta caídas largas sin efectos graves.

Reportes y Archivos Operativos

- **Impacto económico (3/5 – Alto).** La caída de reportes y archivos no frena inmediatamente la facturación ni la producción, pero dificulta el análisis de márgenes, productividad, costos y desviaciones. El impacto económico se siente más en el mediano plazo, al tomar decisiones con menos información o con retraso.
- **Impacto operativo (2/5 – Moderado).** Afecta la comodidad y agilidad para consultar información, pero en la mayoría de los casos la operación diaria puede continuar, aunque sea con menos datos o con fuentes alternativas (formatos manuales, consultas al ERP).
- **Impacto regulatorio (3/5 – Alto).** Si en este servidor se guardan reportes, historiales e informes que se usan en auditorías internas, de clientes o de entes externos, su indisponibilidad o pérdida puede dificultar demostrar cumplimiento. Por eso no se considera bajo, aunque sí menos sensible que ERP o MES/SCADA en tiempo real.
- **Impacto reputacional (2/5 – Moderado).** Aquí el impacto es más diferido: un auditor que recibe tarde la información, un cliente que percibe poca transparencia, etc. No suele afectar la operación diaria visible, pero sí la imagen en auditorías o revisiones.

Conclusión: El servicio de reportes se ubica en un nivel global 3 (Alto), con MTPD de 24 horas. La empresa puede priorizar primero la continuidad de ERP y MES/SCADA y, en una segunda ola, fortalecer este componente como soporte a la trazabilidad y a las decisiones.

Priorización de Servicios y Brechas de Continuidad

El BIA permitió priorizar los servicios desde la perspectiva de continuidad del negocio:

- **Prioridad 1 – MES/SCADA Ignition:** crítico para la operación de planta, con MTPD muy corto (4 h) y brechas significativas entre el tiempo tolerable y la capacidad real de recuperación.
- **Prioridad 2 – ERP SIESA:** muy alto impacto en términos de inventarios, facturación y compromisos contractuales, con brechas relevantes en RTO/RPO.
- **Prioridad 3 – Reportes y archivos:** impacto alto, pero con mayor tolerancia al tiempo de interrupción, aunque con riesgos importantes en términos de pérdida de información histórica.

Estas prioridades y brechas de continuidad constituyen el insumo principal para la matriz de riesgos y para el diseño de la arquitectura TO-BE en Microsoft Azure, donde se busca reducir los RTO y RPO a valores coherentes con los MTPD definidos por el negocio. En los apartados siguientes se profundiza en la valoración de riesgos y en el análisis comparativo entre la situación actual y la solución propuesta en la nube.

Definición de Parámetros Ideales para la Arquitectura en Azure (TO-BE)

Para la futura implementación en la nube, los objetivos se han ajustado para cumplir con el principio de **"Gap de Continuidad Positivo"** (donde RTO < MTPD).

- **RTO Objetivo (Meta):** Se define buscando que la recuperación ocurra dentro del primer cuarto del tiempo tolerable. Para servicios críticos como MES/SCADA, el objetivo es **< 1 hora**, minimizando el tiempo "a ciegas" en planta.
- **RPO Objetivo (Meta):** Se alinea con la exigencia de integridad de datos del sector farmacéutico. El objetivo es reducir la pérdida de datos a **< 15 minutos** mediante replicación continua, garantizando la trazabilidad del lote en curso.

Matriz de Resultados del BIA y Requisitos de Recuperación

La siguiente tabla 8 consolida los hallazgos del BIA, contrastando la tolerancia del negocio (MTPD) con la realidad actual (AS-IS) y definiendo los objetivos técnicos para la migración (TO-BE).

Tabla 8.
Matriz de Resultados del BIA y Definición de Requisitos (RTO/RPO).

Servicio Crítico	MTPD (Límite del Negocio)	RTO Actual (AS-IS)	RPO Actual (AS-IS)	RTO Ideal (Meta Azure)	RPO Ideal (Meta Azure)	Justificación del Requisito
MES / SCADA Ignition	**4 horas**	6 - 12 h	> 12 h	**< 1 hora**	**< 15 min**	La planta no puede perder visibilidad de variables críticas. La pérdida de datos >15 min compromete la validación de calidad del lote farmacéutico.
ERP SIESA (App + BD)	**4 horas**	8 - 12 h	> 12 h	**< 1 hora**	**< 15 min**	La facturación y logística soportan máximo un turno caído. Se requiere restaurar el servicio antes de afectar el despacho del día.
Reportes y Archivos	**4 horas**	24 - 48 h	> 24 h	**< 1 hora**	**< 15 min**	Soporte a auditorías. Aunque menos urgente, la pérdida permanente de históricos es un riesgo legal que debe mitigarse con backups en la nube.

Nota: Esta tabla contrasta la tolerancia del negocio (MTPD) con la realidad actual (AS-IS) y definiendo los objetivos técnicos para la migración (TO-BE) a partir de entrevistas a actores clave y diagnóstico de infraestructura. Fuente: Elaboración propia.

Análisis de Brecha (Gap Analysis): AS-IS vs. Necesidad del Negocio

El análisis de brecha cuantifica el déficit de capacidad actual. La tabla 9 demuestra que la infraestructura *on-premise* vigente no cumple con los requisitos mínimos de supervivencia operativa definidos por la propia dirección.

Tabla 9.
Análisis de Brecha de Continuidad (Gap Analysis)

Servicio	Requisito de Negocio (MTPD)	Capacidad Actual de Recuperación (RTO AS-IS)	Brecha (Déficit)	Estado del Riesgo	Conclusión para la Migración
MES / SCADA	4 h	+12 h (Peor escenario)	**- 8 horas**	**CRÍTICO**	La infraestructura actual excede en un 200% el tiempo máximo tolerable. **Requiere Alta Disponibilidad (HA) inmediata.**
ERP SIESA	4 h	+12 h (Peor escenario)	**- 8 horas**	**MUY ALTO**	Existe riesgo inminente de incumplir cierres diarios. Se necesita reducir el RTO a la mitad mediante automatización en nube.
Reportes y Archivos	4 h	+24 h (Backup diario)	**- 20 horas**	**ALTO**	El esquema de backup diario es insuficiente para procesos de manufactura continua. Se requiere replicación transaccional.

Nota: La tabla evidencia que la infraestructura *on-premise* vigente no cumple con los requisitos mínimos de supervivencia operativa definidos por la propia dirección. Fuente: Elaboración propia.

Actualmente, Laminados de Occidente S.A. opera con una brecha de continuidad negativa: los sistemas tardan más en recuperarse de lo que el negocio puede soportar. Específicamente, en el sistema SCADA, el riesgo de una parada de 12 horas frente a una tolerancia de 4 horas implica una exposición financiera y reputacional directa. La arquitectura propuesta en Microsoft Azure tiene como objetivo técnico cerrar esta brecha, alineando los

tiempos de recuperación (RTO TO-BE) por debajo de los umbrales de dolor (MTPD) identificados.

Gestión y Valoración de Riesgos de Seguridad y Continuidad

Tras determinar en el BIA la criticidad de los procesos y los tiempos máximos tolerables de interrupción, el siguiente paso fue identificar qué escenarios podrían materializar dichas interrupciones. Este capítulo presenta la evaluación de riesgos realizada sobre la infraestructura actual (AS-IS) de Laminados de Occidente S.A., identificando las amenazas que explotan las vulnerabilidades técnicas diagnosticadas y calculando el nivel de exposición real de la organización.

Enfoque metodológico: ISO/IEC 27005

Para la gestión del riesgo se adoptó un enfoque alineado con la norma ISO/IEC 27005:2018 (Gestión de riesgos de seguridad de la información) y los principios de la ISO 31000, integrando la estructura lógica de identificación de activos, amenazas y vulnerabilidades. El proceso se desarrolló en cuatro fases:

1. **Identificación de Activos:** Inventario de los recursos tecnológicos críticos que soportan los procesos priorizados en el BIA.
2. **Modelado de Amenazas y Vulnerabilidades:** Asociación de posibles eventos adversos (amenazas) con las debilidades intrínsecas de la infraestructura actual (vulnerabilidades).
3. **Valoración del Riesgo Inherente (AS-IS):** Cálculo del nivel de riesgo actual mediante la fórmula Riesgo = Probabilidad x Impacto.
4. **Tratamiento y Riesgo Residual (TO-BE):** Proyección de la reducción del riesgo tras la implementación de la arquitectura en Microsoft Azure.

Fase 1: Identificación y Clasificación de Activos

De acuerdo con la norma ISO/IEC 27005:2018, el proceso de gestión de riesgos debe iniciar con la identificación de los activos, entendidos como cualquier elemento que tenga valor para la organización y que requiera protección. Esta fase no se limita a un inventario de hardware, sino que abarca la identificación de activos primarios (información y procesos de negocio) y activos de soporte (hardware, software, redes y personal).

Para efectos de esta investigación, y en coherencia con el alcance definido, se han seleccionado los activos que soportan directamente los procesos críticos de producción y facturación. Adicionalmente, se ha realizado una valoración cualitativa de sus propiedades de seguridad, criterio fundamental para estimar el impacto de una potencial vulneración:

- **Confidencialidad (C):** Garantía de que la información es accesible solo para quienes están autorizados.
- **Integridad (I):** Salvaguarda de la exactitud y completitud de la información y los métodos de procesamiento.
- **Disponibilidad (D):** Garantía de que los usuarios autorizados tienen acceso a la información y a los recursos relacionados cuando lo requieren.

En la Tabla 10 se presenta el inventario consolidado, vinculando cada activo con su área propietaria y su nivel de exigencia en términos de seguridad.

Tabla 10.
Inventario y Clasificación de Activos Críticos de Información (AS-IS)

ID	Nombre del Activo	Tipo	Descripción y Función	C	I	D	Propietario del Riesgo
A01	**IND-SRV-MES01**	Hardware / Software	Servidor físico HP ProLiant Gen8 alojando el sistema SCADA Ignition 7.8.5.	Alta	Alta	Alta	Responsable de Tecnología / Sistemas
A02	**IND-SRV-ERP01**	Hardware / Software	Servidor físico HP ProLiant G6 alojando ERP SIESA y SQL Server 2014.	Alta	Alta	Alta	Responsable de Tecnología / Sistemas
A03	**Base de Datos SQL**	Datos	Repositorio central de información transaccional (pedidos, inventarios, costos).	Alta	Alta	Alta	Responsable de Tecnología / Sistemas
A04	**Históricos SCADA**	Datos	Registros de variables de proceso, alarmas y trazabilidad de lotes.	Alta	Alta	Alta	Jefe de planta / Producción
A05	**Red OT/IT**	Comunicaciones	Infraestructura de red que conecta la planta (PLCs) con los servidores administrativos.	Alta	Alta	Alta	Responsable de Tecnología / Sistemas
A06	**Backups Locales**	Soporte	Copias de seguridad almacenadas en discos externos y medios locales.	Alta	Alta	Alta	Responsable de Tecnología / Sistemas

Nota. La valoración cualitativa se expresa en niveles (Alta, Media, Baja) indicando la exigencia de seguridad del activo. **C:** Confidencialidad; **I:** Integridad; **D:** Disponibilidad. La clasificación de *Propietario del Riesgo* sigue los lineamientos de asignación de responsabilidad de la norma ISO/IEC 27001. Fuente: Elaboración propia a partir del levantamiento de infraestructura y entrevistas.

Fase 2: Identificación de Amenazas y Vulnerabilidades

Uno de los hallazgos más relevantes del diagnóstico fue la correlación entre la obsolescencia tecnológica y la exposición a amenazas. A diferencia de un entorno moderno, la infraestructura de Laminados de Occidente S.A. presenta vulnerabilidades técnicas que elevan la probabilidad de ocurrencia de incidentes, los resultados se evidencian en la tabla 11.

Tabla 11.
Diccionario de Amenazas y Vulnerabilidades Identificadas

Código	Amenaza (Evento Potencial)	Vulnerabilidad Explotada (Debilidad AS-IS)	Origen
AM-01	**Falla Física de Hardware** (Discos/Fuente)	Servidores con >10 años de uso (End-of-Life). **Ausencia de arreglos RAID** en discos principales.	Técnico / Accidental
AM-02	**Corrupción Lógica / Error de Software**	Sistemas operativos (Windows Server 2012) y Motores de BD (SQL 2014) fuera de soporte o sin parches de seguridad.	Técnico
AM-03	**Ransomware / Malware Lateral**	**Segmentación de red débil** entre planta (OT) y corporativo (IT). Ausencia de controles Zero Trust.	Intencional / Externo
AM-04	**Error Humano / Borrado Accidental**	Procesos manuales de backup y restauración. Falta de automatización.	Humano
AM-05	**Desastre Físico (Incendio/Falla Eléctrica)**	Ausencia de sitio alterno de recuperación (DRP). Todo concentrado en un único rack.	Ambiental

Nota. La tabla establece la relación causal entre los eventos adversos potenciales (Amenazas) y las debilidades intrínsecas identificadas en la infraestructura tecnológica actual (Vulnerabilidades). **AM:** Código de identificación de Amenaza. El análisis refleja el escenario *AS-IS* documentado en el diagnóstico técnico. Fuente: Elaboración propia basada en la metodología de identificación de riesgos de la norma ISO/IEC 27005:2018.

Fase 3: Escalas de Valoración del Riesgo

De acuerdo con la cláusula 6.1.2 de la norma ISO/IEC 27001:2022 y las directrices de ISO/IEC 27005:2018, la organización debe establecer y mantener criterios de aceptación del riesgo y criterios para realizar evaluaciones de seguridad de la información.

Para evitar la subjetividad en el análisis, se ha definido un modelo de valoración semi-cuantitativo. Este enfoque asigna valores numéricos a las variables cualitativas, permitiendo calcular la magnitud del riesgo mediante la función:

Nivel de Riesgo (R) = Probabilidad (P) x Impacto (I)

Criterios de Probabilidad. La probabilidad se evalúa considerando la frecuencia histórica de incidentes, la exposición a amenazas del entorno y la presencia de vulnerabilidades técnicas en los activos (obsolescencia). La Tabla 12 detalla la escala parametrizada utilizada para esta evaluación.

Tabla 12.
Escala de Probabilidad de Ocurrencia del Riesgo

Código	Categoría	Valor (P)	Nivel de Probabilidad	Frecuencia Estimada	Color
MB	Muy Baja	1	Rara vez	Evento improbable. No se ha presentado en los últimos 5 años.	
B	Baja	2	Improbable	Podría ocurrir en circunstancias excepcionales (1 vez cada 3-5 años).	
M	Media	3	Posible	Ha ocurrido en el pasado o existen condiciones para que ocurra 1 vez cada 2 años.	
A	Alta	4	Probable	Las condiciones técnicas (ej. falta de soporte) favorecen su aparición al menos 1 vez al año.	
MA	Muy Alta	5	Casi certeza	El evento es inminente o se manifiesta de manera recurrente (varias veces al año).	

Nota. La escala clasifica la posibilidad de materialización de una amenaza basándose en la frecuencia histórica y las condiciones de vulnerabilidad actuales. *Fuente:* Elaboración propia adaptada de ISO/IEC 27005.

Matriz de Calor (Heat Map). Para visualizar la severidad de los riesgos, se utiliza una matriz de doble entrada que cruza los niveles de Probabilidad (Tabla 13) con los niveles de Impacto Global definidos previamente en el BIA (donde 1 es Insignificante y 5 es Crítico).

Esta herramienta gráfica permite identificar rápidamente aquellos riesgos que exceden el apetito de riesgo de la organización.

Tabla 13.

Matriz de Evaluación de Riesgos (Mapa de Calor 5x5)

Matriz de Evaluación de Riesgos	Impacto (I)				
Probabilidad (P)	**1 (Bajo)**	**2 (Menor)**	**3 (Medio)**	**4 (Alto)**	**5 (Crítico)**
5 (Muy Alta)	5	10	15	**20**	**25**
4 (Alta)	4	8	12	**16**	**20**
3 (Media)	3	6	9	12	15
2 (Baja)	2	4	6	8	10
1 (Muy Baja)	1	2	3	4	5

Nota. La matriz permite valorar el nivel de riesgo combinando la probabilidad de ocurrencia (filas) con el impacto potencial (columnas). Las celdas representan el *Nivel de Riesgo (R)* resultante, facilitando la priorización de acciones. *Fuente:* Elaboración propia.

Clasificación y Tratamiento del Riesgo. Una vez calculado el valor numérico en la matriz de calor, es necesario categorizar el riesgo para determinar la urgencia y el tipo de respuesta requerida. La Tabla 14 define los cinco niveles de severidad y las directrices de tratamiento alineadas con la norma ISO/IEC 27005.

Tabla 14.

Niveles de Clasificación y Directrices de Tratamiento del Riesgo

Código	Nivel de Riesgo (Valor R)	Descripción del Riesgo	Tratamiento Sugerido (ISO 27005)
C	**CRÍTICO** (20 - 25)	**Riesgo Extremo.** Amenaza la continuidad operativa y la viabilidad del negocio. Requiere acción inmediata.	**Mitigar / Evitar** de inmediato. Prioridad absoluta de inversión.
MA	**MUY ALTO** (15 - 19)	**Riesgo Grave.** Afecta significativamente la operación o el cumplimiento. No debe asumirse sin una evaluación profunda.	**Mitigar / Transferir.** Requiere controles correctivos urgentes.
A	**ALTO** (10 - 14)	**Riesgo Importante.** Impacto considerable que requiere atención a corto plazo para evitar su escalamiento.	**Mitigar.** Implementar controles para reducir probabilidad o impacto.
M	**MEDIO** (5 - 9)	**Riesgo Tolerable.** Riesgo moderado que puede ser aceptado temporalmente, siempre que se mantenga bajo monitoreo.	**Monitorear / Aceptar.** Evaluar costo-beneficio de controles adicionales.

Tabla 14. (continuación)

Código	Nivel de Riesgo (Valor R)	Descripción del Riesgo	Tratamiento Sugerido (ISO 27005)
B	**BAJO** (1 - 4)	**Riesgo Aceptable.** Riesgo menor o insignificante. El costo de tratarlo suele superar el beneficio.	**Aceptar.** Se asume el riesgo documentando su existencia.

Nota. La tabla desglosa los niveles de riesgo resultantes del cálculo P x I, asignando una directriz de tratamiento para cada rango. Los umbrales aseguran una cobertura completa de la escala de 1 a 25 puntos. *Fuente:* Elaboración propia.

Matriz de Riesgos Inherente (Escenario AS-IS). Aplicando la metodología descrita a la totalidad de los activos identificados en la Fase 1, se ha consolidado la evaluación de riesgos inherentes. Esta matriz integral evalúa la exposición de cada componente crítico (hardware, datos y comunicaciones) antes de cualquier migración. Los resultados, presentados en la Tabla 15, evidencian la criticidad de mantener la operación en servidores obsoletos.

Tabla 15.
Matriz de Riesgos Inherente y Priorización (Escenario AS-IS)

ID Riesgo	Activo Afectado	Amenaza Principal	Probabilidad (P)	Impacto Global (I)	Nivel de Riesgo (P×I)	Clasificación
R01	**SCADA Srv** (A01)	**AM-01:** Falla Física de Hardware (Disco único)	**4 (Alta)**	**5 (Crítico)**	**20**	**CRÍTICO**
R02	**ERP Srv** (A02)	**AM-01:** Falla Física de Hardware (Obsoleto)	**4 (Alta)**	**4 (Muy Alto)**	**16**	**MUY ALTO**
R03	**BD SQL** (A03)	**AM-02:** Corrupción Lógica / Vulnerabilidad por falta de soporte (SQL 2014)	**4 (Alta)**	**5 (Crítico)**	**20**	**CRÍTICO**
R04	**Históricos** (A04)	**AM-04:** Pérdida de integridad/trazabilidad (Sin RAID/Integridad de datos)	**3 (Media)**	**5 (Crítico)**	**15**	**MUY ALTO**
R05	**Red OT/IT** (A05)	**AM-03:** Propagación de Ransomware (Falta de segmentación)	**3 (Media)**	**5 (Crítico)**	**15**	**MUY ALTO**
R06	**Backups** (A06)	**AM-05:** Pérdida física/Robo en sitio (Sin réplica externa)	**2 (Baja)**	**5 (Crítico)**	**10**	**ALTO**

Nota. Evaluación del riesgo actual para los seis activos críticos inventariados. El riesgo **R03** destaca la criticidad de operar bases de datos transaccionales sin soporte del fabricante. El riesgo **R04** refleja el impacto regulatorio de perder datos históricos farmacéuticos. *Fuente:* Elaboración propia.

Fase 4: Estrategia de Tratamiento y Riesgo Residual

De acuerdo con la norma ISO 27005, una vez evaluado el riesgo, se debe seleccionar una opción de tratamiento. Para la totalidad de los riesgos identificados, la estrategia seleccionada es **Mitigar y Transferir** mediante las capacidades nativas de la nube.

La Tabla 16 detalla cómo la arquitectura TO-BE en Azure neutraliza las amenazas específicas de cada uno de los 6 activos.

Tabla 16.
Plan de Tratamiento y Proyección de Riesgo Residual

ID	Activo	Estrategia	Salvaguarda / Control en Azure (TO-BE)	Probabilidad Residual	Impacto Residual	Nuevo Nivel
R01 (Fallo SCADA)	A01	**Mitigar**	Redundancia Zonal (2 VMs) + Discos Premium.	1 (MB)	5	**5 (MEDIO)**
R02 (Fallo ERP)	A02	**Mitigar**	Redundancia Zonal + Azure Site Recovery (ASR).	1 (MB)	4	**4 (BAJO)**
R03 (Fallo Base de Datos SQL)	A03	**Transferir**	Migración a **Azure SQL Managed Instance** (PaaS). Microsoft garantiza parches y disponibilidad (SLA 99.99%).	1 (MB)	5	**5 (MEDIO)**
R04 (Pérdida de integridad/trazabilidad)	A04	**Mitigar**	Almacenamiento con **Integridad de Datos** y Backup PITR (Point-in-Time Restore) de 15 min.	1 (MB)	5	**5 (MEDIO)**
R05 (Propagación de Ransomware, Falta de segmentación)	A05	**Mitigar**	Segmentación VNet Peering, NSG y Azure Firewall.	2 (B)	3	**6 (MEDIO)**
R06 (Pérdida Backup)	A06	**Mitigar**	Azure Backup con **GRS** (Geo-Redundancia) en región alterna (Central US).	1 (MB)	2	**2 (BAJO)**

Nota. Proyección de reducción de riesgos. **MB:** Muy Baja; **B:** Baja. La estrategia PaaS (Plataforma como Servicio) para el activo A03 (Base de Datos) transfiere la gestión de vulnerabilidades del sistema operativo y motor de base de datos al proveedor de nube (Microsoft), eliminando la obsolescencia como vector de ataque. *Fuente:* Elaboración propia.

Conclusión del Análisis de Riesgos

El análisis comparativo evidencia la eficacia del modelo propuesto:

1. **Reducción del Perfil de Riesgo:** Se logra transformar los riesgos críticos de infraestructura (R01, R02), asociados a la obsolescencia física, en riesgos gestionados de nivel Bajo o Medio.
2. **Eliminación de Puntos Únicos de Fallo:** La arquitectura en Azure elimina la dependencia de componentes individuales (como el disco único del servidor actual) mediante la alta disponibilidad zonal.
3. **Alineación Normativa:** La implementación de controles como la segmentación y los respaldos geográficos responde directamente a los dominios de la norma ISO 27001, cerrando las brechas de cumplimiento detectadas.

Este capítulo confirma que la inversión en la migración a Azure no es solo una actualización tecnológica, sino una medida de contención de riesgos necesaria para garantizar la viabilidad operativa de Laminados de Occidente S.A.

Diseño de la Arquitectura de Referencia en Microsoft Azure (TO-BE)

La arquitectura propuesta para Laminados de Occidente S.A. no se limita a una reubicación de servidores (Lift & Shift), sino que constituye una transformación hacia un modelo de nube híbrida resiliente. Este diseño responde directamente a la pregunta de investigación, demostrando cómo la tecnología puede fortalecer la continuidad operativa mediante la eliminación de puntos únicos de fallo y la automatización de la recuperación.

A partir del diagnóstico de la infraestructura actual (AS-IS), del Análisis de Impacto al Negocio (BIA) y de la matriz de riesgos, se definió una arquitectura de referencia (TO-BE) en

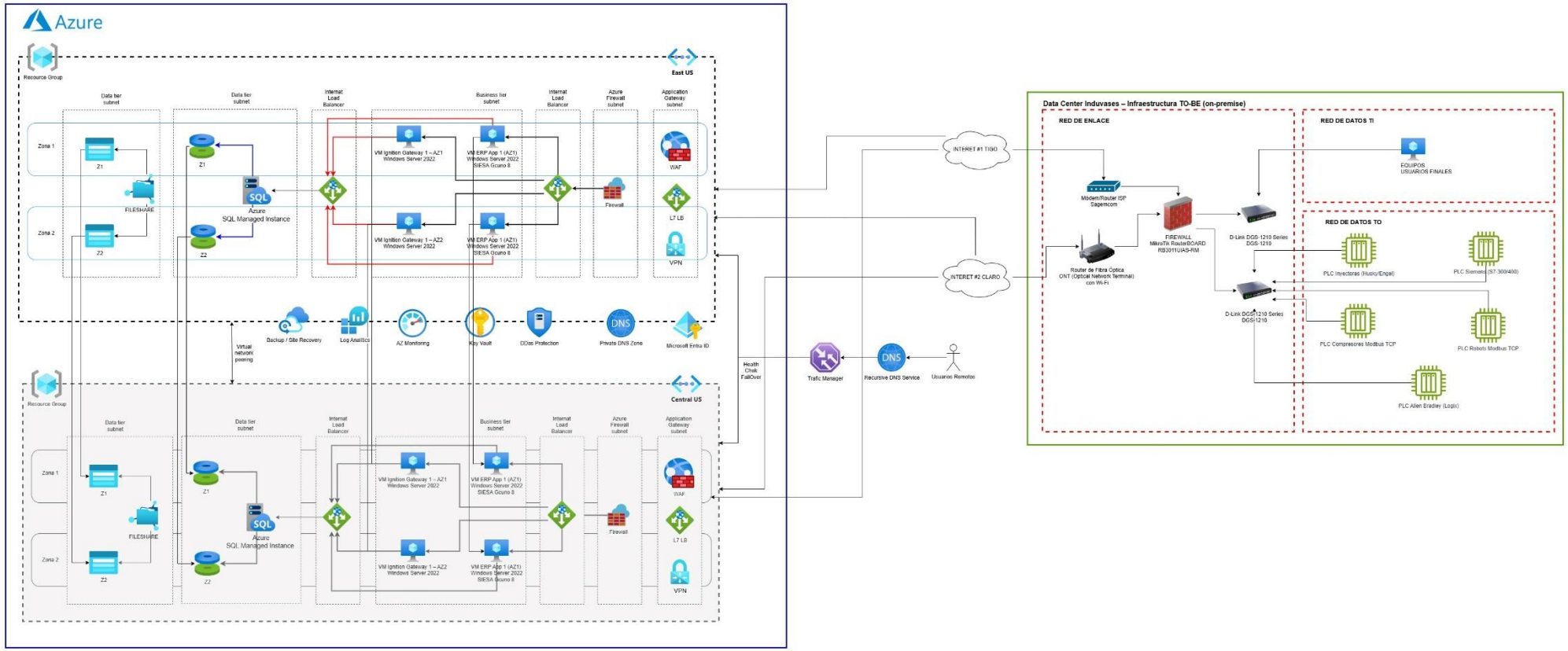
Microsoft Azure orientada a incrementar la resiliencia de los servicios críticos de Laminados de Occidente S.A., en particular del ERP SIESA Gcuno 8, del sistema MES/SCADA Ignition y de los servicios de reportes y archivos operativos.

La propuesta se apoya en los principios del Azure Well-Architected Framework, especialmente en el pilar de fiabilidad (Reliability), que recomienda diseñar las soluciones pensando en la tolerancia a fallos, la recuperación ante errores y la capacidad de volver a un estado estable tras una interrupción.

De igual forma, se tienen en cuenta las capacidades de alta disponibilidad y continuidad de negocio de servicios gestionados como Azure SQL Managed Instance, Azure Backup y Azure Site Recovery, así como el uso de Availability Zones y despliegues multirregión para reducir el riesgo de interrupciones prolongadas.

La Figura 7 resume la arquitectura TO-BE propuesta en Microsoft Azure para los servicios críticos de Laminados de Occidente S.A. En ella se diferencian claramente la región principal (East US), donde se alojan los entornos de producción del ERP, del MES/SCADA y de reportes, y la región secundaria (Central US), utilizada como sitio de recuperación ante desastres mediante la replicación de máquinas virtuales y bases de datos. El diseño incorpora redes virtuales segmentadas, servicios gestionados de base de datos, mecanismos de backup y Site Recovery, así como controles de seguridad y monitorización, alineados con el pilar de fiabilidad del Azure Well-Architected Framework.

Figura 7.
Arquitectura de Referencia TO-BE propuesta en Microsoft Azure para los servicios críticos de Laminados de Occidente S.A. S.A.



Nota. El diagrama ilustra el despliegue activo-pasivo entre las regiones East US y Central US, integrando zonas de disponibilidad y conectividad híbrida segura con la planta de producción. *Fuente:* Elaboración propia (2025).

Estrategia de Regiones y Alta Disponibilidad

Para mitigar el riesgo de indisponibilidad total por desastres naturales o fallos masivos (Riesgos R01 y R06), la arquitectura implementa un esquema de redundancia en tres niveles de profundidad:

1. **Nivel Zonal (Alta Disponibilidad):** En la región primaria (**East US**), las cargas de trabajo del ERP SIESA y el Gateway SCADA Ignition se distribuyen en **Zonas de Disponibilidad 1 y 2**. Esto garantiza que, si un centro de datos físico de Microsoft falla, la aplicación continúa operando en el otro sin interrupción perceptible (SLA 99.99%).
2. **Nivel Regional (Recuperación ante Desastres):** Se establece **Central US** como región secundaria pasiva. Mediante *Azure Site Recovery* y *SQL Failover Groups*, se replican los datos y máquinas virtuales. En caso de caída total de East US, la operación conmuta a Central US.
3. **Nivel de Enrutamiento Global:** El componente **Azure Traffic Manager** actúa como punto de entrada DNS inteligente. Monitorea la salud de la región primaria y, ante un fallo, redirige automáticamente el tráfico de usuarios remotos hacia la región de contingencia.

Especificación de Componentes de Infraestructura

La selección de cada servicio en la nube no es arbitraria; responde a la necesidad de cerrar las brechas de rendimiento y seguridad identificadas en el diagnóstico AS-IS. La **Tabla 17** detalla la configuración técnica de la capa de cómputo y datos visualizada en la Figura 7.

Tabla 17.
Especificación de Componentes de Infraestructura y Servicios Azure (TO-BE)

Capa / Componente	Servicio Azure Seleccionado	Configuración y Justificación Técnica
Enrutamiento Global	**Azure Traffic Manager**	Método de enrutamiento por *Prioridad*. Garantiza que el RTO no dependa de la propagación manual de DNS en caso de desastre regional.
Balanceo Regional	**Azure Application Gateway (WAF)**	Balanceador de capa 7 con *Web Application Firewall*. Protege las interfaces web del ERP y SCADA contra ataques OWASP y distribuye la carga entre las Zonas 1 y 2.
Cómputo (App Tier)	**Azure Virtual Machines (Windows Server 2022)**	Hosts para *Ignition Gateway* y *Siesa App*. Se despliegan en un *Availability Set* distribuidos en zonas distintas. Se eliminan los sistemas operativos heredados (2012/2016) identificados como vulnerables.
Datos (Data Tier)	**Azure SQL Managed Instance (Business Critical)**	Sustituye al SQL Server 2014. La opción *Business Critical* ofrece redundancia zonal nativa (Always On) y replicación asíncrona a la región secundaria, cumpliendo el RPO < 15 min exigido por el BIA.
Almacenamiento	**Azure Files Premium / NetApp Files**	Reemplaza al servidor de archivos físico. Proporciona recursos compartidos SMB de alto rendimiento con replicación GRS (Geo-Redundante) para proteger los históricos de calidad.
Balanceo Interno	**Azure Load Balancer (Standard)**	Gestiona el tráfico interno entre la capa web y la capa de negocio, asegurando que las peticiones del SCADA siempre lleguen a una instancia de base de datos activa.

Nota. La arquitectura desacopla la capa de datos (PaaS) de la capa de aplicación (IaaS), permitiendo escalar cada una según la demanda operativa sin afectar la otra. *Fuente:* Elaboración propia basada en las especificaciones técnicas de Microsoft Azure.

Arquitectura de Seguridad y Segmentación (Zero Trust)

Uno de los hallazgos críticos de la matriz de riesgos (R05) fue la falta de segmentación, lo que exponía a la planta a ataques de Ransomware. La arquitectura TO-BE implementa un modelo de Defensa en Profundidad, donde la seguridad no depende solo del perímetro ver tabla 18.

Tabla 18.
Matriz de Controles de Seguridad y Segmentación de Red

Capa de Seguridad	Control Implementado	Función de Protección
Perímetro de Red	**Azure Firewall Premium**	Inspección profunda de paquetes (IDPS) para todo el tráfico saliente y entre regiones. Bloquea comunicaciones de Comando y Control (C2) típicas de malware.
Micro-segmentación	**Network Security Groups (NSG)**	Reglas de "Deny All" por defecto entre subredes. La subred de datos solo acepta tráfico de la subred de negocio por el puerto 1433 (SQL). Aísla la base de datos de accesos directos.
Gestión de Identidad	**Microsoft Entra ID + MFA**	Autenticación centralizada. Se exige *Multifactor Authentication* para todos los administradores y usuarios remotos, mitigando el robo de credenciales.
Protección DDoS	**Azure DDoS Protection**	Protección estándar activada en la VNet para mitigar ataques volumétricos que intenten saturar los enlaces de internet y detener la facturación.
Gestión de Secretos	**Azure Key Vault**	Almacenamiento seguro de cadenas de conexión de base de datos y certificados SSL. Evita que las contraseñas queden expuestas en archivos de configuración del SCADA.

Nota. Estos controles responden a los requisitos de la Ley 1273 de 2009 y la norma ISO 27001 citadas en el marco legal, garantizando la confidencialidad e integridad de la información sensible.
Fuente: Elaboración propia.

Conectividad Híbrida y Protección de Flujos OT

La integración entre la nube y la planta de producción (On-premise) es el desafío técnico más complejo. Como se observa en la parte derecha de la **Figura 7**, la planta cuenta con una red de datos OT donde residen los PLCs (Siemens, Allen Bradley) y robots.

Para garantizar que el sistema SCADA en la nube pueda leer las variables de estos equipos con baja latencia y alta seguridad, se define la siguiente estrategia de conectividad híbrida. Ver tabla 19.

Tabla 19.
Estrategia de Conectividad Híbrida IT/OT

Componente de Conexión	Función en la Arquitectura	Mecanismo de Resiliencia
VPN Gateway (VpnGw2AZ)	Establece un túnel IPSec encriptado entre el Firewall local (MikroTik) y la VNet de Azure. Permite la telemetría segura de planta a nube.	**Activo-Activo:** Se configuran dos túneles simultáneos utilizando los dos proveedores de internet (Tigo y Claro). Si un ISP falla, el tráfico conmuta automáticamente.
Ignition Edge / Gateway Local	Se mantiene una instancia ligera de Ignition en planta (Edge Computing) que actúa como *buffer*.	Si la conexión a Internet se pierde, el Edge almacena los datos (Store-and-Forward) y los sincroniza con Azure al restablecerse el enlace, garantizando **cero pérdida de datos (RPO)**.
Private Link	Acceso privado a servicios PaaS (SQL, Storage) sin exponerlos a Internet pública.	El tráfico entre la planta y la base de datos viaja exclusivamente por el túnel VPN, invisible a amenazas externas.

Nota. Esta configuración híbrida asegura que la latencia de red no afecte la operación crítica de los PLCs, delegando el control en tiempo real a la red local y el análisis/histórico a la nube. *Fuente:* Elaboración propia.

Validación de la Arquitectura frente a Metas de Continuidad

Para validar que este diseño resuelve el problema de investigación, se presenta la correspondencia directa entre los componentes tecnológicos propuestos y los objetivos de recuperación (RTO/RPO) definidos en el BIA.

Tabla 20.
Mecanismos de Resiliencia y Alineación con Metas de Recuperación

Servicio Crítico	Meta BIA (RTO)	Solución Tecnológica en Azure	RPO Estimado TO-BE	Validación
MES / SCADA	**< 1 hora**	**Azure Site Recovery (ASR):** Replicación continua de VMs. En caso de desastre, el script de recuperación levanta el entorno en Central US automáticamente.	**<15 min**	**CUMPLE.** Se reduce el tiempo de indisponibilidad de 12 horas (actual) a minutos.

Tabla 20. (continuación)

Servicio Crítico	Meta BIA (RTO)	Solución Tecnológica en Azure	RPO Estimado TO-BE	Validación
ERP SIESA	**2 - 4 horas**	**SQL Auto-failover Groups:** Conmutación automática de la base de datos. Las VMs de aplicación se recuperan vía ASR con prioridad alta.	**< 15 min**	**SUPERA.** La arquitectura ofrece una recuperación más rápida que la exigencia del negocio.
Datos Históricos	**RPO < 15 min**	**Point-in-Time Restore (PITR):** SQL Managed Instance permite restaurar la BD a cualquier segundo de los últimos 35 días.	**< 5 min**	**CUMPLE.** Garantiza la trazabilidad total de lotes farmacéuticos exigida por regulación.

Nota. La validación confirma que la arquitectura TO-BE cierra las brechas de continuidad identificadas en el diagnóstico, transformando el perfil de riesgo de la organización. *Fuente:* Elaboración propia basada en SLAs de Microsoft

Conclusión del Diseño Arquitectónico y Cumplimiento del Objetivo

El diseño de la arquitectura de referencia TO-BE en Microsoft Azure presentado en este capítulo materializa el cumplimiento del Objetivo Específico 3 de esta investigación. Más allá de la selección de componentes tecnológicos, la propuesta constituye una respuesta integral a la pregunta de investigación formulada, demostrando que la migración a la nube permite transformar estructuralmente la capacidad de resiliencia de Laminados de Occidente S.A.

En contraste con la infraestructura *on-premise* diagnosticada, caracterizada por su obsolescencia y puntos únicos de fallo, el modelo diseñado garantiza:

1. **Continuidad Operativa por Diseño:** La implementación de redundancia en tres niveles zonal (Availability Zones), regional (Azure Site Recovery) y global (Traffic Manager) asegura que los servicios críticos ERP y SCADA permanezcan operativos incluso ante desastres mayores, eliminando la dependencia de un único centro de datos físico.
2. **Protección de la Información y Trazabilidad:** La adopción de servicios gestionados como *Azure SQL Managed Instance* y almacenamiento inmutable con replicación

geográfica (GRS) mitiga de raíz los riesgos de pérdida de datos por corrupción o ransomware, asegurando el cumplimiento de los estrictos requisitos de integridad del sector farmacéutico (RPO < 15 minutos).

3. **Gobernanza y Seguridad:** La arquitectura incorpora un modelo de *Defensa en Profundidad* mediante la segmentación de redes y la gestión de identidad centralizada, cerrando las brechas de seguridad detectadas en el entorno actual.

Esta arquitectura no solo viabiliza técnicamente la migración, sino que alinea la infraestructura tecnológica con la estrategia de negocio, proveyendo la elasticidad y confiabilidad necesarias para soportar el crecimiento futuro de la organización sin comprometer su estabilidad operativa.

Plan de Migración Gradual y Transición de Servicios Críticos

En respuesta al cuarto objetivo específico de esta investigación, se ha diseñado un plan de migración estructurado que trasciende la ejecución técnica para enfocarse en la continuidad operativa durante la transición. Reconociendo la criticidad de los procesos de manufactura continua de Laminados de Occidente S.A., se descarta una estrategia de corte total en favor de un enfoque incremental por olas, alineado con las fases de Assess, Migrate, Optimize del Microsoft Cloud Adoption Framework.

Estrategia de Migración: Rehosting y Replatforming

Para cada carga de trabajo identificada en el diagnóstico, se ha seleccionado la estrategia de migración que mejor equilibra el riesgo técnico con el beneficio operativo (ver Tabla 21).

Tabla 21.
Definición de Estrategias de Migración por Servicio

Servicio Crítico	Estrategia Seleccionada	Justificación Técnica y Operativa
ERP SIESA (App)	**Rehost (Lift & Shift)**	Se migra la aplicación "tal cual" a Máquinas Virtuales en Azure. Esto minimiza el riesgo de incompatibilidad de la versión *legacy* (Gcuno 8) con nuevos entornos, asegurando que la lógica de negocio permanezca intacta.
Base de Datos SQL	**Replatform**	Se migra de SQL Server 2014 *on-premise* a **Azure SQL Managed Instance**. Aunque implica un cambio de plataforma (PaaS), es necesario para mitigar el riesgo de obsolescencia y ganar capacidades nativas de alta disponibilidad sin reescribir código.
MES / SCADA	**Rehost (Con Redundancia)**	Se replican las configuraciones del *Gateway* Ignition a nuevas VMs en Azure. Se mantiene el modelo de servidor, pero se implementa en arquitectura de alta disponibilidad (Active-Standby) que no existía localmente.
Archivos / Reportes	**Replatform**	Se sustituye el servidor de archivos físico por **Azure Files**. Elimina la gestión de sistema operativo para una función que es puramente de almacenamiento (*Commodity*).

Nota. La selección de estrategias prioriza la estabilidad operativa sobre la modernización radical del código, reduciendo la incertidumbre durante la fase de transición. *Fuente:* Elaboración propia basada en el análisis de compatibilidad de aplicaciones

Fases de Ejecución y Cronograma Lógico

El plan se divide en cuatro fases secuenciales. Cada fase actúa como una compuerta de calidad: no se avanza a la siguiente hasta estabilizar la anterior. Esto protege al núcleo del negocio (ERP/SCADA) al exponerlo solo cuando la infraestructura base (Redes/Identidad) ha sido validada. La siguiente Tabla 22 evidencia el plan detallado de migración gradual y ventanas de riesgo.

Tabla 22.
Plan Detallado de Migración Gradual y Ventanas de Riesgo

Fase / Hito	Alcance Técnico y Actividades Críticas	Ventana de Afectación	Criterio de Éxito (KPI)
Fase 0: Cimientos (Landing Zone)	Despliegue de la VNet, configuración de VPN Site-to-Site redundante y extensión del Directorio Activo (Entra ID Connect).	**Nula** (Trabajo en paralelo)	Latencia estable entre Planta y Azure (< 60ms). Autenticación de usuarios sincronizada.
Fase 1: Servicios de Soporte	Migración de *File Server* a Azure Files y servicios de impresión/reportes. Validación de acceso remoto.	**Baja** (Fin de semana)	Usuarios acceden a históricos y reportes desde la red local de forma transparente.
Fase 2: Núcleo Administrativo (ERP)	Replicación de datos a SQL MI mediante *Azure DMS* (Database Migration Service). Corte del ERP y cambio de DNS.	**Media** (Ventana de 12 horas - Fin de semana)	Cierre de facturación y despacho exitoso desde el entorno Azure el primer día hábil.
Fase 3: Operación Industrial (SCADA)	Activación de Gateways Ignition en Azure. Conexión de túneles con PLCs. Sincronización de históricos (*Store-and-Forward*).	**Alta** (Parada de planta planificada - 4 a 6 horas)	Visualización de variables de proceso en tiempo real sin *lag* operativo. Integridad de datos históricos.

Nota. La Fase 3 es la más crítica. Se contempla un periodo de operación híbrida ("Parallel Run") donde el SCADA local sigue activo como "maestro" mientras el de la nube actúa como "esclavo" para validar la integridad de los datos antes del corte final. *Fuente:* Elaboración propia.

Gestión de Riesgos de Transición y Plan de Retorno (Rollback)

Un componente esencial para "mantener la operación activa" es la capacidad de revertir cambios fallidos. Para cada hito crítico, se ha definido un procedimiento de Rollback que garantiza el retorno al estado AS-IS en un tiempo inferior al MTPD. La Tabla 23 evidencia la matriz de riesgos de transición y protocolos de rollback

Tabla 23.
Matriz de Riesgos de Transición y Protocolos de Rollback

Hito de Migración	Riesgo Potencial (Fallo)	Disparador de Rollback (Trigger)	Procedimiento de Retorno (Plan B)	Tiempo Estimado de Retorno
Corte del ERP (Fase 2)	Inconsistencia de datos o corrupción en la migración a SQL MI.	Errores en el balance de prueba o descuadre de inventario en las pruebas post-migración.	1. Redirigir DNS internos al servidor físico local (que permanece encendido). 2. Cancelar la sincronización de datos. 3. Reactivar servicios locales.	< 1 Hora
Conexión SCADA (Fase 3)	Latencia excesiva (>100ms) que provoca pérdida de paquetes desde los PLCs.	Pérdida de visualización de variables críticas o desconexión intermitente de controladores.	1. Conmutar el *Ignition Edge* local a modo autónomo. 2. Desconectar el túnel VPN de datos OT. 3. Restaurar la visualización en el servidor local.	< 30 Minutos
Acceso Usuarios	Fallo en la autenticación o lentitud en escritorio remoto.	> 20% de usuarios reportando incapacidad de acceso.	Mantener habilitado el acceso RDP local temporalmente mientras se ajusta el ancho de banda del túnel VPN.	Inmediato

Nota. El principio rector es que la infraestructura antigua no se desmantela ni se formatea hasta superar un periodo de estabilización de 30 días post-migración (*Hyper-care period*). *Fuente:* Elaboración propia basada en ISO 22301.

Estructura de Gobierno y Asignación de Responsabilidades

La ejecución exitosa del plan de migración requiere una estructura de gobierno clara que evite la dilución de responsabilidades. Para ello, se ha definido una Matriz de Asignación de Responsabilidades (RACI) que vincula los roles organizacionales de Laminados de Occidente S.A. con las actividades críticas del proyecto de continuidad en la nube.

Esta estructura asegura que la validación técnica (TI) esté acompañada de la validación funcional (Negocio), condición sin la cual no se pueden ejecutar para los hitos de "Go/No-Go". La Tabla 24 evidencia la matriz de responsabilidades para la migración (Modelo RACI)

Tabla 24.
Matriz de Responsabilidades para la Migración (Modelo RACI)

Actividad / Fase	Gerente General (Patrocinador)	Responsable de TI (Líder Proyecto)	Jefe de Planta (Dueño SCADA)	Jefes Admin / Logística (Dueños ERP)	Asesoría Externa / Partner Azure
Diseño de Arquitectura y Landing Zone	I	R (Responsable)	I	I	C (Consultado)
Validación de Presupuesto y Costos Cloud	A (Aprobador)	R	I	I	C
Migración Fase 1 (Archivos/Reportes)	I	A / R	I	C	C
Pruebas Funcionales ERP (UAT)	I	C	-	R (Validador)	I
Corte y Go-Live ERP (Fase 2)	A	R	I	C	Support
Pruebas de Latencia y Datos SCADA	I	C	R (Validador)	-	Support
Conexión Híbrida y Corte SCADA (Fase 3)	A	R	A	-	Support
Activación de Plan de Retorno (Rollback)	A	R	C	C	C

Nota. **R:** Responsable de la ejecución; **A:** Aprobador final (Accountable); **C:** Consultado (aporta criterio); **I:** Informado. La separación de roles garantiza que TI no apruebe unilateralmente la salida a producción de sistemas críticos para la planta o la facturación. *Fuente:* Elaboración propia basada en el organigrama de Laminados de Occidente S.A.

Cronograma Maestro de Implementación (Horizonte 1 Año)

Considerando las restricciones operativas de una planta de producción continua y la capacidad limitada del equipo de TI, se ha proyectado un cronograma de ejecución de **12 meses**. Este horizonte temporal permite ventanas de estabilización entre fases, mitigando el riesgo de fatiga del equipo o acumulación de incidentes.

El cronograma (ver tabla 25) se estructura en trimestres (Q1-Q4) alineados con las fases técnicas definidas anteriormente.

Tabla 25.

Cronograma de Ejecución del Proyecto de Migración y Continuidad

Fase del Proyecto	Actividades Clave	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
Fase 0: Preparación	Habilitación de Tenant Azure, VPN S2S, Sincronización Identidad.												
Fase 1: Soporte	Migración File Server, DC Secundario, Pruebas de Backup.												
Fase 2: ERP (Core)	Replicación de Datos SQL, Pruebas de Rendimiento, UAT Admin.												
HITO CRÍTICO	Corte ERP (Fin de Semana) y Estabilización.												
Fase 3: SCADA (OT)	Despliegue Gateway Azure, Pruebas Túnel PLC, Validación Latencia.												
HITO CRÍTICO	Conexión Híbrida Planta-Nube y Validación Operativa.												
Fase 4: Optimización	Ajuste de Costos (Rightsizing), Documentación, Cierre Proyecto.												
Gestión del Cambio	Capacitación a usuarios y Simulacros de Recuperación (DR Drill).												

Nota. El cronograma contempla hitos de parada que deben coordinarse con las ventanas de mantenimiento de la planta. Los meses 6 y 10 son críticos y requieren congelamiento de cambios operativos en la empresa. *Fuente:* Elaboración propia.

Este plan de trabajo detallado permite a Laminados de Occidente S.A. visualizar la ruta crítica hacia la modernización, transformando la estrategia de continuidad en un conjunto de acciones ejecutables, medibles y auditables.

Pruebas de Aceptación y Validación (Go/No-Go)

Para asegurar el cumplimiento del objetivo de "mantener la operación activa", se establece un comité de cambios que debe validar los siguientes criterios antes de autorizar el paso a producción de cada fase:

1. **Prueba de Integridad de Datos:** Validación cruzada (Checksum) entre la base de datos local y la de Azure para asegurar cero pérdida de registros (RPO = 0 en migración).
2. **Prueba de Carga:** Simulación de concurrencia de usuarios (ERP) y tráfico de tags (SCADA) para confirmar que el dimensionamiento en Azure soporta la operación real.
3. **Validación de Latencia:** Confirmación de que el tiempo de respuesta aplicación-base de datos se mantiene dentro de los umbrales tolerables para el usuario final.

Este plan de migración no solo responde al desafío técnico de mover bits y bytes, sino que gestiona la continuidad del negocio como la prioridad absoluta, asegurando que la modernización tecnológica no se convierta en un riesgo operativo para Laminados de Occidente S.A.

Lineamientos de Monitoreo, Capacitación y Mejora Continua del Modelo

El diseño de una arquitectura resiliente y la ejecución de una migración exitosa constituyen solo el punto de partida de la continuidad del negocio. Para dar cumplimiento al quinto objetivo específico, se establece un marco de gobierno operativo diseñado para garantizar que la solución en Microsoft Azure mantenga su alineación con los requisitos del negocio (MTPD, RTO, RPO) a lo largo del tiempo.

Este apartado se estructura en tres pilares fundamentales: Observabilidad Técnica, Gestión de Competencias y Ciclo de Mejora Continua, alineados con el requisito de "Evaluación

del Desempeño" de la norma ISO 22301:2019 y el principio de Excelencia Operativa del Azure Well-Architected Framework.

Estrategia de Observabilidad y Monitoreo Proactivo

A diferencia del escenario AS-IS, donde el monitoreo era reactivo, la nueva arquitectura requiere una supervisión integral que combine métricas de infraestructura con indicadores de negocio. Se ha definido una **Matriz de Observabilidad** (ver Tabla 26) que instrumentaliza las herramientas nativas de Azure para vigilar la salud de los servicios críticos.

Tabla 26.
Matriz de Monitoreo y Alertas para Servicios Críticos (TO-BE)

Dominio de Monitoreo	Recurso Crítico	Métrica / Indicador Clave (KPI)	Umbral de Alerta (Threshold)	Herramienta Azure
Disponibilidad	**VPN Gateway (IT/OT)**	*Tunnel Connectivity Status* / *Bandwidth Usage*	Estado = Desconectado o Uso > 85% por 5 min.	Azure Monitor Network Insights
Rendimiento	**SQL Managed Instance**	*CPU Percentage* / *IO Requests*	CPU > 90% (Sostenido 10 min) o Latencia disco > 20ms.	Azure SQL Analytics
Continuidad (RPO)	**Replicación SQL**	*Replication Lag* (Segundos)	Lag > 60 segundos (Riesgo de incumplir RPO de 15 min).	Azure Monitor Metrics
Continuidad (RTO)	**Azure Site Recovery**	*Replication Health* / *RPO Status*	Estado = Crítico/Warning.	Recovery Services Vault Alerts
Integridad	**Backups**	*Backup Job Failure*	Fallo en la ejecución diaria o integridad fallida.	Backup Center
Seguridad	**Identity (Entra ID)**	*Failed Logins* / *Risky Sign-ins*	> 5 intentos fallidos en 1 min o inicio desde ubicación anómala.	Entra ID Protection

Nota. Las alertas críticas deben integrarse con el sistema de mesa de ayuda para generar tickets de incidente de prioridad alta (P1) automáticamente. *Fuente:* Elaboración propia basada en las capacidades de *Azure Monitor*.

Plan de Capacitación y Gestión del Cambio

La migración hacia un modelo de nube híbrida exige nuevas competencias que no residen actualmente en la organización. Para mitigar el riesgo de error humano y asegurar la operatividad, se propone un Plan de Formación Escalonado dirigido a tres perfiles organizacionales. La tabla 27 evidencia el plan de desarrollo de competencias y capacitación

Tabla 27.
Plan de Desarrollo de Competencias y Capacitación

Perfil Objetivo	Foco de la Capacitación	Competencias Críticas a Desarrollar	Acciones Formativas Sugeridas
Equipo TI (Administradores)	**Gestión Operativa Azure**	Administración de IaaS/PaaS, Gestión de Costos (*Cost Management*), Operación de *Site Recovery* y *Backup Center*.	Curso AZ-104 (Azure Administrator). Talleres prácticos de *Disaster Recovery* con el partner.
Líderes de Proceso (Dueños de Dato)	**Continuidad del Negocio**	Procedimientos de activación de contingencia manual. Validación funcional post-recuperación. Comprensión de SLA y RTO/RPO.	Simulacros de escritorio (*Tabletop exercises*). Sesiones de sensibilización sobre el BCP.
Usuarios Finales (ERP/SCADA)	**Seguridad y Acceso**	Uso de Autenticación Multifactor (MFA). Detección de Phishing. Procedimientos de acceso remoto seguro (VPN/Bastion).	Cápsulas de micro-learning sobre Ciberseguridad. Guías rápidas de acceso en contingencia.

Nota. La capacitación de los líderes de proceso es vital para que, en caso de fallo, sepan autorizar la conmutación a contingencia (*Failover*) basándose en el impacto al negocio y no solo en aspectos técnicos. *Fuente:* Elaboración propia.

Ciclo de Mejora Continua y Mantenimiento del Modelo (PDCA)

La continuidad del negocio no es un proyecto estático, sino un sistema de gestión vivo. Se establece un ciclo anual de actividades basado en el modelo Plan-Do-Check-Act (PDCA) para garantizar que la arquitectura evolucione junto con Laminados de Occidente S.A. La Tabla 28 evidencia el calendario de actividades de mantenimiento y mejora continua

Tabla 28.
Calendario de Actividades de Mantenimiento y Mejora Continua

Frecuencia	Actividad de Gobierno	Descripción y Entregable	Responsable
Mensual	**Prueba de Restauración (Backup)**	Restauración aleatoria de un archivo crítico y una base de datos de prueba para validar integridad ("Data Integrity Check").	Coord. Infraestructura
Trimestral	**Revisión de Accesos y Costos**	Auditoría de cuentas activas en Azure AD y revisión de recursos subutilizados (Rightsizing) para optimizar la factura de nube.	Gerente TI / CISO
Semestral	**Simulacro de Recuperación (DR Drill)**	Ejecución de un Test Failover en Azure Site Recovery hacia la región secundaria (sin afectar producción) para medir el RTO real.	Todo el equipo TI + Dueños de Proceso
Anual	**Actualización del BIA y Riesgos**	Revisión de los tiempos MTPD y nuevos riesgos (ej. nuevas amenazas cibernéticas o cambios en líneas de producción). Ajuste de políticas.	Gerencia General + Comité BCP

Nota. Los resultados de los simulacros semestrales deben documentarse en un informe de auditoría interna, registrando las brechas entre el RTO teórico y el RTO logrado para implementar acciones correctivas. *Fuente:* Elaboración propia basada en ISO 22301.

Conclusión del Modelo de Gobierno

La implementación de estos lineamientos transforma la continuidad del negocio en una capacidad organizacional medible y auditable. Al integrar el monitoreo proactivo (Tecnología), el cierre de brechas de conocimiento (Personas) y la validación recurrente a través de simulacros (Procesos), Laminados de Occidente S.A. asegura que la inversión tecnológica en Microsoft Azure se traduzca efectivamente en una operación resiliente, capaz de resistir y recuperarse ante la incertidumbre.

Validación de Hipótesis y Respuesta a la Pregunta de Investigación

Como cierre del análisis de resultados, este apartado integra los hallazgos del diagnóstico, la valoración de riesgos y el diseño arquitectónico para dar respuesta formal a la pregunta problema y someter a contraste las hipótesis planteadas al inicio del estudio.

Respuesta a la Formulación del Problema

La investigación se planteó el interrogante: ¿Cómo el diseño de un modelo de continuidad del negocio y aseguramiento de la información, basado en la migración de los servicios críticos de TI de Laminados de Occidente S.A. a Microsoft Azure, puede fortalecer la continuidad operativa, la protección de la información y la recuperación oportuna de los sistemas y datos críticos ante fallas de infraestructura?

A partir de los resultados obtenidos, se determina que el modelo diseñado fortalece dichas dimensiones mediante tres mecanismos estructurales que no existen en la situación actual:

1. **Transformación de la Arquitectura de Disponibilidad:** El paso de una infraestructura monolítica *on-premise* (expuesta a fallos físicos únicos) a una arquitectura distribuida en Zonas de Disponibilidad y Regiones Azure elimina la dependencia del hardware físico. Esto fortalece la continuidad operativa al garantizar que los servicios críticos (ERP y SCADA) permanezcan activos incluso ante la pérdida de un centro de datos completo.
2. **Aseguramiento por Diseño:** La protección de la información se robustece mediante la implementación de bases de datos gestionadas (*SQL Managed Instance*) y almacenamiento inmutable con redundancia geográfica (GRS). Esto mitiga los riesgos de corrupción y pérdida de datos identificados en la matriz de riesgos, asegurando la integridad transaccional exigida por el sector.
3. **Automatización de la Recuperación:** La recuperación oportuna deja de depender de procesos manuales de restauración (susceptibles a error humano y demoras) para basarse en la orquestación automatizada de Azure Site Recovery. Esto permite reducir los tiempos de recuperación de horas a minutos, alineándose con las ventanas de tolerancia (MTPD) del negocio.

Contraste y Validación de Hipótesis

Para la validación estadística y técnica de las hipótesis, se contrastan los indicadores de desempeño proyectados del modelo (Escenario TO-BE) contra la línea base levantada en el diagnóstico (Escenario AS-IS).

Hipótesis

El diseño de un modelo de continuidad del negocio y aseguramiento de la información para Laminados de Occidente S.A., orientado a la migración de sus servicios críticos hacia Microsoft Azure y basado en los principios de disponibilidad, resiliencia y gobernanza tecnológica, permite mejorar los niveles de disponibilidad de los servicios, reducir los tiempos de recuperación (RTO/RPO) y disminuir la exposición a fallas operativas y pérdidas de información frente al esquema de infraestructura local actual.

Evidencia:

1. **Mejora en Disponibilidad:** Se transita de una disponibilidad (sin garantías contractuales y dependiente de hardware obsoleto) a una arquitectura con Acuerdos de Nivel de Servicio (**SLA**) garantizados financieramente del **99.99%** para bases de datos y cómputo.
2. **Reducción de Tiempos de Recuperación (Eficiencia):**
    - El **RTO** del sistema SCADA se reduce de **12 horas** (AS-IS) a **< 1 hora** (TO-BE), una mejora del **91%** en la velocidad de respuesta.
    - El **RPO** del ERP se reduce de **> 12 horas** (copia diaria) a **< 15 minutos** (replicación continua), disminuyendo la pérdida potencial de datos en un **98%**.
3. **Disminución de Exposición al Riesgo:** La Matriz de Riesgos Residuales (Tabla 16) demuestra que los riesgos críticos de infraestructura (R01, R02) se mitigan a niveles **Bajos** o **Medios** tras la aplicación de los controles de nube.

Decisión:

Con base en la evidencia técnica presentada, que demuestra una reducción cuantificable en los tiempos de interrupción y una mitigación efectiva de los riesgos críticos.

Hipótesis Nula:

El diseño de un modelo de continuidad del negocio y aseguramiento de la información para Laminados de Occidente S.A., orientado a la migración de sus servicios críticos hacia Microsoft Azure y basado en los principios de disponibilidad, resiliencia y gobernanza tecnológica, no tendrá efecto significativo en los niveles de disponibilidad de los servicios, ni en los tiempos de recuperación (RTO/RPO), ni en la exposición a fallas operativas y pérdidas de información frente al esquema de infraestructura local actual.

Decisión:

Los resultados del análisis de brecha y la proyección de riesgo residual refutan la premisa de que no existen efectos significativos. La diferencia estructural entre operar sobre servidores sencillos sin redundancia y operar sobre una plataforma de nube hiperescalar con replicación geográfica constituye un cambio significativo y medible en la resiliencia organizacional. Por lo tanto, se rechaza la Hipótesis Nula.

Discusión

El desarrollo de este trabajo permitió pasar de una comprensión intuitiva de los riesgos tecnológicos de Laminados de Occidente S.A. a un análisis estructurado de su capacidad de continuidad del negocio frente a la migración de sus servicios críticos a Microsoft Azure. En este capítulo se discuten los principales hallazgos a la luz del marco teórico y normativo revisado, se contrastan los resultados con la literatura sobre continuidad del negocio y se exponen las implicaciones prácticas para la organización.

Síntesis interpretativa de los resultados

El diagnóstico AS-IS evidenció una infraestructura fuertemente concentrada en unos pocos servidores físicos obsoletos, sin redundancia de discos ni sitios alternos de recuperación. El ERP, el sistema MES/SCADA y los servicios de reportes y dominio se ejecutan sobre equipos con más de una década de uso, con sistemas operativos y motores de base de datos cercanos o incluso más allá de su fin de soporte, y con esquemas de respaldo locales de alcance limitado. Esta realidad explica por qué el BIA y la matriz de riesgos arrojaron niveles de riesgo altos y críticos para los servicios más estrechamente vinculados a la producción y a la facturación.

El Análisis de Impacto al Negocio mostró una brecha clara entre lo que la organización puede tolerar (MTPD) y lo que la infraestructura actual es capaz de ofrecer en términos de RTO y RPO. El MES/SCADA se clasificó con impacto global crítico y un MTPD del orden de 4 horas, mientras que los RTO y RPO reales se ubican entre 6–12 horas y 12 horas o más, respectivamente. En el caso del ERP, el impacto muy alto y un MTPD de 8–12 horas contrastan con tiempos de recuperación equivalentes o superiores, acompañados de un posible RPO de medio día o más. Incluso los servicios de reportes y archivos, siendo menos sensibles en tiempo

real, presentan ventanas de recuperación de 24–48 horas y riesgo de pérdida de información histórica relevante.

Sobre esta base, la arquitectura TO-BE en Microsoft Azure, junto con el comparativo AS-IS vs TO-BE, evidencia que es técnicamente viable reducir de manera significativa los RTO y RPO mediante el uso de servicios gestionados, redundancia zonal y replicación entre regiones. El diseño propuesto sitúa al MES/SCADA en un escenario con RTO ≤ 1 hora y RPO ≤ 15 minutos, y al ERP con RTO de ≤ 1 hora para la capa de aplicación y ≤ 15 minutos para la base de datos, con RPO que puede llegar al rango de 5–15 minutos. Estos valores se ajustan mejor a los MTPD definidos y reducen de forma tangible la exposición de la organización frente a interrupciones prolongadas.

El plan de migración gradual y los lineamientos de monitoreo y mejora continua muestran que la transición a la nube no se limita a un cambio tecnológico, sino que implica nuevos hábitos de operación, roles más claramente definidos y una aproximación más sistemática a la continuidad del negocio.

Comparación con teorías y marcos de referencia

Los resultados del estudio se alinean con los postulados de marcos internacionales de continuidad y gestión de riesgos, como ISO 22301 e ISO/IEC 27005, en varios aspectos clave.

En primer lugar, la identificación de procesos críticos, la determinación del MTPD y la derivación de objetivos de RTO y RPO constituyen precisamente los pasos que la norma de continuidad plantea para construir una estrategia de recuperación coherente con las necesidades del negocio. El BIA desarrollado confirma que, sin un entendimiento cuantitativo de estos

parámetros, la percepción del riesgo se mantiene difusa y las decisiones de inversión se apoyan más en sensaciones que en evidencia.

En segundo lugar, la matriz de riesgos construida a partir de una matriz 5×5 de probabilidad e impacto concuerda con los enfoques cualitativos y semicuantitativos que recomiendan tanto ISO 31000 como las guías de análisis de riesgo en seguridad de la información. La concentración de riesgos críticos en los servidores de ERP y MES/SCADA no es un hallazgo aislado, sino un patrón recurrente en entornos industriales donde la modernización tecnológica se ha retrasado, mientras que los procesos de negocio se han vuelto más exigentes en términos de disponibilidad y trazabilidad.

Por otro lado, la arquitectura TO-BE diseñada tomando como referencia el Azure Well-Architected Framework y las capacidades de alta disponibilidad, backup y recuperación ante desastres de Microsoft Azure, coincide con las buenas prácticas descritas en la literatura sobre migración de cargas críticas a la nube. La separación de capas, el uso de servicios gestionados de base de datos, la distribución de máquinas virtuales en Availability Zones y la utilización de regiones secundarias para escenarios de desastre son elementos recomendados de forma consistente en casos de estudio y guías técnicas para sectores que requieren alta resiliencia.

En este sentido, los resultados del trabajo no contradicen la teoría vigente; más bien, la confirman y la aterrizan a la realidad de una empresa manufacturera de tamaño medio, con limitaciones de recursos, pero con necesidades reales de continuidad ante la presión de clientes y auditorías de calidad.

Explicación de hallazgos relevantes

Más allá de la alineación con marcos teóricos, varios hallazgos merecen un comentario específico:

La brecha estructural entre los MTPD del negocio y los RTO/RPO que ofrece la infraestructura actual no es fruto de decisiones individuales, sino de un proceso acumulado de inversión diferida en TI. Los servidores han seguido haciendo el trabajo mientras las exigencias de disponibilidad, regulación y trazabilidad crecían, hasta llegar a un punto donde cualquier incidente serio puede tener consecuencias desproporcionadas.

La concentración de funciones críticas en pocos servidores (por ejemplo, ERP + base de datos en el mismo equipo, o un controlador de dominio en un hardware no diseñado para uso corporativo) agrava el riesgo y, al mismo tiempo, dificulta la planificación de cambios. Migrar estos servicios sin una estrategia de continuidad clara puede percibirse como demasiado arriesgado, lo que lleva a postergar decisiones y, paradójicamente, a aumentar el riesgo.

La propuesta de arquitectura en Azure muestra que es posible redistribuir ese riesgo sin requerir una complejidad inasumible. Al aprovechar servicios gestionados y mecanismos nativos de alta disponibilidad, la organización deja de depender de capacidades internas de administración de hardware y se centra en la definición de políticas, pruebas de recuperación y monitoreo.

La incorporación de un plan de migración gradual, que comienza con servicios de soporte y avanza hacia ERP y MES/SCADA, responde tanto a la teoría de gestión del cambio como a la experiencia práctica: los proyectos de migración más exitosos no son los que cambian todo de una vez, sino los que permiten aprender en cada fase, ajustar la arquitectura y ganar confianza en la operación en la nube.

Implicaciones para la gestión de TI y la continuidad del negocio

Los resultados del estudio tienen implicaciones directas para la forma en que Laminados de Occidente S.A. gestiona su infraestructura tecnológica y su continuidad del negocio:

Cambio de modelo de responsabilidad: al pasar de una infraestructura on-premise a una arquitectura en Azure, la organización ya no es únicamente responsable de mantener el hardware y el software básico, sino de administrar relaciones de servicio, definir configuraciones y políticas coherentes y monitorear de forma activa el cumplimiento de los niveles de servicio.

Necesidad de gobernanza y priorización: el BIA y la matriz de riesgos no deben verse como documentos estáticos, sino como insumos que orientan la asignación de presupuesto y esfuerzos. Si el MES/SCADA y el ERP concentran el mayor riesgo, es coherente que las inversiones iniciales en arquitectura y capacitación se centren allí.

Reforzamiento de la cultura de continuidad: la arquitectura TO-BE y el plan de migración son tan robustos como la disciplina con la que se ejecuten pruebas de backup, restauración y conmutación por desastre. El estudio muestra que la adopción de herramientas de BCDR en la nube facilita estas pruebas, pero no las reemplaza; la organización debe incorporar estos ejercicios como parte habitual de su calendario operativo.

Articulación entre TI y negocio: los hallazgos evidencian que la continuidad del negocio no puede quedarse en el ámbito técnico. Definir MTPD, RTO y RPO requiere diálogo entre las áreas de negocio y tecnología, y la operación de la nueva arquitectura en Azure exigirá mantener esa conversación en el tiempo para ajustar la solución cuando cambien procesos, volúmenes o requisitos regulatorios.

Conclusiones

La presente investigación culmina con el diseño de un modelo integral de continuidad del negocio para Laminados de Occidente S.A., concebido no solo como una actualización tecnológica, sino como una respuesta estratégica ante la vulnerabilidad operativa detectada. El modelo articula el diagnóstico técnico, la gestión de riesgos y la arquitectura en la nube para trazar una hoja de ruta que garantiza la disponibilidad de los servicios críticos bajo los principios de resiliencia y gobernanza.

En relación con el diagnóstico de la infraestructura (Objetivo 1), se evidenció una realidad técnica insostenible: la organización opera sobre una base obsoleta y frágil, caracterizada por la concentración de servicios críticos como el ERP y el sistema MES/SCADA en servidores únicos, sin redundancia de discos y con sistemas operativos próximos a su fin de soporte. Esta configuración representa un punto único de fallo que eleva drásticamente la probabilidad de interrupciones prolongadas y pérdida de datos transaccionales.

Al contrastar esta precariedad técnica con las necesidades del negocio mediante el Análisis de Impacto al Negocio (Objetivo 2), se objetivó una "brecha de continuidad" crítica. Los resultados demostraron cuantitativamente que los tiempos reales de recuperación (RTO) y los puntos de recuperación de datos (RPO) actuales exceden los umbrales de tolerancia de la organización. Esta disparidad entre la capacidad tecnológica instalada y las exigencias de auditoría y servicio al cliente valida la urgencia de abandonar el esquema on-premise actual.

Para cerrar dicha brecha, la arquitectura de referencia diseñada en Microsoft Azure (Objetivo 3) transforma el paradigma de disponibilidad de la empresa. Al sustituir servidores físicos aislados por servicios gestionados (como Azure SQL Managed Instance) y distribuir las cargas de trabajo en Zonas de Disponibilidad y regiones geográficas alternas, la propuesta logra

alinear técnicamente la infraestructura con los objetivos de recuperación exigentes que el negocio requiere, eliminando la necesidad de invertir en un segundo centro de datos físico propio.

La viabilidad operativa de esta transformación se sustenta en el plan de migración gradual (Objetivo 4), el cual demuestra que es posible transitar hacia la nube sin comprometer la producción en curso. La estructuración del cambio por fases iniciando con servicios de soporte para luego abordar el núcleo crítico, junto con la definición de criterios de éxito y mecanismos de retorno (rollback), aporta la seguridad necesaria para gestionar el riesgo inherente a la transición tecnológica.

El estudio concluye que la tecnología por si sola no garantiza la resiliencia; por ello, los lineamientos de gobernanza y mejora continua (Objetivo 5) se integran como el componente vital para la sostenibilidad del modelo. La adopción de herramientas de observabilidad, sumada a la institucionalización de pruebas periódicas de recuperación y planes de capacitación, asegura que la solución propuesta mantenga su efectividad frente a nuevas amenazas. En conjunto, este trabajo confirma que la migración planificada a Microsoft Azure constituye la oportunidad definitiva para que Laminados de Occidente S.A. asegure su operación y fortalezca la confianza de sus partes interesadas.

Referencias

Arévalo-Chávez, P., Cruz-Cárdenas, J., Guevara-Maldonado, C., Palacio-Fierro, A., Bonilla-Bedoya, S., Estrella-Bastidas, A., Guadalupe-Lanas, J., Zapata-Rodríguez, M., Jadán-Guerrero, J., Arias-Flores, H., & Ramos-Galarza, C. (2020). *Actualización en metodología de la investigación científica.* Quito, Ecuador: Editorial Universidad Tecnológica Indoamérica.

Congreso de la República de Colombia. (1999). *Ley 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Diario Oficial No. 43.673.* https://www.suin-juriscol.gov.co/viewDocument.asp?id=1662013

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos". Diario Oficial No. 47.223*. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Endo, P., Rodrigues, M., Gonçalves, G., Kelner, J., Sadok, D., & Curescu, C. (2016). *High availability in clouds: systematic review and research challenges*. Journal of Cloud Computing, 5(1), Artículo 16. https://link.springer.com/article/10.1186/s13677-016-0066-8

Forrester Consulting. (2024). *The Total Economic Impact™ of Microsoft Azure VMware Solution.* https://tei.forrester.com/go/microsoft/azurevmwaresolution//docs/TheTEIOfMicrosoftAzureVMwareSolution.pdf

IBM. (2024). *What is cloud computing?* IBM Cloud Education. https://www.ibm.com/think/topics/cloud-computing

IBM. (2025). *Cost of a Data Breach Report 2025*. https://www.ibm.com/reports/data-breach

IBM. (2025). *What is cyber resilience?* https://www.ibm.com/think/topics/cyber-resilience

International Society of Automation. (2010). *ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod): Enterprise-Control System Integration - Part 1: Models and Terminology*. https://www.isa.org/standards-and-publications/isa-standards/isa-95-standard

InterRisk Asia (Thailand) Co., Ltd. (22 de octubre de 2025). *What is MTPD? A critical factor in BCP planning that businesses must understand.* https://www.interriskthai.co.th/blog/mtpd/

ISO. (2019). *ISO 22301:2019*. https://www.iso.org/obp/ui/en/#iso:std:iso:22301:ed-2:v1:en

ISO. (2021). *ISO/TS 22317:2021*. Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Directrices para el análisis del impacto empresarial. https://www.iso.org/standard/79000.html

ISO. (2022). *ISO/IEC 27001:2022*. https://www.iso.org/es/norma/27001

ISO. (2025). *ISO 22300:2025*. Security and resilience — Vocabulary. https://www.iso.org/es/contents/data/standard/08/57/85749.html

Laminados de Occidente S.A. (2025). *Existimos para trabajar contigo*. https://LaminadosdeOccidente.com/nosotros

Laminados de Occidente S.A. (2025). *Misión*. https://LaminadosdeOccidente.com/nosotros

Laminados de Occidente S.A. (2025). *Tubos colapsibles de aluminio y tipo laminados*. https://LaminadosdeOccidente.com/

Laminados de Occidente S.A. (2025). *Visión*. https://LaminadosdeOccidente.com/nosotros

Microsoft. (26 de agosto de 2021). *El papel fundamental de Confianza Cero en la seguridad de nuestro mundo*. Microsoft News Center Latinoamérica. https://news.microsoft.com/es-xl/el-papel-fundamental-de-confianza-cero-en-la-seguridad-de-nuestro-mundo/

Microsoft. (2025). *¿Qué es la confianza cero?* https://learn.microsoft.com/es-es/security/zero-trust/zero-trust-overview

Microsoft. (2025). *¿Qué son la continuidad empresarial, la alta disponibilidad y la recuperación ante desastres?* https://learn.microsoft.com/es-es/azure/reliability/concept-business-continuity-high-availability-disaster-recovery

Microsoft. (2025). *Azure Architecture Center*. https://learn.microsoft.com/en-us/azure/architecture/

Microsoft. (2025). *Azure Availability Zones*. https://azure.microsoft.com/es-es/explore/global-infrastructure/availability-zones

Microsoft. (2025). *Azure Well-Architected Framework*. https://learn.microsoft.com/en-us/azure/well-architected/

Microsoft. (2025). *Overview of Well-Architected for Industry*. https://learn.microsoft.com/en-us/industry/well-architected/overview

Microsoft. (2025). *Principios de diseño de fiabilidad*. https://learn.microsoft.com/es-es/azure/well-architected/reliability/principles

Microsoft. (2025). *Principios de diseño de fiabilidad*. https://learn.microsoft.com/es-es/azure/well-architected/reliability/principles

Microsoft. (2025). *Selección de las estrategias de migración a la nube*. https://learn.microsoft.com/es-es/azure/cloud-adoption-framework/plan/select-cloud-migration-strategy

Microsoft. (Noviembre de 2025). *Service Level Agreements (SLA) for Online Services*. https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services

Microsoft Learn. (2025). *Continuidad empresarial y recuperación ante desastres*. https://learn.microsoft.com/es-es/azure/cloud-adoption-framework/ready/landing-zone/design-area/management-business-continuity-disaster-recovery

Moore, J. (2024). *What is BCDR? Business continuity and disaster recovery guide*. https://www.techtarget.com/searchdisasterrecovery/definition/Business-Continuity-and-Disaster-Recovery-BCDR

Nascimento, B., Santos, R., Henriques, J., Bernardo, M., & Caldeira, F. (2024). *MDPI*. Availability, Scalability, and Security in the Migration from Container-Based to Cloud-Native Applications. https://www.mdpi.com/2073-431X/13/8/192

nehatiwari1994. (2024). *Business Continuity and Disaster Recovery for on-premises workloads in Microsoft Azure Cloud*. https://techcommunity.microsoft.com/blog/azureinfrastructureblog/business-continuity-and-disaster-recovery-for-on-premises-workloads-in-microsoft/4083157

NIST. (11 de 11 de 2010). *NIST SP 800-34 Rev. 1*. Contingency Planning Guide for Federal Information Systems. https://doi.org/10.6028/NIST.SP.800-34r1

NIST. (2023). *Guide to Industrial Control Systems (ICS) Security (NIST SP 800-82r3)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3

Organización Internacional de Normalización. (2019). *ISO 22301:2019. Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Requisitos*. https://www.iso.org/standard/75106.html

Organización Internacional de Normalización. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos*. https://www.iso.org/standard/27001

Rahman, A., Sara, U., Kundu, D., Islam, S., Islam, M., Hasan, M., Rahman, Z., & Nasir, M. (2020). *DistB-SDoIndustry: Enhancing security in Industry 4.0 services based on distributed blockchain through software defined networking-IoT enabled architecture.* International Journal of Advanced Computer Science and Applications, 11(9).. https://doi.org/10.14569/IJACSA.2020.0110980

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (NIST Special Publication 800-207).* National Institute of Standards and Technology.. https://doi.org/10.6028/NIST.SP.800-207

Anexos

Anexo A: Guía de entrevista semiestructurada – Gerente General.

Entrevista semiestructurada N° 1	Proyecto: Modelo de continuidad del negocio y aseguramiento de la información para Laminados de Occidente S.A.
Entrevistado: Jairo *	Cargo: Gerente General
Área: Dirección General	Fecha: 12/11/2025
Hora inicio: 09:00	Entrevistador: Investigador – Especialización en Seguridad Informática

Esta entrevista hace parte de un proyecto de investigación de la especialización en Seguridad Informática. El objetivo es entender mejor cómo funcionan los procesos de la empresa, qué tan críticos son para el negocio y cómo dependen de los sistemas de información (ERP Siesa, MES/SCADA Ignition y otros). La información se usará solo con fines académicos y se tratará de manera confidencial. No se publicarán nombres propios. La entrevista dura aproximadamente entre 30 y 45 minutos.

P1. ¿Cómo describiría, en términos simples, la actividad principal de Laminados de Occidente S.A. y sus clientes más importantes?

R1. Laminados de Occidente S.A. se dedica principalmente a la fabricación de envases laminados y tubos colapsibles para los sectores farmacéutico, cosmético e industrial. Nuestros clientes clave son laboratorios, empresas de cuidado personal y algunas compañías de alimentos que requieren empaques primarios confiables, con altos estándares de calidad y trazabilidad.

P2. Desde su perspectiva, ¿cuáles son los procesos más críticos para que la empresa funcione día a día?

R2. Los procesos más críticos son producción, control de calidad, gestión de inventarios de materia prima y producto terminado, y el proceso de facturación y despacho. Si alguno de ellos se detiene, rápidamente se ven afectados los compromisos con los clientes y el flujo de caja.

P3. Pensando en esos procesos críticos, ¿qué tipo de consecuencias tendría una interrupción prolongada de la operación?

R3. Las consecuencias serían retrasos en entregas, posibles penalidades contractuales con algunos clientes estratégicos, pérdida de confianza en nuestra capacidad de respuesta, afectación a auditorías de calidad y, en un escenario extremo, cancelación de contratos o pérdida de mercado.

P4. Si el sistema ERP SIESA Gcuno 8 se detiene completamente, ¿en cuánto tiempo empezaría a notar un impacto serio en el negocio?

R4. Diría que luego de unas 4 a 6 horas de caída el impacto empieza a ser serio, porque dejamos de registrar pedidos, movimientos de inventario y facturación. A partir de un periodo de 8 a 12 horas la afectación ya es crítica para la operación y el cierre del día.

P5. Y si el sistema MES/SCADA Ignition se cae, ¿cuáles serían las principales consecuencias?

R5. El MES/SCADA es clave para supervisar la producción y registrar lo que ocurre en planta. Una caída implica pérdida de visibilidad sobre variables de proceso, eventos y alarmas. Podemos seguir operando un tiempo de forma manual, pero con mayor riesgo de errores, desperdicio de material y reprocesos. Más de 4 horas sin este sistema se vuelve muy delicado.

P6. ¿Cuál diría que es el tiempo máximo tolerable de interrupción para producción, inventarios, facturación y despachos?

R6. Para producción y el sistema MES/SCADA, el tiempo máximo tolerable es de unas 4 horas. Para inventarios y despachos podría ser de hasta 8 horas, y para facturación y cierre contable, máximo un día, siempre que se pueda registrar la información acumulada posteriormente sin perder datos.

P7. Desde su experiencia, ¿cuáles son hoy los riesgos más preocupantes para la continuidad del negocio?

R7. La obsolescencia de nuestra infraestructura de servidores, que todavía utiliza versiones como Windows Server 2012 y SQL Server 2014 sin soporte, la falta de redundancia de discos (sin RAID), la ausencia de un sitio alterno y el riesgo creciente de ataques de ransomware. También me preocupa que nuestros respaldos sean locales y no se prueben con la frecuencia que deberían.

P8. ¿Qué percepción tiene sobre el uso de servicios en la nube (por ejemplo, Microsoft Azure) para soportar sistemas críticos de la empresa?

R8. Considero que la nube es una opción viable y necesaria si se implementa con una buena planificación. Nos permitiría mayor disponibilidad, replicación geográfica y mejores prácticas de seguridad, siempre que tengamos claridad sobre los costos, los acuerdos de nivel de servicio y los mecanismos de control y auditoría.

Anexo B: Guía de entrevista semiestructurada – Jefe de Planta / Producción (MES/SCADA).

Entrevista semiestructurada N° 2	Proyecto: Modelo de continuidad del negocio y aseguramiento de la información para Laminados de Occidente S.A.
Entrevistado: Jaime *	Cargo: Jefe de Planta
Área: Producción	Fecha: 12/11/2025
Hora inicio: 10:00	Entrevistador: Investigador – Especialización en Seguridad Informática

Esta entrevista hace parte de un proyecto de investigación de la especialización en Seguridad Informática. El objetivo es entender mejor cómo funcionan los procesos de la empresa, qué tan críticos son para el negocio y cómo dependen de los sistemas de información (ERP Siesa, MES/SCADA Ignition y otros). La información se usará solo con fines académicos y se tratará de manera confidencial. No se publicarán nombres propios. La entrevista dura aproximadamente entre 30 y 45 minutos.

P1. ¿Podría describir brevemente el flujo del proceso de producción de envases y tubos colapsibles?

R1. El proceso inicia con la recepción de la bobina de aluminio o lámina, pasa por corte, impresión, formado, sellado y finalizando con el empaque. En cada etapa controlamos variables como temperatura, presión, velocidad de línea y condiciones de curado.

P2. ¿En qué puntos del proceso intervienen sistemas de información como el MES/SCADA Ignition y el ERP SIESA?

R2. El MES/SCADA Ignition interviene en la supervisión en tiempo real de las líneas, el registro de variables, la gestión de alarmas y el almacenamiento de históricos de producción. El ERP SIESA se utiliza para la programación de órdenes de producción, el consumo de materia prima y el registro del producto terminado en inventario.

P3. ¿Qué tareas realiza diariamente utilizando el sistema MES/SCADA Ignition?

R3. Monitoreamos el estado de las máquinas, verificamos que las variables se mantengan dentro de los rangos establecidos, hacemos seguimiento a las alarmas, revisamos los históricos de producción y analizamos las causas de paradas y desperdicios.

P4. Si el sistema MES/SCADA se cae en plena jornada de producción, ¿qué ocurre en los primeros minutos?

R4. Perdemos visibilidad de las variables y alarmas. Las máquinas pueden seguir operando, pero quedamos más expuestos a errores y a no detectar desviaciones a tiempo. En general se reduce la velocidad de producción por precaución y se incrementa la presión sobre el equipo.

P5. ¿Cuánto tiempo podrían operar sin MES/SCADA antes de que el impacto sea grave?

R5. En mi opinión, más de 2 o 3 horas sin MES/SCADA ya es muy riesgoso, porque no tenemos trazabilidad de eventos ni registro confiable de lo que está pasando en la línea. A las 4 horas la situación es claramente inaceptable.

P6. En el caso del ERP SIESA, ¿qué pasa cuando el sistema no está disponible durante un turno?

R6. Se atrasan las órdenes de producción, no se actualizan los consumos de materia prima ni el inventario de producto terminado. Luego hay que hacer ajustes manuales para cuadrar la información y eso toma mucho tiempo y esfuerzo.

P7. ¿Recuerda algún incidente reciente en el que un sistema haya fallado y haya impactado la producción?

R7. Hace unos meses tuvimos un problema con el servidor del MES/SCADA y estuvimos casi medio día trabajando sin históricos. No paró por completo la producción, pero se dificultó el análisis posterior, se incrementó el desperdicio y hubo discusiones sobre los tiempos reales de parada.

P8. Desde su cargo, ¿qué le pediría a un modelo de continuidad del negocio?

R8. Que garantice respaldos frecuentes de las configuraciones y recetas, que permita restaurar rápidamente el servidor del MES/SCADA en otro equipo o en la nube, y que mantenga la integración con el ERP para no perder trazabilidad de la producción y de los lotes fabricados.

Anexo C: Guía de entrevista semiestructurada – Jefe de Logística y Distribución.

Entrevista semiestructurada N° 3	Proyecto: Modelo de continuidad del negocio y aseguramiento de la información para Laminados de Occidente S.A.
Entrevistado: Andrés *	Cargo: Jefe de Logística y Distribución
Área: Logística	Fecha: 12/11/2025
Hora inicio: 11:00	Entrevistador: Investigador – Especialización en Seguridad Informática

Esta entrevista hace parte de un proyecto de investigación de la especialización en Seguridad Informática. El objetivo es entender mejor cómo funcionan los procesos de la empresa, qué tan críticos son para el negocio y cómo dependen de los sistemas de información (ERP Siesa, MES/SCADA Ignition y otros). La información se usará solo con fines académicos y se tratará de manera confidencial. No se publicarán nombres propios. La entrevista dura aproximadamente entre 30 y 45 minutos.

P1. ¿Cuáles son las principales actividades del área de logística y distribución en Laminados de Occidente S.A.?

R1. Gestionamos el almacenamiento de producto terminado, la planificación de despachos, la coordinación con transporte, la preparación de documentación y la confirmación de entregas a los clientes.

P2. ¿Qué sistemas de información utilizan para gestionar inventarios y despachos?

R2. Principalmente el módulo de inventarios y ventas del ERP SIESA, además de algunas hojas de cálculo de apoyo para programar rutas y priorizar pedidos según compromisos con los clientes.

P3. ¿Qué sucede si el ERP no está disponible durante parte del día?

R3. No podemos registrar salidas ni verificar existencias en tiempo real. Esto genera retrasos en la preparación de pedidos, riesgo de despachar sin la documentación adecuada y mayor probabilidad de errores o reprocesos en la información.

P4. ¿Cómo asegurar hoy la trazabilidad de los productos despachados?

R4. Se hace a través de los documentos generados en el ERP, donde se registran lotes, fechas y destinos. Cuando el sistema falla, se recurre a formatos manuales, pero luego es complejo conciliar la información y asegurar que todo quedó bien registrado.

P5. Imagine que el sistema de inventarios y despacho deja de funcionar durante una jornada completa. ¿Qué consecuencias tendría?

R5. Probablemente tendríamos que suspender parte de los despachos o trabajar con mucha incertidumbre. Esto podría generar retrasos importantes, acumulación de pedidos pendientes y reclamos de los clientes por incumplimientos en las fechas acordadas.

P6. ¿Cuál es el tiempo máximo tolerable sin los sistemas que soportan inventarios y despachos?

R6. Diría que máximo 8 horas. Más allá de eso el nivel de atraso y desorden sería muy difícil de recuperar sin afectar seriamente el servicio y la percepción de confiabilidad que tienen los clientes.

P7. ¿Qué mejoras considera prioritarias para garantizar continuidad en su área?

R7. Tener un sistema disponible de forma más estable, contar con un procedimiento claro de contingencia, asegurar que la información clave esté respaldada y si es posible, que ciertos reportes críticos puedan consultarse incluso si la oficina principal tiene problemas técnicos.

Anexo D: Guía de entrevista semiestructurada – Responsable de Tecnología / Sistemas.

Entrevista semiestructurada N° 4	Proyecto: Modelo de continuidad del negocio y aseguramiento de la información para Laminados de Occidente S.A.
Entrevistado: Fernando *	Cargo: Responsable de Tecnología
Área: Tecnología / Sistemas	Fecha: 13/11/2025
Hora inicio: 09:00	Entrevistador: Investigador – Especialización en Seguridad Informática

Esta entrevista hace parte de un proyecto de investigación de la especialización en Seguridad Informática. El objetivo es entender mejor cómo funcionan los procesos de la empresa, qué tan críticos son para el negocio y cómo dependen de los sistemas de información (ERP Siesa, MES/SCADA Ignition y otros). La información se usará solo con fines académicos y se tratará de manera confidencial. No se publicarán nombres propios. La entrevista dura aproximadamente entre 30 y 45 minutos.

P1. ¿Puede describir brevemente la arquitectura actual de TI de Laminados de Occidente S.A.?

R1. Actualmente contamos con una infraestructura local compuesta por varios servidores físicos HP ProLiant antiguos. Por ejemplo: IND-SRV-ERP01, un HP ProLiant DL380 G6 (2009) donde corren simultáneamente la aplicación ERP SIESA Gcuno 8 y la base de datos en SQL Server 2014 sobre Windows Server 2012, con un solo disco sin RAID; IND-SRV-MES01, un HP ProLiant DL360p Gen8 (2012) con el MES/SCADA Ignition 7.8.5 sobre Windows Server 2016, también con un único disco; IND-SRV-REP01 para reportes y archivos, y un servidor reciclado para dominio (IND-SRV-DC01) en Windows Server 2012 R2.
En general, es una plataforma monolítica, obsoleta y con varios puntos únicos de falla.

P2. ¿Qué mecanismos de backup y recuperación están hoy implementados para estos sistemas?

R2. Se realizan copias de seguridad diarias a un almacenamiento local en los mismos servidores o en discos adicionales, y copias semanales en discos USB externos que se rotan de forma manual. No contamos con replicación automatizada fuera del sitio ni con un repositorio en la nube. Las pruebas formales de restauración se hacen esporádicamente, no con la frecuencia recomendada.

P3. ¿Se cuenta con algún esquema de alta disponibilidad o replicación?

R3. No. Los servidores de ERP, MES/SCADA y reportes tienen un solo disco y no están configurados en clúster ni en arreglos de alta disponibilidad. Si falla el disco o el servidor, el servicio se detiene por completo hasta que podamos restaurar desde backup o recuperar el hardware.

P4. ¿Han tenido incidentes graves de caída de servidores o ataques?

R4. Sí, hemos tenido caídas por fallas de hardware y por problemas de energía. En algunos casos se afectó el ERP y el MES/SCADA durante varias horas. No hemos tenido un incidente de ransomware confirmado, pero el nivel de exposición es alto porque hay sistemas sin parches recientes, versiones fuera de soporte y segmentación débil entre la red de planta y la red corporativa.

P5. ¿Qué tiempos reales de recuperación han observado en incidentes anteriores?

R5. En incidentes simples, como reinicios controlados, hemos logrado recuperar servicios en 2 o 3 horas. Pero cuando se trata de fallas de hardware, restauración de backups o problemas de base de datos, los tiempos reales de recuperación han estado entre 6 y 12 horas, e incluso cercanos a un día completo en situaciones más complicadas.

P6. Desde la perspectiva técnica, ¿cuáles son hoy los principales puntos únicos de falla?

R6. El servidor IND-SRV-ERP01, que concentra la aplicación y la base de datos del ERP en un único disco; el servidor IND-SRV-MES01, que hospeda el MES/SCADA sin redundancia; y el almacenamiento donde se guardan los backups locales. Además, dependemos de un solo enlace principal de Internet y de equipos de red sin redundancia, lo que aumenta el riesgo de indisponibilidad.

P7. ¿Qué servicios de Azure considera más adecuados para la empresa?

R7. Considero que una combinación de máquinas virtuales en Azure para las aplicaciones legadas, Azure SQL Managed Instance para la base de datos del ERP, Azure Backup para copias automáticas con almacenamiento georredundante y Azure Site Recovery para replicar las máquinas virtuales clave entre regiones es una buena base. Complementaría con Azure Firewall, Network Security Groups, Private Link y Azure Monitor/Log Analytics para seguridad y observabilidad.

P8. ¿Qué requisitos de integración ve entre los sistemas en planta y los componentes que eventualmente residan en Azure?

R8. Necesitamos una conectividad segura y estable, idealmente mediante VPN y una arquitectura que minimice la latencia para no impactar la operación de planta. También debemos asegurar que los componentes críticos de tiempo real permanezcan en la red OT, mientras que Azure se utilice para bases de datos, históricos, respaldos y servicios de soporte a la operación.

Anexo E: Guía de entrevista semiestructurada – Usuario clave ERP (Administración y Finanzas).

Entrevista semiestructurada N° 5	Proyecto: Modelo de continuidad del negocio y aseguramiento de la información para Laminados de Occidente S.A.
Entrevistado: Laura *	Cargo: Analista Senior ERP
Área: Administración y Finanzas	Fecha: 13/11/2025
Hora inicio: 10:00	Entrevistador: Investigador – Especialización en Seguridad Informática

Esta entrevista hace parte de un proyecto de investigación de la especialización en Seguridad Informática. El objetivo es entender mejor cómo funcionan los procesos de la empresa, qué tan críticos son para el negocio y cómo dependen de los sistemas de información (ERP Siesa, MES/SCADA Ignition y otros). La información se usará solo con fines académicos y se tratará de manera confidencial. No se publicarán nombres propios. La entrevista dura aproximadamente entre 30 y 45 minutos.

P1. ¿Qué tipo de tareas realiza diariamente en el ERP SIESA?

R1. Registro y revisión de facturas de venta, notas crédito, conciliaciones de cartera, generación de reportes de ventas y apoyo al cierre contable mensual.

P2. ¿Qué tan posible es realizar esas tareas sin el ERP?

R2. De forma temporal se podría registrar información en hojas de cálculo y formatos manuales, pero el riesgo de errores es alto y luego la carga de trabajo para ponerse al día es muy grande. Además, se pierde visibilidad integrada de la información.

P3. ¿Ha tenido experiencias recientes en las que el ERP haya estado caído o muy lento?

R3. Sí, en varias ocasiones el sistema estuvo muy lento y en una oportunidad estuvo caído casi medio día. Tuvimos que detener la facturación, acumular documentos físicos y luego registrar todo de manera acelerada al final de la jornada.

P4. Si el ERP se detuviera por toda una jornada, ¿qué consecuencias ve para su área?

R4. Habría retrasos importantes en la facturación, posibles problemas de cierre contable, impacto en el flujo de caja al no poder registrar oportunamente las ventas y mayor presión sobre el equipo para lograr ponerse al día en poco tiempo.

P5. ¿Cuál diría que es el tiempo máximo que podrían estar sin el ERP antes de que el problema sea muy grave?

R5. Creo que más de 8 horas continuas ya representa una situación muy grave para el área administrativa y financiera. A partir de ese punto es difícil evitar que se afecten cierres y compromisos internos.

P6. ¿Cuánta información podría perderse sin que sea imposible de reconstruir?

R6. Tal vez unas pocas horas de registros, siempre que se conserven los soportes físicos, pero el esfuerzo de reconstrucción sería alto. Idealmente no deberíamos perder ninguna transacción registrada en el día.

P7. ¿Qué le gustaría mejorar en términos de disponibilidad y velocidad del sistema?

R7. Que el sistema responda de manera más estable en horas pico, que se reduzcan las caídas y que exista un plan claro para continuar trabajando o recuperar rápidamente la operación si se presenta una falla prolongada.

Anexo F: Guía de entrevista semiestructurada – Usuario clave ERP (Área Comercial).

Entrevista semiestructurada N° 6	Proyecto: Modelo de continuidad del negocio y aseguramiento de la información para Laminados de Occidente S.A.
Entrevistado: Juan *	Cargo: Coordinador Comercial
Área: Comercial	Fecha: 13/11/2025
Hora inicio: 11:00	Entrevistador: Investigador – Especialización en Seguridad Informática

Esta entrevista hace parte de un proyecto de investigación de la especialización en Seguridad Informática. El objetivo es entender mejor cómo funcionan los procesos de la empresa, qué tan críticos son para el negocio y cómo dependen de los sistemas de información (ERP Siesa, MES/SCADA Ignition y otros). La información se usará solo con fines académicos y se tratará de manera confidencial. No se publicarán nombres propios. La entrevista dura aproximadamente entre 30 y 45 minutos.

P1. ¿Qué tareas realiza en el ERP relacionadas con clientes y ventas?

R1. Registro de pedidos, seguimiento al estado de las órdenes, consulta de historial de compras por cliente, revisión de niveles de inventario para prometer fechas de entrega y apoyo a la gestión de cartera desde el área comercial.

P2. ¿Es posible gestionar pedidos y clientes sin acceso al ERP?

R2. Solo de manera muy limitada, usando correos y hojas de cálculo. Pero se pierde visibilidad sobre el estado real de los pedidos, sobre la disponibilidad de inventario y sobre el historial de cada cliente, lo que complica la atención.

P3. ¿Qué tan frecuente es que necesite información en tiempo real para atender a un cliente?

R3. Prácticamente todos los días. Los clientes preguntan por fechas de entrega, disponibilidad y estado de sus órdenes, y esa información la consultamos directamente en el sistema para dar una respuesta confiable.

P4. Cuando el ERP no está disponible, ¿qué tareas se detienen?

R4. No podemos ingresar nuevos pedidos, ni actualizar el avance de los existentes, ni validar en línea el inventario disponible. La atención se vuelve más lenta y toca prometer cosas con menos certeza, lo que genera incomodidad en los clientes.

P5. ¿Cuál es el tiempo máximo que considera tolerable sin el ERP para seguir atendiendo clientes sin deteriorar la relación comercial?

R5. Unas 4 horas como máximo. A partir de ahí el atraso en la atención empieza a sentirse, se acumulan solicitudes pendientes y se incrementan los reclamos.

P6. ¿Qué impacto estima que tendría una caída de un día completo del sistema en ventas e imagen?

R6. Podríamos perder oportunidades de venta, incumplir fechas prometidas, generar reprocesos internos y erosionar la confianza de los clientes más importantes, que esperan un servicio ágil y confiable.

P7. ¿Qué cambios o mejoras le gustaría que se lograran con un proyecto de continuidad y posible migración a Azure?

R7. Mayor estabilidad del sistema, disponibilidad casi permanente, mejor desempeño en los cierres de mes y un mecanismo que permita consultar información clave incluso si hay problemas con la infraestructura local.