Continuidad de servicios TIC y *cloud computing* en minería

Modelo para la seguridad y disponibilidad de la información



Coord.

Wendy Dominguez Oliva

Tecnológico Universitario EDUPRAXIS

Universidad INCCA de Colombia

Editorial Plagcis

Continuidad de servicios TIC y cloud computing en minería

Modelo para la seguridad y disponibilidad de la información

Wendy Dominguez Oliva

Pedro Pablo Prieto Monzón

Carlos Alberto Castro Carreño

Carlos Ignacio Gallo Aguila

Luis Alberto Talledo Curo

El presente libro ha sido sometido a un riguroso proceso de revisión (pares externos) mediante el sistema de arbitraje de doble ciego. La publicación cuenta con el aval del Comité Científico de la editorial PLAGCIS, de la Universidad INCCA de Colombia y el Tecnológico Universitario Edupraxis, tras haber superado los protocolos editoriales estandarizados que aseguran el cumplimiento de las normas académicas establecidas para publicaciones de carácter científico.

Continuidad de servicios TIC y cloud computing en minería: Modelo para la seguridad y disponibilidad de la información

Primera publicación: mayo, 2026

De esta edición:

Fondo Editorial PLAGCIS, adscrito a la Plataforma de Acción, Gestión e investigación Social S.A.S.

Calle 13B 12-74, Sincelejo - Colombia

Tel.: +57 301 498 9039; director@plagcis.org / www.plagcis.org

Universidad INCCA de Colombia

Cra 13 # 24-15, Bogotá – Colombia

Tecnológico Universitario Edupraxis

Juan Benigno Vela 07-56 y Montalvo. Ambato – Ecuador.

Esta publicación es el resultado de investigación bajo el auspicio de la Plataforma de Acción, Gestión e investigación Social S.A.S – (PLAGCIS) en alianza con la Universidad INCCA de Colombia bajo el convenio marco de cooperación, firmado el 18 de junio del 2025 y con el Tecnológico Universitario Edupraxis.

Este texto está protegido por una licencia Creative Commons 4.0.
https://creativecommons.org/licenses/by/4.0/deed.es



ISBN: 978-628-97608-5-9

DOI: 10.69821/PLAGCIS.60

Acceso abierto / Open Access

Continuidad de servicios TIC y cloud computing en minería: Modelo para la seguridad y disponibilidad de la información / Wendy Dominguez Oliva, Pedro Pablo Prieto Monzón, Carlos Alberto Castro Carreño, Carlos Ignacio Gallo Aguila y Luis Alberto Talledo Curo: Universidad INCCA de Colombia, 2026, Tecnológico Universitario Edupraxis, 2026 & Plataforma de Acción, Gestión e Investigación Social S.A.S., 2026.

ISBN: 978-628-97608-5-9

86 páginas.

1. Continuidad de servicios TIC 2. Computación en la nube 3. Seguridad de la información 4. Resiliencia digital 5. Gobernanza tecnológica 6. Sector minero

Materia: 375.87 - Tecnología (Ciencias aplicadas) en la enseñanza media Libros de texto

Clasificación Thema: UBL - Tecnologías digitales y de la información: aspectos legales de la informática

Libro de investigación No. 60

Cita sugerida (APA 7ma): Dominguez Oliva, W., Prieto Monzón, P. P., Castro Carreño, C. A., Gallo Aguila, C. I., & Talledo Curo, L. A. (2026). *Continuidad de servicios TIC y cloud computing en minería: Modelo para la seguridad y disponibilidad de la información*. Editorial PLAGCIS. https://doi.org/10.69821/PLAGCIS.60

EDITORA EN JEFE

PhD. En Educación Gilma Álamo Sánchez. Plataforma de Acción, Gestión e Investigación Social S.A.S. Chile. https://orcid.org/0000-0002-8342-6597

COORDINADORA EDITORIAL

PhD. Lourdes Meza Ruiz. Plataforma de Acción, Gestión e Investigación Social S.A.S. Argentina. https://orcid.org/0000-0002-3333-7051

ASISTENTE DE EDICIÓN

Plga. Mayra Cujilán, Plataforma de Acción, Gestión e Investigación Social S.A.S. Esmeraldas, Ecuador. https://orcid.org/0009-0006-8074-5011

DIAGRAMADORA

Lic. Diana Rivero

PRACTICANTE

Br. Josue Medina Mencia. Universidad Simón Bolívar. Venezuela

CORRECTOR DE ESTILO

Santiago Ballesteros Gallo. Universidad de Antioquia. Medellín, Colombia. https://orcid.org/0000-0001-7033-1284

TRADUCTOR

Syed Harun Jamallullail. Universiti Teknologi Petronas. Malasia. https://orcid.org/0000-0003-1947-2422

COMITÉ CIENTÍFICO INTERNACIONAL

Esp. Elena Graterol. Universidad Pedagógica Experimental Libertador. Venezuela. https://orcid.org/0000-0002-0110-3672

Mgter. Steeven Moreira, Universidad Nacional de Educación UNAE, Ecuador. https://orcid.org/0000-0001-6696-4185

PhD. Alejandra Carolina Hidalgo de Camba. Universidad Unidos. Panamá. https://orcid.org/0000-0002-7049-2982.

PhD. Carlos Jorge Landaeta Mendoza. Universidad Privada San Francisco de Asís. Bolivia. https://orcid.org/0000-0003-0297-7029

PhD. Dustin Tahisin Gómez Rodríguez, Ph.D. Universitaria Agustiniana - Uniagustiniana, Colombia. https://orcid.org/0000-0001-5359-2300

PhD. Evelyn Ereú. Universidad Pedagógica Experimental Libertador. Venezuela. https://orcid.org/0000-0001-9455-7501

PhD. Haylen Perines Véliz. Universidad Internacional de Valencia. España. https://orcid.org/0000-0002-7020-1014

PhD. Lilian del Carmen López. Universidad Pedagógica Nacional Francisco Morazán. Honduras. https://orcid.org/0000-0002-3645-4659

PhD. Raúl Alberto Rengifo Lozano. Ph.D. Universidad Nacional Mayor de San Marcos. https://orcid.org/0000-0002-6545-6442

PhD. Yajaira Rodríguez Noriega. Sociedad Papiro C.A. Venezuela. https://orcid.org/0000-0001-5441-7838

PhD. Norma. Caira-Tovar. Universidad del Zulia. Venezuela. https://orcid.org/0000-0002-7629-8216.

PhD. Renata Moncini-Marrufo. Universidad Alonso Ojeda. Venezuela. https://orcid.org/0000-0003-4975-9272.

PhD. Voltar Varas Violante. Centro Interdisciplinario de Talento Humano. México. https://orcid.org/0000-0002-6442-6735.

PRESIDENTA

Dra. Susan Rodríguez

RECTORA

Dra. Andrea Sotelo

VICERRECTOR ACADÉMICO

Dr. Santiago Sepúlveda

COORDINADORA DE INVESTIGACIÓN

Jhina Luz Gómez Villera

LÍDER ACADÉMICA INCC'ONNECTION

Kelli Johana Vergara

RECTORA

Mg. Carmen Dominga Pino Avila

VICERRECTOR ACADÉMICO

Ing. Mario Vásquez

VICERRECTOR DE INVESTIGACIÓN

Mg. Byron Andrade

PROMOTORA DE LA INSTITUCIÓN

Mg. Orfa Jacome

Contenido

RESUMEN 10
INTRODUCCIÓN 11
Capítulo 1 14
Continuidad digital y gestión de la información en minería 14
Capítulo 2 22
Fundamentos de cloud computing, continuidad y seguridad de la información 22
Capítulo 3 36
Contexto del estudio y ruta de investigación 36
Capítulo 4 46
Hallazgos del caso y necesidades identificadas 46
Capítulo 5 55
Modelo de continuidad de servicios TIC basado en cloud computing 55
Capítulo 6 67
Alcance, transferibilidad y proyección del modelo 67
REFERENCIAS 78
REFLEXIONES FINALES 82
SOBRE LOS AUTORES 84

RESUMEN

Esta obra examina la continuidad de los servicios de tecnologías de la información y la comunicación en organizaciones del sector minero, con especial atención a la gestión de la información, la seguridad de los datos y la capacidad institucional para sostener operaciones en entornos de creciente dependencia digital. A partir del estudio desarrollado en una empresa vinculada a la minería no metálica en el Perú, el libro construye una lectura aplicada del problema y propone una respuesta estructurada basada en cloud computing, orientada a fortalecer la disponibilidad, el acceso seguro, el resguardo y la recuperación de la información crítica. Lejos de abordar la computación en la nube como una solución exclusivamente tecnológica, la obra la sitúa dentro de una lógica más amplia de continuidad operativa, gobernanza del servicio y reducción de vulnerabilidades. En este marco, se desarrollan los fundamentos conceptuales del cloud computing, los principios de continuidad del negocio y los componentes esenciales de la seguridad de la información, con particular énfasis en la confidencialidad, la integridad y la disponibilidad. Sobre esta base, se interpretan los hallazgos del caso estudiado, entre ellos las debilidades en el control de la información, la necesidad de reforzar la seguridad de los datos y la importancia de contar con proveedores que ofrezcan condiciones confiables de soporte, disponibilidad y resguardo. Como resultado, el libro presenta un modelo de continuidad de servicios TIC con valor analítico y aplicación potencial en contextos organizacionales semejantes. Su principal aporte consiste en mostrar que la continuidad digital no debe entenderse como un aspecto accesorio de la gestión tecnológica, sino como una condición estratégica para la resiliencia, la estabilidad y la sostenibilidad institucional.

INTRODUCCIÓN

Hay problemas organizacionales que solo se vuelven plenamente visibles cuando la interrupción los expone. La continuidad de los servicios de tecnologías de la información y la comunicación pertenece a ese tipo de problemas. Mientras la información circula, los sistemas responden y los procesos se sostienen sin fricción aparente, su importancia suele quedar absorbida por la rutina del funcionamiento. Sin embargo, allí donde el acceso falla, donde la disponibilidad se vuelve incierta o donde la protección de los datos resulta insuficiente, lo que aparece no es únicamente una dificultad técnica. Aparece, con mayor claridad, la trama de dependencias que sostiene a la organización y la medida en que su estabilidad descansa sobre servicios digitales cuya continuidad ya no puede darse por supuesta.

Esta constatación adquiere una densidad particular en el sector minero. No solo por la complejidad de sus operaciones o por la dispersión geográfica que con frecuencia las caracteriza, sino porque en ese entorno la información acompaña decisiones, articula procesos y permite sostener una coordinación que difícilmente podría preservarse bajo condiciones de acceso frágil o interrumpido. La información, en este contexto, no funciona como un simple registro de lo ocurrido. Participa activamente en la organización del trabajo. Por ello, cuando su disponibilidad se debilita o cuando los servicios que la soportan no ofrecen garantías razonables de continuidad, la afectación trasciende el plano tecnológico y alcanza el orden mismo de la operación.

Es en este marco donde se sitúa la presente obra. Su punto de partida es una investigación aplicada desarrollada en el contexto de Américas Potash Perú S. A., empresa vinculada a un proyecto de minería no metálica, cuyo estudio permitió reconocer debilidades en el control de la información, preocupaciones significativas en torno a la seguridad de los datos y la necesidad de disponer de servicios más confiables en términos de disponibilidad, soporte y resguardo. A partir de esa base, el libro no propone una adhesión inmediata a la computación en la nube ni una defensa abstracta de la innovación tecnológica. Lo que propone es una reflexión estructurada sobre las condiciones bajo las cuales el cloud

computing puede integrarse en una estrategia de continuidad de servicios TIC orientada a fortalecer la gestión de la información y a reducir vulnerabilidades institucionales (Dominguez Oliva, 2018).

En este sentido, el interés del libro no reside únicamente en la tecnología que examina, sino en el problema que esa tecnología permite repensar. A lo largo de estas páginas, la nube no aparece como una solución autosuficiente ni como un destino inevitable de la transformación digital. Aparece, más bien, como una posibilidad cuya pertinencia depende de su articulación con criterios de seguridad, de gobierno de la información, de evaluación del proveedor y de capacidad de recuperación ante incidentes. La cuestión decisiva no es, por tanto, si una organización adopta o no servicios cloud en términos generales, sino bajo qué arquitectura de decisión, de control y de continuidad lo hace. Desplazar la discusión hacia ese nivel es una de las intenciones centrales de esta obra.

Esa intención responde también a una cautela metodológica. La evidencia empírica que sustenta el libro proviene de un caso situado y de un momento específico del proceso organizacional. No se la presenta, por ello, como una descripción actual de la empresa ni como una representación exhaustiva del sector minero. Su valor es otro. Haber permitido reconocer una necesidad institucional concreta y haber ofrecido una base suficiente para construir, a partir de ella, una propuesta con sentido analítico y potencial de adaptación a contextos semejantes. La obra no busca extender indebidamente el alcance del caso, sino mostrar de qué manera una experiencia particular puede iluminar un problema más amplio y abrir una discusión pertinente sobre continuidad digital, seguridad de la información y resiliencia operativa.

La estructura del libro responde a esa lógica de avance. El primer capítulo sitúa la discusión en el ámbito de la continuidad digital y de la gestión de la información en minería. El segundo desarrolla los fundamentos conceptuales del cloud computing, la continuidad del negocio y la seguridad de la información. El tercero reencuadra la base metodológica del estudio y explica la ruta de investigación que sostiene la propuesta. El cuarto examina los hallazgos del caso y las necesidades identificadas. El quinto formula el

modelo de continuidad de servicios TIC basado en cloud computing. El sexto, finalmente, discute su alcance, su transferibilidad y su proyección. Las reflexiones finales cierran la obra retomando la convicción que la atraviesa de principio a fin, la continuidad de los servicios digitales no constituye un aspecto accesorio de la gestión tecnológica, sino una dimensión que incide directamente en la estabilidad, la previsión y la sostenibilidad de la organización.

En última instancia, este libro parte de una idea simple, aunque exigente. Allí donde la información sostiene la operación, la continuidad de los servicios TIC no puede resolverse mediante decisiones fragmentarias ni por medio de soluciones adoptadas sin una comprensión suficiente de sus implicaciones. Exige una mirada capaz de articular tecnología, seguridad, acceso, respaldo y gobierno de la información dentro de una misma arquitectura de sentido. Esa es la orientación que guía las páginas que siguen. No la promesa de una respuesta total, sino la búsqueda de una formulación más cuidadosa, más fundada y útil frente a un problema que hoy ocupa un lugar central en la experiencia de las organizaciones.

Capítulo 1
Continuidad digital y gestión de la información en minería

En las organizaciones mineras, la información ya no puede entenderse como un recurso auxiliar que acompaña la operación desde un plano secundario. Más bien, ocupa un lugar central en la coordinación de actividades, en la circulación de reportes, en la toma de decisiones técnicas y administrativas, y en la forma en que la organización mantiene cierta estabilidad cuando el entorno se vuelve más exigente. En ese marco, la continuidad de los servicios de tecnologías de la información y la comunicación adquiere un peso particular, porque de ella depende que los datos estén disponibles, que los sistemas respondan a tiempo y que la comunicación entre áreas no se interrumpa justo cuando más se la necesita.

Esta realidad adquiere una densidad particular en el sector minero. La dispersión geográfica de las operaciones, la interacción constante entre áreas técnicas y administrativas, y la necesidad de mantener flujos de información estables en contextos de alta exigencia operativa confieren a los servicios digitales un valor que excede con mucho la dimensión instrumental. En este ámbito, la información no constituye un simple soporte documental del trabajo; estructura decisiones, articula procesos y sostiene la coordinación que permite a la organización operar con orden y previsibilidad. Cuando el acceso a la información se debilita, cuando su resguardo es insuficiente o cuando los servicios que la soportan no ofrecen garantías razonables de continuidad, lo que se compromete no es solo un recurso tecnológico. Se compromete una parte sustantiva del equilibrio organizacional.

Desde esta perspectiva, la continuidad digital en minería debe ser comprendida como una dimensión inseparable de la gobernanza institucional. No basta con disponer de

herramientas informáticas o con ampliar la infraestructura de acceso. La cuestión central radica en asegurar que la información relevante permanezca disponible, protegida y recuperable en el momento en que la operación lo requiera. Clarke (2012) lo expresó con una formulación especialmente reveladora al señalar que la computación ha alcanzado un estatus semejante al de una utilidad esencial. La observación no es menor. Permite advertir hasta qué punto las organizaciones han pasado a depender de servicios digitales cuya indisponibilidad puede alterar la continuidad del trabajo con una rapidez antes impensable. En el sector minero, donde la coordinación y la oportunidad del dato inciden directamente en la estabilidad de los procesos, esta dependencia se manifiesta con especial claridad.

La continuidad de los servicios TIC no puede reducirse, por tanto, a la simple permanencia técnica de un sistema en funcionamiento. Exige condiciones más complejas y rigurosas. La información debe encontrarse accesible cuando se la necesita, resguardada frente a pérdida o alteración, y disponible bajo condiciones que no comprometan la seguridad ni la integridad de los procesos. Cajamarca-Palomo et al. (2019) recuerdan que la continuidad operativa depende, en buena medida, de que los datos y los servicios permanezcan disponibles sin interrupciones no deseadas ni demoras inesperadas. Esta afirmación adquiere particular relevancia en organizaciones donde los tiempos de respuesta, la coordinación interáreas y la trazabilidad documental no admiten márgenes amplios de error. No basta, en consecuencia, con hablar de acceso a la información en términos generales; lo decisivo es la calidad institucional de ese acceso y la estabilidad que lo sostiene.

A ello se suma una consideración que conviene subrayar. La continuidad digital no es sinónimo de conectividad. Tampoco equivale, sin más, a la adopción de soluciones tecnológicas recientes. Una organización puede disponer de plataformas modernas y, aun así, sostener prácticas débiles en materia de control informacional, seguridad o recuperación ante incidentes. Wielki (2015) ha mostrado que atributos como la disponibilidad, la robustez, la resiliencia y la recuperabilidad se proyectan sobre dimensiones empresariales de alto impacto, entre ellas la calidad del servicio, la continuidad del negocio y la propia supervivencia institucional. Esta relación obliga a desplazar la discusión desde una visión puramente técnica hacia una comprensión más amplia, en la que la continuidad se asume como un componente de la estabilidad organizacional. Allí donde falla la continuidad, no cae solo una aplicación. Se resiente también la capacidad de respuesta, la coordinación y la confianza en el sistema que sostiene la operación.

El caso de Américas Potash Perú S. A., estudiado por Dominguez Oliva (2018), permite observar esta problemática en un contexto concreto. La investigación que sirve de base a esta obra identificó la necesidad de fortalecer el almacenamiento, el acceso y el resguardo de la información dentro de la organización, en un escenario donde la seguridad, la disponibilidad y la confidencialidad de los datos eran percibidas como asuntos especialmente sensibles. Lo relevante de este diagnóstico no reside únicamente en la identificación de una carencia tecnológica, sino en la forma en que el problema fue comprendido. No se trataba simplemente de cambiar de plataforma o de incorporar una nueva herramienta. Lo que se advertía era la necesidad de construir condiciones más sólidas para gestionar información crítica, compartirla con mayor orden, protegerla frente

a pérdida o indisponibilidad y sostener, sobre esa base, una continuidad más confiable del servicio.

Es en este punto donde la discusión se abre hacia el cloud computing. Sin embargo, esa transición requiere prudencia conceptual. La computación en la nube puede ofrecer ventajas significativas en términos de elasticidad, acceso remoto, sincronización y respaldo, pero no debe ser leída como una solución autosuficiente ni como una respuesta automática frente a cualquier debilidad organizacional. Su potencial solo se vuelve significativo cuando se integra en un marco más amplio de gestión, seguridad y continuidad. Mahalle et al. (2021) sostienen que el crecimiento del cloud computing ha transformado la manera en que las organizaciones conciben su infraestructura tecnológica, desplazando progresivamente modelos rígidos hacia esquemas más flexibles y orientados al servicio. No obstante, esta transformación no cancela por sí misma los riesgos. Más bien los reconfigura. Amplía ciertas capacidades, pero también exige nuevas formas de control, evaluación y responsabilidad.

Ese matiz es decisivo para el argumento de este capítulo. La nube no resuelve, por sí sola, las debilidades de una organización en materia de control de la información. Puede mejorar la disponibilidad, pero también redistribuir la dependencia. Puede facilitar el acceso, pero al mismo tiempo exigir una gestión más rigurosa de permisos, respaldos y seguridad. Puede ofrecer escalabilidad, aunque también demandar criterios más exigentes respecto del proveedor y de la gobernanza del servicio. Gupta et al. (2023) advierten, en esa línea, que la adopción de soluciones cloud debe examinarse desde una lógica de gestión del riesgo, donde las decisiones tecnológicas se apoyen en criterios institucionales,

operativos y estratégicos. La observación resulta particularmente pertinente cuando se trata de organizaciones que operan con información sensible, pues en ellas la conveniencia de una arquitectura tecnológica no depende solo de su eficiencia aparente, sino de su capacidad para sostener la continuidad del servicio bajo condiciones de control y confiabilidad.

En el ámbito minero, esta discusión adquiere un relieve adicional. Se trata de organizaciones que no operan en entornos homogéneos ni bajo flujos lineales de información. Los datos circulan entre áreas, respaldan decisiones técnicas y administrativas, acompañan procesos dispersos y deben mantenerse bajo condiciones de acceso y resguardo que no siempre son fáciles de garantizar. Cuando esos flujos pierden estabilidad, la organización no enfrenta únicamente retrasos o desorden documental; enfrenta una forma de vulnerabilidad que se extiende sobre su capacidad de coordinar, de registrar, de responder y de sostener la operación con la consistencia requerida. Por ello, la continuidad digital no puede ser tratada como un problema marginal o exclusivamente técnico. Se trata de una dimensión que incide de manera directa en la solidez de la gestión y en la fortaleza operativa de la institución.

La propuesta desarrollada por Dominguez Oliva (2018) conserva interés, precisamente, porque sitúa el cloud computing dentro de esta exigencia mayor. Su valor no se agota en el caso que le da origen, sino en la forma en que vuelve visible un problema que trasciende a una organización específica: la necesidad de pensar la continuidad de los servicios TIC como una arquitectura de gestión y no como una suma dispersa de herramientas o soluciones parciales. En esta lectura, el cloud computing no es relevante

únicamente por la infraestructura que ofrece, sino por la posibilidad de integrarlo en un esquema donde acceso, seguridad, disponibilidad, respaldo y capacidad de recuperación se articulen con criterios de gobierno y con una comprensión más madura de la información como activo estratégico.

De ahí que la continuidad digital no pueda agotarse en una conversación sobre modernización. Su sentido más profundo aparece cuando se la vincula con la reducción de vulnerabilidades, con la estabilidad institucional y con la construcción de un entorno informacional más confiable. En organizaciones como las mineras, donde la dependencia de la información es elevada y la presión operativa suele ser constante, la continuidad de los servicios TIC representa una condición de orden, de previsión y de sostenibilidad. Pensarla de otro modo sería reducirla a un asunto técnico, cuando en realidad pertenece también al campo de la estrategia, de la seguridad y de la gobernanza.

A la luz de estas consideraciones, este capítulo sostiene que la continuidad digital en minería debe ser entendida como una exigencia estructural de la organización contemporánea. No se trata solo de mantener operativas ciertas plataformas ni de facilitar el acceso remoto a determinados recursos. Se trata de asegurar que la información crítica pueda sostener la operación bajo condiciones de disponibilidad, seguridad y control. En ese marco, el cloud computing aparece como una alternativa con potencial significativo, siempre que su adopción no se limite a una lógica instrumental y se inserte, en cambio, en un modelo más amplio de continuidad de servicios TIC. Esa es la perspectiva que abre el recorrido de esta obra y la que justifica, a partir del caso estudiado, la necesidad de

avanzar hacia una propuesta capaz de articular tecnología, información y resiliencia organizacional.

Capítulo 2

Fundamentos de cloud computing, continuidad y seguridad de la información

Comprender el cloud computing exige algo más que describir una tecnología emergente o enumerar sus ventajas operativas. Supone, en realidad, reconocer un desplazamiento de fondo en la manera de concebir la infraestructura digital, el acceso a los recursos tecnológicos y la responsabilidad sobre los servicios que sostienen la información de una organización. Allí donde antes predominaba una lógica de propiedad, instalación local y administración cerrada de recursos, comenzó a imponerse una lógica de provisión bajo demanda, escalabilidad y servicio distribuido. El cambio no es menor. Afecta la arquitectura técnica, desde luego, pero también modifica la forma en que las organizaciones piensan el control, la dependencia, la seguridad y la continuidad de los servicios que respaldan su funcionamiento.

En este sentido, la computación en la nube no debe reducirse a la idea, todavía frecuente, de almacenamiento remoto o acceso a aplicaciones por internet. Se trata de una forma específica de organizar y consumir capacidad tecnológica. Cajamarca-Palomo et al. (2019) recuerdan que una de las definiciones más ampliamente aceptadas remite a un conjunto de recursos, características y modelos que permiten proveer servicios tecnológicos a través de internet. En una línea convergente, Senyo et al. (2018) sostienen que el cloud computing supone la entrega bajo demanda de infraestructura y aplicaciones a individuos y organizaciones, desplazando progresivamente modelos basados en la posesión directa de los recursos. Lo decisivo de ambas formulaciones no está únicamente en el medio técnico, sino en la transformación conceptual que introducen. La nube no designa solo un entorno distinto; designa una manera distinta de relacionarse con la infraestructura, con el servicio y con la lógica misma de la provisión tecnológica.

Esta transformación ha sido impulsada por atributos que, con el tiempo, pasaron a ser casi estructurales dentro del discurso y de la práctica del cloud computing. Rai et al. (2024) destacan entre ellos el autoservicio bajo demanda, la escalabilidad, la elasticidad, el pago por uso, la alta disponibilidad, la automatización y la incorporación de mecanismos de seguridad. Tales rasgos explican buena parte de su expansión, pero su importancia no reside simplemente en la novedad. Reside en la posibilidad de responder con mayor flexibilidad a necesidades que las infraestructuras tradicionales atienden con dificultad, especialmente cuando la demanda tecnológica es variable, cuando los procesos se distribuyen entre varias sedes o cuando la organización necesita sostener acceso continuo a la información sin asumir todos los costos de una infraestructura propia de gran escala.

Desde luego, el cloud computing no surgió de manera súbita ni aislada. Hussen et al. (2019) explican que su aparición se vincula con la convergencia de desarrollos previos, entre ellos la computación distribuida, la virtualización, la computación paralela y otros enfoques de red que prepararon el terreno para una nueva generación de servicios digitales. Ladan (2019) interpreta esta evolución como parte de una transición hacia modelos de utilidad, semejantes a otros servicios esenciales en los que el usuario accede a una capacidad sin cargar con la totalidad de su infraestructura. Esta lectura ayuda a comprender por qué Clarke (2012) llegó a presentar la computación como una especie de quinta utilidad. Más allá de la fuerza retórica de la expresión, lo que en ella se vuelve visible es el lugar central que la infraestructura digital ha adquirido en la vida organizacional contemporánea. No como accesorio, sino como soporte estable del funcionamiento cotidiano.

El crecimiento de la nube debe leerse, por tanto, en relación con necesidades concretas de las organizaciones. Ma et al. (2015) señalan que ha pasado de ser una idea prometedora por consolidarse como uno de los segmentos de mayor expansión en la industria tecnológica. Carneiro y Paula (2017), por su parte, destacan beneficios percibidos con bastante claridad por las instituciones, entre ellos el bajo costo de entrada, el pago según uso efectivo, la rapidez de despliegue y el acceso a recursos actualizados. Sin embargo, sería simplificador interpretar su adopción solo como una decisión económica. La nube se expande porque responde a un cambio más profundo en la forma de concebir la relación entre operación, información e infraestructura. Permite, en muchos casos, mover la atención desde la posesión de recursos hacia la continuidad y la calidad del servicio que esos recursos deben sostener.

Para comprender mejor esta lógica conviene distinguir los modelos de servicio que organizan la oferta cloud. Aunque suelen presentarse como una clasificación básica, esa distinción tiene una importancia decisiva, porque define niveles diferentes de control, delegación y responsabilidad. Según Senyo et al. (2018), los tres modelos más extendidos son Software as a Service, Platform as a Service e Infrastructure as a Service. En ellos no solo cambia el tipo de recurso entregado, cambia también la arquitectura de la relación entre el usuario y el proveedor. En otras palabras, no se trata únicamente de elegir un servicio; se trata de definir cuánto control se conserva, cuánto se delega y en qué condiciones se sostiene la dependencia tecnológica.

El modelo de Software as a Service, o SaaS, representa la expresión más visible y, en muchos casos, más accesible de la nube. Aquí el usuario accede a aplicaciones alojadas

en la infraestructura del proveedor, generalmente a través de interfaces web o programas cliente, sin necesidad de instalación local ni administración directa de la plataforma subyacente. Cajamarca-Palomo et al. (2019) destacan precisamente esta simplificación del uso, mientras que Senyo et al. (2018) subrayan que se trata de aplicaciones que residen en la infraestructura del proveedor y son consumidas por el usuario como servicio. Esta forma de provisión reduce la carga operativa interna y acelera la puesta en marcha, pero también desplaza buena parte del control hacia el proveedor. Allí radica, a la vez, su principal fortaleza y una de sus mayores limitaciones.

Hashizume et al. (2013) advierten que, debido al elevado grado de abstracción de SaaS, la responsabilidad principal sobre la seguridad recae en quien provee el servicio. Iqbal et al. (2016) agregan que en este entorno aparecen amenazas asociadas a credenciales débiles, protocolos inseguros, vulnerabilidades propias de aplicaciones web y uso abusivo de la infraestructura. Dhirani y Newe (2020) añaden que el modelo permite escalar según demanda y pagar en función del uso efectivo, lo que explica buena parte de su atractivo. Aun así, su conveniencia depende del tipo de organización y del nivel de criticidad de la información gestionada. Allí donde la personalización, la sensibilidad del dato o la exigencia de control son elevadas, la comodidad del modelo puede no ser suficiente.

Entre el SaaS y la infraestructura más básica se ubica Platform as a Service, o PaaS. Este modelo no entrega una aplicación terminada, pero tampoco exige al usuario administrar directamente la infraestructura base. Ofrece, más bien, un entorno de desarrollo y despliegue sobre el cual es posible construir, probar y ejecutar aplicaciones.

Hussen et al. (2019) lo describen como una plataforma de cómputo que incluye sistemas operativos, bases de datos, servidores web y herramientas para el desarrollo. Senyo et al. (2018) lo presentan como un espacio soportado por el proveedor para que los usuarios creen y ejecuten aplicaciones mediante interfaces de programación específicas. En términos organizacionales, PaaS representa una cesión parcial del control, pero también una ampliación de la capacidad de construir soluciones propias sin asumir toda la complejidad de la capa infraestructural.

Ma et al. (2015) sostienen que este modelo reduce la complejidad y los costos asociados a la compra y administración de capas de hardware y software base. Dhirani y Newe (2020) destacan su utilidad cuando se requieren entornos ya preparados para desarrollo, pruebas o gestión de bases de datos. No obstante, la mayor flexibilidad no suprime los riesgos. Hashizume et al. (2013) recuerdan que el control adicional que ofrece PaaS trae consigo preocupaciones ligadas al acceso privilegiado, a la ubicación de los datos y a la seguridad de las aplicaciones construidas sobre la plataforma. La nube, en este nivel, no elimina la necesidad de gobernanza. La hace más compleja.

En la base del ecosistema cloud se encuentra Infrastructure as a Service, o IaaS. Se trata del modelo que entrega mayor margen de control al cliente y, al mismo tiempo, una mayor cuota de responsabilidad. Cajamarca-Palomo et al. (2019) lo describen como una forma de hospedaje en centros de datos donde el usuario dispone de servidores virtuales con características definidas según necesidad. Song y Young-Woo (2022) sostienen que este modelo se enfoca en la provisión y mantenimiento de recursos virtualizados, como capacidad de cómputo y almacenamiento. Bhuvana y Bhuvana (2024) amplían esta idea y

explican que IaaS permite delegar servidores, redes, procesamiento, máquinas virtuales y otros componentes de infraestructura. Aquí la nube deja de ser un servicio visible para convertirse en la base sobre la que pueden construirse otras capas.

Clarke (2012) señala que una diferencia decisiva entre IaaS y SaaS es el nivel de control que conserva el usuario sobre la solución. Esa mayor libertad puede resultar especialmente valiosa en organizaciones que requieren configuraciones específicas, mayores niveles de supervisión o políticas propias de seguridad y recuperación. Sin embargo, Hashizume et al. (2013) advierten que una menor abstracción no equivale a menor riesgo. Simplemente redistribuye las responsabilidades. Abdullahi (2023) subraya que los entornos virtualizados pueden exponer a amenazas específicas, incluidas aquellas derivadas de ataques entre máquinas virtuales. A pesar de ello, IaaS mantiene una relevancia particular para la continuidad, precisamente porque ofrece un margen mayor para diseñar esquemas de disponibilidad y recuperación acordes con la criticidad del servicio.

La relación entre estos modelos no debe entenderse como una simple secuencia clasificatoria. Existe entre ellos una dependencia profunda. PaaS y SaaS suelen construirse sobre IaaS, de modo que una vulnerabilidad en la infraestructura puede proyectarse hacia las capas superiores. Hashizume et al. (2013) advierten que esta dependencia vertical obliga a pensar la seguridad y la continuidad como una arquitectura integrada. El servicio visible para el usuario es solo la superficie de una estructura más amplia, compuesta por múltiples capas de control, exposición y responsabilidad. De ahí que la discusión sobre cloud computing no pueda agotarse en la interfaz o en la comodidad del acceso. Lo

decisivo está, con frecuencia, en la solidez de las dependencias invisibles que sostienen el servicio.

Junto a los modelos de servicio, los modelos de despliegue cumplen un papel determinante. No basta con definir qué se consume; también importa dónde y bajo qué configuración se aloja. La nube pública ofrece recursos compartidos a múltiples organizaciones o usuarios a través de internet y resulta especialmente atractiva por su economía de escala y su capacidad de acceso a infraestructura sofisticada sin grandes inversiones iniciales. Patni (2021) la presenta como un entorno de recursos compartidos, mientras que Bhuvana y Bhuvana (2024) recuerdan que esta modalidad introduce interrogantes relacionadas con multitenencia, soberanía del dato y responsabilidades compartidas de seguridad. Su fortaleza reside en la amplitud y la eficiencia. Su límite aparece cuando la organización necesita niveles de control más estrictos o trata con información especialmente sensible.

En contraste, la nube privada permite un grado mayor de control sobre la localización de los datos y sobre las condiciones de acceso. Okuonghae y Bakare (2023) destacan que este modelo favorece la privacidad y la seguridad, precisamente porque la información se mantiene en un entorno restringido a la propia organización. No obstante, esa ganancia en control suele venir acompañada de costos más altos y de una mayor carga de administración. En la práctica, la elección entre nube pública y privada no puede resolverse de forma abstracta. Depende del equilibrio que cada organización establezca entre costo, control, sensibilidad del dato y exigencia regulatoria.

La nube híbrida surge, en buena medida, como intento de conciliación. Xu et al. (2014) señalan que combina recursos públicos y privados, permitiendo que información sensible o aplicaciones críticas permanezcan en entornos más controlados, mientras otras cargas se distribuyen en servicios públicos. Palos-Sánchez (2017) sostiene que esta modalidad favorece la colaboración y la eficiencia sin obligar a una renuncia total al control sobre los datos más delicados. Esa flexibilidad explica buena parte de su atractivo. No resuelve por sí sola las tensiones entre costo, acceso y seguridad, pero ofrece una arquitectura de equilibrio razonable para organizaciones que necesitan avanzar con cautela y criterio.

La literatura reciente también concede creciente atención a las estrategias multicloud y a otros esquemas de diversificación del servicio. Marinho et al. (2021) sugieren que la madurez tecnológica influye en la adopción de estas modalidades, mientras que Palos-Sánchez (2017) destaca que el uso de múltiples nubes puede disminuir la dependencia respecto de un único proveedor y reducir la exposición frente a pérdidas de datos o caídas del servicio. En términos de continuidad, esta observación es especialmente relevante. Diversificar no implica necesariamente complejizar sin sentido. En determinados contextos, puede significar aumentar la capacidad de resistencia de la organización frente a la interrupción.

La discusión sobre cloud computing conduce, inevitablemente, a la cuestión de la continuidad del negocio. Clarke (2012) vincula esta continuidad con la confiabilidad y con la distribución geográfica de los centros de datos, mientras que Cajamarca-Palomo et al. (2019) recuerdan que la operación solo puede sostenerse si los datos y servicios

permanecen disponibles cuando se los requiere. Bajo esta perspectiva, la continuidad no consiste simplemente en poseer copias de respaldo o contratar un proveedor conocido. Consiste en asegurar que las funciones esenciales de la organización puedan sostenerse antes, durante y después de una interrupción. Se trata de una lógica temporal más exigente. No basta con recuperar. Importa también resistir y sostener.

Wielki (2015) aporta aquí una relación especialmente fecunda al vincular atributos técnicos como disponibilidad, robustez, resiliencia y recuperabilidad con atributos de negocio como calidad del servicio, continuidad organizacional y supervivencia institucional. Esta conexión permite evitar un error frecuente, reducir la continuidad a una preocupación exclusiva del área de tecnología. Cuando un servicio digital falla, no se interrumpe solo una aplicación. Se afecta, potencialmente, la coordinación, la trazabilidad, la comunicación y la capacidad de tomar decisiones oportunas. En organizaciones complejas, esta relación se vuelve todavía más evidente. La continuidad digital no es un apéndice del negocio. Es una de sus condiciones de posibilidad.

Entre los componentes de esa continuidad, la disponibilidad ocupa un lugar central. Song y Young-Woo (2022) recuerdan que la dependabilidad no es un atributo único, sino una combinación de disponibilidad, confiabilidad, seguridad, mantenibilidad y otras propiedades. Bhuvana y Bhuvana (2024) advierten que la ausencia de disponibilidad sigue siendo una de las preocupaciones más sensibles en los servicios cloud, mientras que Okai-Ugbaje et al. (2014) muestran que incluso con acuerdos de nivel de servicio la disponibilidad real puede situarse por debajo de lo prometido. La tensión es clara. En

cloud no interesa solo que el servicio exista, sino que responda con estabilidad y con niveles previsibles de desempeño.

La continuidad en la nube exige también prestar atención a la recuperación ante desastres y a la protección de los datos. Cajamarca-Palomo et al. (2019) advierten que eventos como la quiebra del proveedor, su adquisición o fallas severas pueden comprometer el acceso a la información. Paraïso et al. (2014) recuerdan, además, que los sistemas cloud están expuestos a vulnerabilidades, ataques y caídas del servicio, y documentan interrupciones temporales en servicios ampliamente utilizados. Carneiro y Paula (2017) sostienen, por ello, que los criterios de selección del proveedor deben incluir redes redundantes, energía redundante y planes documentados de recuperación y continuidad. La confianza en la nube no puede descansar únicamente en la visibilidad comercial de una marca. Debe examinar su arquitectura de resiliencia.

Todo lo anterior conduce al núcleo más sensible del capítulo, la seguridad de la información. En el ámbito del cloud computing, esta cuestión se organiza con frecuencia a partir de la conocida triada CIA: confidencialidad, integridad y disponibilidad. Hussen et al. (2019) sostienen que estos tres principios ofrecen una base conceptual robusta para comprender los desafíos de seguridad en la nube. Yang (2016) coincide al presentarlos como bloques fundamentales en el diseño de sistemas seguros. La importancia de esta triada radica en que permite leer la seguridad no como un conjunto disperso de controles, sino como una arquitectura de protección que debe asegurar acceso restringido, exactitud del dato y continuidad en su disponibilidad.

La confidencialidad remite a la necesidad de que la información solo sea accesible para quienes están autorizados. Şaykol y Avcı (2015) recuerdan que esta preocupación es crítica para organizaciones que manejan datos propios y de terceros. Xu et al. (2014) explican que la externalización de datos introduce riesgos ligados a la falta de visibilidad, al control disminuido, a la multitenencia y a vulnerabilidades de virtualización. Hashizume et al. (2013) añaden que delegar servicios esenciales en terceros vuelve más compleja la protección de la privacidad. Bajo estas condiciones, la confidencialidad no puede pensarse como un simple requisito técnico. Es una condición de confianza y de legitimidad en la gestión de la información.

La integridad, por su parte, exige que la información conserve exactitud, completitud y ausencia de modificaciones no autorizadas. Ma et al. (2015) advierten que la verificación de integridad en servidores no confiables constituye una de las principales preocupaciones del almacenamiento cloud. Slamanig y Raß (2011) insisten en la necesidad de esquemas de confianza y de controles que permitan validar la corrección del dato, mientras que Afroz y Goswami (2023) destacan que la infraestructura del lado del servidor debe ofrecer medidas sólidas para proteger integridad y disponibilidad de manera simultánea. La nube no solo debe almacenar. Debe ofrecer garantías razonables de que lo almacenado sigue siendo correcto, trazable y utilizable.

La disponibilidad, finalmente, conecta seguridad y continuidad. Bhuvana y Bhuvana (2024) señalan que ataques distribuidos, errores de configuración o fallas del proveedor pueden interrumpir servicios SaaS, PaaS o IaaS. Patni (2021) sostiene que los sistemas cloud deben diseñarse para resistir perturbaciones en recursos compartidos y mantener

disponibilidad continua. En este punto aparece una de las tensiones más delicadas de la arquitectura digital contemporánea. Proteger no puede significar bloquear el acceso legítimo. La seguridad, bien entendida, no restringe de forma indiscriminada; asegura que el acceso correcto ocurra en el momento correcto y bajo condiciones estables.

La adopción de soluciones cloud, en consecuencia, no puede decidirse solo por entusiasmo tecnológico ni por expectativa de ahorro. Marinho et al. (2021) identifican factores como ventaja relativa, compatibilidad, complejidad, preparación tecnológica, competencia organizacional, apoyo de la alta dirección, presión competitiva, soporte del proveedor y cumplimiento regulatorio. Palos-Sánchez (2017) agrega que entre las barreras más frecuentes aparecen la seguridad, la confidencialidad, la privacidad y la confiabilidad del proveedor. Clarke (2012) advierte, además, que servicios aparentemente muy atractivos por su elasticidad o movilidad pueden esconder dependencias y riesgos menos visibles. La conveniencia del cloud computing, por tanto, no puede evaluarse al margen del contexto organizacional. Debe ser leída a la luz de las exigencias reales de la operación.

Si se observa el panorama regional, la adopción de la nube continúa siendo desigual. Cajamarca-Palomo et al. (2019) describen el caso ecuatoriano como incipiente y muestran una brecha entre conocimiento del cloud computing y uso efectivo del servicio. Carneiro y Paula (2017) señalan que Brasil posee el mayor mercado de servicios computacionales en América Latina, aunque también enfrenta tensiones relacionadas con seguridad, conectividad, costos y entorno económico. Chimezie et al. (2024) sugieren, a su vez, que en distintos contextos latinoamericanos las aplicaciones cloud mantienen un potencial

considerable para consolidar infraestructura tecnológica con eficiencia y calidad de servicio. La tendencia general apunta al crecimiento, pero no a una adopción homogénea ni lineal. Persisten barreras, dudas y desigualdades que obligan a pensar la nube con criterio y no como una solución universal.

De todo lo anterior se desprende una conclusión decisiva para esta obra. El cloud computing no debe ser leído como una tendencia que deba adoptarse por simple inercia ni como una respuesta única frente a los problemas de continuidad. Su valor depende de la claridad con que se comprendan sus modelos de servicio, sus formas de despliegue, sus implicancias para la continuidad del negocio y las exigencias de seguridad que acompañan su adopción. Allí radica, en el fondo, su verdadera relevancia. No en la promesa abstracta de modernización, sino en la posibilidad de construir, con mayor madurez, una arquitectura de servicios capaz de sostener la información bajo condiciones de acceso, seguridad y resiliencia.

Este capítulo ha querido ofrecer precisamente esa base. No un catálogo de herramientas ni una defensa simplificada de la nube, sino un marco conceptual desde el cual resulte posible interpretar con mayor rigor cualquier propuesta de continuidad de servicios TIC. Sin esa base, la adopción tecnológica corre el riesgo de volverse intuitiva, fragmentaria o excesivamente dependiente de promesas comerciales. Con ella, en cambio, la organización puede evaluar con mayor discernimiento qué modelo le conviene, qué riesgos está dispuesta a asumir y qué condiciones debe exigir para que la continuidad de sus servicios digitales no sea una expectativa difusa, sino una posibilidad real de estabilidad operativa.

Capítulo 3

Contexto del estudio y ruta de investigación

Toda propuesta sólida necesita explicar desde qué experiencia concreta surge y en qué condiciones adquiere legitimidad. En una obra como esta, esa exigencia no puede resolverse mediante la reproducción mecánica de un marco metodológico de tesis ni mediante una enumeración rígida de categorías técnicas que interrumpan la lectura sin aportar verdadera inteligibilidad. Lo que corresponde, más bien, es esclarecer el lugar desde el cual se construye la reflexión, la naturaleza de la evidencia que la sostiene y el tipo de inferencia que resulta razonable a partir de ella. No se trata únicamente de mostrar cómo se investigó. Se trata de dejar en claro por qué esa ruta permite sostener, con fundamento, la propuesta que el libro desarrolla en sus capítulos posteriores.

La presente obra encuentra su base empírica en una investigación aplicada desarrollada en el contexto de Américas Potash Perú S. A., empresa vinculada a un proyecto de minería no metálica en el Perú. Ese caso permitió reconocer una necesidad organizacional precisa, fortalecer la continuidad de los servicios TIC en un entorno donde el acceso a la información, su resguardo y su disponibilidad constituían condiciones sensibles para la operación. El interés del estudio no se orientó a probar experimentalmente una tecnología ni a comparar de manera controlada varias soluciones disponibles en el mercado. Su propósito fue de otra naturaleza, comprender una situación organizacional concreta, identificar sus tensiones principales y, sobre esa base, formular una respuesta técnicamente viable y conceptualmente consistente. Esa precisión es importante, porque delimita el alcance del libro y evita una lectura equívoca de la evidencia. Lo que aquí se presenta no es un diagnóstico actualizado de la empresa, sino la reelaboración analítica de un caso que permitió estructurar una propuesta de continuidad basada en cloud computing (Dominguez Oliva, 2018).

Desde esta perspectiva, la metodología no debe entenderse como un apéndice técnico ni como una obligación formal que el texto cumple por exigencia académica. Su función es otra. Permitir que el lector comprenda de qué manera un problema organizacional situado se transforma en conocimiento aplicable y, posteriormente, en propuesta. Maxwell (2013) ha insistido en que la fuerza de una investigación no depende de la acumulación de procedimientos, sino de la coherencia entre preguntas, decisiones metodológicas, evidencia e interpretación. Ravitch y Carl (2021) desarrollan una idea semejante al señalar que el diseño metodológico debe ser leído como una relación articulada entre lo conceptual, lo empírico y lo interpretativo. Bajo esta comprensión, el capítulo no busca reiterar la estructura universitaria de la tesis original, sino reencuadrar su lógica en una forma más adecuada para el libro.

Ese reencuadre conduce de manera natural a comprender la investigación como un estudio de caso aplicado. Yin (2018) ha señalado que el estudio de caso resulta especialmente pertinente cuando se busca analizar un fenómeno en su contexto real, sobre todo cuando los límites entre el fenómeno y el entorno que lo condiciona no son del todo nítidos. La continuidad de los servicios TIC responde precisamente a esa condición. No puede separarse con claridad de la organización, de sus prácticas, de sus debilidades internas, de su relación con el proveedor ni de la forma en que la información circula y se protege dentro de su operación cotidiana. Stake (1995), desde otra tradición, también subraya que el valor del caso no radica solo en su singularidad, sino en la comprensión densa que puede ofrecer sobre una situación específica. Esta perspectiva resulta especialmente fecunda para una obra como la presente, porque permite sostener el carácter situado de la evidencia sin renunciar a su capacidad de proyección analítica.

Bajo esa lógica, la obra se apoya en una investigación aplicada, leída como estudio de caso, desarrollada desde un paradigma pragmático y con predominio del enfoque cuantitativo. La elección de este paradigma no responde a una moda metodológica ni a una búsqueda terminológica de sofisticación. Responde a la naturaleza misma del problema. Creswell y Creswell (2018) explican que el pragmatismo se centra en la pregunta de investigación, en las consecuencias prácticas del conocimiento y en la selección de aquellos métodos que permitan responder de manera más pertinente a una situación concreta. Morgan (2014) refuerza esta idea al sostener que el pragmatismo permite superar oposiciones rígidas entre lo cuantitativo y lo cualitativo, poniendo el énfasis en la utilidad epistemológica de las decisiones tomadas. En el caso que da origen a este libro, esa utilidad fue nítida, se trataba de comprender una necesidad institucional vinculada con la continuidad de los servicios TIC y de traducir esa comprensión en una propuesta viable de mejora.

El predominio cuantitativo de la investigación se explica por el tipo de evidencia que hizo posible ordenar el problema. Hernández Sampieri y Mendoza (2018) señalan que este enfoque permite medir fenómenos, identificar regularidades y trabajar con información estructurada mediante procedimientos de recolección y análisis sistemáticos. Creswell y Creswell (2018) añaden que resulta especialmente adecuado cuando el interés se centra en describir tendencias o patrones dentro de una población acotada. En el estudio de base, esta elección permitió organizar la información en torno a dimensiones específicas, el control de la información, la seguridad de la información y los requerimientos externos asociados al servicio. No se trataba de capturar exhaustivamente la subjetividad de los actores ni de producir una teoría emergente sobre el contexto

organizacional. Se trataba, más bien, de estructurar evidencia suficiente para reconocer necesidades, interpretar su alcance y sostener una propuesta.

En cuanto a su alcance, la investigación puede ser comprendida con mayor precisión, para los fines de este libro, como descriptiva con orientación propositiva. Bernal (2016) recuerda que los estudios descriptivos buscan especificar rasgos, propiedades y condiciones de un fenómeno o de una situación determinada. Aquí esa función fue central. La investigación permitió caracterizar una debilidad institucional en materia de control informacional, seguridad de los datos y relación con el soporte externo del servicio. Sin embargo, el estudio no se agota en esa descripción. Su sentido pleno aparece cuando esos hallazgos se proyectan hacia la formulación de un modelo. De ahí la pertinencia de hablar de una orientación propositiva. No porque el estudio pretenda demostrar experimentalmente la superioridad de una solución, sino porque convierte un diagnóstico situado en base razonada para una propuesta de continuidad.

La ruta metodológica combinó dos procedimientos que, en conjunto, resultan especialmente adecuados para este tipo de trabajo, diagnóstico organizacional estructurado y revisión documental. Bowen (2009) ha mostrado que la revisión documental no debe ser tratada como un recurso secundario o auxiliar, sino como una técnica capaz de contextualizar, contrastar y enriquecer la comprensión del fenómeno investigado. En el caso de esta obra, esa revisión permitió recuperar el sentido de la investigación original, delimitar el problema, reconocer la lógica de las dimensiones analizadas y vincular la propuesta con una base documental trazable. El diagnóstico organizacional estructurado, por su parte, hizo posible ordenar evidencia empírica sobre la forma en que el problema

era percibido dentro de la organización. Rodríguez, Gil y García (1999) ya advertían que, incluso en diseños de orientación más estructurada, el acercamiento al contexto institucional requiere procedimientos que hagan visible cómo los actores leen y experimentan su propia realidad. Aquí esa evidencia no se presenta como una medición vigente del presente, sino como el soporte empírico que permitió construir la propuesta inicial.

El diseño del estudio fue no experimental y de corte transversal. Esta caracterización conserva pertinencia en el libro, siempre que se la comprenda desde una lógica de síntesis metodológica y no de formalismo innecesario. Hernández Sampieri y Mendoza (2018) recuerdan que los diseños no experimentales observan los fenómenos tal como ocurren en su contexto natural, sin manipular deliberadamente variables ni imponer tratamientos artificiales. Esa definición se ajusta con precisión a la investigación de base. La organización fue observada en su propia realidad operativa, sin alterar las condiciones en que se producía el problema. A su vez, Creswell y Creswell (2018) sostienen que los estudios transversales ofrecen una visión analítica de un fenómeno en un momento determinado, lo que resulta pertinente cuando se busca describir una situación y derivar de ella decisiones o propuestas. En este libro, esa temporalidad no se oculta. Al contrario, se asume con claridad. La evidencia corresponde a un momento específico y debe leerse como tal.

Esta precisión tiene implicaciones importantes. El valor del libro no depende de presentar esa evidencia como si describiera el estado actual de la empresa, sino de reconocer que se trata de un caso situado cuya fuerza reside en haber permitido hacer

visible un problema y formular una arquitectura de respuesta. Yin (2018) es especialmente claro en este punto cuando sostiene que el valor del estudio de caso no exige universalidad, sino claridad respecto del tipo de conocimiento que produce y del alcance de las inferencias que permite sostener. En esta obra, esa inferencia es razonable y acotada. Los hallazgos del caso no habilitan generalizaciones automáticas sobre el sector minero en su conjunto, pero sí fundamentan una propuesta con capacidad de diálogo y adaptación en contextos organizacionales semejantes.

Uno de los méritos de la investigación de base radica, precisamente, en la coherencia entre problema, evidencia y propuesta. Maxwell (2013) insiste en que una investigación sólida debe mostrar con claridad la relación entre sus preguntas, su diseño y las inferencias que de él se derivan. Flick (2018), desde otra tradición metodológica, advierte igualmente que la credibilidad de un trabajo aplicado depende de la coherencia interna de sus componentes. En este caso, la secuencia resulta clara. Primero, se reconoce una necesidad organizacional vinculada con la continuidad de los servicios TIC. Después, se organiza una ruta diagnóstica que permite comprender cómo se manifiesta esa necesidad en el caso estudiado. Finalmente, a partir de esa evidencia, se formula una propuesta basada en cloud computing. No hay salto arbitrario entre problema y modelo. Hay mediación metodológica. Y esa mediación es la que el presente capítulo busca poner en evidencia.

A modo de síntesis, la lógica del estudio puede entenderse como una cadena de construcción del conocimiento aplicado. El problema organizacional da lugar a la delimitación del caso. El caso exige recuperación documental y diagnóstico estructurado.

Esa evidencia, interpretada por dimensiones, permite reconocer necesidades concretas. Y son esas necesidades las que, a su vez, hacen posible el diseño del modelo de continuidad de servicios TIC.

Esta secuencia se sintetiza en la Tabla 1, donde se presenta la ruta metodológica que sustenta el estudio y su reelaboración en formato libro. En ella se integran el paradigma adoptado, el tipo de investigación, la estrategia general, el enfoque predominante, el alcance, el diseño, las técnicas empleadas y el producto metodológico derivado del proceso investigativo. La inclusión de esta tabla no responde al propósito de rigidizar la lectura, sino al de ofrecer una visión ordenada y comprensible de la arquitectura metodológica que sostiene la obra y da consistencia a la propuesta desarrollada en los capítulos siguientes.

Tabla 1

Ruta metodológica del estudio aplicada al libro

Componente	Formulación adoptada	Sustento metodológico
Paradigma	Pragmático	Privilegia la pertinencia del método en función del problema de estudio y de la utilidad práctica del conocimiento producido (Creswell & Creswell, 2018; Morgan, 2014).
Tipo de investigación	Aplicada	Se orienta a comprender una necesidad concreta y a construir una respuesta con utilidad organizacional y técnica (Bernal, 2016).
Estrategia general	Estudio de caso	Permite analizar un fenómeno en su contexto real y comprender con profundidad una situación particular sin aislarla artificialmente de su entorno (Stake, 1995; Yin, 2018).
Enfoque predominante	Cuantitativo, con función diagnóstica	Facilita organizar evidencia estructurada, identificar tendencias y fundamentar decisiones a partir de datos sistematizados (Hernández Sampieri & Mendoza, 2018; Creswell & Creswell, 2018).
Alcance	Descriptivo y propositivo	Describe condiciones existentes del caso y proyecta una propuesta de solución basada en los hallazgos obtenidos (Bernal, 2016).

Diseño	No experimental, de corte transversal	Examina el fenómeno en su contexto natural y en un momento específico, sin manipulación deliberada de variables (Hernández Sampieri & Mendoza, 2018; Creswell & Creswell, 2018).
Técnicas principales	Diagnóstico organizacional estructurado y revisión documental	Permiten articular contexto, evidencia empírica y trazabilidad analítica para la formulación de propuestas aplicadas (Bowen, 2009).
Base empírica	Caso de Américas Potash Perú S. A.	Proporciona evidencia situada para comprender una necesidad institucional y sustentar la formulación del modelo (Dominguez Oliva, 2018).
Producto metodológico	Modelo de continuidad de servicios TIC basado en cloud computing	Surge de la articulación entre problema organizacional, evidencia diagnóstica, revisión conceptual y diseño propositivo.

Del mismo modo, el flujo de trabajo metodológico, que más adelante podrá representarse visualmente, sintetiza con claridad la progresión del estudio, problema organizacional identificado, delimitación del caso, revisión documental, diagnóstico estructurado, interpretación de hallazgos, diseño del modelo y proyección analítica. Esta secuencia no debe leerse como una linealidad cerrada, sino como una forma de mostrar que la propuesta no surge de una intuición tecnológica ni de una extrapolación forzada. Surge de una lectura ordenada de una necesidad institucional.

En este punto conviene detenerse en una cuestión que fortalece la honestidad académica del libro. La evidencia empírica utilizada proviene de un momento específico del estudio original y, por lo mismo, no puede presentarse como reflejo actual del estado de la empresa ni del sector. Esta aclaración no debilita la obra. Le confiere mayor seriedad. Como sostiene Yin (2018), una buena investigación no necesita simular una universalidad que no posee; necesita, más bien, explicitar con claridad sus límites y el tipo de transferencia que permite. Aquí esa transferencia es razonable porque el problema de fondo, continuidad de los servicios TIC, seguridad de la información, acceso confiable a los datos y necesidad de arquitecturas más resilientes, mantiene su vigencia más allá de

la temporalidad concreta del caso. Lo que cambia con el tiempo no es la relevancia del desafío, sino el entorno particular desde el cual fue observado.

Este capítulo, por tanto, cumple una función decisiva dentro de la estructura del libro. No reproduce un marco metodológico en clave universitaria, ni convierte el diseño del estudio en una demostración formalista. Su propósito es otro. Mostrar que detrás de la propuesta de continuidad basada en cloud computing existe una ruta de investigación clara, razonada y defendible. La obra no se apoya en intuiciones ni en un entusiasmo tecnológico desvinculado de la experiencia organizacional. Se apoya en una investigación aplicada, leída como estudio de caso, que permitió convertir un problema institucional en una propuesta con fundamento analítico y proyección práctica.

En definitiva, la base metodológica de esta obra debe entenderse como una mediación entre la experiencia del caso y la formulación del modelo. Esa mediación es la que resguarda la legitimidad del libro. Sin ella, la propuesta correría el riesgo de aparecer como una solución abstracta, ajena al contexto que la hizo necesaria. Con ella, en cambio, la continuidad de los servicios TIC puede ser pensada desde una relación más fértil entre investigación, organización y diseño de respuesta. Ese es, en el fondo, el sentido de este capítulo. Mostrar que toda propuesta sólida necesita algo más que consistencia conceptual. Necesita una ruta de construcción que permita comprender de dónde viene, qué evidencia la sostiene y por qué puede ser considerada, con pleno derecho, una contribución de investigación aplicada.

Capítulo 4

Hallazgos del caso y necesidades identificadas

Todo estudio aplicado adquiere verdadero espesor cuando los hallazgos dejan de presentarse como una suma de datos y comienzan a revelar una estructura de problemas. Ese es el lugar que ocupa este capítulo dentro de la obra. No se trata aquí de reproducir de manera mecánica los resultados de la investigación de base ni de reiterar tablas como si el valor del análisis dependiera de su acumulación. Lo que interesa es reconocer qué hizo visible el caso estudiado, qué tipo de fragilidades organizacionales permitió identificar y de qué manera esas fragilidades configuran una necesidad real de continuidad de los servicios TIC. Bajo esta perspectiva, el capítulo no opera como una simple sección de resultados, sino como un espacio de interpretación. Un punto de inflexión entre el diagnóstico y la propuesta.

La evidencia de partida procede del estudio desarrollado en Américas Potash Perú S. A., empresa vinculada a un proyecto de minería no metálica, y debe leerse, por tanto, como evidencia situada. Esto significa que su valor no radica en ofrecer una descripción actualizada del estado de la organización, sino en haber permitido reconocer una problemática institucional concreta en torno al control de la información, la seguridad de los datos y las condiciones externas necesarias para sostener la continuidad del servicio (Dominguez Oliva, 2018). Esta precisión no reduce el alcance del capítulo. Al contrario, lo fortalece. Permite leer los hallazgos con el rigor que corresponde a un caso aplicado y evita proyectarlos indebidamente como si constituyeran una radiografía vigente del presente.

La importancia del caso se entiende mejor cuando se lo sitúa en el marco más amplio discutido en los capítulos precedentes. Clarke (2012) advirtió que la computación ha

llegado a ocupar un lugar comparable al de una utilidad esencial, no por un exceso retórico, sino por la dependencia real que las organizaciones contemporáneas han desarrollado respecto de sus servicios digitales. Wielki (2015), en una línea convergente, mostró que la disponibilidad, la robustez, la resiliencia y la recuperabilidad no expresan únicamente atributos técnicos, sino condiciones que se proyectan sobre la continuidad del negocio y la calidad del servicio. Si estas consideraciones se trasladan al sector minero, donde la información acompaña y organiza procesos operativos, administrativos y de coordinación, el sentido del caso se vuelve especialmente nítido. Cuando la información no circula con estabilidad, cuando no puede ser localizada con oportunidad o cuando no existen garantías suficientes para su resguardo y recuperación, la organización no experimenta una simple incomodidad tecnológica. Enfrenta una forma de vulnerabilidad que toca el núcleo de su funcionamiento.

A partir de la investigación de base, pueden identificarse tres núcleos problemáticos que organizan la lectura del caso y que, al mismo tiempo, permiten comprender por qué la propuesta posterior adquiere pertinencia. El primero remite al control de la información. El segundo se relaciona con la seguridad de los datos. El tercero se vincula con los requerimientos externos del servicio, particularmente con la necesidad de contar con proveedores que ofrezcan condiciones confiables de soporte, disponibilidad y confidencialidad. Esta tríada no es arbitraria. Reúne dimensiones que la propia investigación hizo visibles y que resultan plenamente coherentes con la literatura sobre continuidad del negocio, gobernanza del servicio y seguridad en entornos cloud (Dominguez Oliva, 2018; Hussen et al., 2019; Xu et al., 2014).

El primer hallazgo significativo del caso se relaciona con el control de la información. La evidencia levantada mostró una percepción mayoritaria de insuficiencia en el manejo, organización y control de los datos institucionales, así como una aceptación plena de la necesidad de una propuesta de mejora. Este punto merece una lectura que vaya más allá del dato en sentido estricto. Lo que se vuelve visible no es solo una dificultad en el almacenamiento o en la clasificación de la información, sino una debilidad más profunda en la manera en que la organización ordena uno de sus recursos centrales. Cuando la información no puede localizarse con facilidad, cuando no existe una lógica clara de organización o cuando el acceso depende de prácticas poco estructuradas, lo que se deteriora no es únicamente la eficiencia documental. Se debilita también la trazabilidad, la capacidad de respuesta y la consistencia del proceso decisional. En organizaciones intensivas en información, el desorden informacional no es un defecto menor. Es una señal de fragilidad operativa.

A esta primera dimensión se añade una segunda, quizás más sensible, la seguridad de la información. La investigación original mostró una percepción ampliamente extendida sobre la necesidad de reforzar la protección de los datos, debido a la vulnerabilidad existente frente a pérdida, acceso inadecuado o eventual indisponibilidad (Dominguez Oliva, 2018). Este hallazgo no puede interpretarse en términos exclusivamente técnicos. Lo que revela es una percepción institucional de exposición. Una conciencia de que la información no se encontraba resguardada bajo condiciones plenamente confiables. A la luz de la literatura revisada, este punto adquiere un peso particular. Hussen et al. (2019) y Yang (2016) han insistido en que la confidencialidad, la integridad y la disponibilidad constituyen la base sobre la cual se organiza la seguridad en entornos digitales. Cuando una organización percibe debilidad en cualquiera de estas dimensiones, lo que se

compromete no es solo su protección frente a amenazas externas, sino también su capacidad de sostener la continuidad del servicio con un mínimo de confianza.

La relación entre control informacional y seguridad resulta, en este punto, especialmente reveladora. No son dimensiones independientes. Una gestión deficiente de la información aumenta la exposición a errores, accesos improcedentes, pérdidas documentales y respuestas tardías ante incidentes. Del mismo modo, una seguridad insuficiente vuelve más frágil el control de los datos, incluso cuando estos se encuentran formalmente almacenados. El caso de Américas Potash Perú S. A. permite advertir precisamente esa convergencia. La organización no solo requería proteger mejor la información; requería también gobernarla con mayor claridad. El problema no era simplemente dónde se almacenaban los datos, sino bajo qué lógica de acceso, resguardo y continuidad se los integraba a la operación. Esa diferencia es decisiva, porque desplaza el foco desde la herramienta aislada hacia la arquitectura de gestión que la sustenta.

El tercer hallazgo del caso introduce una dimensión que, con frecuencia, queda relegada en la discusión tecnológica, los requerimientos externos del servicio. La totalidad de los participantes consideró necesario que los servicios TIC se apoyaran en proveedores capaces de cumplir estándares de seguridad y confidencialidad (Dominguez Oliva, 2018). La relevancia de este hallazgo excede el plano contractual. Lo que en él se reconoce es que la continuidad del servicio no depende solo de decisiones internas ni de la calidad de la infraestructura adoptada. Depende también del entorno externo sobre el cual esa infraestructura se sostiene. En un esquema cloud, el proveedor deja de ser un actor periférico. Se convierte en una pieza constitutiva de la confiabilidad del sistema. Xu et

al. (2014) subrayan esta cuestión al mostrar que los acuerdos de nivel de servicio, los criterios de seguridad y las responsabilidades compartidas entre proveedor y organización son determinantes para comprender la verdadera solidez de una solución cloud. En otras palabras, no basta con contratar un servicio funcional. Resulta indispensable evaluar las condiciones reales que sostienen su continuidad.

Bajo esta lectura, el caso analizado no revela una suma de carencias aisladas, sino una configuración de necesidades estrechamente vinculadas entre sí. Un control insuficiente de la información incrementa el desorden y dificulta la trazabilidad. Una seguridad percibida como frágil amplía la sensación de exposición frente a pérdidas, accesos indebidos o indisponibilidad. Una relación poco exigente con el proveedor compromete la estabilidad del servicio y debilita la confianza en la infraestructura adoptada. En conjunto, estos elementos configuran una problemática de continuidad más que una lista dispersa de deficiencias. Y es precisamente esa condición estructural la que otorga al caso su valor analítico. Lo que emerge de él no es solo un diagnóstico organizacional, sino una necesidad de rediseño.

Con el propósito de sintetizar esta lectura, la Tabla 2 reúne las tres dimensiones centrales del caso, el hallazgo principal asociado a cada una de ellas, su significado organizacional y la necesidad identificada. La tabla 2 no sustituye la interpretación del capítulo, pero sí ofrece una visión ordenada de la estructura del problema. Su inclusión resulta pertinente porque permite al lector apreciar con mayor claridad la relación entre evidencia y propuesta, y comprender que el modelo presentado en el capítulo siguiente

no surge de una intuición tecnológica, sino de necesidades organizacionales reconocibles y analíticamente articuladas.

Tabla 2

Síntesis de hallazgos del caso y necesidades identificadas

Dimensión analizada	Hallazgo del caso	Lectura organizacional	Necesidad identificada
Control de la información	Se evidenció una percepción mayoritaria de insuficiencia en el control informacional y una aceptación plena de la necesidad de una propuesta de mejora	El manejo de la información presentaba debilidades en organización, acceso y trazabilidad	Fortalecer la gestión, disponibilidad y orden de la información
Seguridad de la información	La mayoría de los participantes consideró necesaria una mejora en seguridad debido a la vulnerabilidad de los datos	La protección de la información no ofrecía suficiente confianza frente a pérdida, acceso inadecuado o interrupción	Reforzar controles, políticas de seguridad y mecanismos de resguardo
Requerimientos externos	La totalidad de los participantes consideró necesario trabajar con proveedores que cumplieran estándares de seguridad y confidencialidad	La continuidad del servicio dependía también de condiciones externas de confiabilidad y soporte	Definir criterios de selección, evaluación y exigencia al proveedor

La lectura conjunta de estos hallazgos permite advertir una cuestión de fondo. La organización requería algo más que una herramienta de almacenamiento o una mejora puntual en alguno de sus procesos tecnológicos. Requería una arquitectura de continuidad. Una estructura capaz de integrar gestión de la información, seguridad, disponibilidad y soporte del servicio en un mismo marco operativo. Esta observación es importante, porque muestra que la propuesta basada en cloud computing no puede ser comprendida como una modernización aislada ni como un simple cambio de plataforma. Su sentido aparece cuando se la piensa como respuesta a una necesidad más amplia, la de construir condiciones de estabilidad para el manejo de la información y para la continuidad del trabajo en un entorno organizacional exigente.

A la luz de la literatura revisada, esta necesidad no resulta excepcional. Cajamarca-Palomo et al. (2019) y Dhirani y Newe (2020) han insistido en que la disponibilidad de datos y servicios constituye un elemento decisivo para sostener la operación, mientras que Hashizume et al. (2013) advierten que la adopción cloud exige una lectura cuidadosa de los problemas de seguridad que emergen en cada capa del servicio. Palos-Sánchez (2017) y Gupta et al. (2023), por su parte, recuerdan que la confianza en la nube depende tanto de los beneficios percibidos como de la capacidad para gestionar riesgos, seleccionar proveedores adecuados y establecer marcos claros de gobernanza. Bajo esta perspectiva, el caso de Américas Potash Perú S. A. se vuelve especialmente fértil, porque hace visible, en una escala concreta, tensiones que la literatura ha venido reconociendo en distintos contextos organizacionales. No es un caso anecdótico. Es una expresión situada de un problema más amplio.

El valor de este capítulo, por tanto, no reside en reiterar porcentajes ni en sobrecargar la lectura con datos que pertenecen a un momento específico. Su aporte consiste en haber reconstruido el sentido organizacional de los hallazgos y en haber mostrado que las debilidades identificadas en el caso no pueden leerse como fallas separadas, sino como síntomas de una necesidad de continuidad insuficientemente resuelta. Esa reconstrucción es la que permite comprender por qué el modelo del capítulo siguiente no nace de una adhesión abstracta al cloud computing, sino de la necesidad de articular tecnología, información, seguridad y soporte dentro de una lógica más robusta de continuidad de servicios TIC.

Este capítulo sostiene que el caso estudiado permitió reconocer tres necesidades decisivas, fortalecer el control de la información, reforzar la seguridad de los datos y establecer relaciones más exigentes con el proveedor del servicio. Estas necesidades, lejos de agotarse en la descripción del contexto investigado, constituyen la base sobre la cual puede formularse una propuesta de mayor alcance conceptual y organizacional. Esa propuesta será desarrollada en el capítulo siguiente. Su sentido no se comprendería plenamente sin el recorrido que aquí se ha realizado. Porque antes de diseñar un modelo, era necesario entender con claridad qué tipo de problema debía ser resuelto.

Capítulo 5

Modelo de continuidad de servicios TIC basado en cloud computing

La propuesta que se desarrolla en este capítulo surge de una convicción ya insinuada en los apartados anteriores, las debilidades identificadas en el caso estudiado no podían resolverse mediante ajustes aislados ni por la simple incorporación de una herramienta tecnológica. El problema observado en Américas Potash Perú S. A. remitía a una exigencia más amplia, construir condiciones de continuidad para la gestión de la información, fortalecer la seguridad de los datos y establecer una relación más exigente con el soporte externo del servicio. A partir de ese punto, el cloud computing deja de aparecer como una promesa genérica de modernización y comienza a adquirir sentido como parte de una arquitectura orientada a la disponibilidad, al control, al respaldo y a la recuperación de la información crítica. Esa es la lógica que organiza el modelo que aquí se presenta, no una adhesión automática a la nube, sino la formulación de una respuesta estructurada frente a un problema organizacional concreto (Dominguez Oliva, 2018).

La pertinencia de esta propuesta se comprende mejor cuando se advierte que la continuidad de los servicios TIC no se agota en la dimensión técnica del funcionamiento digital. Clarke (2012) señaló que la computación ha pasado a ocupar un lugar semejante al de una utilidad esencial, precisamente porque su ausencia compromete el funcionamiento cotidiano de las organizaciones. De manera convergente, Wielki (2015) mostró que la disponibilidad, la resiliencia, la robustez y la recuperabilidad se proyectan sobre dimensiones tan decisivas como la continuidad del negocio, la calidad del servicio y la estabilidad institucional. Bajo esta lectura, un modelo de continuidad no puede reducirse a un esquema de acceso remoto o a una solución de almacenamiento. Debe integrar la organización de la información, la protección de los datos, la evaluación del proveedor, la capacidad de recuperación ante incidentes y la gobernanza de los recursos

que sostienen la operación. Solo en ese cruce el cloud computing adquiere verdadero espesor organizacional.

El modelo propuesto se fundamenta, por ello, en tres principios que atraviesan toda la obra. El primero es la continuidad del servicio como capacidad institucional para sostener funciones críticas aun en escenarios de interrupción parcial, degradación del acceso o falla localizada. El segundo es la seguridad de la información, entendida no como un añadido correctivo, sino como una condición constitutiva de la gestión de los datos, organizada a partir de la confidencialidad, la integridad y la disponibilidad. El tercero es la gobernanza del servicio, es decir, la definición de responsabilidades, criterios de uso, condiciones de evaluación del proveedor y mecanismos de control que permitan dar consistencia al modelo en el tiempo. Estos principios no operan por separado. Se implican mutuamente. Donde no hay continuidad, la seguridad se vuelve frágil. Donde no hay gobernanza, la continuidad depende de inercias o improvisaciones. Donde no hay seguridad, el acceso deja de ser una ventaja y se convierte en una fuente de exposición.

A partir de esta base, el modelo se orienta a cumplir cinco propósitos centrales. En primer lugar, ordenar el ciclo de la información dentro de la organización, desde su generación y clasificación hasta su almacenamiento, consulta, respaldo y eventual recuperación. En segundo término, fortalecer la protección de los datos mediante controles de acceso, autenticación y resguardo acordes con su criticidad. En tercer lugar, habilitar acceso remoto y oportuno a la información sin perder de vista la necesidad de control institucional. En cuarto lugar, reducir el impacto de fallas locales o interrupciones físicas sobre la continuidad del trabajo. Finalmente, establecer una relación más sólida

con el proveedor del servicio, de modo que la confianza en la infraestructura cloud repose en criterios verificables de disponibilidad, soporte, seguridad y capacidad de recuperación. El modelo no pretende, en consecuencia, añadir complejidad a la organización. Busca, más bien, reorganizar una complejidad ya existente bajo una lógica más coherente y segura.

La Figura 1 representa la arquitectura general del modelo y permite apreciar, de manera sintética, la estructura que lo sostiene. En ella se distinguen dos planos íntimamente articulados. El primero corresponde al plano organizacional, integrado por usuarios, áreas operativas y administrativas, responsables TIC, criterios de clasificación de la información y políticas de acceso y uso. El segundo corresponde al plano tecnológico, conformado por la infraestructura cloud, los mecanismos de sincronización, el almacenamiento, el respaldo, la recuperación y el monitoreo del servicio. La lógica de la figura es deliberada, la continuidad no se produce exclusivamente en la nube ni exclusivamente dentro de la organización. Se construye en la interfaz entre ambas. Es allí donde se decide cómo se organiza la información, quién accede, en qué condiciones se resguarda y qué capacidad real existe para sostener la operación cuando el servicio se ve comprometido. La figura, por tanto, no cumple una función decorativa. Hace visible la tesis central del capítulo, la continuidad de los servicios TIC es una arquitectura de articulación entre gestión, seguridad, infraestructura y soporte.

Figura 1

Arquitectura del modelo de continuidad de servicios TIC



En el núcleo de esa arquitectura se encuentra la gestión de la información. Este componente constituye el primer nivel de orden del modelo, porque ninguna continuidad resulta sostenible si la organización no sabe con claridad qué información gestiona, cuál es su criticidad, cómo debe clasificarse y en qué condiciones puede ser accedida. La evidencia del caso mostró que precisamente allí se encontraba una de las fragilidades más visibles, el control informacional era percibido como insuficiente y la necesidad de una propuesta de mejora aparecía de manera unánime. El modelo responde a esa debilidad mediante una lógica de clasificación, organización y trazabilidad que busca reducir dispersión, evitar accesos difusos y facilitar la localización de los datos relevantes para la operación. Antes de almacenar, antes de respaldar, antes de migrar, hay que saber qué se gestiona y bajo qué criterio se gobierna. Ese orden inicial condiciona todo lo que viene después.

El segundo componente del modelo es el control de acceso y la seguridad de la información. En esta capa se define quién puede acceder a los datos, con qué nivel de permisos, bajo qué mecanismos de autenticación y con qué restricciones de uso. Hussen et al. (2019) y Yang (2016) recuerdan que la confidencialidad, la integridad y la disponibilidad continúan siendo la base más robusta para estructurar la seguridad en entornos cloud. Bajo esa premisa, el modelo organiza la protección de la información desde una lógica de perfiles de usuario, autenticación controlada, niveles diferenciados de acceso y procedimientos de verificación y resguardo. La seguridad no aparece aquí como una respuesta posterior al riesgo. Está integrada desde el diseño. Esa decisión tiene especial importancia en el caso estudiado, donde la vulnerabilidad percibida en torno a la información era uno de los factores que justificaban la necesidad de la propuesta. Controlar el acceso no significa bloquear indiscriminadamente. Significa garantizar que el dato correcto llegue al usuario autorizado en el momento requerido y sin comprometer la estabilidad del servicio.

A continuación, se sitúa la infraestructura cloud como soporte para el almacenamiento, la sincronización y la disponibilidad remota de la información. Aquí conviene introducir una precisión relevante. El modelo no presupone una migración indiscriminada ni una cesión absoluta del control al proveedor. Su lógica es más bien selectiva y, en ciertos escenarios, próxima a una arquitectura híbrida. Palos-Sánchez (2017) ha subrayado que las configuraciones híbridas permiten equilibrar acceso, eficiencia y resguardo, manteniendo información sensible en entornos de mayor control y aprovechando la nube para cargas que exigen disponibilidad, escalabilidad o colaboración distribuida. Esa lectura resulta especialmente útil para el tipo de organización que esta

obra examina. La nube no sustituye la gobernanza institucional de la información. La extiende, siempre que la organización defina con claridad qué aloja, cómo lo protege y bajo qué criterios mantiene capacidad de supervisión y recuperación. En este componente, el valor del cloud computing radica en ofrecer acceso oportuno, sincronización entre espacios de trabajo y disponibilidad sostenida, no en disolver la responsabilidad organizacional sobre los datos.

El cuarto componente corresponde al respaldo y la recuperación del servicio. Sin esta capa, la continuidad quedaría reducida a un ideal de disponibilidad ordinaria y perdería espesor frente a escenarios de interrupción. Dhirani y Newe (2020) han insistido en que la continuidad requiere no solo servicios estables, sino también capacidad de detección de fallas, respuesta y restablecimiento. Paraïso et al. (2014), en un plano complementario, destacan que la portabilidad, la elasticidad y la alta disponibilidad solo adquieren verdadero valor cuando forman parte de una arquitectura pensada para soportar incidentes y redistribuir cargas. En esa línea, el modelo incorpora mecanismos de copia de seguridad, restauración y procedimientos de recuperación que permitan reducir el impacto de fallas técnicas, errores humanos o eventos no previstos. La continuidad, en este punto, deja de depender de la simple esperanza de que el servicio no falle y se transforma en capacidad organizada de responder cuando efectivamente falla. Ese desplazamiento es uno de los rasgos que distinguen al modelo de una solución tecnológica convencional.

El quinto componente está conformado por el monitoreo del servicio y la respuesta ante incidentes. La continuidad no puede sostenerse sin vigilancia. Un sistema digital

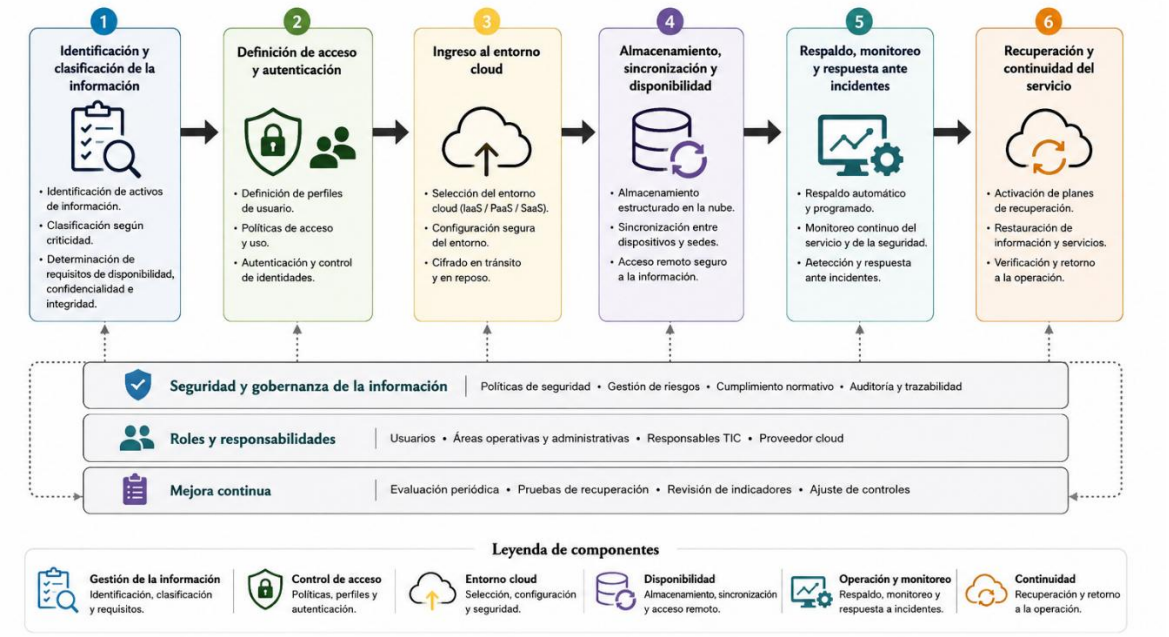
puede parecer estable y, sin embargo, acumular señales tempranas de degradación, fallos intermitentes, problemas de acceso o comportamientos anómalos que, si no son detectados a tiempo, terminan comprometiendo la operación. El monitoreo, en este contexto, no se limita a revisar si un servicio está encendido o disponible. Supone supervisar desempeño, capacidad de respuesta, tiempos de acceso, eventos críticos y cualquier alteración que afecte la experiencia de uso o la integridad del flujo informacional. Integrar este componente al modelo significa pasar de una lógica reactiva a una lógica preventiva. No se espera la caída para actuar; se observa el comportamiento del servicio para anticipar la interrupción o reducir su impacto.

El último componente, y uno de los más sensibles, es la gestión del proveedor. La investigación de base mostró que la totalidad de los participantes consideraba necesario trabajar con proveedores que ofrecieran estándares adecuados de seguridad y confidencialidad. Este hallazgo no puede interpretarse como una preferencia abstracta. Lo que expresa es una comprensión incipiente, pero importante, de que la continuidad del servicio también depende de condiciones externas. Xu et al. (2014) mostraron que los acuerdos de nivel de servicio, las competencias de seguridad del proveedor y la claridad de las responsabilidades compartidas son elementos decisivos en entornos cloud. De ahí que el modelo incluya criterios explícitos para la evaluación del proveedor, disponibilidad comprometida, soporte técnico, confidencialidad, cumplimiento normativo y capacidad de recuperación. La continuidad no puede quedar librada a una relación contractual débil o a la confianza genérica en una marca. Debe apoyarse en estándares verificables y en mecanismos de supervisión institucionalmente definidos.

La interacción de estos componentes puede apreciarse con mayor nitidez en la Figura 2, donde se representa el flujo operativo del modelo. En esa secuencia, la información es primero identificada y clasificada según su criticidad y su función dentro de la organización. A continuación, se definen las condiciones de acceso y autenticación para los distintos perfiles de usuario. Posteriormente, los datos ingresan al entorno cloud seleccionado, donde se habilitan procesos de almacenamiento, sincronización y disponibilidad remota. De forma paralela, se activan mecanismos de respaldo, monitoreo y respuesta ante incidentes que permiten sostener la continuidad del servicio en condiciones ordinarias y extraordinarias. La figura tiene un valor especial porque traduce una arquitectura conceptual en una secuencia operativa inteligible. Hace visible que el modelo no consiste en "subir información a la nube", sino en organizar un recorrido gobernado de la información desde su producción hasta su resguardo y eventual recuperación.

Figura 2

Flujo operativo del modelo de continuidad de servicios TIC



La viabilidad del modelo depende, no obstante, de un conjunto de condiciones mínimas que no deben quedar implícitas. La Tabla 3 muestra esos requisitos de implementación y muestra que la continuidad de los servicios TIC exige algo más que la contratación de una infraestructura cloud. Requiere, en primer lugar, criterios claros de clasificación y organización de la información. Requiere, además, una política de seguridad que defina niveles de acceso, autenticación y protección del dato. Demanda, igualmente, la selección de una infraestructura cloud compatible con la criticidad de los procesos, así como mecanismos de respaldo y recuperación capaces de responder frente a incidentes. A ello se suma la necesidad de criterios explícitos para la evaluación del proveedor, procedimientos de monitoreo del servicio y una estructura mínima de gobernanza interna que distribuya responsabilidades y asegure seguimiento. La tabla resulta útil porque muestra, de forma condensada, que la continuidad no puede sostenerse sobre una única decisión tecnológica. Depende de un ensamblaje de condiciones organizacionales, técnicas y de gobierno.

Tabla 3

Condiciones mínimas para la implementación del modelo de continuidad de servicios TIC basado en cloud computing

Componente	Condición mínima requerida	Finalidad dentro del modelo	Implicación operativa
Gestión de la información	Definir criterios de clasificación, organización y resguardo de la información institucional	Facilitar el acceso oportuno, la trazabilidad y el control de los datos	Permite diferenciar información crítica, operativa y administrativa, y establecer prioridades de tratamiento
Política de seguridad	Establecer lineamientos de acceso, autenticación, permisos y protección de la información	Fortalecer la confidencialidad, integridad y disponibilidad de los datos	Reduce accesos no autorizados, errores de manipulación y exposición de información sensible
Infraestructura cloud	Seleccionar una solución cloud compatible con el nivel de criticidad de los	Sostener el almacenamiento, la sincronización y el	Asegura que la plataforma tecnológica responda a los

	procesos y con las necesidades de disponibilidad institucional	acceso remoto a la información	requerimientos reales de continuidad del servicio
Respaldo y recuperación	Implementar mecanismos de copia de seguridad, restauración y recuperación ante incidentes	Minimizar el riesgo de pérdida de información y reducir tiempos de interrupción	Favorece la continuidad operativa frente a fallas técnicas, errores humanos o eventos imprevistos
Monitoreo del servicio	Establecer procedimientos de supervisión de disponibilidad, desempeño y eventos críticos	Detectar fallas, anticipar riesgos y sostener la continuidad del servicio	Permite una gestión preventiva y mejora la capacidad de respuesta institucional
Proveedor del servicio	Definir criterios de evaluación del proveedor en materia de soporte, disponibilidad, confidencialidad y cumplimiento	Garantizar condiciones externas confiables para la operación del modelo	Reduce la dependencia acrítica del proveedor y fortalece la gobernanza del servicio
Gobernanza interna	Designar responsables, procedimientos y mecanismos de seguimiento del modelo	Asegurar sostenibilidad, control y mejora continua de la propuesta	Vincula la solución tecnológica con decisiones organizacionales y responsabilidades concretas

Nota. Elaboración propia con base en Dominguez Oliva (2018), Xu et al. (2014), Hussen et al. (2019), Dhirani y Newe (2020) y Gupta et al. (2023).

En términos de valor organizacional, el modelo ofrece una contribución que conviene subrayar. No propone simplemente mejorar el almacenamiento de la información ni añadir una capa de seguridad sobre procesos existentes. Propone reorganizar la continuidad de los servicios TIC desde una lógica más madura, más integral y mejor alineada con las necesidades identificadas en el caso. Senyo et al. (2018) advirtieron que buena parte de la literatura sobre cloud computing ha privilegiado la dimensión tecnológica en detrimento de su articulación con contextos organizacionales concretos. Esta obra busca corregir, en parte, ese desequilibrio. La propuesta no nace del entusiasmo por la nube como símbolo de modernización, sino de la constatación de que la continuidad digital exige una arquitectura donde gestión, tecnología, seguridad y proveedor se piensen de forma coordinada. Esa articulación es, en rigor, el núcleo del modelo.

También es necesario precisar su alcance. El modelo no pretende resolver por sí solo todas las tensiones asociadas a la operación digital ni sustituir la necesidad de revisión periódica, actualización de políticas o evaluación continua del proveedor. Su aporte consiste en ofrecer una estructura razonada para fortalecer la continuidad de los servicios TIC, mejorar el control de la información y reducir la vulnerabilidad institucional frente a interrupciones, pérdidas o fallas de acceso. Nace de un caso específico, desde luego, pero sus componentes poseen una capacidad de transferencia analítica que permite pensarlo más allá del contexto que le dio origen. Esa posibilidad no autoriza copias mecánicas. Exige adaptación. Pero confirma, al mismo tiempo, que la propuesta no se agota en el caso. Tiene valor como marco de decisión para organizaciones que enfrentan problemas semejantes.

El modelo de continuidad de servicios TIC basado en cloud computing debe ser entendido como una respuesta articulada a los hallazgos del caso estudiado y como una propuesta académicamente sustentada por la literatura sobre continuidad del negocio, seguridad de la información y servicios cloud. La Figura 1 hace visible su arquitectura general. La Figura 2 muestra la lógica de su funcionamiento.

Capítulo 6

Alcance, transferibilidad y proyección del modelo

Toda propuesta de investigación aplicada requiere, llegado cierto punto, ser leída no solo por lo que formula, sino también por aquello que permite sostener, transferir y proyectar. Ese es el lugar que ocupa este capítulo dentro de la obra. Después de haber reconstruido el problema, examinado sus fundamentos conceptuales, delimitado la ruta metodológica, interpretado los hallazgos del caso y formulado un modelo de continuidad de servicios TIC basado en cloud computing, corresponde ahora situar esa propuesta dentro de un horizonte más amplio. No para exagerar su alcance ni para presentarla como solución universal, sino para definir con claridad qué aporta, hasta dónde puede llegar y en qué condiciones conserva su valor.

El modelo desarrollado a partir del caso de Américas Potash Perú S. A. debe entenderse, ante todo, como una respuesta estructurada frente a una necesidad organizacional concreta. Su mérito principal no reside en ofrecer una promesa tecnológica novedosa, sino en haber articulado evidencia empírica, fundamentos conceptuales y criterios de diseño en una propuesta coherente de continuidad. Lo que el caso permitió mostrar fue una convergencia de fragilidades, debilidades en el control de la información, insuficiencias percibidas en la seguridad de los datos y necesidad de relaciones más exigentes con el soporte externo del servicio. El modelo responde precisamente a esa convergencia y la reorganiza en una arquitectura donde gestión, seguridad, acceso, respaldo, monitoreo y evaluación del proveedor dejan de aparecer como dimensiones dispersas para integrarse en una lógica de continuidad más sólida y legible desde el punto de vista organizacional (Dominguez Oliva, 2018).

En este sentido, uno de los principales aportes de la obra consiste en desplazar la discusión sobre cloud computing fuera del marco estrecho de la modernización tecnológica. A lo largo de estas páginas se ha sostenido que la computación en la nube solo adquiere verdadero espesor cuando se la piensa en relación con la continuidad del servicio, la seguridad de la información y la capacidad institucional para sostener operaciones en contextos de creciente dependencia digital. Clarke (2012) advirtió que la computación ha llegado a ocupar un lugar comparable al de una utilidad esencial, mientras que Wielki (2015) mostró que atributos como la disponibilidad, la resiliencia y la recuperabilidad se proyectan sobre dimensiones decisivas del funcionamiento organizacional. El modelo propuesto recoge esa comprensión y la traduce en una arquitectura aplicada. No concibe la nube como destino tecnológico inevitable, sino como una posibilidad que solo se vuelve valiosa cuando se integra dentro de una estrategia de continuidad pensada con criterios de control, seguridad y gobierno.

A partir de ello, el alcance del modelo debe ser precisado con cuidado. No se trata de una formulación abstracta ni de una construcción desligada de la experiencia empírica. Nace de un caso específico, de un momento particular del proceso organizacional y de una investigación desarrollada bajo determinadas condiciones metodológicas. Por esa razón, los hallazgos que le dan origen no pueden ser interpretados como descripción actual del estado de la empresa ni como representación exhaustiva del sector minero en su conjunto. Esta limitación no reduce el valor de la propuesta. Lo define con mayor rigor. Una investigación situada no necesita simular universalidad para ser relevante; necesita mostrar con claridad qué tipo de conocimiento produce y en qué condiciones puede ser transferido. En este libro, el caso funciona precisamente de esa manera. No como

fundamento de generalizaciones apresuradas, sino como base analítica para pensar un problema que desborda a la organización concreta que lo hizo visible.

Esa precisión abre paso a la cuestión de la transferibilidad. El modelo no debe ser entendido como una plantilla para reproducción mecánica, sino como una estructura de principios y componentes susceptible de adaptación a contextos semejantes. Su capacidad de transferencia se encuentra en la lógica que organiza, clasificación y gobierno de la información, control de acceso, seguridad basada en confidencialidad, integridad y disponibilidad, respaldo, monitoreo y exigencias claras respecto del proveedor. Tales componentes no pertenecen exclusivamente al caso que los hizo visibles. Pueden dialogar con otras organizaciones que operan con información crítica, que dependen de servicios digitales para sostener procesos centrales y que necesitan reducir su exposición frente a interrupciones, pérdidas o debilidades de acceso. En esa medida, el modelo conserva valor más allá del entorno inmediato en que fue formulado. No por su literalidad, sino por su arquitectura conceptual y operativa.

Esta posibilidad de transferencia resulta particularmente relevante en sectores y organizaciones que comparten ciertas condiciones estructurales con el caso estudiado. Empresas mineras con operación distribuida, instituciones con sedes múltiples, organizaciones con alta dependencia documental o entidades que requieren acceso estable a información sensible pueden encontrar en la propuesta una base razonada para orientar decisiones sobre continuidad digital. El valor del modelo, sin embargo, depende de que esa eventual adopción sea contextualizada. No se trata de suponer que toda organización presenta el mismo grado de madurez tecnológica, idénticas exigencias

regulatorias o similares relaciones con sus proveedores. La transferencia exige interpretación. Exige reconocer qué elementos del modelo resultan nucleares, cuáles requieren ajuste y qué condiciones internas deben construirse para que la propuesta conserve su consistencia.

La literatura discutida a lo largo del libro refuerza esta cautela. Cajamarca-Palomo et al. (2019) y Dhirani y Newe (2020) han mostrado que la disponibilidad del servicio y la capacidad de recuperación constituyen factores decisivos para la continuidad operativa. Palos-Sánchez (2017) y Gupta et al. (2023) recuerdan, por su parte, que la confianza en la nube depende tanto de sus beneficios percibidos como de la capacidad de gestionar riesgos, seleccionar proveedores adecuados y establecer marcos de gobernanza claros. De ahí que el modelo no pueda reducirse a un conjunto de pasos técnicos ni a una decisión de migración. Su fuerza está en la relación entre sus componentes. En la manera en que la continuidad se sostiene sobre una articulación entre información, seguridad, infraestructura y control institucional. Esa articulación es precisamente la que permite pensar el modelo como una contribución con potencial de uso en escenarios distintos, aunque no idénticos.

Junto a su alcance y su capacidad de transferencia, el modelo presenta también límites que conviene explicitar. El primero es de naturaleza empírica. La propuesta se deriva de una investigación diagnóstica y propositiva, no de una validación longitudinal posterior ni de una implementación comparada entre múltiples organizaciones. El segundo es de escala. El caso que da origen al libro ofrece una base analítica robusta, pero no autoriza extrapolaciones directas sobre el conjunto del sector sin mediación

interpretativa. El tercero es de temporalidad. El ecosistema cloud evoluciona con rapidez, y con él cambian los servicios disponibles, los modelos de despliegue, los riesgos de seguridad, las exigencias contractuales y las condiciones normativas que inciden sobre su adopción. Estas limitaciones no son un problema que deba ocultarse. Son, por el contrario, parte de la seriedad de la propuesta. Delimitan el tipo de afirmaciones que el libro puede sostener y preservan su credibilidad frente al lector académico y profesional.

Sin embargo, el hecho de que el modelo posea límites no reduce su contribución. Más bien la hace más precisa. En el plano organizacional, el aporte de la propuesta consiste en mostrar que la continuidad de los servicios TIC no puede seguir tratándose como una preocupación subordinada al área tecnológica. La investigación revisada en esta obra permite afirmar que la continuidad digital se vincula de manera directa con la calidad de la gestión de la información, con la confianza en los mecanismos de seguridad y con la capacidad institucional para establecer relaciones maduras con sus proveedores. Dicho de otra manera, la continuidad no es solo un problema de infraestructura. Es una cuestión de organización. De criterios. De decisiones que atraviesan la cultura institucional y que inciden sobre la forma en que una entidad protege, ordena y pone a disposición la información que sostiene su operación.

En el plano profesional, el libro busca ofrecer una utilidad igualmente concreta. La propuesta no se dirige únicamente a especialistas en arquitectura tecnológica o administración de sistemas. Puede ser leída también por responsables de TIC, directivos, consultores, investigadores y decisores que necesitan comprender de qué manera la continuidad digital incide sobre la estabilidad institucional. En ese sentido, el modelo

funciona como una herramienta de lectura y de decisión. Permite orientar discusiones sobre clasificación de la información, acceso seguro, respaldo, monitoreo del servicio, criterios de proveedor y gobernanza de la infraestructura digital. No propone una plataforma comercial específica ni prescribe una solución única. Propone una forma de pensar el problema con mayor rigor y con una visión menos fragmentaria. Ese desplazamiento, aunque parezca modesto, constituye uno de los aportes más valiosos de la obra.

En el plano académico, el libro deja abiertas varias líneas de proyección. Una de ellas consiste en validar el modelo en otros contextos organizacionales del sector minero, con el fin de observar qué componentes se mantienen estables y cuáles requieren adaptación según escala, complejidad operativa o condiciones regulatorias. Otra línea posible sería comparar la aplicabilidad del modelo en arquitecturas públicas, privadas, híbridas o multicloud, particularmente en entornos donde la continuidad del servicio se relaciona con mayores exigencias de redundancia y control. También resultaría pertinente explorar la relación entre continuidad digital y madurez organizacional, considerando variables como cultura de seguridad, apoyo de la alta dirección, preparación tecnológica o experiencia previa en gestión de información. Estas proyecciones no pretenden subsanar una carencia del libro, sino indicar la fecundidad del problema que aborda. Allí donde una obra es capaz de abrir preguntas nuevas, confirma que su aporte no se agota en la formulación inmediata de su propuesta.

De forma complementaria, sería valioso avanzar hacia procesos de validación aplicada o experta del modelo, que permitan contrastar su funcionamiento en escenarios

de implementación. Un desarrollo de esa naturaleza ofrecería la posibilidad de pasar del diseño fundamentado a la observación de su comportamiento bajo condiciones reales de uso. En contextos donde la transformación digital avanza con velocidad, pero no siempre con suficiente gobernanza, este tipo de continuidad investigativa resulta especialmente pertinente. No para desautorizar lo ya construido, sino para volverlo más fino, más contrastado y útil frente a nuevos escenarios institucionales. Toda propuesta seria deja, en algún punto, un margen de trabajo futuro. No porque esté incompleta, sino porque reconoce que los problemas organizacionales complejos exigen pensamiento continuo y no soluciones cerradas de una vez por todas.

A la luz de lo anterior, el aporte general de la obra puede leerse en dos niveles. En el primero, ofrece una interpretación rigurosa del problema de la continuidad de los servicios TIC en una organización del sector minero, mostrando que las debilidades en control de la información, seguridad de los datos y soporte del servicio no son asuntos accesorios, sino factores que afectan directamente la estabilidad operativa. En el segundo, transforma esa interpretación en una propuesta de modelo sustentada en cloud computing, capaz de integrar gestión de la información, seguridad, continuidad y gobernanza del proveedor en un mismo marco de análisis y acción. Esa doble condición, diagnóstica y propositiva, otorga a la obra un perfil particularmente valioso dentro del campo de la gestión tecnológica aplicada.

La continuidad de los servicios TIC debe ser entendida hoy como una dimensión constitutiva de la organización contemporánea. Allí donde la operación depende de información crítica, el acceso, el resguardo, la disponibilidad y la recuperación de los

datos dejan de ser funciones secundarias para convertirse en condiciones de sostenibilidad institucional. A la luz del caso estudiado y de la literatura examinada, el cloud computing puede ofrecer una base significativa para responder a ese desafío, siempre que su adopción no se confunda con un acto de modernización superficial y se acompañe, en cambio, de criterios sólidos de seguridad, monitoreo, continuidad y gobernanza. Esa es, en el fondo, la convicción que cierra esta obra. No la fe en una tecnología salvadora, sino la certeza de que las organizaciones necesitan arquitecturas mejor pensadas para sostener, con mayor estabilidad y responsabilidad, los servicios digitales de los que dependen.

REFLEXIONES FINALES

A lo largo de estas páginas se ha sostenido una idea central, la continuidad de los servicios de tecnologías de la información y la comunicación no puede seguir siendo comprendida como una preocupación secundaria ni como una cuestión confinada al plano estrictamente técnico. Allí donde la información sostiene la operación, articula procesos y respalda decisiones, su disponibilidad, su resguardo y su capacidad de recuperación se convierten en condiciones de estabilidad institucional. En ese horizonte, la continuidad digital deja de ser una aspiración funcional para convertirse en una exigencia de gobierno, de previsión y de responsabilidad organizacional.

El caso que da origen a esta obra permitió reconocer con claridad que las debilidades en el control de la información, la fragilidad percibida en la seguridad de los datos y la necesidad de contar con proveedores más confiables no constituyen problemas aislados. Forman parte de una misma estructura de vulnerabilidad. Allí radica, precisamente, el valor de la investigación de base. No solo en haber identificado carencias específicas, sino en haber mostrado que la continuidad de los servicios TIC exige una mirada más amplia, capaz de articular gestión de la información, seguridad, acceso, soporte y capacidad de respuesta dentro de una misma arquitectura de sentido (Dominguez Oliva, 2018).

Desde esa perspectiva, el cloud computing adquiere en esta obra un lugar preciso. No aparece como una promesa tecnológica autosuficiente ni como una fórmula de modernización que baste por sí sola para resolver los desafíos de la organización. Su relevancia surge cuando se lo sitúa dentro de una lógica de continuidad, es decir, cuando se lo piensa en relación con la disponibilidad del servicio, la protección de la información,

la gobernanza del proveedor y la resiliencia operativa. Solo entonces la nube deja de ser una herramienta atractiva por sus ventajas aparentes y comienza a consolidarse como parte de una estrategia más madura de fortalecimiento institucional.

El modelo propuesto debe leerse, en consecuencia, como una contribución de investigación aplicada. Su valor no reside en ofrecer una solución universal, sino en haber construido, a partir de un caso situado, una respuesta estructurada y conceptualmente defendible frente a un problema que hoy atraviesa a numerosas organizaciones. Allí donde la dependencia de los servicios digitales es alta y donde la interrupción del acceso compromete el orden operativo, resulta indispensable avanzar hacia arquitecturas de continuidad mejor pensadas, más seguras y coherentes con la criticidad de la información que se gestiona.

Esta obra parte y concluye en una misma convicción. La transformación digital solo adquiere verdadero sentido cuando se acompaña de continuidad, de control y de capacidad de respuesta. No basta con incorporar tecnología. Es necesario asegurar que esa tecnología sostenga la operación bajo condiciones de estabilidad, confianza y previsión. Esa es, en el fondo, la exigencia que hoy se impone a las organizaciones y la razón por la cual la continuidad de los servicios TIC debe ser entendida como una dimensión estratégica de su sostenibilidad presente y futura.

REFERENCIAS

Afroz, Md., & Goswami, B. (2023). A Vulnerability to Storage Security for Cloud Computing. 893–910. n: Satyasai Jagannath Nanda and Rajendra Prasad Yadav (eds), Data Science and Intelligent Computing Techniques, SCRS. https://doi.org/10.56155/978-81-955020-2-8-76

Bernal, C. A. (2016). *Metodología de la investigación: Administración, economía, humanidades y ciencias sociales*. Pearson.

Bhuvana P.G., & Bhuvana, J. (2024). Survey on Cloud Computing Security Issue. *International Journal of Research Publication and Reviews*, *5*(3), 4742–4747. https://doi.org/10.55248/gengpi.5.0324.0809

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal,* *9*(2), 27 a 40. https://www.emerald.com/insight/content/doi/10.3316/qrj0902027/full/pdf

Cajamarca-Palomo, G., Quisimalin-Santamaría, M., & Medina-Chicaiza, P. (2019). Current status of the use of cloud computing in SMEs in the city of Latacunga, Ecuador. *Open Journal of Business and Management, 7*(2), 633-649. https://doi.org/10.4236/ojbm.2019.72043

Carneiro, G. de F., & Paula, A. C. de. (2017). Open Perspectives on the Adoption of Cloud Computing: Challenges in the Brazilian Scenario. *I GranDSI-BR* 119–131. https://doi.org/10.5753/sbc.2884.0.10

Clarke, R. (2012). How reliable is cloudsourcing? A review of articles in the technical media 2005–11. *Computer Law & Security Review, 28*(1), 90-95. https://doi.org/10.1016/j.clsr.2011.11.010.

Creswell, J. W., y Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE.

Dhirani, L. L., & Newe, T. (2020). Hybrid cloud SLAs for Industry 4.0: Bridging the gap. *Annals of Emerging Technologies in Computing, 4*(5), 41-60. https://doi.org/10.33166/AETIC.2020.05.003.

Dominguez Oliva, W. (2018). *Modelo de continuidad de servicios de las tecnologías de la información y comunicación utilizando cloud computing en la empresa Americas Potash Perú S.A., proyecto de minería no metálica en el año 2016* [Tesis de maestría, Universidad Católica Los Ángeles de Chimbote]. RENATI. https://repositorio.uladech.edu.pe/handle/20.500.13032/2377

Flick, U. (2018). *An introduction to qualitative research*. SAGE.

Gupta, S., Pani, S. K., Muduli, K., Vaish, A., & Kumar, A. (2023). Risk managed cloud adoption: An ANP approach. *International Journal of Mathematical, Engineering and Management Sciences, 8*(1), 78-93. https://doi.org/10.33889/IJMEMS.2023.8.1.005.

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4*, Article 5. https://doi.org/10.1186/1869-0238-4-5.

Hernández Sampieri, R., y Mendoza, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw Hill.

Hussen, M. O., Sharma, N., El-Sofany, H. F., & Abbas, F. (2019). A NOVEL MODEL FOR SECURING ACCESS OF CLOUD-BASED E-LEARNING SYSTEMS. *International Journal of Engineering Applied Sciences and Technology*, *04*(07), 1–9. https://doi.org/10.33564/ijeast.2019.v04i07.001

Iqbal, S., Kiah, M. L. M., Anuar, N. B., Daghighi, B., Wahab, A. W. A., & Khan, S. (2016). Service delivery models of cloud computing: security issues and open challenges. *Security and Communication Networks*, *9*(17), 4726–4750. https://doi.org/10.1002/sec.1585

Ladan, M. I. A. (2019, July). Security issues in cloud-based businesses. In *9th International Conference on Computer Science, Engineering and Applications (CCSEA 2019)*. https://doi.org/10.5121/csit.2019.90929

Ma, X., Huang, Y., Zhang, Y., & You-yuan, L. (2015). *Research on the Data Storage Security based on Cloud Computing*. Atlantis Press. https://doi.org/10.2991/ameii-15.2015.59

Marinho, M., Prakash, V., Garg, L., Savaglio, C., & Bawa, S. (2021). Effective Cloud Resource Utilisation in Cloud ERP Decision-Making Process for Industry 4.0 in the United States. *Electronics*, *10*(8), 959. https://doi.org/10.3390/electronics10080959

Maxwell, J. A. (2013). *Qualitative research design: An interactive approach*. SAGE.

Morgan, D. L. (2014). Pragmatism as a paradigm for social research. *Qualitative Inquiry, 20*(8), 1045 a 1053. https://journals.sagepub.com/doi/abs/10.1177/1077800413513733

Okai-Ugbaje, S., Uddin, M., Arshad, A., Alsaqour, R., & Shah, A. (2014). Cloud Computing Adoption Model for Universities to Increase ICT Proficiency. Sage Open, 4(3). https://doi.org/10.1177/2158244014546461

Okuonghae, N., & Bakare, O. D. (2023). Cloud Computing: a tool for effective records and information management system in Nigerian academic libraries. *Folia Toruniensia*, *23*, 35–52. https://doi.org/10.12775/ft.2023.002

Palos-Sánchez, P. R. (2017). Drivers and barriers of the cloud computing in SMEs: The position of the European Union. *Harvard Deusto Business Research, 6*(2), 116-132. https://doi.org/10.3926/hdbr.125

Paraïso, F., Merle, P., & Seinturier, L. (2014). soCloud: a service-oriented component-based PaaS for managing portability, provisioning, elasticity, and high availability across multiple clouds. Computing, 98(5), 539–565. https://doi.org/10.1007/s00607-014-0421-x

Patni, J. C. (2021). Cloud Security in Middleware. *Middleware Architecture*, 75. https://doi.org/10.5772/intechopen.98541

Rai, S., Pratap, R., & Irram, S. (2024). A SURVEY PAPER ON FAULT TOLERANCE IN CLOUD COMPUTING ENVIRONMENT. *International Journal of Innovative Research in Computer Science & Technology. (12)* https://doi.org/10.55524/csistw.2024.12.1.6

Ravitch, S. M., y Carl, N. M. (2021). *Qualitative research: Bridging the conceptual, theoretical, and methodological*. SAGE.

Şaykol, E., & Avcı, A. S. (2015). Pivotal Points in Utilizing Cloud Services in Turkey. https://doi.org/10.36880/c06.01252

Senyo, P. K., Addae, E., & Boateng, R. (2018). Cloud computing research: A review of research themes, frameworks, methods and future research directions. *International Journal of Information Management, 38*(1), 128-139. https://doi.org/10.1016/j.ijinfomgt.2017.07.007.

Slamanig, D., & Raß, S. (2011). ON SECURITY AND PRIVACY IN CLOUD COMPUTING. *Proceedings of the 1st International Conference on Cloud Computing and Services Science CLOSER - Volume 1*. SciTePress. https://doi.org/10.5220/0003382106040609

Song, C.-H., & Young-Woo, S. (2022). The influence of dependability in cloud computing adoption. *The Journal of Supercomputing, 78*(10), 12159–12201. https://doi.org/10.1007/s11227-022-04346-1

Stake, R. E. (1995). *The art of case study research*. SAGE.

Wielki, J. (2015). The impact of the cloud computing model on functioning and competitive abilities of SMEs. *Applied Mechanics and Materials, 795*, 243-252. https://doi.org/10.4028/www.scientific.net/AMM.795.243

Yang, Y. (2016). Proceedings of the 2016 4th International Conference on Machinery, Materials and Computing Technology. Cloud Computing Security Challenges and Critical Technologies of Its Protection. *Atlantis Press*. https://doi.org/10.2991/icmmct-16.2016.75

Yin, R. K. (2018). *Case study research and applications: Design and methods*. SAGE.

REFLEXIONES FINALES

La continuidad de los servicios TIC ha dejado de ser un asunto periférico para convertirse en una condición sustantiva de estabilidad organizacional. En contextos como el minero, donde la operación depende de información crítica, de flujos de trabajo coordinados y de una respuesta oportuna ante contingencias, la disponibilidad, la seguridad y la capacidad de recuperación de los servicios digitales adquieren un valor estratégico. Desde esta perspectiva, la presente obra ha buscado mostrar que la continuidad tecnológica no puede reducirse a la adquisición de herramientas, sino que exige una arquitectura de gestión capaz de articular información, seguridad, soporte y gobernanza.

El caso analizado permitió reconocer que las debilidades en el control de la información, la preocupación por la seguridad de los datos y la necesidad de contar con servicios más confiables no constituyen problemas aislados, sino expresiones de una misma exigencia institucional. A partir de ello, el modelo propuesto se presenta como una respuesta estructurada, orientada a fortalecer la resiliencia digital de la organización y a ofrecer una base aplicable a otros entornos con características semejantes.

En ese mismo sentido, una de las principales contribuciones de este libro consiste en situar el cloud computing dentro de una lógica de continuidad y no solo de modernización tecnológica. Su valor no reside únicamente en la flexibilidad operativa que ofrece, sino en la posibilidad de integrarlo a políticas de seguridad, criterios de acceso, mecanismos de respaldo y procesos de recuperación que sostengan la estabilidad del servicio en el tiempo.

Pensar la continuidad de los servicios TIC implica asumir que la transformación digital solo adquiere sentido cuando se acompaña de decisiones organizacionales maduras, de criterios claros de gestión de la información y de una visión preventiva frente al riesgo. Esa es, en el fondo, la convicción que atraviesa esta obra. No basta con digitalizar. Es necesario asegurar continuidad, confianza y capacidad de respuesta.

Declaración conflictos de interés

No existe conflicto de interés

Financiamiento

No se contó con financiamiento

Aprobación de comité de ética

No se requirió experimentación, por lo cual no hubo revisión de comité de ética.

Declaración de responsabilidad autoral

Conceptualización: Wendy Dominguez Oliva

Curación de datos: Carlos Ignacio Gallo Aguila

Investigación: Pedro Pablo Prieto Monzón y Wendy Dominguez Oliva

Metodología: Carlos Alberto Castro Carreño

Supervisión: Pedro Pablo Prieto Monzón y Wendy Dominguez Oliva

Validación: Wendy Dominguez Oliva

Redacción (borrador original, corrección y edición): Wendy Dominguez Oliva, Pedro Pablo Prieto Monzón, Carlos Alberto Castro Carreño, Carlos Ignacio Gallo Aguila y Luis Alberto Talledo Curo

Información adicional

La responsabilidad ética y jurídica sobre los contenidos presentados en esta publicación recae exclusivamente en sus autores, incluyendo el cumplimiento de la normativa vigente en materia de propiedad intelectual y derechos de autor. La editorial queda eximida de cualquier compromiso derivado de dichos contenidos y de su uso por parte de terceros.

Derechos de Autor (Copyright) 2026 © Wendy Dominguez Oliva, Pedro Pablo Prieto Monzón, Carlos Alberto Castro Carreño, Carlos Ignacio Gallo Aguila y Luis Alberto Talledo Curo

Este texto está protegido por una licencia Creative Commons 4.0.



Usted es libre de compartir, copiar y redistribuir el material en cualquier medio o formato, así como de adaptarlo, remezclarlo, transformarlo y crear a partir de él para cualquier propósito, incluso con fines comerciales. Sin embargo, debe cumplir con la condición de atribución, lo que significa que debe otorgar el crédito correspondiente a la obra original de manera adecuada, proporcionar un enlace a la licencia e indicar si se han realizado modificaciones. Puede hacerlo en cualquier formato razonable, pero no de manera que sugiera que cuenta con el respaldo del licenciante o que recibe algún beneficio por el uso de la obra.

Resumen de licencia - Texto completo de la licencia

SOBRE LOS AUTORES

Wendy Dominguez Oliva

Universidad Tecnológica del Perú, Piura, Perú

https://orcid.org/0000-0003-0330-0095; c20045@utp.edu.pe

Ingeniera de Sistemas, doctora en Tecnologías de la Información y Comunicaciones, y magíster en Ingeniería de Sistemas, así como en Ingeniería Ambiental y Seguridad Industrial. Cuenta con más de quince años de experiencia en docencia universitaria, investigación y desarrollo de tecnologías de la información. Actualmente se desempeña como docente universitaria y desarrolladora de contenido académico y profesional en innovación tecnológica y finanzas. En esta obra participa como autora principal y coordinadora general.

Pedro Pablo Prieto Monzón

Universidad César Vallejo, Piura, Perú

https://orcid.org/0000-0002-1019-983X; pprietom@ucvvirtual.edu.pe

Ingeniero de Sistemas, con maestría con mención en Tecnologías de Información y Comunicaciones, maestría en Docencia Universitaria y doctorado en Tecnologías de la Información y Comunicaciones. Se desempeña como docente de pregrado y posgrado en la Universidad César Vallejo. Su trayectoria académica se ha orientado a la formación universitaria y al desarrollo de competencias vinculadas con tecnologías de información, gestión del conocimiento y docencia superior.

Carlos Alberto Castro Carreño

Universidad Tecnológica del Perú, Piura, Perú

https://orcid.org/0000-0001-7136-4774; Correo: ccastroca@utp.edu.pe

Ingeniero Informático por la Universidad Nacional de Piura y magíster en Administración con mención en Gerencia Gubernamental por la misma casa de estudios. Cuenta con estudios concluidos de doctorado en Administración. Su experiencia académica y

profesional se vincula con la gestión pública, la administración y el análisis de procesos apoyados en tecnologías de la información, con especial interés en la articulación entre sistemas, organización y mejora institucional.

Carlos Ignacio Gallo Aguila

Universidad César Vallejo, Piura, Perú

https://orcid.org/0000-0003-1382-0545; cigalloa@ucvvirtual.edu.pe

Ingeniero Industrial por la Universidad Nacional de Piura, maestro en Docencia Universitaria y Gestión Educativa por la Universidad Alas Peruanas, y doctor en Ciencias de la Educación por la Universidad Enrique Guzmán y Valle. Su trayectoria integra formación en ingeniería, educación superior y gestión académica, con énfasis en procesos de enseñanza, desarrollo institucional y fortalecimiento de capacidades en contextos universitarios.

Luis Alberto Talledo Curo

SENATI, Piura, Perú

https://orcid.org/0000-0003-2973-4756; ltalledo@senati.edu.pe

Ingeniero de Sistemas, magíster en Administración con mención en Gerencia Empresarial y doctor en Tecnologías de la Información y Comunicaciones. Ha desarrollado una trayectoria destacada en los campos de la ingeniería de sistemas, la administración y las TIC. En SENATI ha ocupado funciones como instructor de Computación e Informática, coordinador de la unidad de negocio del Programa Nacional de Informática, especialista de desarrollo de medios didácticos de TI y jefe nacional de Tecnologías Digitales para el Aprendizaje. Además, se desempeña como docente universitario de posgrado en la Universidad Nacional de Piura.

Esta obra se publicó en primera edición durante el mes de mayo del año 2026, como resultado de la colaboración entre instituciones comprometidas con la difusión del conocimiento académico.

El proceso editorial fue desarrollado por el Fondo Editorial PLAGCIS, perteneciente a la Plataforma de acción, gestión, e investigación social S.A.S. Sincelejo, Sucre (Colombia).

