TRABAJO DE GRADO
Opción Seminario-Diplomado.

Gestión de activos tecnológicos y migración a la nube:

Evaluación de cómo la administración de hardware, software y la transición a modelos cloud se potencia al externalizar funciones TI

Corporación Universitaria Remington.
Facultad de Ingenierías
Ingeniería en Sistemas

Jorge Andrés Granada Castro — Cristian Jiménez Callejas
Mag. Jorge Mauricio Sepúlveda Castaño
Seminario de Grado
2026

Dedicatoria

A nuestras familias. Fueron el sostén real de estos cinco años: el que aguanta el mal humor cuando no sale una entrega de un trabajo como se esperaba, el que no dice nada cuando amaneces frente al computador, el que pregunta cómo vas, aunque no entienda del todo qué estás haciendo.

La pandemia lo complicó todo. Estudiar desde casa suena cómodo hasta que te das cuenta de que nadie te obligara a levantarte o a prestar atención a la clase. Ustedes pusieron algo ahí donde la disciplina no alcanzaba.

No hubo nota ni calificación que valiera lo que valió una sola frase dicha en el momento justo. Este trabajo también es de ustedes.

Agradecimientos

A la Corporación Universitaria Remington y su Facultad de Ingenierías, por la formación recibida durante estos 5 años.

A los compañeros de carrera, con quienes se compartieron dudas, trabajos en equipo y debates que, en retrospectiva, nos aportaron mucho durante todas las clases. Nadie estudia ingeniería solo, o al menos no debería.

A quienes desde entornos profesionales permitieron contrastar lo aprendido en clase con problemas concretos de la vida real. Trabajar mientras se estudia no es fácil, pero da una perspectiva que los libros no dan.

A todas las personas que, desde distintos lugares, pusieron algo en este proceso ya que somos la suma de todas las experiencias que vivimos.

Tabla de Contenidos

Resumen

Este informe nació de una pregunta concreta: ¿vale la pena migrar a la nube si el costo puede superar el problema que resuelve? Para responderla, se tomó el caso de Arcor Soluciones S.A.S, nombre de referencia que daremos a la compañía evaluada que, por fines de privacidad y autorización, no se hará pública su razón social registrada en cámara de comercio, esta corresponde al sector de alimentos con sede principal en la ciudad de Pereira, cuenta con cuarenta empleados que trabajan bajo una operación híbrida. El punto de partida no era catastrófico, pero tenía un problema serio:

1. Todo dependía de una sola persona
2. Servidor Ubuntu local
3. *Backups* manuales cada mes
4. Correo desde cPanel
5. Acceso remoto con Fortinet

Funcionaba. Pero si el técnico de TI no estaba, no había nadie más. Desde ese diagnóstico, se armó una propuesta de migración a Microsoft 365 Business Standard, administrada por Telefónica Colombia cubriendo cuatro frentes:

1. Licencias para los cuarenta usuarios
2. Migración de 3,6 tb de información histórica con *backup* automático
3. Soporte bajo acuerdo de nivel de servicio
4. El proveedor que se hiciera cargo del día a día de TI

El costo: USD $320 al mes. Pero lo que importa no es el número. Es que la empresa dejó de sostener una infraestructura con gastos imprevisibles para tener un costo fijo que escala si el negocio escala. Para una empresa de cuarenta personas, eso es bastante más valioso de lo que parece.

Palabras clave

Gestión de activos tecnológicos, migración a la nube, outsourcing TI, Microsoft 365, continuidad operativa.

Marco conceptual y contextual

1. Gestión de activos tecnológicos en organizaciones medianas

La gestión de activos tecnológicos es el conjunto de procesos con los que una organización administra, controla y optimiza el ciclo de vida de sus recursos de hardware y software. En empresas medianas, esto importa más de lo que parece: el área de TI suele tener recursos limitados y la operación depende fuertemente de la infraestructura disponible.

Los activos se dividen en dos grandes categorías. Hardware: servidores, equipos de cómputo, dispositivos de red, almacenamiento, seguridad perimetral. Software: sistemas operativos, aplicaciones de productividad, licencias, plataformas de colaboración. Cada categoría tiene sus propios problemas.

El hardware tiene vida útil limitada, entre cinco y diez años para servidores en operación continua, y sus fallas no siempre avisan. El software acumula deuda técnica si no se actualiza: sin parches, queda expuesto; con malas actualizaciones, puede romper procesos críticos.

Uno de los problemas más comunes en empresas medianas es que el inventario tecnológico no nació de una planificación. Nació de decisiones acumuladas: ese equipo llegó porque el anterior se dañó, ese disco lo compró alguien que ya no trabaja ahí, ese servidor lleva siete años funcionando y nadie sabe bien cómo está configurado. Sin inventario estructurado no hay prioridades de mantenimiento, no hay plan de reemplazo, no hay control de riesgo. Solo reacción permanente.

El otro problema es que en empresas medianas el técnico de TI suele ser generalista por necesidad, no por vocación. Tiene que administrar el servidor, atender los equipos de los usuarios, manejar el correo, configurar las VPN y ejecutar los *backup*s.

Todo eso al mismo tiempo. Esa concentración de responsabilidades en una sola persona no es eficiente, pero tampoco es fácil de cambiar sin una estrategia clara. La gestión de activos tecnológicos, bien hecha, es precisamente lo que permite tomar esas decisiones con información y no simplemente reaccionar cuando algo falla.

2. Outsourcing TI: Trasladar el riesgo, sin perder el control

El outsourcing de tecnologías de la información consiste en externalizar una o varias funciones del área de TI a un proveedor especializado, que asume la responsabilidad de su gestión, operación y cumplimiento bajo condiciones formalmente establecidas.

Hay una confusión frecuente en las organizaciones: creer que externalizar equivale a perder el control.

No es así. Lo que se externaliza es la operación; la responsabilidad estratégica sobre los servicios tecnológicos sigue siendo de la organización.

Lo que formaliza y hace funcionar esa relación es el Acuerdo de Nivel de Servicio (ANS). Un ANS bien construido incluye los indicadores técnicos del servicio, los mecanismos de escalamiento y las compensaciones económicas ante incumplimientos. Sin esas condiciones, el ANS no protege a nadie: solo tranquiliza al que firma. Con consecuencias concretas, obliga al proveedor a cumplir plazos o pagar penalidades, y protege los intereses de la organización contratante.

Esto tiene peso particular en organizaciones donde una sola persona de TI debe atender a cuarenta usuarios, administrar el servidor y ejecutar los *backup*s al mismo tiempo. Cualquier ausencia, por incapacidad, vacaciones o renuncia, puede comprometer la continuidad de todos los servicios tecnológicos de la empresa.

El outsourcing no es un modelo para empresas grandes que quieren reducir costos. Es también, y con frecuencia principalmente, una solución de continuidad para empresas medianas que no pueden permitirse tener un equipo interno de TI completo. En ese contexto, externalizar no es delegar lo que no importa.

Es garantizar que lo que más importa siempre tenga quien lo atienda, sin importar el día de la semana ni si el único técnico interno está disponible.

3. Migración a la nube: infraestructura de otra persona, con condiciones claras

Migrar a la nube implica trasladar total o parcialmente la infraestructura, las aplicaciones y los datos de una organización desde entornos locales hacia plataformas gestionadas por proveedores externos.

Lo que cambia no es que los problemas desaparezcan, sino quién los resuelve, con qué nivel de especialización y bajo qué condiciones formales.

Para organizaciones como Arcor Soluciones S.A.S., adoptar Microsoft 365 significa operar bajo el modelo SaaS (*Software as a Service*). En ese esquema, el proveedor gestiona la infraestructura subyacente, aplica las actualizaciones de seguridad, garantiza la disponibilidad del servicio y administra el almacenamiento de los datos.

Microsoft describe este modelo en su comparativa de planes empresariales: el proveedor asume la capa de infraestructura y operaciones, y el cliente gestiona únicamente el uso de los servicios. El técnico interno deja de administrar un servidor y pasa a supervisar que el proveedor cumpla lo comprometido.

El otro cambio importante es financiero. La migración a la nube implica pasar de CAPEX (inversión en capital: activos físicos que se deprecian y eventualmente hay que reemplazar) a OPEX (gasto operativo: suscripciones periódicas con costos predecibles). Para el área financiera de una empresa de alimentos, esa previsibilidad tiene un valor concreto: permite saber cuánto cuesta el servicio cada mes, en lugar de esperar a ver cuándo falla el servidor.

Cuando la migración a la nube se combina con un modelo de outsourcing, los efectos se multiplican.

El proveedor externo aporta conocimiento especializado, herramientas de monitoreo proactivo y experiencia de múltiples clientes, lo que le permite ofrecer niveles de servicio que difícilmente alcanzaría un equipo interno de una sola persona.

4. Seguridad de la información: el problema que nadie quiere ver hasta que ocurre

El *ransomware* no es un riesgo hipotético ni exclusivo de grandes corporaciones. Las organizaciones que operan con *backups* locales dentro de la misma red son las más vulnerables ante este tipo de ataque, porque los atacantes pueden cifrar simultáneamente los archivos del servidor y las copias de seguridad.

En el caso de Arcor Soluciones S.A.S., los discos externos de *backup* permanecían conectados al mismo servidor durante el proceso de copia. Un ataque ejecutado en ese momento habría dejado a la organización sin información y sin respaldo. No hace falta un atacante sofisticado: basta con que alguien abra un correo con un archivo adjunto equivocado.

La protección de activos de información requiere controles en tres capas: preventivos, detectivos y correctivos. En el modelo local de Arcor Soluciones S.A.S., prácticamente ninguno de estos controles estaba implementado de forma sistemática. El firewall Fortinet cumplía una función perimetral básica, pero no protegía contra amenazas que ingresan por correo electrónico, que es el vector de ataque más común en organizaciones de este tamaño y perfil.

La situación no es exclusiva del sector alimentario. Incluso organizaciones del sector tecnológico han debido replantear sus estrategias de seguridad ante la evolución del panorama de amenazas. Si una empresa que vive de la tecnología necesita repensarlo, una que fabrica alimentos y depende de un único servidor tiene razones de sobra para hacerlo antes de que ocurra un incidente.

La adopción de servicios en la nube con gestión delegada a un proveedor especializado transforma este panorama: los *backups* se replican en infraestructura geográficamente separada, los parches de seguridad se aplican de forma automática y el monitoreo de amenazas opera de manera continua, sin depender de la disponibilidad de una sola persona.

5. Gestión de incidentes: diferencias entre «un problema» y «lo estamos resolviendo»

En la práctica, muchas organizaciones medianas gestionan sus incidentes de TI por WhatsApp. No porque sean irresponsables, sino porque nadie les ha mostrado una alternativa funcional que no requiera una inversión que no tienen. El modelo de outsourcing con mesa de ayuda formal y ANS es precisamente esa alternativa.

La clasificación de incidentes por impacto y urgencia, combinada con procesos de escalamiento claros, es el factor que más incide en la reducción de tiempos de resolución y en la satisfacción de los usuarios. Esto puede parecer evidente desde fuera; deja de serlo cuando hay cuarenta usuarios necesitando atención y una sola persona disponible para responder.

Las organizaciones deben contar con procedimientos formales para identificar, clasificar, notificar y resolver incidentes, con trazabilidad completa desde el reporte hasta el cierre.

Esto incluye registros que permitan analizar patrones, identificar causas raíz y tomar decisiones informadas sobre la infraestructura. Sin trazabilidad, cada incidente es tratado como un evento aislado y se pierden oportunidades de mejora sistemática.

La formalización de la gestión de incidentes no requiere grandes inversiones cuando se cuenta con un proveedor externo especializado.

La mesa de ayuda del outsourcing sustituye el WhatsApp informal por un sistema de tickets con prioridades, tiempos de respuesta comprometidos en el ANS y escalamiento automático cuando no se cumplen los plazos.

Para el usuario final, la diferencia es entre saber que su problema está siendo atendido y sentir que está compitiendo por la atención con otros cuarenta compañeros.

6. Arcor Soluciones S.A.S.: el caso de estudio

Arcor Soluciones S.A.S. es una empresa del sector de alimentos con sede principal en la ciudad de Pereira, cuarenta empleados y una operación híbrida entre trabajo presencial y remoto. Por razones de privacidad y autorización, su razón social registrada en cámara de comercio no se hace pública en este informe.

Su infraestructura tecnológica al momento del diagnóstico no era precaria: contaba con un servidor Ubuntu Server 23 virtualizado con RAID 5, firewall Fortinet para seguridad perimetral y acceso VPN, correo corporativo administrado desde cPanel y dos canales de fibra óptica con proveedores distintos. Todo operativo. Todo en verde en el inventario.

El problema no era técnico: era estructural. La totalidad de la operación tecnológica de la empresa dependía de una sola persona. Ese técnico administraba el servidor, gestionaba los accesos remotos, ejecutaba los backups manualmente cada mes y atendía las incidencias de los cuarenta usuarios. No porque nadie más quisiera ayudar, sino porque el modelo nunca fue diseñado para que hubiera alguien más.

Esa concentración de responsabilidades convertía cualquier ausencia, por incapacidad, vacaciones o renuncia, en una interrupción potencial de todos los servicios tecnológicos de la empresa al mismo tiempo. Arcor no necesitaba un ataque cibernético ni una falla catastrófica para quedarse sin soporte: bastaba con que el técnico no estuviera disponible un día crítico.

Este caso fue seleccionado como objeto de estudio precisamente porque representa una situación frecuente en empresas medianas del Eje Cafetero: infraestructura funcional, operación dependiente de un solo eslabón humano, y una brecha real entre lo que la tecnología podría garantizar y lo que efectivamente garantiza cuando ese eslabón falla.

7. Antecedentes: casos colombianos de migración a la nube y outsourcing TI

El caso de Arcor Soluciones S.A.S. no es un experimento sin contexto. Otras organizaciones colombianas han recorrido el mismo camino, con los mismos miedos y, en la mayoría de los casos, con resultados que confirman la dirección.

TEK Soluciones Tecnológicas S.A.S. — Eje Cafetero

El trabajo más cercano geográfica y temáticamente a este informe es el de García (s.f.) sobre la implementación de una línea de outsourcing TI para pymes del Eje Cafetero. La investigación documentó algo que cualquier técnico de la región reconoce: en las pymes locales, la brecha entre lo que la tecnología podría hacer y lo que realmente hace no es un problema de recursos, sino de tres cosas concretas, desconocimiento, miedo a adoptar herramientas nuevas y reluctancia a invertir en activos que no aparecen directamente en los estados financieros. El outsourcing TI, en ese contexto, no es un lujo de empresa grande. Es la única forma realista de cerrar esa brecha sin contratar un equipo interno que la mayoría no puede sostener.

World Office — Colombia

World Office lleva más de treinta años vendiendo software contable a pymes colombianas. Cuando decidieron migrar su plataforma a Microsoft Azure, documentaron algo que vale la pena citar sin rodeos: la migración les permitió dejar de mantener servidores propios y eliminar los costos de hardware asociados (Microsoft News, 2023). Más importante aún, su gerente de desarrollo reconoció que la mayoría de sus clientes pymes no tienen personal de TI propio y necesitan a alguien externo para que la tecnología funcione. No es una observación menor: es la descripción exacta del problema de Arcor antes de la migración.

Industria Licorera de Caldas — Eje Cafetero

La Licorera de Caldas es un caso regional directo. Empresa industrial con décadas de operación, arrancó con un ERP instalado localmente y cinco años después migró todo a Microsoft Dynamics 365 en la nube. El resultado más concreto que reportaron fue la reducción de costos de actualización e integración de software, junto con la capacidad de escalar los servicios sin depender de la infraestructura física (AlfaPeople, 2024). Lo que hace relevante este caso para el presente informe no es la escala, sino el patrón: una empresa de producción en el Eje Cafetero que operaba con tecnología local, reconoció el techo de ese modelo y tomó la decisión de migrar antes de que una falla se la impusiera.

Qué tienen en común estos tres casos con Arcor

Los tres arrancaron desde el mismo punto: tecnología local que funcionaba, pero que dependía de condiciones frágiles para seguir funcionando. Un servidor que nadie reemplaza porque nadie quiere justificar el gasto mientras esté encendido. *Backups* que alguien ejecuta cuando se acuerda. Una persona que sabe cómo está configurado todo y que un día va a renunciar o a enfermarse.

Los tres migraron a plataformas en la nube de Microsoft. Y los tres reportaron el mismo cambio fundamental: dejar de administrar hardware para empezar a administrar resultados. Eso no es un slogan de proveedor, es lo que pasa cuando el técnico de TI deja de gastar su semana apagando incendios operativos y empieza a trabajar en cosas que la empresa realmente necesita.

Hay otro punto en común que no aparece en ninguno de los tres informes pero que está implícito en todos: ninguna de esas organizaciones migró porque estuviera en crisis. Migraron porque alguien hizo la pregunta correcta antes de que la crisis llegara. Eso es exactamente lo que diferencia una decisión de TI estratégica de una decisión reactiva. World Office no esperó a quedarse sin capacidad de almacenamiento. La Licorera de Caldas no esperó a que el ERP local dejara de funcionar. Arcor no esperó a que el servidor de siete años tomara la decisión por ellos.

En el Eje Cafetero, donde la mayoría de empresas medianas todavía operan con infraestructura local administrada por una o dos personas, ese patrón de decisión anticipada sigue siendo la excepción. Estos casos muestran que no tiene por qué serlo.

Desarrollo e implementación del aprendizaje

1. Diagnóstico: inventario de activos tecnológicos

El punto de partida fue un diagnóstico detallado de la infraestructura tecnológica de Arcor Soluciones S.A.S., con el objetivo de identificar el inventario de activos existentes, sus características técnicas, su estado actual y los riesgos asociados a su operación continua (ver Tabla 1).

Lo que llama la atención no es el estado de los equipos en sí: todos figuran como operativos. Lo relevante es la concentración del riesgo.

Todo depende del mismo servidor. Todos los usuarios están expuestos si ese servidor falla o si la red se ve comprometida. Y el único que sabe cómo administrarlo es una persona que puede renunciar, enfermarse o simplemente no estar disponible el día que algo falle.

El RAID 5 protege contra la falla de un disco, no contra un incendio, una inundación, un ataque de *ransomware* ni contra el hecho de que el único técnico de la empresa no recuerde exactamente cómo está configurado el entorno de virtualización.

Esas limitaciones no aparecen en las especificaciones técnicas del equipo, pero son las que más importan al evaluar el riesgo real de la organización.

2. Análisis de riesgos de la infraestructura actual

Antes de definir cualquier solución, fue necesario dimensionar el impacto real de cada brecha identificada en el diagnóstico y priorizar las acciones de mejora.

El riesgo más grave no es el más probable: es el de mayor impacto si ocurre. Un ataque de *ransomware* sobre la red de Arcor, con los *backups* conectados al mismo servidor durante el proceso de copia, podría significar la pérdida total de cinco años de información sin posibilidad de recuperación.

El segundo riesgo más relevante es la dependencia de una sola persona. No porque ese técnico no sea capaz de manejar los equipos, sino porque ningún esquema de continuidad operativa puede sostenerse sobre un solo eslabón.

Cuando esa persona no está disponible, no hay soporte, no se administra el servidor y no se ejecutan los *backups*. Todo se detiene. Ese no es un problema técnico: es un problema de diseño organizacional que la tecnología sola no puede resolver (ver Tabla 2).

3. Propuesta de migración: cuatro servicios integrados

Con base en el diagnóstico y el análisis de riesgos, se desarrolló la propuesta de migración hacia Microsoft 365 Business Standard a través del proveedor Telefónica Colombia, aliado de Microsoft en Latinoamérica. Cuatro alcances integrados, cada uno respondiendo directamente a una brecha específica identificada en el diagnóstico.

Servicio 1: Optimización del recurso actual de TI.

El cambio más relevante no aparece en ninguna fila del comparativo. Es el cambio en lo que el único técnico de TI de Arcor tiene que ocupar su tiempo. En el modelo actual, una parte importante de su jornada se va en tareas operativas: administrar el servidor, ejecutar los *backups*, gestionar la VPN, atender incidencias.

En el modelo propuesto, esas tareas las asume el proveedor externo. El técnico interno puede orientar su trabajo hacia cosas que realmente aportan valor: seguridad adaptada al contexto del negocio, mejoras en flujos de trabajo digitales, capacitación de usuarios. Ese desplazamiento de lo operativo a lo estratégico es el beneficio más duradero de todo el proceso, y el más difícil de justificar en una presentación financiera porque no tiene un número asociado.

Servicio 2: Licenciamiento y administración de Microsoft 365 Business Standard.

Cuarenta licencias a USD $8 por usuario al mes: USD $320 mensuales en total. Cada usuario accede a las aplicaciones de productividad de escritorio y web, 1 TB de almacenamiento personal en OneDrive y correo electrónico corporativo con Exchange Online, que reemplaza el servicio de cPanel actual. La gestión de archivos compartidos entre áreas migra de Samba a SharePoint Online.

El número que más importa no es el costo mensual aislado, es la comparación con lo que costaría renovar el servidor local cuando llegue al final de su vida útil: nuevo hardware, migración de datos, configuración del entorno, interrupciones de servicio durante el proceso. Ese costo es impredecible y ocurre en el peor momento posible. Los USD $320 mensuales son un gasto fijo y planificado (ver Tabla 5).

Servicio 3: Migración y backup automático en la nube.

Contempla la migración ordenada de los 3,6 TB de información histórica desde el servidor local hacia SharePoint Online y OneDrive, respetando la estructura de carpetas y permisos existentes.

Una vez finalizada la migración, se configuran copias de seguridad automáticas diarias con retención de versiones por noventa días.

El proceso de backup manual actual puede tardar hasta dos días en completarse y genera un único punto de recuperación al mes.

Con el nuevo esquema, el punto de recuperación máximo tolerable es de veinticuatro horas (RPO) y el tiempo de restauración ante una contingencia es de máximo cuatro horas (RTO). Para una empresa que procesa facturas, contratos y reportes financieros de forma diaria, esa diferencia no es un detalle menor.

Servicio 4: Soporte TI administrado.

Administración completa del tenant de Microsoft 365, gestión de usuarios, grupos, permisos y políticas de seguridad incluyendo autenticación multifactor (MFA) y acceso condicional.

Atención de incidencias para los cuarenta usuarios con mesa de ayuda de lunes a viernes de 8:00 a.m. a 6:00 p.m., y atención 24x7x365 para incidencias críticas de prioridad P1.

Lo que este servicio resuelve en el fondo es el problema del punto único humano de falla: no importa si el técnico de TI está de vacaciones, con incapacidad o ha renunciado; la plataforma sigue siendo administrada y los incidentes críticos siguen teniendo respuesta en treinta minutos.

4. Proceso de migración: cuatro fases para no interrumpir la operación

El proceso de migración de los 3,6 TB de información histórica desde el servidor local hacia SharePoint Online y OneDrive se estructuró en cuatro fases para minimizar el impacto sobre la operación diaria de la organización (ver Figura 1 y Figura 2).

Fase 1:

Inventario y limpieza. Revisión completa de la información almacenada en el servidor, identificando archivos obsoletos que no requieren migración y estructurando las carpetas de destino en SharePoint según la jerarquía de áreas de la organización.

Esta fase también define los permisos de acceso por área y perfil de usuario para replicarlos en la plataforma destino.

Fase 2:

Migración incremental. Traslado de la información comenzando por los archivos de menor peso y mayor antigüedad, para validar la integridad del proceso antes de migrar los datos más recientes y críticos.

Esta estrategia permite detectar y corregir problemas de compatibilidad o permisos en una muestra pequeña antes de comprometer el volumen total.

Fase 3:

Convivencia temporal. Durante este período, el servidor local y la plataforma en la nube operan en paralelo.

Los usuarios pueden acceder a la información desde ambos entornos mientras se adaptan a las nuevas herramientas sin interrumpir el acceso a la información histórica. Esta fase es crítica para la adopción: los usuarios que sienten que tienen una red de seguridad adoptan los cambios con menos resistencia.

Fase 4:

Desmontaje del servidor Samba. Una vez validada la integridad total de la migración y la estabilidad de los servicios en la nube, se procede al desmontaje del servidor Samba local.

El servidor físico no se elimina de inmediato: permanece disponible como respaldo temporal durante un período acordado antes de su desincorporación definitiva del inventario de activos.

El acceso remoto experimenta una transformación relevante con este proceso. En el modelo actual, los empleados fuera de la sede dependen simultáneamente del firewall Fortinet, del canal de internet de la empresa y del servidor local: una falla en cualquiera de esos tres componentes interrumpe el trabajo de todos los remotos al mismo tiempo.

En el modelo propuesto, el acceso va directamente desde los servidores de Microsoft a través de internet, eliminando esa dependencia de la infraestructura local.

5. Acuerdo de Nivel de Servicio (ANS): donde los compromisos se vuelven reales

Un ANS sin métricas verificables y sin sanciones reales es un documento que existe para tranquilizar a quien firma, no para proteger al cliente. El ANS construido para este ejercicio definió métricas en cuatro dimensiones rendimiento, calidad, velocidad y eficiencia— con metas ideales y mínimos aceptables diferenciados.

La diferencia entre meta y mínimo no es cosmética: es lo que permite distinguir entre un proveedor que está trabajando bien y uno que está haciendo lo mínimo para evitar la sanción.

El régimen de sanciones contempla compensaciones económicas calculadas sobre el valor del servicio mensual de USD $320, con créditos que oscilan entre el 10% y el 30% del valor mensual según la gravedad del incumplimiento (ver Tabla 3).

El incumplimiento reiterado durante tres meses consecutivos otorga al cliente el derecho a cancelar el contrato sin penalidad.

Que existan consecuencias económicas reales cambia la dinámica de la relación: sin consecuencias, los compromisos son aspiracionales; con consecuencias, son obligaciones.

6. Evaluación del impacto: antes y después en la gestión de activos

La implementación del modelo de outsourcing en la nube transforma la forma en que Arcor Soluciones S.A.S. gestiona sus activos tecnológicos, modificando tanto la naturaleza de los activos administrados como la estructura de responsabilidades del área de TI.

En el modelo actual, los activos principales son físicos y tienen una vida útil limitada que obliga a planificar reemplazos periódicos. En el modelo propuesto, los activos principales son licencias de software gestionadas por el proveedor, cuya vigencia se mantiene mientras dure la suscripción, sin deterioro físico ni necesidad de reemplazo (ver Tabla 4).

El cambio más difícil de cuantificar, y probablemente el más importante, es el que ocurre en la cabeza del área financiera.

Pasar de un modelo donde el costo de TI es impredecible porque depende de cuándo falla el próximo equipo a uno donde el costo es fijo y conocido de antemano cambia la manera de planear el presupuesto. Para una empresa de cuarenta personas que opera con márgenes ajustados, eso no es un detalle contable: es la diferencia entre poder proyectarse y vivir apagando incendios.

Figuras y Tablas

Tabla 1

Inventario de activos tecnológicos actuales de Arcor Soluciones S.A.S.

Activo	**Descripción técnica**	**Estado**	**Riesgo identificado**
Servidor local	Ubuntu Server 23, virtualizado, RAID 5, 2 discos de 4 TB	Operativo	Punto único de falla, vida útil limitada por uso continuo
Firewall Fortinet	Gestión de seguridad perimetral y acceso remoto VPN	Operativo	Configuración gestionada por una sola persona
Discos de *backup*	Copias de seguridad manuales mensuales en discos externos	Operativo	Proceso manual de hasta dos días, sin copia *offsite*
Correo cPanel	Correo corporativo con almacenamiento limitado	Operativo	Sin herramientas de colaboración, capacidad reducida
Red interna	Dos canales de fibra óptica con proveedores distintos	Operativo	Dependencia de conectividad para acceso a información local
UPS y planta	Protección energética del servidor principal	Operativo	No cubre fallas prolongadas, requiere mantenimiento periódico

Nota. Elaboración propia con base en el diagnóstico de infraestructura tecnológica de Arcor Soluciones S.A.S. (2026).

Tabla 2

Matriz de análisis de riesgos de la infraestructura tecnológica actual

Criterio	**Situación actual**	**Riesgo identificado**	**Impacto**
Disponibilidad	Servidor local con dependencia de red interna y VPN	Interrupción ante falla del servidor o la conectividad	Alto
Seguridad	Red compartida sin 2fa, *backup* solo local	Vulnerabilidad ante *ransomware*, posible pérdida total de datos	Crítico
Continuidad	Un solo responsable de TI	Parálisis operativa ante su ausencia por cualquier motivo	Alto
Escalabilidad	Capacidad limitada por hardware físico	Imposibilidad de crecer sin nueva inversión en infraestructura	Medio
Productividad	Sin herramientas de colaboración en la nube	Limitaciones para trabajo simultáneo y acceso remoto eficiente	Medio
Costos	Gastos variables por mantenimiento y reemplazo	Imprevisibilidad presupuestal del área de TI	Medio

Nota. Elaboración propia con base en el análisis de riesgos de la infraestructura tecnológica actual de Arcor Soluciones S.A.S. (2026).

Tabla 3

Métricas principales del ANS para Arcor Soluciones S.A.S.

Dimensión	**Indicador**	**Meta**	**Mínimo aceptable**
Rendimiento	Disponibilidad de Microsoft 365	≥ 99.9%	99.5%
Rendimiento	Tiempo de procesamiento de *backups*	< 2 horas/día	< 4 horas/día
Calidad	Integridad de datos en *backups*	100%	99%
Calidad	Satisfacción del usuario	≥ 4.0 / 5.0	3.5 / 5.0
Velocidad	Primer contacto P1 (crítico)	≤ 30 min	≤ 60 min
Velocidad	Resolución P1 (crítico)	≤ 4 horas	≤ 8 horas
Eficiencia	RTO ante contingencia	≤ 4 horas	≤ 8 horas
Eficiencia	RPO máximo	≤ 24 horas	≤ 72 horas

Nota. Elaboración propia con base en la evaluación comparativa del modelo de gestión tecnológica de Arcor Soluciones S.A.S. (2026).

Tabla 4

Comparativo entre el modelo de gestión actual y el modelo propuesto

Criterio	**Modelo actual (infraestructura local)**	**Modelo propuesto (outsourcing en la nube)**
Tipo de activo principal	Hardware físico (servidor, discos, UPS)	Licencias de software y servicios en la nube
Almacenamiento	8 TB físicos en RAID 5	40 TB en la nube (1 TB por usuario)
Backup	Manual mensual, hasta 2 días de proceso	Automático diario, retención noventa días
Disponibilidad	Variable según estado del servidor y la red	99.9% garantizado por SLA de Microsoft 365
Modelo de costo	CAPEX (inversión en hardware)	OPEX (suscripción mensual fija: USD $320)
Ciclo de vida del software	Responsabilidad del técnico interno	Responsabilidad del proveedor externo
Seguridad activa	Firewall perimetral sin 2fa	2fa, acceso condicional, cifrado integrado
Escalabilidad	Limitada por capacidad física del servidor	Sin límite práctico, sin inversión adicional
Responsable técnico	Una persona interna	Equipo especializado del proveedor
Costo mensual fijo	No determinado (variable)	USD $320

Nota. Elaboración propia con base en la evaluación comparativa del modelo de gestión tecnológica de Arcor Soluciones S.A.S. (2026).

Tabla 5

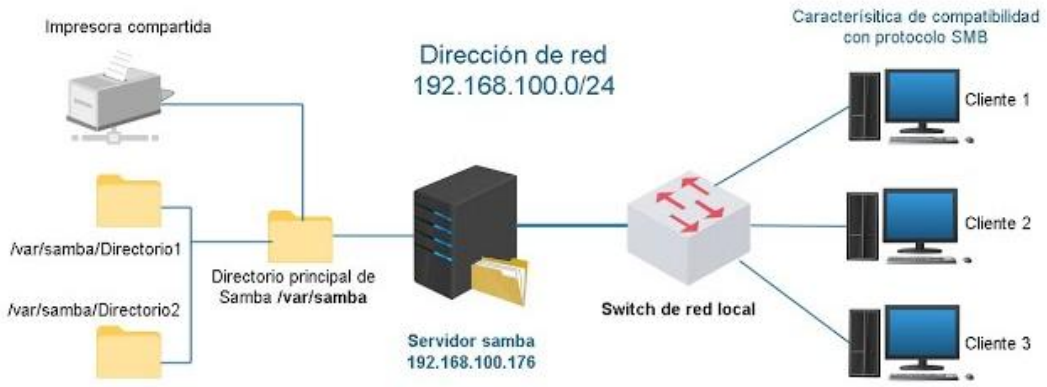
Comparativo de Costo Total de Propiedad (TCO): infraestructura local vs. Nube

Concepto	Modelo local	Modelo nube (M365)
Hardware servidor (amortización cinco años sobre ~$2.500 USD de reemplazo)	$500/año	$ 0
Discos de backup externos (dos discos x $80 USD, reemplazo cada dos años)	$80/año	$ 0
Licencias Office (cuarenta usuarios × ~$6 USD/mes estimado mínimo)	$2.880/año	Incluido en M365
Correo corporativo cPanel (hosting + dominio)	~$180/año	Incluido en M365
UPS y planta eléctrica (mantenimiento anual estimado)	~$120/año	$ 0
Mantenimiento preventivo del servidor (una a dos visitas técnicas/año)	~$200/año	$ 0
Tiempo técnico en tareas operativas (*backups*, parches, admin servidor — estimado 20% de 1 SMLV mensual × 12)	~$480/año	$0 (asumido por proveedor)
Riesgo de falla catastrófica (servidor con 7 años de uso — reemplazo no planificado estimado $2.500-$3.500 USD)	Riesgo latente / no presupuestado	$ 0
Soporte externo en emergencias (estimado uno a dos eventos/año × $100 USD)	~$150/año	Incluido en ANS
Microsoft 365 Business Standard (cuarenta usuarios × $8 USD × 12)	$ 0	$3.840/año
TOTAL ESTIMADO	**$4.590/año + riesgo no cuantificado**	**$3.840/año fijo**

Nota. Elaboración propia con base en la evaluación comparativa del modelo de gestión tecnológica de Arcor Soluciones S.A.S. (2026).

Figura 1

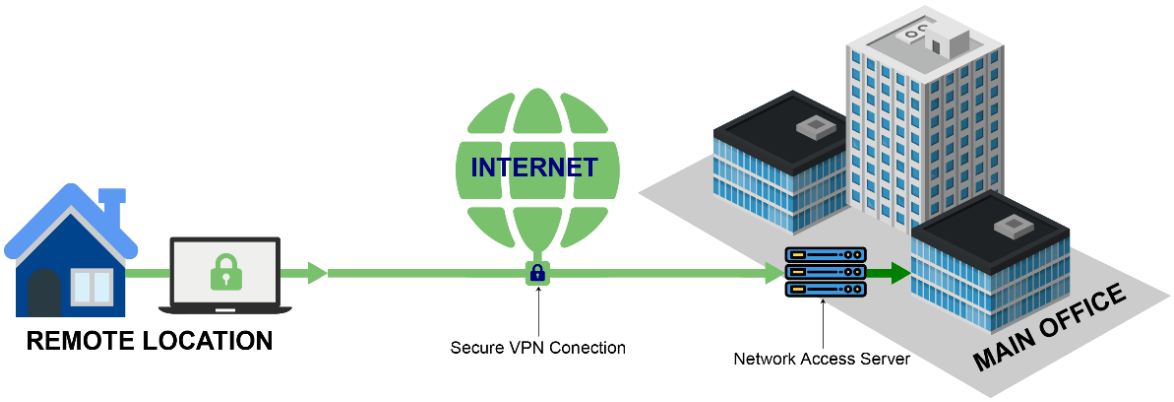
Infraestructura de directorios compartidos



Nota. Diagrama de la infraestructura de directorios compartidos del servidor Samba de Arcor Soluciones S.A.S. Adaptado de Práctica: Instalación y configuración de un servidor de archivos Linux Samba SELinux Webmin Windows (s.f.).

Figura 2

Mapa de acceso mediante VPN



Nota. Diagrama del esquema de acceso remoto mediante VPN implementado en Arcor Soluciones S.A.S. Adaptado de Greyson Technologies (s.f.).

Conclusiones

Arcor Soluciones S.A.S. no tenía un problema de tecnología. Tenía un problema de modelo. Un servidor que funciona, un técnico que sabe lo que hace, un firewall que cumple su rol. Todo operativo, todo en verde en el inventario.

El problema es que ese esquema completo descansaba sobre una sola persona y un solo equipo, y eso, visto desde afuera, no es una limitación técnica: es una falla de diseño.

Eso es lo que este análisis dejó en evidencia. No que la infraestructura local sea mala en sí misma, sino que tiene un techo operativo que se vuelve un problema real en cuanto la empresa crece, contrata más gente, abre otra sede o simplemente tiene un mes difícil porque el técnico de TI se incapacitó. El RAID 5 protege contra la falla de un disco, no protege contra nada de eso.

La migración a Microsoft 365 a través de Telefónica Colombia no fue una actualización de herramientas. Fue un cambio de lógica: dejar de administrar hardware para empezar a administrar resultados. La copia de seguridad dejó de ser una tarea manual que alguien tiene que recordar ejecutar cada mes, un proceso que además podía tardar dos días. La disponibilidad dejó de depender del estado físico de un servidor con siete años de uso continuo. La seguridad pasó de un firewall perimetral sin autenticación de doble factor a MFA, acceso condicional y cifrado integrado en la plataforma.

El costo de USD $320 mensuales merece una mención aparte, no porque sea barato, sino porque es predecible. Para el área financiera de una empresa de alimentos mediana, esa diferencia no es solo contable. Un gasto fijo permite planear. Un gasto de emergencia, que aparece cuando el servidor falla o cuando hay que contratar a alguien de urgencia para recuperar información, obliga a apagar incendios. Son dos lógicas de gestión completamente distintas, y una organización que trabaja con márgenes ajustados no puede darse el lujo de vivir en la segunda.

El análisis de riesgos mostró algo que no siempre aparece en los diagnósticos técnicos: el riesgo más grave no era el más probable. Un ataque de *ransomware* ejecutado mientras los discos de backup estaban conectados al servidor habría dejado a la organización sin información y sin respaldo al mismo tiempo.

No hace falta un atacante sofisticado para eso. Basta con que alguien abra un archivo adjunto equivocado. Ese escenario no ocurrió, pero podría haber ocurrido cualquier mes de los últimos cinco años. Que no haya pasado no significa que el riesgo no existiera.

El Acuerdo de Nivel de Servicio fue la pieza que convierte todo lo anterior en algo concreto. Un ANS sin métricas verificables y sin consecuencias reales por incumplimiento es un documento que existe para tranquilizar a quien firma. El que se construyó para este ejercicio define tiempos de respuesta diferenciados por prioridad, metas e indicadores mínimos aceptables, y sanciones económicas calculadas sobre el valor mensual del servicio. Eso obliga al proveedor a responder. Sin esas condiciones, el outsourcing es una apuesta; con ellas, es un compromiso.

La gestión de incidentes es otro de los cambios que no aparece fácilmente en una presentación de costos, pero que los cuarenta usuarios de Arcor van a notar desde el primer día. Pasar de resolver problemas por WhatsApp a tener una mesa de ayuda con tickets, prioridades y tiempos de resolución comprometidos cambia la experiencia del usuario final.

No es un detalle de confort: es la diferencia entre saber que el problema está siendo atendido y competir por la atención con otros treinta y nueve compañeros. Lo que este caso ilustra, y que es válido para muchas empresas del eje cafetero en situaciones similares, es que modernizarse tecnológicamente no exige grandes inversiones en infraestructura propia.

Exige honestidad sobre las capacidades internas y disposición a firmar compromisos formales con quien sí tiene esa capacidad. Las grandes empresas no tienen mejor tecnología porque gastan más en servidores. Aprendieron hace tiempo que no tiene sentido administrar lo que otros pueden administrar mejor. Esa lógica ya está al alcance de las medianas también.

Para organizaciones en situaciones parecidas, la recomendación concreta es iniciar con un diagnóstico formal del inventario tecnológico antes de contratar cualquier proveedor de outsourcing, y asegurarse de que el ANS incluya cláusulas explícitas de portabilidad de datos y procedimientos claros de salida al finalizar el contrato. Entrar es fácil; salir en condiciones ordenadas requiere haberlo previsto desde el principio.

Como limitación de este estudio, el análisis de costos no incluye una proyección del costo total de propiedad a tres o cinco años, ni una comparación con otras plataformas como Google Workspace o AWS, que podrían ser más adecuadas según el perfil de cada organización. Eso queda como trabajo pendiente, y es trabajo que vale la pena hacer antes de firmar cualquier contrato de largo plazo.

Referencias

Carlos, E., López, V., Cecilia, S., Camacho, M., Esteban, D., López, M., & Salazar, M. (s.f.). Plan estratégico de tecnología de la información 2017-2020: Empresa para la Seguridad Urbana (ESU). Empresa para la Seguridad Urbana. https://www.esu.com.co/wpcontent/uploads/2021/09/Plan-Estrategico-de-Tecnologia-de-la-informacion-2017-2020-v5_1.pdf

Instituto de Ciencias Aplicadas y Tecnología (ICAT). (s.f.). Estrategias de ciberseguridad en empresas proveedoras de equipo y tecnología: el caso de Huawei. Universidad Nacional Autónoma de México. https://www.icat.unam.mx/wpcontent/uploads/2024/08/EstrategiaDeCiberseguridad_CasoHuawei.pdf

Colpensiones. (s.f.). Anexo técnico No. 2: Acuerdos de niveles de servicio. https://www.colpensiones.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=9464

de Cómputo, M. del C. (s.f.). Gestión de monitoreo y operaciones: Términos y definiciones (MPFT0311P-03). Acueducto de Bogotá. https://acueducto.com.co/wps/wcm/connect/EAB2/fd953799-2244-49bb-88d9-26d46c6c0cad/MPFT0311P-03+Gestion+de+Monitoreo+y+Operaciones.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE.Z18_K862HG82NOTF70QEKDBLFL3000-fd953799-2244-49bb-88d9-26d46c6c0cad-o5DRpqn

García, L. M. (s.f.). Implementación de una línea de servicio de outsourcing de tecnología informática en la empresa Tek Soluciones Tecnológicas S.A.S. para las pymes de la región del eje cafetero [Trabajo de grado]. Universidad EAFIT. https://repository.eafit.edu.co/server/api/core/bitstreams/fdc6eab8-5318-4d23-a68c-0d193819bca5/content

Microsoft. (s.f.-a). Microsoft 365 para particulares: Suscripción a aplicaciones de productividad. https://www.microsoft.com/es-co/microsoft-365

Microsoft. (s.f.-b). Comparar planes de Microsoft 365 Empresa. https://www.microsoft.com/es-co/microsoft-365/microsoft-365-business

Microsoft. (s.f.-c). ¿Qué es el ransomware? Guía completa. https://www.microsoft.com/es-co/security/business/security-101/what-is-ransomware

MinTIC. (s.f.). Guía de gestión de incidentes de seguridad digital (G21). Gobierno Digital Colombia. https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf

Odinsa. (s.f.). Lineamientos de ciberseguridad (OD-TI-002). https://www.odinsa.com/wp-content/uploads/OD-TI-002-Lineamientos-de-Ciberseguridad.pdf

Bolsa Mercantil de Colombia. (s.f.). Anexo 31 — Políticas de seguridad de la información y ciberseguridad. https://www.bolsamercantil.com.co/sites/default/files/2023-11/Anexo%2031.%20Pol%C3%ADticas%20de%20Seguridad%20de%20la%20Informaci%C3%B3n%20y%20Ciberseguridad.pdf

Serrano Saenz, Y. (2024). Metodología para gestionar riesgos y mejorar los niveles de atención de eventos o incidentes informáticos de las mesas de servicios TI en las organizaciones [Trabajo de grado]. Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/handle/10596/56740

Tecnológica de Antioquia. (s.f.). [Documento institucional sobre outsourcing TI]. TdeA. https://dspace.tdea.edu.co/server/api/core/bitstreams/f73fc677-1f8e-4f8e-b616-b0480af354dd/content

Edge Seguridad Informática y SysAdmin. (s.f.). Práctica: Instalación y configuración de un servidor de archivos Linux Samba SELinux Webmin Windows [Video]. YouTube. https://youtu.be/E8z_gYR3BOM

Greyson Technologies. (s.f.). Remote access VPN guide. https://www.greyson.com/remote-access-vpn-guide/

Microsoft News. (2023). World Office migra la contabilidad y finanzas de las pymes a la nube.

https://news.microsoft.com/es-xl/world-office-migra-la-contabilidad-y-finanzas-de-las-pymes-a-la-nube/

AlfaPeople. (2024). Crónica de la transformación digital de Industria Licorera de Caldas.

https://alfapeople.com/latam/cronica-de-la-transformacion-digital-de-industria-licorera-de-caldas/