TRABAJO DE GRADO
Opción Seminario-Diplomado.

Modelo de Automatización de Procesos de Infraestructura TI mediante Outsourcing: Gestión de Backups, Recuperación ante Desastres (DRP) y Mantenimiento Preventivo en PrintPo S.A.S.

Corporación Universitaria Remington.
Facultad de Ingenierías
Programa de Ingeniería en Sistemas

Fabian Andres Jaramillo Acosta
Jorge Mauricio Sepúlveda Castaño

Transformación Digital y Outsourcing Inteligente en TI.
2026.

Dedicatoria

A mi familia, especialmente a mi esposa y mi hija, por ser el motor fundamental y el apoyo incondicional durante este proceso de formación profesional.

Agradecimientos

A la Corporación Universitaria Remington y al cuerpo docente del seminario por las herramientas conceptuales brindadas. Asimismo, a la empresa PrintPo S.A.S. por permitir el análisis de su infraestructura tecnológica como caso de estudio práctico para este trabajo de grado.

Tabla de Contenidos

Resumen 5
Objetivos 7
Objetivo General 7
Objetivos Específicos 7
Marco conceptual y contextual 8
Marco contextual 8
Marco conceptual 8
Desarrollo e implementación del aprendizaje 10
Metodología de Determinación de RTO y RPO (Análisis de Impacto en el Negocio) 10
Arquitectura de la Solución Propuesta 10
Políticas y Automatización de Copias de Seguridad (Backups) 11
Mantenimiento Preventivo Automatizado de Servidores 12
Gobernanza y Matriz de Autorización para Restauraciones 12
Tabla 1. Parámetros Técnicos y Métricas de Contingencia para PrintPo S.A.S. 12
Estructura Integral del Acuerdo de Nivel de Servicio (ANS) 13
Tabla 2. Matriz de Niveles de Servicio (ANS) para la Operación Tercerizada 13
Conclusiones 15
Referencias 16

Resumen

El presente informe técnico formula un modelo de tercerización de servicios de infraestructura tecnológica enfocado en la automatización de copias de seguridad (backups), continuidad operativa mediante recuperación ante desastres (Disaster Recovery Plan - DRP) y mantenimiento preventivo programado para la empresa PrintPo S.A.S., ubicada en Yumbo, Colombia. La compañía sustenta sus dos líneas operativas (manufactura industrial de plásticos y programas corporativos de incentivos para clientes multinacionales como Kenvue) sobre el ERP Odoo, respaldado por bases de datos PostgreSQL en servidores locales y plataformas web en servidores virtuales en la nube. Ante la ausencia de monitoreo extendido y personal interno dedicado a la infraestructura crítica, la organización enfrenta riesgos de pérdida de información y tiempos de inactividad que comprometerían los turnos de manufactura y los acuerdos comerciales.

El trabajo adopta un esquema de responsabilidad compartida sustentado en las normas ISO/IEC 20000-1, ISO 22301 e ISO/IEC 27001, en el cual PrintPo delega la ejecución técnica en un Centro de Operaciones de Red (NOC) especializado, conservando la gobernanza, control de accesos privilegiados y rendición de cuentas. Se define una arquitectura híbrida con la regla de respaldo 3-2-1-1-0, inmutabilidad WORM, cifrado AES-256 y un RPO ≤ 1 hora con RTO ≤ 2 horas, justificados mediante un análisis de impacto en el negocio. Asimismo, se establecen rutinas de parcheo con protocolos de reversión (*rollback*), simulacros semestrales y un tablero integral de Acuerdos de Nivel de Servicio (ANS) dotado de penalizaciones y créditos de servicio.

Palabras clave

1. Outsourcing TI
2. Automatización de infraestructura
3. Recuperación ante Desastres
4. Copias de Seguridad
5. Acuerdos de Nivel de Servicio

Objetivos

Objetivo General

Estructurar un modelo técnico y de gobernanza para la tercerización y automatización de la infraestructura crítica de TI en PrintPo S.A.S., enfocado en la gestión de copias de seguridad, continuidad operativa ante desastres (DRP) y mantenimiento preventivo sistemático, asegurando la disponibilidad, integridad y resiliencia de las operaciones de negocio bajo Acuerdos de Nivel de Servicio (ANS).

Objetivos Específicos

- Realizar un análisis de impacto en el negocio (BIA) para fundamentar metodológicamente las metas de Objetivo de Punto de Recuperación (RPO $\leq$ 1 hora) y Objetivo de Tiempo de Recuperación (RTO $\leq$ 2 horas) para las bases de datos de Odoo y las plataformas web de clientes corporativos.
- Formular la arquitectura técnica híbrida de copias de seguridad inmutables (regla 3-2-1-1-0) y contingencia en nube (DRaaS), definiendo procedimientos de verificación, simulacros periódicos y matrices de autorización para la restauración de datos.
- Diseñar el plan de mantenimiento preventivo y monitoreo continuo 24/7 mediante agentes de administración remota (RMM), incorporando protocolos automatizados de actualización del sistema operativo y procedimientos de reversión (*rollback*) ante incidentes post-mantenimiento.
- Establecer el marco de gobernanza, responsabilidades compartidas y el catálogo de Acuerdos de Nivel de Servicio (ANS), con indicadores cuantitativos (KPIs), régimen de penalidades, retención de logs y protocolos de escalamiento jerárquico.

Marco conceptual y contextual

Marco contextual

Nota metodológica sobre confidencialidad: La denominación «PrintPo S.A.S.» corresponde a un seudónimo utilizado con fines estrictamente académicos para proteger la identidad, reserva comercial y confidencialidad de la información técnica de la organización tomada como caso de estudio real.

El presente ejercicio de aplicación técnica se desarrolla sobre el entorno organizacional de PrintPo S.A.S., una compañía con sede principal en el municipio de Yumbo, Valle del Cauca, Colombia. La empresa opera bajo dos líneas de negocio críticas: la manufactura industrial de productos plásticos y la gestión integral de programas de incentivos corporativos mediante plataformas B2B para clientes de alto perfil internacional, como Kenvue.

Tecnológicamente, el corazón operativo de PrintPo S.A.S. reside en el sistema de planificación de recursos empresariales (ERP) Odoo, cuya base de datos transaccional (PostgreSQL) administra los inventarios, la producción en planta y la facturación. Esta infraestructura opera sobre servidores físicos locales, mientras que las plataformas web para clientes se alojan en un entorno de servidores virtuales en la nube (Cloud). Actualmente, la organización no dispone de una estructura robusta de Mesa de Ayuda (Help Desk) interna ni de personal técnico dedicado exclusivamente a monitorear la salud de los servidores en horario extendido, lo que genera un nivel de exposición alto frente a posibles caídas del sistema o pérdida de datos que paralizarían tanto la línea de manufactura como la atención a cuentas corporativas.

Marco conceptual

Para brindar solución a la problemática de PrintPo S.A.S., este informe articula los siguientes conceptos técnicos y de gestión propios del Seminario en Outsourcing de TI:

- **Outsourcing de TI y Responsabilidad Compartida:** Práctica mediante la cual una organización delega la administración, control y ejecución de procesos tecnológicos específicos a un proveedor externo especializado para focalizarse en su core business (MinTIC, 2021). Conforme a la norma NTC-ISO/IEC 20000-1 (ICONTEC, 2020a), el outsourcing no transfiere el riesgo legal ni la rendición de cuentas del negocio; la empresa retiene la gobernanza, las autorizaciones de acceso y la supervisión de los niveles de servicio, mientras que el proveedor asume la responsabilidad de la ejecución técnica.
- **Automatización de Mantenimiento Preventivo (RMM):** Empleo de plataformas de telemetría y gestión remota (Remote Monitoring and Management) para supervisar recursos físicos (CPU, memoria, arreglos RAID) y aplicar parches de seguridad de manera desatendida fuera del horario de producción (MinTIC, 2021).

- **Copias de Seguridad (Backups) y Regla 3-2-1-1-0:** Directriz de resiliencia ante ciberataques (ICONTEC, 2023) que exige mantener 3 copias de los datos, en 2 medios diferentes, 1 copia fuera del sitio principal (nube), 1 copia inmutable bajo tecnología WORM (Write Once, Read Many) protegida contra ransomware, y 0 errores mediante verificaciones automáticas de restauración.
- **Plan de Recuperación ante Desastres (DRP):** Conjunto de procedimientos y recursos orientados a restablecer los servicios de TI tras una contingencia grave (ICONTEC, 2020b). Se sustenta en dos métricas analizadas por Calder (2018):
    - *RTO (Recovery Time Objective):* Tiempo máximo tolerable que el sistema puede estar inactivo antes de afectar gravemente el negocio.
    - *RPO (Recovery Point Objective):* Volumen máximo de datos que la organización está dispuesta a perder, medido en tiempo (por ejemplo, los datos de la última hora).
- **Acuerdos de Nivel de Servicio (ANS / SLA):** Instrumento formal de gestión de servicios (ICONTEC, 2020a) que fija métricas cuantitativas, tiempos de respuesta, compromisos de disponibilidad, canales de escalamiento y compensaciones o créditos de servicio ante incumplimientos del proveedor.

Desarrollo e implementación del aprendizaje

Esta sección expone los resultados del informe técnico mediante el diseño y parametrización del modelo de outsourcing para PrintPo S.A.S., integrando la automatización de infraestructura, la arquitectura de contingencia y la medición del servicio.

Metodología de Determinación de RTO y RPO (Análisis de Impacto en el Negocio)

Para establecer los umbrales de recuperación de PrintPo S.A.S. se efectuó una evaluación de impacto operacional sobre sus dos unidades de negocio:

1. **Línea de Manufactura Plástica (ERP Odoo / PostgreSQL):**
   La operación de planta en Yumbo trabaja con órdenes de producción secuenciales y despachos continuos. La detención de Odoo paraliza el ingreso de insumos y la facturación ante la DIAN, derivando en lucro cesante por mano de obra inactiva. Se determinó un $\text{RPO} \leq 1$ hora para evitar la reconstrucción manual de transacciones físicas de inventario, y un $\text{RTO} \leq 2$ horas como tiempo máximo tolerable de paro antes de comprometer los despachos programados a distribuidores.

2. **Plataformas Web de Incentivos (Clientes Multinacionales - Kenvue):**
   La interrupción del portal corporativo genera penalidades comerciales directas y daño a la reputación institucional. Se estableció un $\text{RPO} \leq 4$ horas soportado en capturas periódicas de disco (*snapshots*) y un $\text{RTO} \leq 2$ horas mediante orquestación de encendido automático de máquinas de contingencia en la nube.

Arquitectura de la Solución Propuesta

Para garantizar la disponibilidad y la integridad operativa de la planta en Yumbo y los servicios web corporativos, se diseñó una topología híbrida gestionada de forma remota por un Centro de Operaciones de Red (NOC) tercerizado.

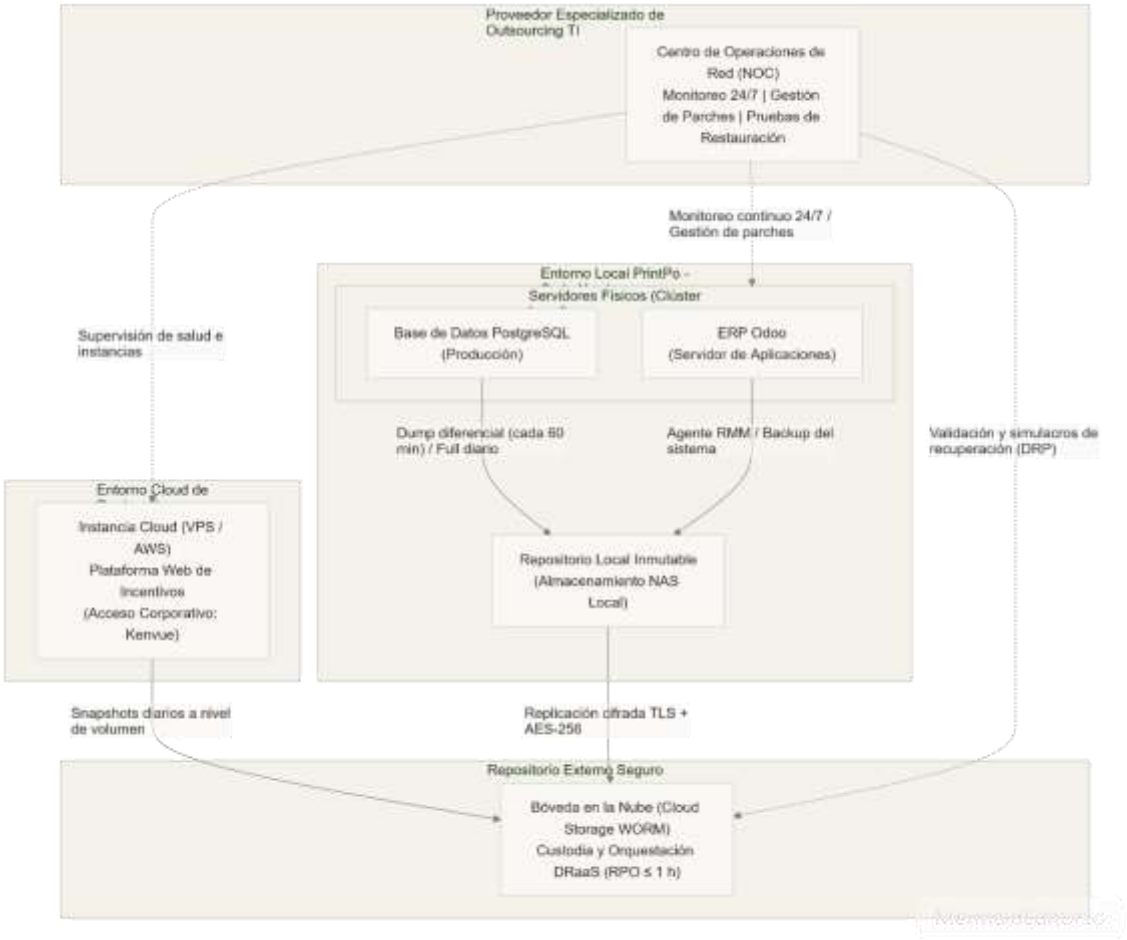


Figura 1. Arquitectura híbrida de automatización de respaldos y monitoreo para PrintPo S.A.S.
Fuente: Elaboración propia a partir del levantamiento de infraestructura (2026).

Políticas y Automatización de Copias de Seguridad (Backups)

El esquema implementado adopta la regla 3-2-1-1-0 para neutralizar fallos lógicos y secuestro de información por ransomware:

- **Base de Datos Odoo (PostgreSQL):** Respaldos diferenciales automáticos cada 60 minutos durante los turnos operativos de planta, acompañados de un volcado completo (*full backup*) en frío a las 23:00 horas.
- **Plataformas Web de Incentivos:** Snapshots diarios a nivel de volumen de la instancia en la nube, garantizando la preservación del estado transaccional de los usuarios de Kenvue.
- **Inmutabilidad y Cifrado:** Transferencia de datos con cifrado AES-256 hacia un repositorio de almacenamiento en la nube con política WORM (*Write Once, Read Many*) bloqueada contra borrado por 30 días.

Mantenimiento Preventivo Automatizado de Servidores

A través de agentes RMM instalados en los servidores, se automatizan las rutinas de administración sin comprometer los turnos laborales de la planta:

- **Ventana de Mantenimiento:** Domingos entre 00:00 y 04:00 horas.
- **Mantenimiento del Motor de Base de Datos:** Optimización quincenal de índices y ejecución de VACUUM ANALYZE sobre PostgreSQL para sostener el desempeño transaccional de Odoo.
- **Monitoreo Continuo:** Sondas de supervisión sobre capacidad de disco, carga de procesador, memoria swap y estado del arreglo RAID en la sede Yumbo.
- **Procedimiento Obligatorio de Reversión (*Rollback*):**
    - *Paso 1 (Snapshot Previo):* Diez minutos antes de la ventana, el sistema genera una instantánea completa del estado de la máquina virtual o servidor a intervenir.
    - *Paso 2 (Despliegue de Parches):* Instalación desatendida de actualizaciones y parches de seguridad críticos.
    - *Paso 3 (Smoke Test Automatizado):* Ejecución de scripts automáticos de prueba que verifican la respuesta del puerto de Odoo, conectividad con PostgreSQL y persistencia de datos.
    - *Paso 4 (Criterio de Reversión):* Si el sistema presenta fallas funcionales o falta de respuesta tras quince (15) minutos del reinicio, se revierte automáticamente el servidor a la instantánea previa (*Rollback*), restableciendo la producción y notificando al NOC para apertura de ticket de análisis forense.

Gobernanza y Matriz de Autorización para Restauraciones

Se delimitan formalmente las atribuciones para prevenir daños o sobreescritura accidental sobre el entorno de producción:

- **Ambiente de Pruebas (Sandbox):** El ingeniero del NOC ejecuta restauraciones periódicas de prueba sin autorización previa para validar la integridad de los respaldos.
- **Restauraciones de Archivos Aislados:** Requieren ticket formal remitido por el responsable de TI de PrintPo.
- **Restauración Destructiva sobre Producción (Odoo / PostgreSQL):** Queda estrictamente prohibida su ejecución sin la autorización digital documentada y aprobada exclusivamente por el **Líder de TI** o la **Gerencia General de PrintPo S.A.S.**

Tabla 1. Parámetros Técnicos y Métricas de Contingencia para PrintPo S.A.S.

Componente Tecnológico	Criticidad Operativa	Estrategia de Respaldo	RPO Objetivo	RTO Objetivo	Ventana de Mantenimiento

Base de Datos ERP Odoo (PostgreSQL)	Alta (Crítica)	Dump diferencial cada 60 min + Full diario + Nube WORM	≤ 1 hora	≤ 2 horas	Domingos 00:00 - 04:00
Plataformas Web Incentivos (Kenvue)	Alta	Snapshots diarios en la nube + exportación externa	≤ 4 horas	≤ 2 horas	Domingos 02:00 - 04:00
Servidor de Archivos y Diseños	Media	Copia incremental diaria local + réplica nocturna	≤ 24 horas	≤ 8 horas	Sábados 19:00 - 23:00
Hipervisores y Sistemas Base	Media	Backup de imágenes de configuración mensual	≤ 7 días	≤ 4 horas	Mensual programada

Fuente: Elaboración propia (2026).

Estructura Integral del Acuerdo de Nivel de Servicio (ANS)

- **Cobertura Horaria:** Monitoreo automatizado y atención de incidentes críticos de infraestructura (P1) en modalidad 24/7/365. Solicitudes de cambio y requerimientos ordinarios de lunes a viernes de 07:00 a 18:00 horas (8x5).
- **Canales de Atención y Escalamiento:** Portal web ITSM con autenticación de doble factor, buzón automatizado de alertas de monitoreo y canal telefónico directo para eventos críticos P1 (N1 Monitoreo NOC 0-15 min → N2 SysAdmin Odoo 15-45 min → N3 Especialista DRP 45-90 min).
- **Retención de Logs:** Los registros de auditoría de monitoreo, respaldos y accesos se conservan en repositorios inmutables por un periodo mínimo de doce (12) meses para cumplimiento legal y auditorías.
- **Exclusiones:** Quedan excluidos el soporte presencial a computadores de usuario final, corrección de errores en código de módulos a la medida de Odoo y fallas por caída del enlace de internet local de Yumbo no imputables a los equipos administrados.
- **Penalidades y Créditos de Servicio:**
    - Dos fallas consecutivas en el cumplimiento del RPO o ventana de parcheo en un trimestre generan una nota crédito del 3% de la facturación mensual.
    - La imposibilidad de recuperar los datos tras una contingencia o el incumplimiento del RTO en un incidente crítico imputable al NOC causa una penalización del 8% sobre la facturación del mes y habilita la terminación justificada del contrato.

Tabla 2. Matriz de Niveles de Servicio (ANS) para la Operación Tercerizada

Indicador (KPI)	Definición y Fórmula	Meta Contractual	Frecuencia	Mecanismo de Control
Efectividad de Backups	$\frac{\text{Respaldos exitosos verificados}}{\text{Total respaldos programados}} \times 100$	$\geq 99.50\%$	Mensual	Verificación automática de logs y alertas tempranas.
Tiempo de Respuesta P1 (TRI)	Tiempo transcurrido entre la alerta de caída de Odoo y la atención del NOC.	≤ 15 min	Eventual	Registro en consola RMM y apertura de ticket crítico.
Tiempo de Recuperación (TTR / RTO)	Tiempo total para levantar el servicio tras contingencia declarada.	≤ 2 horas	Eventual	Registro de cierre de ticket crítico.
Cumplimiento de Mantenimiento	$\frac{\text{Servidores parchados sin incidentes}}{\text{Total servidores programados}} \times 100$	$\geq 95.00\%$	Mensual	Informe consolidado de estado de parches y reinicios.
Restauraciones Exitosas	$\frac{\text{Pruebas de restauración conformes}}{\text{Total simulaciones realizadas}} \times 100$	100%	Mensual	Acta técnica de restauración en laboratorio.
Cumplimiento Simulacro DRP	Validación de failover del ERP Odoo a la nube en tiempo ≤ 2 h.	Conforme / Aprobado	Semestral	Certificado de simulacro de contingencia.
Disponibilidad Servicios Críticos	$\frac{\text{Tiempo en línea (Odoo + Plataforma Web)}}{\text{Tiempo total del periodo}} \times 100$	$\geq 99.70\%$	Mensual	Telemetría continua del agente RMM (24/7).
Tiempo de Detección (MTTD)	Tiempo transcurrido entre la caída del servicio y la alerta automática en NOC.	≤ 5 minutos	Continuo	Sondas de monitoreo sobre puertos de servicio.

Fuente: Elaboración propia (2026).

Conclusiones

- La delegación estratégica de la infraestructura crítica en PrintPo S.A.S. mediante outsourcing resuelve la brecha operativa originada por la falta de un equipo técnico dedicado 24/7, permitiendo a la empresa blindar su proceso de manufactura y su reputación ante clientes corporativos sin incrementar su nómina fija.
- La implementación de la regla 3-2-1-1-0 y la automatización de respaldos inmutables sobre PostgreSQL eliminan el riesgo de parálisis prolongada en Odoo frente a incidentes de corrupción de datos o ataques de ransomware, estableciendo una capacidad de restauración verificable (RPO $\leq$ 1 h y RTO $\leq$ 2 h).
- La incorporación de un marco riguroso de Acuerdos de Nivel de Servicio (ANS) y mantenimiento preventivo programado transforma la gestión de TI en PrintPo de un enfoque reactivo a uno proactivo, mitigando las fallas de hardware en Yumbo y optimizando el costo total de propiedad (TCO) de la infraestructura.
- La delimitación de responsabilidades bajo las directrices de ISO/IEC 20000-1, ISO 22301 e ISO/IEC 27001 asegura que PrintPo retiene la gobernanza y la propiedad de sus datos, estableciendo una matriz de autorizaciones donde ninguna restauración destructiva sobre el ERP productivo puede ejecutarse sin el aval de la Gerencia o TI de la empresa.
- **Limitaciones y Requisitos de Implementación Real:** Se debe precisar que este informe constituye una propuesta de ingeniería basada en un modelo semicuantitativo de negocio, donde los valores económicos ($4.200.000 COP/mes) y capacidades corresponden a estimaciones de mercado. Para llevar a cabo una implementación real en planta, PrintPo S.A.S. debe cumplir previamente con los siguientes requisitos:
    - Levantamiento de un inventario detallado de hardware y matriz de dependencias de red en la sede Yumbo.
    - Suscripción formal de Acuerdos de Confidencialidad (NDA) para salvaguardar los datos de clientes estratégicos como Kenvue.
    - Implementación de un esquema de Gestión de Accesos Privilegiados (PAM) con autenticación multifactor (MFA) para el acceso remoto de los ingenieros del proveedor.
    - Contratación de un enlace secundario de internet redundante en la sede Yumbo para garantizar la replicación de copias hacia la nube sin afectar el ancho de banda transaccional de planta.

Referencias

- Congreso de la República de Colombia. (2012, 17 de octubre). *Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.589.
- Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2020a). *Tecnología de la información — Gestión del servicio — Parte 1: Requisitos del sistema de gestión del servicio* (Norma Técnica Colombiana NTC-ISO/IEC 20000-1). ICONTEC.
- Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2020b). *Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de continuidad del negocio — Requisitos* (Norma Técnica Colombiana NTC-ISO 22301). ICONTEC.
- Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2023). *Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos* (Norma Técnica Colombiana NTC-ISO/IEC 27001). ICONTEC.
- Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2021). *Guía de gestión y continuidad digital: Lineamientos para la tercerización y aseguramiento de servicios de TI*. MinTIC.