**TRABAJO DE GRADO**
**Opción Seminario-Diplomado.**

# Gestión de ciberseguridad en servicios tercerizados

Corporación Universitaria Remington.
Ingeniería de sistemas

Mauricio Loaiza Gonzalez
Docente: Jorge Mauricio Sepúlveda Castaño
Seminario-Diplomado.
2026

## Dedicatoria

En primer lugar quiero agradecer a Dios por darme la vida y la salud para llegar donde estoy hoy a punto de culminar este proceso académico.

En segundo agradecerle a toda mi familia que me ha apoyado en todo este proceso, ya que han sido mi motivación y mi mas grande apoyo.

## Agradecimientos

Agradezco a la Corporación Universitaria Remington por brindarme la oportunidad de formarme como profesional y adquirir conocimientos fundamentales para mi desarrollo académico y laboral.

De manera especial, agradezco al docente del seminario por su orientación, acompañamiento y aportes durante el desarrollo de este trabajo, los cuales fueron clave para fortalecer su contenido y enfoque.

Asimismo, agradezco a todas las personas que hicieron parte de este proceso, ya sea con su apoyo, consejos o motivación, contribuyendo de manera significativa al logro de este objetivo.

**Tabla de Contenidos**

## Resumen

En este informe técnico presento la gestión de la ciberseguridad en los servicios tercerizados en las tecnologías de información, se basa en la empresa Papeles Nacionales S.A.S. en la cual evidenciamos unas limitaciones de seguridad, disponibilidad de los servicios y la gestión de los riesgos tecnológicos.

Con este informe quiero dejar mi análisis de los riesgos asociados al outsourcing en TI, en temas como protección de datos y los cumplimientos legales y así dejar una propuesta de un modelo de gestión que les ayude a disminuir las amenazas.

Planteo una metodología correspondiente al análisis del caso que se basa en la revisión actual de como se encuentra la empresa, identificando riesgos y aplicando buenas practicas tomando como referencia la ITIL e ISO 27001.

Con este resultado propongo un modelo que integre controles técnicos, administrativos, dejando claro la definición de acuerdos de nivel de servicios ANS, con esto se permite mejorar la seguridad, mejorar el flujo de trabajo y el cumplir la normatividad en los entornos de outsourcing.



## Palabras clave

Outsourcing TI, Ciberseguridad, Protección de datos, ANS, Gestión de riesgos

## Marco conceptual y contextual

En la actualidad las organizaciones dependen mucho de la tecnología para desarrollo de las operaciones, teniendo esto en cuenta el outsourcing se convierte en una estrategia muy utilizada para así delegar los procesos tecnológicos a proveedores especializados para así mejorar e incrementar la eficiencia de sus operaciones e incluso reducir costos (Laudon, 2020).

En Papeles Nacionales S.A.S. se entiende que no solo se contrata un proveedor externo, se entiende que se esta aplicando una estrategia para mejorar y solucionar sus problemas actuales y así poder suplir las necesidades que el equipo de TI no puedo cubrir como en temas de seguridad, disponibilidad 24/7 y capacidad de operación.

Desde mi perspectiva, el outsourcing no es solo la tercerización de los servicios esto implica dar el control de los sistemas de datos a estos terceros volviéndose esto un riesgo de ciberseguridad, por esto se vuelve algo fundamental tener medidas claras de ciberseguridad dentro de estos modelos de outsourcing ya que la información se puede filtrar o perderse ya que la manejan y la procesan los proveedores externos (Garcia Arias, 2017).

La ciberseguridad se entiende como un conjunto de prácticas para proteger la confidencialidad, integridad y disponibilidad de la información, se debe gestionada de una manera integral cuando se contratan estos servicios tercerizados. De acuerdo con la norma ISO/IEC 27001 (ISO, 2022), las organizaciones deben establecer controles adecuados para proteger su información cuando estos son compartidos con terceros.

Adicionalmente los marcos de referencias como ITIL resaltan lo importante de la gestión de los servicios de TI bajo unos acuerdos formales donde se defina los niveles de calidad, disponibilidad y seguridad. Los Acuerdos de Nivel de Servicio (ANS) se convierten en una herramienta clave para asegurarse que los proveedores cumplan con las condiciones establecidas (AXELOS, 2019).

Aplicando esto a Papeles Nacionales se evidencia que no solo necesitan externalizar los servicios de TI, sino realizarlo bajo un enfoque bien estructurado de ciberseguridad. Esto implicara establecer controles técnicos administrativos y contractuales que permitan disminuir los riesgos asociados al acceso de terceros a la información.

En este sentido, la integración entre outsourcing y ciberseguridad no se deberían entender como independientes uno del otro, se debe entender como un modelo en conjunto que les permite a las empresas mejorar sus capacidades de operación sin comprometer la seguridad de sus datos.

## Desarrollo e implementación del aprendizaje

Partiendo del diagnóstico realizado en la empresa Papeles Nacionales S.A.S., se logró identificar que la organización presenta unos niveles básicos en la gestión de tecnologías de información. En la actualidad, las medidas de seguridad son el uso de antivirus tradicionales y copias de seguridad locales y esto es insuficiente frente a las amenazas actuales del entorno digital.

Teniendo este contexto claro, la implementación de un modelo de outsourcing TI con enfoque en ciberseguridad representa una oportunidad de mejora significativa. Sin embargo, este proceso debe realizarse de manera estructurada, considerando tanto los beneficios como los riesgos asociados.

En primer lugar, planteamos la tercerización de servicios como la mesa de ayuda (Service Desk), una gestión de infraestructura, la seguridad informática y los sistemas de respaldo en la nube. Estos servicios permitirían que la empresa cuente con un soporte mas especializado con una mayor disponibilidad y con un acceso a las tecnologías mas avanzadas.

De igual forma, la tercerización también puede traer algunos riesgos relevantes. Uno de los principales es la posible fuga de información ya que el proveedor tendrá el acceso a los datos sensibles de la organización. De igual forma se identifican los riesgos relacionados a los accesos no autorizados el uso inadecuado de las credenciales y la dependencia tecnológica del proveedor.

De acuerdo con la ISO/IEC 27001 (ISO, 2022), estos riesgos deben ser gestionados mediante la implementación de controles adecuados. En ese sentido, se propone la adopción de controles técnicos como firewalls avanzados, sistemas de detección de intrusos (IDS/IPS) y mecanismos de cifrado de la información.

Desde el punto de vista administrativo, es fundamental establecer políticas de seguridad claras, definir roles y responsabilidades, y restringir los accesos a la información según el principio de mínimo privilegio. Estas medidas permiten reducir la probabilidad de incidentes internos y mejorar el control sobre los sistemas.

Por otro lado, los controles contractuales juegan un papel clave en el modelo de outsourcing. Los ANS deben incluir no solo aspectos operativos, sino también indicadores de seguridad, tiempos de respuesta ante incidentes y cláusulas de confidencialidad. Según ITIL (AXELOS, 2019), estos acuerdos permiten alinear las expectativas entre cliente y proveedor.

Como resultado de la implementación de estas medidas, se espera que la empresa logre mejoras en la disponibilidad de los servicios, pasando de un esquema limitado a un

modelo de soporte continuo 24/7. Asimismo, se proyecta una reducción en los incidentes de seguridad, una mayor protección de los datos y un mejor cumplimiento de normativas relacionadas con la gestión de la información.

Finalmente, se propone la realización de auditorías periódicas al proveedor, con el fin de verificar el cumplimiento de los acuerdos establecidos y garantizar un proceso de mejora continua en la gestión de los servicios tercerizados.

# Análisis

## Diagnóstico inicial

**Papeles Nacionales presenta:**

- Seguridad básica (antivirus y backups locales)
- Sin políticas de seguridad formal
- Sin monitoreo de amenazas
- Riesgo alto de fallos y ataques

## Implementación del outsourcing TI

Servicios a tercerizar:

- Mesa de ayuda (Service Desk)
- Seguridad informática
- Infraestructura y redes
- Gestión de servidores
- Backup en la nube

## Riesgos de la ciberseguridad en outsourcing

**Riesgos principales:**

1. Fuga de información
    - Acceso del proveedor a datos sensibles
2. Accesos no autorizados
    - Credenciales mal gestionadas
3. Dependencia del proveedor
    - Dificultad para cambiar de proveedor
4. Falta de cumplimiento legal
    - Incumplimiento de normas de protección de datos
5. Ataques externos
    - Mayor superficie de ataque

## Gestión de riesgos

**Se recomienda aplicar:**

- Identificación de activos críticos
- Evaluación de vulnerabilidades
- Análisis de impacto
- Planes de mitigación

## Controles de ciberseguridad

**Técnicos:**
- Firewall avanzado
- Sistemas IDS/IPS
- Encriptación de datos
- Backup en la nube

**Administrativos:**
- Políticas de seguridad
- Control de accesos
- Auditorías periódicas

**Contractuales:**
- Cláusulas de confidencialidad

## Figuras y tablas

Riesgos de ciberseguridad

| Riesgo | Impacto | Probabilidad | Mitigación |
|---|---|---|---|
| Fuga de datos | Alto | Media | Encriptación |
| Accesos no autorizados | Alto | Alta | Control de accesos |
| Fallas del proveedor | Alto | Media | ANS y respaldo |
| Ataques externos | Alto | Alta | Firewalls |

Controles de seguridad

| Tipo | Control |
|---|---|
| Técnico | Firewall, antivirus |
| Administrativo | Políticas |
| Legal | Contratos |

## Conclusiones

Con el análisis realizado se evidencia que el outsourcing es una alternativa muy viable para asi mejorar la gestión de servicios tecnologicos en empresas con limitaciones internas en areas de TI como en Papeles Nacionales S.A.S. de igual manera una implementación sin un enfoque a la ciberseguridad puede incrementar los riesgos asociados a la protección de la información de las empresas.

El principal aprendizaje es que la ciberseguridad se debe tener presente desde la planeación del outsourcing, incluyendo controles técnicos, administrativos y contractuales que garanticen la confidencialidad, integridad y disponibilidad de los datos.

De igual forma, se concluye que los ANS no solo deben enfocarse en disponibilidad y tiempos de respuesta, sino también en indicadores de seguridad y cumplimiento legal.

Para finalizar, el trabajo tiene la limitación de que es un enfoque teórico, ya que no se implementó en la empresa; pero se deja una base sólida para una futura implementacion real con estudios más profundos.

## Referencias

ISO. (2022). ISO/IEC 27001: Information security management systems.

ISO. (2018). ISO/IEC 20000-1: IT service management.

AXELOS. (2019). ITIL Foundation: IT Service Management.

García Arias, L. M. (2017). Outsourcing y gestión de tecnologías de la información.

Laudon, K. C., & Laudon, J. P. (2020). Sistemas de información gerencial. Pearson.