Gestión de ciberseguridad en servicios tercerizados

Presentado por:

Rubio Castro Daniel Felipe

.

PROGRAMA DE INGENIERÍA DE SISTEMAS

FACULTAD DE INGENIERIA CORPORACIÓN UNIVERSITARIA REMINGTON

SAN JUAN DE PASTO

2025

Presentado por:

Rubio Castro Daniel Felipe

Docente:

Jorge Mauricio Sepúlveda Castaño

PRESENTADO A LA FACULTAD DE INGENIERÍA DE SISTEMAS COMO REQUISITO PARCIAL PARA OPTAR AL TÍTULO DE INGENIERO DE SISTEMAS

CORPORACIÓN UNIVERSITARIA REMINGTON

2025

TABLA DE CONTENIDO

RESUMEN

Este trabajo de grado tiene como propósito el analizar la gestión de ciberseguridad en servicios tercerizados, identificando las posibles normas, estrategias aplicables y los principales riesgos que se pueden llegar a presentar para garantizar la protección de la información.

Todo esto en un contexto en el que la tercerización de servicios tecnológicos es cada vez más común y de fácil acceso, las diferentes organizaciones tienen que asumir una posición crítica y proactiva en la supervisión de proveedores terceros, aplicando distintas intervenciones técnicas administrativas y financieras que aseguren la confidencialidad, integridad y disponibilidad de datos (Willcocks, Hindle, & Feeny, 2014; ENISA, 2020).

Gracias a este trabajo se propone dar una guía a las organizaciones para establecer un procedimiento de evaluación, monitoreo y mejora continua en la relación con sus proveedores tecnológicos basándose en un modelo de gestión de ciberseguridad que puede ser tomado por empresas que contratan servicios tercerizados.

Palabras claves: ciberseguridad, servicios tercerizados, ISO 27001, gestión de riesgos, protección de datos.

INTRODUCCIÓN

La manera en que las compañías y organizaciones de nuestro entorno funcionan ha cambiado radicalmente debido a la evolución tecnológica. Es cada vez más frecuente que las empresas subcontraten tareas tecnológicas, desde la gestión de plataformas de software y el almacenamiento de datos en la nube hasta la digitalización de procesos y el mantenimiento de redes.

Aunque este proceso de tercerización tiene beneficios en cuanto a eficiencia, productividad y disminución de costos, también plantea nuevos peligros para la seguridad que requieren una administración apropiada (ISO/IEC, 2014; García-Blandón, 2025).

La ciberseguridad se ha vuelto un componente fundamental para salvaguardar los datos de las empresas y la información personal ante riesgos cibernéticos en un mundo que avanza hacia una digitalización creciente.

Tomando en cuenta estos antecedentes, el presente trabajo tiene como objetivo principal analizar las estrategias de gestión de ciberseguridad en servicios tercerizados y proponer un modelo práctico que permita mitigar y atender los riesgos derivados de la externalización tecnológica.

Ante todo, se busca crear y fortalecer una cultura de responsabilidad compartida entre las empresas y sus proveedores, propiciando el cumplimiento de normas internacionales y leyes nacionales que garanticen el tratamiento adecuado de la información (Ley 1581 de 2012; MinTIC, 2020).

Esta metodología de investigación en ciberseguridad es un enfoque sistemático utilizado para identificar, analizar y mitigar amenazas o brechas en los sistemas de información. Es por ello que, esta propuesta pretende contribuir al fortalecimiento de la seguridad digital en el ámbito empresarial de nuestro entorno.

PLANTEAMIENTO DEL PROBLEMA

En la actualidad, se ha incrementado la dependencia de servicios tercerizados en el ámbito tecnológico, lo que ha generado un panorama de vulnerabilidad cibernética cada vez más complejo. Las empresas, al contratar y delegar funciones sensibles como el almacenamiento de datos, la administración de sistemas o el soporte técnico a terceros, pierden parte del control sobre la seguridad de su información, ocasionando vulnerabilidades en los diversos procesos empresariales.

En Colombia, un sinnúmero de entidades públicas y privadas han afrontado incidentes de ciberseguridad debido a fallas en la gestión de sus proveedores. Casos de fuga de datos, accesos no autorizados y ataques informáticos se han relacionado directamente con deficiencias en los contratos, auditorías o monitoreos de seguridad aplicados a los terceros contratados (García-Blandón, 2025; ENISA, 2020).

El problema central radica en la deficiencia de los mecanismos necesarios que garanticen que los proveedores implementen controles de ciberseguridad acordes con los estándares internacionales. Si bien existen normas y leyes que orientan la protección de datos, muchas organizaciones no cuentan con un modelo moderno y estructurado para gestionar la seguridad en servicios tercerizados (Ley 1581 de 2012; ISO/IEC, 27001:2022).

Por lo tanto, la pregunta de esta investigación que orienta este trabajo es:

¿Cómo podemos implementar y desarrollar una práctica efectiva de ciberseguridad en servicios tercerizados que permita proteger la información institucional o empresarial y reducir los riesgos asociados a la externalización de labores tecnológicas?

JUSTIFICACIÓN

La urgencia de mejorar la seguridad digital en un ambiente de negocios cada vez más competitivo e interconectado es la base de este trabajo. La subcontratación de servicios informáticos es una práctica común, pero la expansión de esta no siempre ha sido respaldada por controles apropiados que aseguren la protección de los datos institucionales y empresariales.

Un seguimiento a la gestión de ciberseguridad adecuada y eficiente en servicios tercerizados contribuye a prevenir incidentes que puedan comprometer la información institucional, la continuidad del negocio y la confianza de los clientes. Asimismo, permite cumplir con las exigencias legales establecidas en la Ley 1581 de 2012 y en las políticas de protección de datos personales del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Desde el punto de vista académico, este trabajo aporta un enfoque integral que combina aspectos teóricos, normativos y prácticos, proporcionando herramientas útiles para ingenieros de sistemas y profesionales encargados de la gestión tecnológica. Además de contribuir con una propuesta práctica, aplicable al contexto empresarial o institucional colombiano.

OBJETIVOS

Objetivo general

Analizar las estrategias de gestión de ciberseguridad aplicables a los servicios tercerizados proponiendo un modelo práctico que fortalezca la protección de la información institucional.

Objetivos específicos

Identificar los principales riesgos de ciberseguridad que se presentan en los servicios tercerizados contrastados.

Describir las normas jurídicas y los normativos internacionales y nacionales que regulan la seguridad de la información.

Evaluar las prácticas de gestión y control que utilizan las organizaciones para supervisar a sus proveedores tecnológicos.

Diseñar un modelo práctico de gestión de ciberseguridad aplicable a empresas que externalizan servicios tecnológicos.

MARCO CONCEPTUAL

1. Concepto de Ciberseguridad

La **ciberseguridad** se refiere a cualquier tecnología, práctica o política destinada a prevenir los ataques cibernéticos y mitigar su impacto. Su objetivo es proteger los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra el *ransomware*, otros programas maliciosos, las estafas de *phishing*, el robo de datos y diversas amenazas cibernéticas (ENISA, 2020)

Tomando en cuenta la norma ISO/IEC 27032:2012, la ciberseguridad busca preservar la confidencialidad, integridad y disponibilidad de la información en el ciberespacio (ISO/IEC, 2012).

En el ámbito empresarial e institucional, la ciberseguridad no se limita a la implementación de programas o software de protección, sino que abarca la gestión integral de riesgos, la capacitación del personal, el manejo adecuado de datos y la adopción de políticas institucionales sólidas de seguridad.

2. Servicios Tercerizados

La tercerización, que en Colombia también se conoce como *outsourcing*, ha sido una práctica habitual en las compañías públicas y privadas durante muchos años. (Willcocks, Hindle, & Feeny, 2014). Si bien, teóricamente, implica la contratación de empresas externas para llevar a cabo tareas o procesos específicos, en la práctica ha suscitado debates debido a la delgada línea que separa la prestación de servicios de una relación laboral directa. *(Johan García Blandón, El Colombiano, 2025).*

El *outsourcing*, también llamado tercerización, se refiere a la contratación de un proveedor externo para ejecutar determinadas tareas que, en principio, eran responsabilidad de la empresa. En el ámbito tecnológico, estos servicios incluyen el desarrollo de software, la asistencia técnica, el mantenimiento de servidores, entre otras actividades (Willcocks, Hindle, & Feeny, 2014).

Es importante tener en cuenta que la tercerización ofrece beneficios significativos en términos de reducción de costos y mejora de la eficiencia; sin embargo, también implica riesgos asociados con el manejo de información sensible por parte de los terceros contratados. Por esta razón, las organizaciones deben establecer controles claros y efectivos que garanticen la seguridad de los datos transferidos o procesados por los proveedores.

3. Riesgos Asociados a la Tercerización de Servicios

Al tercerizar servicios, las empresas pueden enfrentarse a diversos riesgos operativos, financieros y de gestión que afectan tanto su rendimiento como su seguridad. Algunos de los más comunes son:

- Pérdida de control del servicio.
- Concentración excesiva de servicios tercerizados en un solo proveedor.
- Costos mayores a los previstos o proyectados.
- Calidad inferior a la acordada, lo que puede generar insatisfacción entre el personal interno.
- Conflictos internos dentro de la organización.
- Errores en la elección del proveedor.
- Dependencia excesiva del proveedor y posibles conflictos contractuales.
- Pérdida del conocimiento interno sobre procesos críticos.
- Relaciones con terceros sin contratos formales, lo que incrementa la exposición a riesgos legales y de cumplimiento.

En el ámbito de la ciberseguridad, los riesgos se enfocan en la posibilidad de no alcanzar los objetivos de protección establecidos al contratar servicios externos especializados. (ENISA, 2020). Entre los principales se encuentran:

- **Pérdida de control sobre los datos:** al delegar funciones, la empresa pasa a depender de la infraestructura, políticas y prácticas de seguridad del proveedor.

- **Accesos no autorizados:** empleados del proveedor podrían tener acceso indebido a información confidencial o sensible.
- **Fallas en la disponibilidad del servicio:** interrupciones o caídas en los sistemas del proveedor pueden afectar la continuidad operativa de la organización contratante.
- **Incumplimiento normativo:** algunos proveedores podrían no cumplir con las leyes y estándares de protección de datos vigentes, exponiendo a la empresa a sanciones o pérdida de reputación.

En conjunto, estos riesgos evidencian la importancia de una evaluación rigurosa de los proveedores, la implementación de contratos con cláusulas de seguridad claras y la supervisión continua de los servicios tercerizados para garantizar la protección de la información institucional.

4. Relevancia de la administración de ciberseguridad en servicios tercerizados

La administración de la ciberseguridad en servicios subcontratados conlleva la implementación de controles, procedimientos y políticas que garanticen el cumplimiento por parte de los proveedores de estándares apropiados para proteger la información a su cargo. Entre los procesos esenciales se encuentran:

- **Valoración y análisis anticipados del proveedor**: Establecer su grado de madurez en términos de cumplimiento normativo y seguridad, conforme a los parámetros establecidos.
- **Formalización de contratos**: Incluir en los contratos auditorías periódicas, cláusulas de confidencialidad y responsabilidades conjuntas.

- **Supervisión y seguimiento**: Comprobar regularmente si se están cumpliendo los acuerdos de seguridad.

MARCO CONTEXTUAL

A continuación, se plasman algunas normas relacionadas con la ciberseguridad:

1. Normas Internacionales

ISO/IEC 27001:2022: norma internacional que establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Su propósito es proteger la información mediante la gestión de riesgos (ISO/IEC, 2022).

ISO/IEC 27036: guía sobre la gestión de la seguridad en relaciones con proveedores (ISO/IEC, 2013a; ISO/IEC, 2013b).

NIST SP 800-171: lineamientos del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos para proteger información sensible en servicios contratados

GDPR (Reglamento General de Protección de Datos): establece obligaciones de ciberseguridad y protección de datos para proveedores y encargados del tratamiento en la Unión Europea (NIST, 2018).

2. Legislación Colombiana

En cuanto a las leyes y normas establecidas en Colombia, relacionamos las siguientes:

Ley 1581 de 2012 regula la protección de datos personales y establece que las organizaciones deben garantizar el uso responsable y seguro de la información (Congreso de la República de Colombia, 2012).

3. Otras normas relevantes existentes que incluyen:

Decreto 1377 de 2013: reglamenta aspectos de la Ley 1581 relacionados con la autorización del tratamiento de datos (Congreso de la República de Colombia, 2012).

Ley 1266 de 2008: protege la información financiera y crediticia (Congreso de la República de Colombia, 2008)

Ley 1273 de 2009: tipifica los delitos informáticos y protege los datos contenidos en sistemas informáticos (Congreso de la República de Colombia, 2009)

Política Nacional de Seguridad Digital (CONPES 3995 de 2020): promueve la gestión integral de riesgos en el entorno digital colombiano (Consejo Nacional de Política Económica y Social [CONPES], 2020).

PROPUESTA PRÁCTICA: MODELO DE GESTIÓN CIBERSEGURIDAD EN SERVICIOS TERCERIZADOS

1. Descripción general de la propuesta

La propuesta es un modelo de gestión de ciberseguridad práctico que posibilita a las entidades supervisar y controlar con eficacia los riesgos que se derivan al contratar servicios tecnológicos con terceros.

Este modelo se organiza en cuatro etapas fundamentales:

1. Valoración de los riesgos del proveedor.
2. Formalización del contrato con cláusulas de seguridad.
3. Supervisión constante de la ejecución.
4. Revisión y mejora constante.

El objetivo de este modelo es establecer un marco estructurado que fortalezca la relación entre las empresas y sus proveedores, asegurando que los dos cumplan con las regulaciones.

2. Fases del modelo

Fase 1: evaluación de riesgos

La administración de la ciberseguridad tiene que ser dinámica, y por eso se sugiere poner en marcha un ciclo de mejora constante (PHVA: Planear — Hacer — Verificar — Actuar), el cual facilite la actualización de las políticas de seguridad, así como de los contratos, dependiendo de los resultados alcanzados y de las transformaciones tecnológicas que puedan ocurrir (ISO/IEC 27001, 2022).

Acciones clave:

- Reconocer las amenazas vinculadas a la tercerización, entre ellas:
    - Accesos no autorizados y filtraciones de datos
    - Errores humanos o configuraciones inseguras.

    - Dependencia de la tecnología en exceso.
    - Incumplimiento de las normas y debilidades en la cadena de abastecimiento.
- Clasificar los servicios tercerizados según criticidad.

Instrumentos de apoyo:

- Matriz de valoración de riesgos
- Lista de verificación de cumplimiento normativo (ISO/IEC 27001 y Ley 1581 de 2012).
- Formato de control de incidentes.
- Indicadores de desempeño en ciberseguridad.

Fase 2: formalización contractual

Después de elegir al proveedor, se firma un contrato que incluya cláusulas de ciberseguridad conforme a la ley y a los estándares internacionales, tales como:

- Obligaciones de confidencialidad.
- Responsabilidad frente a incidentes o brechas de seguridad.
- Permiso para auditorías o revisiones de cumplimiento.
- Protocolos de notificación ante ataques o pérdidas de información.

Aplicación de estrategias de mitigación:

- Implementación de cláusulas específicas de seguridad y confidencialidad.
- Alineación con ISO/IEC 27036 para la relación cliente-proveedor.

Fase 3: supervisión y control

Se implementan estrategias de mitigación a lo largo de la ejecución del contrato para garantizar que los riesgos detectados se gestionen de manera adecuada:

- Revisiones técnicas periódicas.
- Informes de cumplimiento del proveedor.
- Indicadores de rendimiento (KPIs) relacionados con la seguridad.

- Monitoreo de las vulnerabilidades identificadas.

Propósito: Asegurar que las amenazas detectadas en la Fase 1 permanezcan controladas, adaptando las acciones según los resultados obtenidos y las nuevas condiciones tecnológicas.

Fase 4: monitoreo y mejora permanente

La gestión de la ciberseguridad debe ser dinámica; por ello, se aplica un ciclo de mejora continua (PHVA: Planear — Ejecutar — Verificar — Actuar).

Medidas esenciales:

- Analizar los hallazgos obtenidos durante el monitoreo y control.
- Ajustar procedimientos, contratos y políticas según las nuevas amenazas identificadas.
- Capacitar al personal en nuevas herramientas y prácticas de ciberseguridad.

Efecto previsto: Garantizar una administración proactiva y flexible que reduzca los riesgos, proteja la información y fortalezca continuamente la relación con los proveedores.

Se recomienda instaurar el ciclo de mejora continua (PHVA: Planificar — Ejecutar — Verificar — Actuar) permitiendo actualizar las políticas de seguridad y los contratos según los resultados obtenidos y las modificaciones tecnológicas que puedan surgir.

Acciones clave:

- Analizar los resultados de monitoreo y control.
- Ajustar políticas, contratos y procedimientos según las amenazas emergentes.
- Capacitar al personal en nuevas prácticas y herramientas de ciberseguridad.

Instrumentos de apoyo

Se proponen los siguientes instrumentos de apoyo complementario:

- Matriz de evaluación de riesgos, que permite clasificar los servicios tercerizados según el nivel de criticidad

- Lista de verificación del cumplimiento normativo basado en las normas ISO/IEC 27001 y la ley 1581 del 2012
- Formatos de control de incidentes documento que registra y analiza los eventos de seguridad
- Indicadores de desempeño de ciberseguridad

RESULTADOS ESPERADOS

Al aplicar este modelo, las entidades podrán esperar:

- Reducir los niveles de fuga de la información recolectada y almacenada.
- Garantizar la continuidad y calidad de los servicios tercerizados ante incidentes y amenazas cibernéticas.
- Cumplir con la legislación colombiana en relación con el manejo y la protección de datos.
- Mejorar la confianza entre los diferentes actores del proceso productivo, reflejándose en un manejo serio y confiable de la información y de los servicios tercerizados.

RECOMENDACIONES

- Es necesario capacitar periódicamente al personal en buenas prácticas de ciberseguridad.
- Es fundamental incluir auditorías externas independientes que evalúen continuamente el cumplimiento de las normas bajo estrictos parámetros acordados conjuntamente.
- Actualizar las políticas de seguridad digital conforme a las nuevas amenazas y de acuerdo con las tecnologías emergentes.
- Mantener una comunicación constante entre todos los actores del proceso y realizar revisiones periódicas de todo el proceso administrativo.

CONCLUSIONES

1. La ciberseguridad en servicios tercerizados representa un desafío fundamental para las organizaciones modernas, ya que implica la gestión compartida de riesgos entre la empresa y sus proveedores.

2. La falta de controles adecuados en la contratación y supervisión de terceros puede generar vulnerabilidades críticas que comprometen la información institucional sensible.

3. La aplicación de normas internacionales, como la ISO/IEC 27001 y la ISO/IEC 27036, junto con la legislación colombiana, proporciona herramientas fundamentales y constituye una base sólida para la implementación de políticas de seguridad efectivas (ISO/IEC, 2022; CONPES, 2020; Ley 1581, 2012).

4. El modelo de gestión propuesto permite establecer un enfoque sistemático para evaluar, contratar, monitorear y mejorar la seguridad en servicios tercerizados.

5. La adopción de este modelo fortalecerá la protección de los activos digitales y promoverá el cumplimiento de buenas prácticas en ciberseguridad.

REFERENCIAS

Referencias (APA 7ª edición)

CIS (Center for Internet Security). (2023). *CIS Controls v8: Cybersecurity best practices.* https://www.cisecurity.org

Congreso de la República de Colombia. (2008). Ley 1266 de 2008: Habeas Data. Diario Oficial No. 47.219.

Congreso de la República de Colombia. (2009). Ley 1273 de 2009: Delitos informáticos. Diario Oficial No. 47.223.

Consejo Nacional de Política Económica y Social (CONPES). (2020). *CONPES 3995: Política Nacional de Seguridad Digital*. Departamento Nacional de Planeación.

Deming, W. E. (1986). Out of the crisis. MIT Press.

ENISA. (2020). Guidelines on outsourcing IT services. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/guidelines-on-outsourcing-it-services

García-Blandón, J. (2025). Artículo sobre outsourcing y riesgos en Colombia. El Colombiano. Outsourcing (tercerización) en Colombia: ¿qué es y por qué cambia con la reforma laboral?

Gobierno de Colombia. (2013). *Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2022). Norma Técnica Colombiana NTC-ISO/IEC 27001:2022. Sistemas de gestión de seguridad de la información. ICONTEC.

International Organization for Standardization (ISO). (2014). ISO/IEC 27036-7: Information security for supplier relationships. ISO.

ISO/IEC. (2012). ISO/IEC 27032:2012 – Guidelines for cybersecurity. ISO.

ISO/IEC. (2013a). ISO/IEC 27001:2013 – Information Security Management Systems. ISO ISO/IEC. (2013b). ISO/IEC 27036:2013 – Information security for supplier relationships. ISO.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2020). Política Nacional de Seguridad Digital — CONPES 3995. https://www.mintic.gov.co

Ley 1581 de 2012. Protección de datos personales en Colombia. Diario Oficial No. 48.123.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

Willcocks, L., Hindle, J., & Feeny, D. (2014). Outsourcing and Information Technology. Palgrave Macmillan.