TRABAJO DE GRADO
Opción Seminario-Diplomado.

Título del trabajo

Ciberseguridad en Entornos de Outsourcing

Corporación Universitaria Remington.

Nombre de la facultad:
Ingeniería

Nombre del programa académico:
Ingeniería en sistema

Nombres de los estudiantes autores del trabajo de grado.
Jhon Alexis Palacios Mosquera

Nombre del Tutor del trabajo de grado (docente del seminario o diplomado).
Jorge Mauricio Sepúlveda Castaño

Opción de Trabajo de grado Seminario-Diplomado.
Año de presentación del trabajo de grado.
2025

Dedicatoria

Dedico este trabajo a mi familia y seres queridos, quienes con su apoyo incondicional me motivaron a continuar con mi formación académica.

Agradecimientos

Agradezco a mi docente y compañeros del diplomado, quienes contribuyeron con sus conocimientos y experiencias al desarrollo de este trabajo.

Tabla de Contenidos

Resumen

En este documento, se examina cómo muchas organizaciones actualmente optan por contratar a terceros para gestionar ciertas actividades, con el objetivo de reducir costos y aumentar su eficiencia. Esta práctica, denominada outsourcing, ofrece importantes ventajas, pero también introduce nuevos riesgos, particularmente en el ámbito de la ciberseguridad. Al compartir información sensible con proveedores externos, las empresas se exponen al mal uso de esos datos, accesos no autorizados o interrupciones en la continuidad del servicio. Esto implica que la protección de la información no solo depende de la empresa, sino también del compromiso y las prácticas de seguridad del proveedor. Este trabajo tiene como finalidad proporcionar una guía práctica para que las organizaciones identifiquen los principales riesgos de ciberseguridad asociados al outsourcing y tomen medidas para mitigar estos riesgos. Se analizarán ejemplos, buenas prácticas y herramientas simples que pueden ser implementadas en cualquier tipo de empresa, independientemente de su tamaño. Así, se busca no solo reforzar la seguridad tecnológica, sino también fomentar la confianza entre ambas partes, mejorando así los acuerdos que regulan la relación con los proveedores y asegurando la protección de la información a lo largo de todo el proceso.

Palabras clave

Ciberseguridad, Outsourcing, Protección de datos, Riesgos digitales, Confianza

Marco conceptual y contextual

El outsourcing es una práctica en la que las organizaciones deciden delegar ciertas actividades o procesos a un tercero, que previamente realizaban internamente. Esta estrategia tiene como propósito fundamental reducir costos, optimizar la eficiencia y permitir que las empresas se enfoquen en su misión principal. (Echaiz Moreno, D. (2008)). Se trata de un acuerdo en el que una parte confía a otra la realización de tareas que pueden abarcar desde la gestión tecnológica hasta la atención al cliente o la manipulación de datos. Sin embargo, este enfoque presenta nuevos desafíos en relación con la ciberseguridad, entendida como el conjunto de medidas destinadas a salvaguardar la información y los sistemas de potenciales amenazas, según Castellanos Rojas et al. (2020). La ciberseguridad implica proteger la información como se haría con cualquier activo valioso de una organización, como el capital financiero o los bienes físicos. La relación entre outsourcing y ciberseguridad es clara: al delegar procesos, la empresa comparte información sensible con un tercero, lo que significa que la protección de esos datos ya no es responsabilidad exclusiva de la organización contratante, sino que también depende del compromiso, los procedimientos y las prácticas del proveedor. Según Ospina y Barrio (2017), el ciberespacio carece de fronteras, lo que significa que los riesgos pueden surgir de cualquier lugar y afectar a cualquier organización conectada. Por lo tanto, la confianza y la transparencia en los acuerdos con los proveedores son tan esenciales como las herramientas tecnológicas empleadas. En este contexto, es crucial entender que los riesgos no desaparecen al buscar un tercero para estos servicios, sino que se transforman. La relación con el proveedor necesita un equilibrio entre aspectos técnicos y humanos, donde la transparencia, la comunicación constante y la corresponsabilidad son fundamentales para la seguridad. Mendívil Caldentey et al. (2022) resaltan la importancia del factor humano en la ciberseguridad, enfatizando que la capacitación y la sensibilización son necesarias no solo para los equipos técnicos, sino también para directivos, contratistas y todo el personal involucrado. En la actualidad, el outsourcing se ha consolidado como una práctica común en Colombia y América Latina, sobre todo en sectores como la banca, la salud, la educación y los servicios tecnológicos. De acuerdo con Caiza Narváez et al. (2022), la creciente digitalización de las

organizaciones ha aumentado su dependencia de terceros y, como consecuencia, su exposición a riesgos de seguridad. Las pequeñas y medianas empresas, en particular, tienden a ser más vulnerables, ya que a menudo carecen de políticas claras y recursos suficientes para gestionar adecuadamente la seguridad digital. Además, el Foro Económico Mundial (2021) ha identificado los ciberataques como uno de los principales riesgos globales actuales, lo que subraya la urgencia de fortalecer las prácticas de seguridad a todos los niveles. En países como Colombia, donde el outsourcing es percibido como una herramienta de competitividad y modernización, esto implica no solo la adopción de tecnología, sino también la creación de confianza y el establecimiento de acuerdos contractuales sólidos que incluyan la protección de datos y la continuidad del servicio. En resumen, abordar la ciberseguridad en entornos de outsourcing no se limita a implementar sistemas avanzados de protección, sino que implica reconocer la información como un recurso vital en la era digital, cuya protección requiere tanto medidas técnicas como relaciones basadas en confianza, claridad y responsabilidad compartida. Así, el outsourcing no debe ser considerado una amenaza en sí mismo, sino una oportunidad para forjar alianzas seguras y sostenibles en un mundo interconectado.

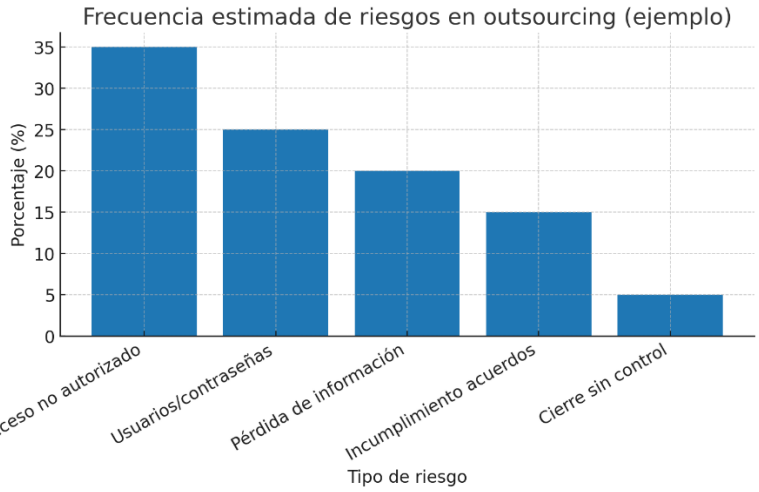
Título 1 Ciberseguridad en Entornos de Outsourcing

Sub-Título 1.1. Identificación de Riesgos de Ciberseguridad en Outsourcing

Desarrollo e implementación del aprendizaje

El desarrollo de este trabajo permitió aplicar los conocimientos adquiridos en el curso, centrándose en el análisis de la ciberseguridad en entornos de outsourcing. Este ejercicio buscó entender cómo las organizaciones, al delegar procesos y servicios a proveedores externos, enfrentan nuevos desafíos para la protección de su información y la continuidad de sus operaciones. Como resultado inicial, se identificaron los riesgos más comunes en este tipo de relaciones, que incluyen el acceso no autorizado a datos, la falta de claridad en la gestión de usuarios y contraseñas, la pérdida de información debido a errores humanos o fallas técnicas y, en algunos casos, el incumplimiento de los acuerdos de servicio. Estos hallazgos coinciden con lo señalado por Ospina y Barrio (2017), quienes advierten que el ciberespacio es un entorno abierto donde cualquier vulnerabilidad puede ser explotada para afectar a las organizaciones. En segundo lugar, se constató que la implementación de medidas sencillas puede tener un impacto significativo en la seguridad de los datos. Acciones como establecer acuerdos de confidencialidad, capacitar al personal, realizar copias de seguridad y definir accesos con autenticación de doble factor resultaron ser soluciones prácticas y efectivas, lo que reafirma lo planteado por Mendívil Caldentey et al. (2022) sobre la relevancia del factor humano y la conciencia en la ciberseguridad. Otro hallazgo importante fue el reconocimiento de que la seguridad no concluye con la firma de un contrato. Es esencial supervisar el cumplimiento de los acuerdos y mantener una comunicación constante con el proveedor, tal como sugieren estudios recientes sobre gestión de riesgos en entornos tercerizados (Borja & Pérez, 2019). De este modo, se promueve una relación basada en la confianza y la corresponsabilidad, que va más allá de lo puramente tecnológico. Finalmente, el aprendizaje aplicado reveló que la finalización de la relación contractual también es un momento crítico. Revocar accesos, eliminar cuentas, recuperar información y verificar el cumplimiento de lo acordado son pasos fundamentales para evitar que los datos queden expuestos. Este aspecto, a menudo pasado por alto por las organizaciones, se demostró crucial en la implementación práctica del proyecto. En conclusión, la experiencia desarrollada confirma que la ciberseguridad en entornos de outsourcing puede ser gestionada de manera efectiva al combinar la identificación

temprana de riesgos, la adopción de medidas preventivas y el fortalecimiento de las relaciones de confianza con los proveedores. Este aprendizaje, acompañado de la comparación, refuerza la idea de que la seguridad de la información no depende únicamente de la tecnología, sino de la integración de personas, procesos y acuerdos claros.



Figuras y tablas

Tabla 1. Riesgos identificados en entornos de outsourcing y medidas de seguridad propuestas

Riesgo identificado	*Medidas de seguridad propuestas*
Acceso no autorizado a datos	Establecer acuerdos de confidencialidad y aplicar controles estrictos de acceso. Santiago, E. J., & Allende, J. S. (2017).
Gestión inadecuada de usuarios y contraseñas	Implementar autenticación de doble factor y definir políticas claras de creación y manejo de claves. Amador Donado, S. (2022)
Perdida de información por errores o fallas técnicas	Realizar respaldos periódicos de la información y diseñar planes de recuperación ante cualquier incidente. Widup, S. (2021).
Incumplimiento de acuerdos de servicio	Monitorear de manera constante el cumplimiento de los SLA y solicitar reportes periódicos. Becerra-Ortiz, J. A. (2018).
Falta de control en el cierre de la relación contractual	Revocar accesos, eliminar cuentas de usuario y auditar el proceso de finalización del contrato. Perez, M. M. (2019

Conclusiones

A lo largo de este estudio, se ha comprendido que la ciberseguridad en entornos de outsourcing no es solo un tema técnico, sino una práctica integral que combina confianza, responsabilidad compartida y medidas preventivas claras. Al delegar procesos a terceros, las organizaciones no solamente transfieren tareas, sino también parte de la responsabilidad sobre su información. Por ello, es fundamental establecer acuerdos sólidos y relaciones basadas en la transparencia. El aprendizaje obtenido indica que la ciberseguridad en el outsourcing no debe ser vista como un obstáculo, sino como una oportunidad para fortalecer la competitividad y la confianza entre organizaciones y proveedores. Una gestión adecuada permite que incluso las pequeñas y medianas empresas, que suelen ser más vulnerables, protejan su información de manera efectiva y construyan relaciones más seguras en un mundo cada vez más interconectado. En conclusión, este proyecto ofrece una visión práctica y accesible de cómo las organizaciones pueden abordar los riesgos de la tercerización, demostrando que la seguridad de la información es alcanzable si se combinan medidas preventivas, formación continua y acuerdos claros que garanticen la responsabilidad compartida.

Referencias

1. Bassett, G., Hylender, D., Pinto, A., & Widup, S. (2021). Data Breach Investigations Report. https://www.researchgate.net/publication/351637233_2021_Verizon_Data_Breach_Investigations_Report

2. Becerra, G., Castorina, J. A., Becerra, G., & Castorina, J. A. (2023). Hacia un análisis de los marcos epistémicos del big data. Cinta de Moebio, 76, 50–63. https://doi.org/10.4067/S0717-554X2023000100050

3. Becerra-Ortiz, J. A., Cotino-Hueso, L., León, I. P., Sánchez-Acevedo, M. E., Torres-Ávila, J., Velandia-Vega, J. A., & Becerra-Ortiz, J. A. (2018). El big data en la ciberdefensa y la ciberseguridad nacional versus el derecho a la privacidad del ciudadano colombiano. https://hdl.handle.net/10983/22999

4. Borja, M. E., & Perez, M. M. (2019). Big Data: Un Analisis Documental de Su Uso y Aplicacion en el Contexto de la Era Digital. Revista La Propiedad Inmaterial, 28. https://heinonline.org/HOL/Page?handle=hein.journals/revpropin28&id=271&div=&collection=

5. Boyd, D., & Crawford, K. (2012). CRITICAL QUESTIONS FOR BIG DATA. Information, Communication & Society, 15(5), 662–679. https://doi.org/10.1080/1369118X.2012.678878

6. Caiza Narvaez, J., Márceles Villalba, K., Amador Donado, S., José Caiza Narváez, J., Márceles Villalba, K., & Amador Donado, S. (2022). Revisión sistemática para la construcción de una arquitectura con tecnologías emergentes IoT, técnicas de inteligencia artificial, monitoreo y almacenamiento de tráfico malicioso.