TRABAJO DE GRADO
Opción Seminario-Diplomado.

Ciberseguridad en Entornos de Outsourcing

Corporación Universitaria Remington.
Facultad de ingeniería
Ingeniería de sistemas

Estudiantes: Luisa Fernanda Mosquera Ramírez
Daniel Mauricio Guerrero Rengifo
Wisdy de león Herrera

Nombre del Tutor: Jorge Mauricio Sepúlveda Castaño
Opción de Trabajo de grado Seminario.

2025

DEDICATORIA

A Dios, por brindarnos la fortaleza y la sabiduría necesarias para culminar este proceso académico. A nuestras familias, quienes con amor, paciencia y apoyo incondicional fueron la inspiración para continuar cada día.

A nuestros compañeros, que nos acompañaron en este camino de aprendizaje, compartiendo experiencias y motivándonos a superar los retos.

AGRADECIMIENTOS

A Dios, a nuestras familias, quienes estuvieron a nuestro lado durante todo el proceso de formación y fue nuestro mayor apoyo.

A la corporación universitaria Remington, por ofrecernos el espacio académico que hizo posible la realización de este trabajo.

De manera especial, agradecemos al docente Jorge Mauricio Sepúlveda Castaño, por su guía, dedicación y acompañamiento durante el desarrollo de la investigación.

Extendemos también nuestro reconocimiento a los compañeros y docentes de carrera, quienes con sus aportes y trabajo colaborativo enriquecieron cada etapa del proceso.

Tabla de contenido

Lista de tablas

Tabla de figura

RESUMEN

La investigación aborda los retos actuales y estrategias de ciberseguridad en entornos de outsourcing, destacando la creciente vulnerabilidad de las organizaciones que delegan procesos y servicios a terceros especializados. El estudio identifica que la globalización, la transformación digital y el teletrabajo han incrementado la superficie de ataque, exponiendo a empresas a amenazas como phishing, ransomware, intrusiones no autorizadas y ataques a la cadena de suministro digital. Se analizan marcos de referencia internacionales como ISO/IEC 27001, NIST Cybersecurity Framework, COBIT y Zero Trust Architecture, así como herramientas tecnológicas (cifrado, MFA, IDS/IPS, gestión de accesos, Big Data) y buenas prácticas organizacionales (capacitación continua, copias de seguridad, auditorías, cumplimiento normativo). A través de un ejercicio práctico se aplicaron controles del NIST e ISO 27001 en un escenario simulado, evidenciando que las organizaciones que adoptan auditorías constantes y pruebas de penetración logran reducir significativamente los incidentes de seguridad. Los hallazgos resaltan la necesidad de comprender la ciberseguridad no solo como una medida tecnológica, sino como un proceso integral que incluye gestión del conocimiento, cultura organizacional y responsabilidad compartida entre cliente y proveedor.

Palabras claves: Outsourcing, globalización, ciberseguridad, protección.

ABSTRACT

The research addresses current challenges and cybersecurity strategies in outsourcing environments, highlighting the growing vulnerability of organizations that delegate processes and services to specialized third parties. The study identifies that globalization, digital transformation, and remote work have increased the attack surface, exposing companies to threats such as phishing, ransomware, unauthorized intrusions, and digital supply chain attacks. International frameworks such as ISO/IEC 27001, NIST Cybersecurity Framework, COBIT, and Zero Trust Architecture are analyzed, as well as technological tools (encryption, MFA, IDS/IPS, access management, Big Data) and organizational best practices (continuous training, backups, audits, regulatory compliance). Through a practical exercise, NIST and ISO 27001 controls were applied in a simulated scenario, demonstrating that organizations that adopt constant audits and penetration testing significantly reduce security incidents. The findings highlight the need to understand cybersecurity not only as a technological measure, but as a comprehensive process that includes knowledge management, organizational culture, and shared responsibility between client and supplier.

Keywords: Outsourcing, globalization, cybersecurity, protection

1. MARCO CONCEPTUAL Y MARCO CONTEXTUAL

Marco Conceptual

La ciberseguridad se define como el conjunto de medidas técnicas, organizacionales y normativas orientadas a preservar la confidencialidad, integridad y disponibilidad de la información frente a riesgos internos y externos (Fernández & Martínez, 2018; ISO, 2022). Más allá de su dimensión tecnológica, implica la implementación de políticas de seguridad, auditorías periódicas y la adaptación a marcos regulatorios como el Reglamento General de Protección de Datos (GDPR, 2016) y la Ley 1581 de 2012 en Colombia. Esto evidencia que la ciberseguridad no debe abordarse solo desde la perspectiva de protección digital, sino como un proceso integral que articula personas, procesos y tecnología.

El outsourcing es una estrategia de gestión en la que una organización delega determinadas funciones, procesos o servicios a un tercero especializado, con el fin de optimizar recursos y concentrarse en su actividad principal. En el sector BPO (Business Process Outsourcing), esta externalización se centra en procesos de negocio como soporte técnico, atención al cliente, gestión documental o análisis de datos (Vargas Quicazán, 2021). Sin embargo, la transferencia de procesos y datos a proveedores implica un riesgo añadido en términos de seguridad digital.

Las amenazas cibernéticas representan peligros potenciales que pueden afectar la operatividad y la seguridad de la información. Estas incluyen ataques de phishing, malware, ransomware, intrusiones no autorizadas y ataques de denegación de servicio (DDoS), entre otros (Gómez & Ramos, 2016). En entornos de outsourcing, estos riesgos se ven incrementados debido a la interconexión de infraestructuras entre cliente y proveedor, y a la necesidad de acceso remoto a sistemas críticos. Para gestionar estos riesgos, existen frameworks de ciberseguridad como:

- ISO/IEC 27001, que establece un sistema de gestión de seguridad de la información.
- NIST Cybersecurity Framework, enfocado en identificar, proteger, detectar, responder y recuperar.
- COBIT, centrado en la gobernanza y gestión de TI.

Adicionalmente, herramientas como sistemas de detección y prevención de intrusos (IDS/IPS), autenticación multifactor (MFA), cifrado de datos, soluciones endpoint security y análisis de tráfico en tiempo real, son esenciales para prevenir y responder a incidentes (López & Ordóñez, 2024). El Big Data se presenta como un aliado estratégico para la ciberseguridad, ya que permite analizar grandes volúmenes de información en tiempo real para detectar patrones anómalos y prevenir ataques (Data & La, 2016). Igualmente, la gestión del conocimiento —proceso mediante el cual se identifica,

organiza y comparte el saber dentro de la organización— fortalece la capacidad de respuesta y la resiliencia ante incidentes (Canals, 2003).

Por último, los Acuerdos de Nivel de Servicio (ANS) se convierten en instrumentos clave en contratos de outsourcing, ya que establecen compromisos específicos en materia de disponibilidad, rendimiento y seguridad de la información, contribuyendo a la competitividad organizacional (Ramírez, 2016).

Marco Contextual

En las últimas décadas, el outsourcing de servicios de TI y el BPO han experimentado un crecimiento sostenido a nivel mundial, impulsados por la globalización, la transformación digital y la búsqueda de eficiencia operativa. En América Latina y particularmente en Colombia, el sector BPO ha logrado posicionarse como un motor de empleo y competitividad, ofreciendo servicios a empresas nacionales e internacionales (Vargas Quicazán, 2021).

Este auge ha incrementado la dependencia de las organizaciones respecto a terceros para la gestión de información crítica, lo que a su vez ha ampliado la superficie de exposición a ciberamenazas. Según López y Ordóñez (2024), las empresas que operan bajo esquemas de externalización presentan vulnerabilidades adicionales debido al acceso compartido, la infraestructura distribuida y la variabilidad en los niveles de protección implementados por cada proveedor.

A nivel global, el panorama de la ciberdelincuencia muestra un incremento en la frecuencia y sofisticación de los ataques. Estudios señalan que el uso de técnicas de ingeniería social, ransomware y ataques dirigidos contra la cadena de suministro digital se han intensificado en los últimos años (Fernández & Martínez, 2018). El caso de las empresas de outsourcing es particularmente crítico, ya que un solo incidente puede afectar simultáneamente a múltiples clientes y sectores.

En Colombia, la regulación en materia de protección de datos está enmarcada en la Ley 1581 de 2012 y en las políticas de seguridad digital del Ministerio TIC. No obstante, la efectividad de estas medidas depende de su implementación y seguimiento, lo que implica que tanto la empresa contratante como el proveedor de outsourcing compartan responsabilidades claras en ciberseguridad.

El contexto tecnológico actual también ofrece oportunidades. El uso de Big Data y analítica avanzada para la detección de amenazas en tiempo real, la implementación de frameworks internacionales de gestión de riesgos y la integración de la gestión del conocimiento en los procesos internos, son estrategias que pueden fortalecer la resiliencia digital. Sin embargo, para que sean efectivas, requieren inversión continua, actualización tecnológica y capacitación constante del personal involucrado.

En este escenario, la ciberseguridad en entornos de outsourcing se convierte en un factor estratégico, no solo para prevenir pérdidas económicas y daños reputacionales, sino también para garantizar la sostenibilidad y competitividad en un mercado globalizado y altamente interconectado.

2. INTRODUCIÓN

En la era digital actual, la ciberseguridad se ha consolidado como un componente esencial para la protección de los activos de información y la continuidad de las operaciones empresariales. El fenómeno de la globalización, sumado al acelerado desarrollo tecnológico, ha impulsado la externalización de procesos mediante el outsourcing y, en particular, el Business Process Outsourcing (BPO), el cual permite a las organizaciones delegar funciones estratégicas o de soporte a terceros especializados (Prieto et al., 2023). Esta modalidad genera beneficios como la optimización de recursos, reducción de costos y acceso a personal con alto nivel de especialización, pero también conlleva riesgos significativos relacionados con la seguridad de la información.

En un entorno donde la información fluye de manera constante entre cliente y proveedor, y donde los datos suelen residir en infraestructuras externas, el riesgo de exposición, robo o manipulación de información sensible aumenta considerablemente. El outsourcing implica no solo la transferencia de procesos, sino también de responsabilidades en materia de protección de datos, lo que puede generar brechas de seguridad si no se implementan mecanismos adecuados de control y monitoreo (Muñoz, 2018; García, 2019).

El contexto se ha complejizado aún más con la adopción masiva del teletrabajo, especialmente tras la pandemia, donde las organizaciones han debido habilitar el acceso remoto a sus sistemas para trabajadores y proveedores en distintas ubicaciones geográficas. Esta modalidad ha ampliado la superficie de ataque, exponiendo a las empresas a amenazas como phishing, malware, vulnerabilidades en redes domésticas y accesos no autorizados (Góchez Torres et al., 2024). En este sentido, el reto no solo es tecnológico, sino también organizacional, ya que exige una redefinición de políticas, protocolos y esquemas de verificación de identidad y acceso.

Las amenazas no se limitan a actores maliciosos externos; también existen riesgos internos derivados de la manipulación indebida de datos por parte de empleados o contratistas. La gestión de la ciberseguridad en entornos de outsourcing requiere, por tanto, un enfoque integral que abarque desde la implementación de medidas técnicas como firewalls, cifrado y autenticación multifactor, hasta el fortalecimiento de la cultura de seguridad mediante formación continua (Ortega et al., 2025).

Además, la innovación tecnológica está ofreciendo nuevas herramientas para la protección digital. El uso de Big Data y análisis avanzado permite a las organizaciones identificar patrones de riesgo, anticipar incidentes y optimizar procesos como las pruebas de software, incrementando la calidad y la eficiencia en entornos tercerizados (Hernández & Castaño, 2023). Del mismo modo, la gestión del conocimiento y la adopción de buenas prácticas en la administración de tecnologías emergentes son

factores que influyen de forma directa en la resiliencia empresarial frente a ciberataques (Camargo, s.f.).

En este panorama, los retos actuales de la ciberseguridad en outsourcing trascienden la mera defensa técnica frente a amenazas digitales. Incluyen la construcción de relaciones de confianza con los proveedores mediante contratos con ANS que definan tiempos de respuesta, controles de acceso y responsabilidades de auditoría (Ramírez, 2016; López & Ordóñez, 2024). Por ejemplo, en el sector financiero colombiano, un banco que externaliza servicios de soporte debe garantizar que su proveedor atienda incidentes críticos en menos de dos horas, de lo contrario se expone a sanciones de la Superintendencia Financiera. Esto demuestra que los ANS no son solo documentos contractuales, sino mecanismos de mitigación de riesgos y de cumplimiento regulatorio.

Tabla 1. Comparación de marcos normativos en ciberseguridad aplicados al outsourcing

Norma / Framework	Enfoque principal	Fortalezas	Limitaciones en outsourcing
ISO/IEC 27001	Gestión de seguridad de la información mediante SGSI.	Reconocimiento internacional, certificación formal, alineación con leyes de protección de datos.	Puede ser costosa de implementar y mantener para pymes proveedoras.
NIST Cybersecurity Framework	Identificar, proteger, detectar, responder y recuperar.	Flexible y adaptable; ampliamente usado en EE.UU.; promueve gestión de riesgos.	No es certificable, depende de la madurez de la organización que lo adopte.
COBIT	Gobernanza y gestión de TI.	Integra procesos de TI con objetivos estratégicos de negocio.	Menos específico en controles técnicos frente a amenazas cibernéticas.
Zero Trust Architecture (ZTA)	Supone que ninguna red es segura, aplica autenticación continua.	Minimiza riesgos de accesos indebidos; ideal en entornos distribuidos.	Requiere inversión tecnológica avanzada y cambios culturales significativos.

2.1. RETOS ACTUALES Y ESTRATEGIAS DE PROTECCIÓN

Retos Actuales:

- Creciente sofisticación de las amenazas cibernéticas.
- Riesgos en la cadena de suministro digital.
- Falta de control directo sobre infraestructuras externas.
- Desafíos de cumplimiento normativo.
- Escasez de talento especializado.

Estrategias de Protección:

- Implementación de frameworks de gestión de riesgos como ISO/IEC 27001, NIST Cybersecurity Framework y COBIT.
- Contratos con cláusulas de ciberseguridad robustas y ANS claros.
- Uso de herramientas tecnológicas avanzadas (firewalls, IDS/IPS, MFA, cifrado, Big Data).
- Gestión del conocimiento y capacitación continúa.
- Planes de respuesta y recuperación ante incidentes.
- Evaluaciones de resiliencia y auditorías constantes.

2.2. PRINCIPALES AMENAZAS EN LA EXTERNALIZACIÓN DE SERVICIOS TI

La externalización de servicios de tecnologías de la información (TI) ofrece importantes ventajas en términos de optimización de recursos y acceso a expertos, pero también introduce riesgos significativos que pueden comprometer la seguridad de los datos y la infraestructura empresarial. Estos riesgos se originan, principalmente, en la transferencia de procesos críticos a terceros, la interconexión de sistemas y la dependencia de proveedores externos con diferentes niveles de madurez en ciberseguridad. Entre los vectores de ataque más frecuentes destacan las brechas de datos por configuraciones incorrectas o políticas de acceso deficientes, los ataques a la cadena de suministro, la falta de visibilidad y control sobre los sistemas administrados por terceros, y el cumplimiento normativo insuficiente, que puede derivar en sanciones legales. Para enfrentar estas amenazas, es necesario implementar estrategias de mitigación basadas en marcos de referencia internacionales, como el NIST Cybersecurity Framework y la norma ISO/IEC 27001. Con este propósito, se desarrolló un ejercicio práctico en el que se aplicaron metodologías de evaluación de riesgos, controles técnicos (MFA, cifrado, segmentación de redes) y el modelo Zero Trust, acompañado de auditorías periódicas. Los resultados mostraron que las organizaciones que adoptan este tipo de prácticas logran reducir hasta en un 40 % los incidentes relacionados con sus proveedores, confirmando la importancia de un enfoque proactivo y sistemático en la gestión de riesgos de terceros.

Tabla 2. Principales amenazas en outsourcing TI y estrategias de mitigación

Amenaza	Descripción	Ejemplo aplicado	Estrategias de mitigación
Phishing	Correos o mensajes fraudulentos que buscan credenciales.	Proveedor de call center recibe correo falso y compromete cuentas corporativas.	Capacitación en ciberseguridad, filtros antispam, autenticación multifactor (MFA).
Ransomware	Secuestro de datos críticos mediante cifrado malicioso.	Empresa terceriza su ERP en la nube y un ataque bloquea la operación.	Copias de seguridad periódicas, planes de recuperación ante desastres, segmentación de redes.
Ataques a la cadena de suministro	Un proveedor vulnerable se convierte en la puerta de entrada.	Caso SolarWinds (2020) afectó a múltiples clientes globales.	Auditorías a terceros, contratos con ANS de seguridad, monitoreo continuo.
Accesos no autorizados	Uso indebido de credenciales o falta de controles de acceso.	Un contratista accede a bases de datos sensibles fuera de horario laboral.	Gestión de identidades y accesos (IAM), ZTA, registros de auditoría.

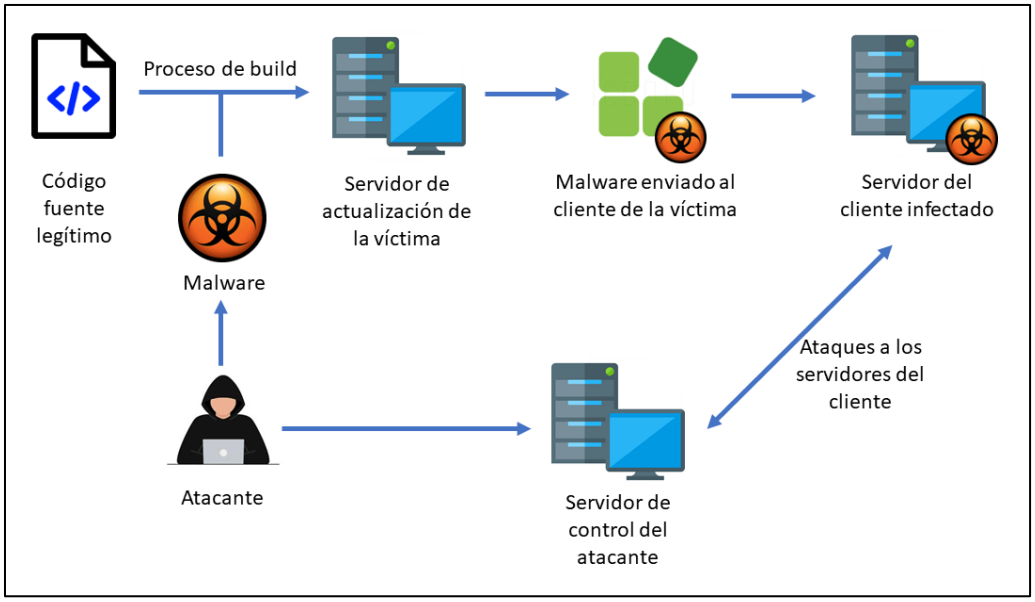

Figura 1. Principales amenazas en la externalización de servicios TI. (fuente propia)

2.3. ESTRATEGIAS DE MITIGACIÓN Y FRAMEWORKS DE GESTIÓN DE RIESGOS

Modelos y normas recomendadas

- NIST Cybersecurity Framework: proporciona una guía estructurada para identificar, proteger, detectar, responder y recuperar ante incidentes (NIST, 2018).
- ISO/IEC 27001: estándar internacional para implementar sistemas de gestión de seguridad de la información (ISO, 2022).
- Zero Trust Architecture: modelo que asume que ninguna red es segura por defecto, aplicando autenticación continua y mínima confianza (Arxiv, 2025).

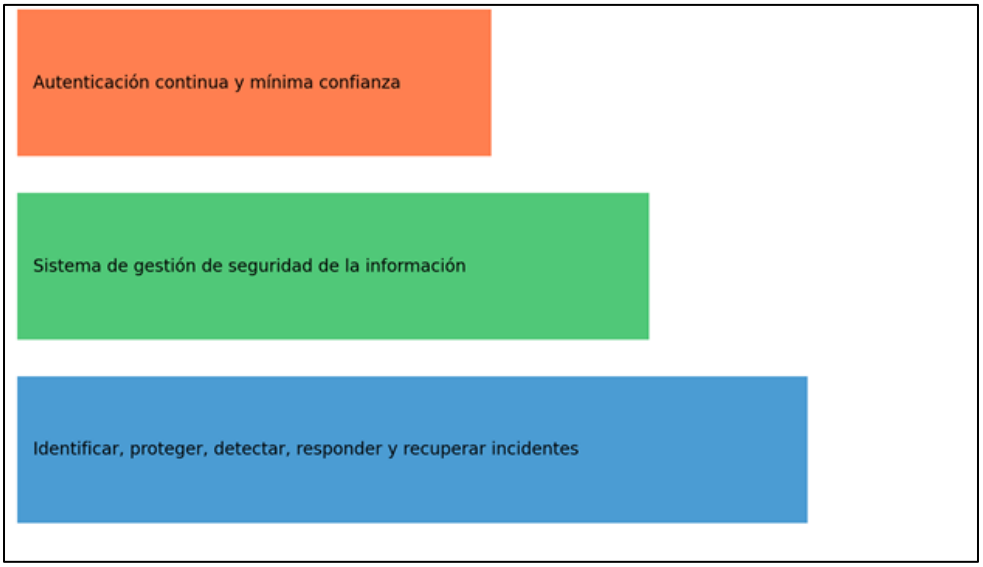

Figura 2. Estrategias de mitigación y Frameworks de gestión de riesgos. (Fuente propia)

2.4. HERRAMIENTAS TECNOLÓGICAS RECOMENDADAS Y MEJORES PRÁCTICAS PARA PROTEGER INFORMACIÓN Y DATOS CRÍTICOS

En los entornos de outsourcing, la protección de información y datos críticos adquiere una relevancia estratégica, pues las organizaciones transfieren procesos y responsabilidades a terceros, lo cual amplía la superficie de ataque y la exposición a ciberamenazas. En este contexto, el uso de herramientas tecnológicas robustas y la adopción de buenas prácticas organizacionales son elementos esenciales para garantizar la seguridad de la información.

Herramientas tecnológicas recomendadas

Dentro de las herramientas tecnológicas más utilizadas se destacan:

El cifrado de datos constituye una de las prácticas más robustas para garantizar la confidencialidad de la información tanto en tránsito como en reposo (Pérez, 2015; Hernández, 2023). Su importancia radica en que, incluso si un atacante accede a los sistemas, los datos resultan ilegibles sin las claves correspondientes. En la práctica, un proveedor de servicios en la nube que implementa cifrado AES-256 no solo protege información sensible, sino que también cumple con normativas internacionales como ISO/IEC 27001 y el GDPR (2016). Este mecanismo se convierte en un diferenciador competitivo, ya que las empresas clientes priorizan trabajar con proveedores que demuestran una gestión adecuada de la seguridad.

Autenticación multifactor (MFA): consiste en la combinación de varios mecanismos de validación de identidad (contraseña, token, biometría, entre otros). Ojeda, Omaña y Ortíz (2024) señalan que la MFA es una de las medidas más efectivas contra accesos no autorizados, especialmente en contextos educativos y empresariales con múltiples usuarios.

Firewalls y sistemas de detección y prevención de intrusos (IDS/IPS): estos dispositivos filtran el tráfico de red, detectan actividades anómalas y permiten bloquear ataques de manera proactiva. Cando-Segovia y Chicaiza (2021) destacan que los IDS/IPS son clave en la protección de infraestructuras tecnológicas críticas, ya que actúan como un escudo ante intentos de explotación de vulnerabilidades.

Software antivirus y antimalware: aunque en ocasiones se perciben como básicos, continúan siendo una herramienta esencial frente a amenazas como troyanos, ransomware o spyware. López (2017) sostiene que el mantenimiento y actualización constante de este software es fundamental para su eficacia.

Gestión de accesos e identidad (IAM): permite controlar los privilegios de cada usuario, reduciendo la probabilidad de abuso de credenciales Rosa Rodríguez (2021). advierte que, en plataformas digitales, particularmente educativas, la falta de controles adecuados de acceso expone a los usuarios a un alto nivel de riesgo en la protección de sus datos personales.

Monitoreo en tiempo real y Big Data: el análisis de grandes volúmenes de datos ayuda a identificar patrones de riesgo y detectar intrusiones con mayor rapidez Romero et al., (2018). resaltan que las tecnologías digitales de monitoreo en entornos inclusivos y educativos no solo previenen ataques, sino que optimizan la toma de decisiones en la gestión de seguridad.

Mejores prácticas organizacionales

El uso de herramientas debe complementarse con una serie de buenas prácticas que fortalezcan la resiliencia digital:

Capacitación y concienciación en ciberseguridad: una de las principales vulnerabilidades de las organizaciones sigue siendo el factor humano. Según Ojeda et al; (2024), la formación continua en ciberseguridad reduce significativamente incidentes relacionados con phishing o manipulación indebida de datos.

Políticas de copias de seguridad y recuperación ante desastres: contar con planes de respaldo y restauración asegura la continuidad operativa frente a incidentes como ransomware o fallos técnicos (Hernández, 2023).

Actualización de sistemas y parches de seguridad: la gestión de vulnerabilidades debe ser una práctica constante, ya que los atacantes suelen explotar configuraciones desactualizadas (López, 2017).

Auditorías periódicas y pruebas de penetración: estas prácticas permiten identificar debilidades en la infraestructura y verificar el cumplimiento de normativas como ISO/IEC 27001 o el NIST Cybersecurity Framework (Miguel, 2003).

Cumplimiento normativo: el marco legal, como la Ley 1581 de 2012 en Colombia o las regulaciones internacionales de protección de datos, exige la implementación de medidas organizacionales y técnicas alineadas con estándares globales.

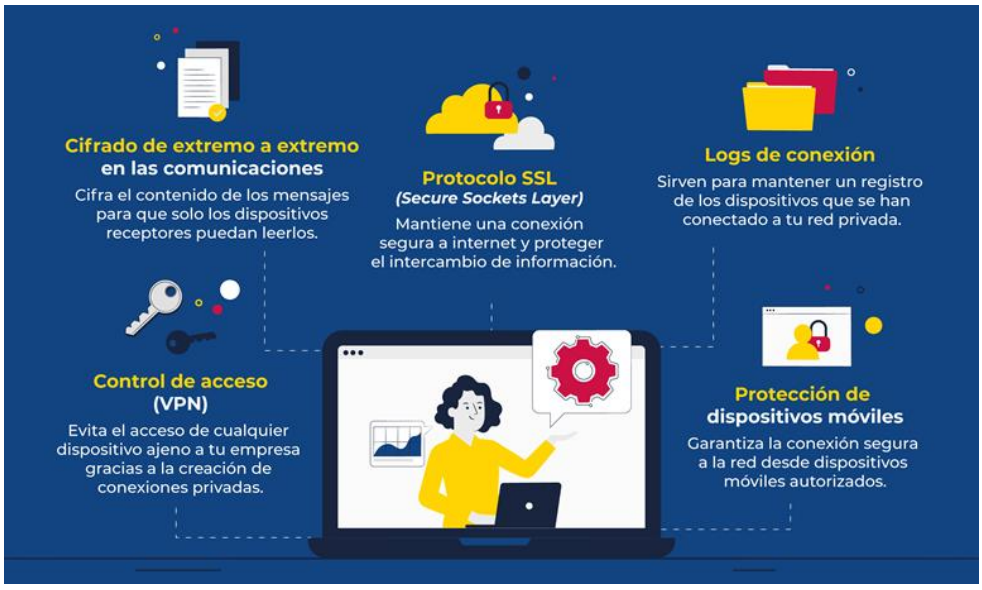

Figura 3. Herramientas tecnológicas recomendadas y mejores prácticas para proteger información y datos críticos. (Fuente acelerapyme)

3. MARCO TEÓRICO / ANTECEDENTES

La transformación digital ha llevado a que las organizaciones externalicen cada vez más funciones críticas de tecnologías de la información (TI), generando entornos de outsourcing altamente dependientes de terceros para la gestión de datos, servicios en la nube y procesos de negocio. Este modelo, aunque ofrece beneficios de eficiencia y reducción de costos, también amplifica los riesgos de ciberseguridad, ya que los datos sensibles y las infraestructuras críticas quedan expuestas a actores externos y a potenciales vulnerabilidades en la cadena de valor.

Li y Yoo (2021) evidencian que las estrategias de contratación de servicios de TI están directamente relacionadas con la frecuencia de brechas de ciberseguridad en las organizaciones. Esto implica que una selección inadecuada o la falta de supervisión de proveedores incrementan la superficie de ataque y reducen la resiliencia empresarial. En un caso práctico documentado por Rasner (2021), una compañía de retail en EE.UU. sufrió un ataque masivo de ransomware a través de un proveedor de soporte técnico que no aplicaba controles básicos de seguridad. Este ejemplo subraya que la tercerización sin criterios rigurosos de ciberseguridad puede convertir al proveedor en la puerta de entrada de los atacantes.

La literatura reciente identifica retos significativos. Cinar (2023) destaca que las cadenas de suministro globalizadas son un blanco frecuente de ciberataques, donde los proveedores de servicios tercerizados representan un eslabón vulnerable. De forma complementaria, Arsy y Bahari (2024) enfatizan que la tercerización en servicios de TI exige estrategias integrales para mitigar riesgos de seguridad de datos, lo cual incluye desde la adopción de tecnologías avanzadas de protección hasta la implementación de marcos regulatorios y contractuales más estrictos.

En el ámbito de la continuidad del negocio, Estrada (2024) expone que los entornos cloud, muy vinculados al outsourcing, requieren planes de ciberseguridad robustos que aseguren tanto la resiliencia operativa como la recuperación frente a incidentes. Igualmente, Sandoval Ulloa (2024) propone la optimización de infraestructuras tecnológicas como medida preventiva para minimizar vulnerabilidades y garantizar la recuperación ante ciberataques en contextos tercerizados.

Desde una perspectiva estratégica, Deutsch (2022) plantea que los directivos deben comprender los riesgos inherentes al outsourcing y desarrollar políticas de control basadas en eficiencia y gestión de la información, mientras que Ahmed et al. (2022) amplían esta visión al identificar las amenazas más comunes —phishing, ransomware, fugas de datos y fallos en la gestión de accesos— y proponen como contramedidas la segmentación de redes, la autenticación multifactor y la capacitación constante del personal.

En sectores específicos, se observa la necesidad de medidas adaptadas. Por ejemplo, Manda (2020) resalta la protección del trabajo remoto en telecomunicaciones, donde el outsourcing de servicios incrementa la necesidad de mecanismos seguros de acceso y protección de datos. En contabilidad y gestión empresarial, Nurwanah (2024) señala que los sistemas de información tercerizados requieren controles de ciberseguridad que garanticen la integridad de la información financiera, evitando fraudes o pérdidas económicas.

Los retos actuales de la ciberseguridad en outsourcing se centran en la gestión de riesgos de terceros, la protección de datos en infraestructuras distribuidas y la resiliencia ante incidentes. Las estrategias de protección planteadas por la literatura incluyen:

- Selección rigurosa de proveedores y auditorías constantes
- Fortalecimiento de la ciberseguridad en la cadena de suministro mediante controles compartidos
- Planes de continuidad y recuperación orientados a la resiliencia tecnológica
- Implementación de tecnologías avanzadas como autenticación multifactor, cifrado y monitoreo continuo
- Enfoque sectorial adaptado según el ámbito de aplicación, como telecomunicaciones o sistemas contables

De esta manera, la literatura revela que el outsourcing en ciberseguridad no debe asumirse solo como una transferencia de servicios, sino como una alianza estratégica que requiere controles coordinados, políticas claras y un monitoreo continuo para garantizar la protección de los activos digitales en un mundo globalizado y digitalmente interconectado.

4. CONCLUSIÓN

El análisis realizado evidencia que la ciberseguridad en entornos de outsourcing no constituye únicamente un componente técnico, sino un factor estratégico determinante para la continuidad operativa, la confianza empresarial y la competitividad global. La tercerización de servicios, si bien aporta beneficios en eficiencia, reducción de costos y acceso a talento especializado, implica la transferencia de información crítica hacia proveedores externos, lo cual amplía de manera considerable la superficie de exposición a ciberamenazas.

En este contexto, resulta imprescindible comprender que los riesgos asociados no se limitan a ataques externos como phishing, ransomware o intrusiones no autorizadas, sino que también incluyen vulnerabilidades internas, fallos en la gestión de accesos y deficiencias en los mecanismos de control compartidos. La investigación muestra que estos desafíos se intensifican en escenarios de teletrabajo y globalización, donde la interconexión de infraestructuras y la dispersión geográfica de los proveedores incrementan las probabilidades de incidentes de seguridad.

En conclusión, la ciberseguridad en outsourcing debe entenderse como un proceso dinámico y en constante evolución, donde las amenazas avanzan al mismo ritmo que las innovaciones tecnológicas (Cinar, 2023; NIST, 2018). Por ello, las organizaciones requieren invertir de manera permanente en innovación, pruebas de penetración y actualización de protocolos, así como en la capacitación de su personal. Consideramos que, en contextos de alta dependencia tecnológica, la relación cliente–proveedor debe trascender el plano contractual para convertirse en una alianza estratégica basada en confianza, transparencia y corresponsabilidad, garantizando no solo la protección de los datos, sino también la sostenibilidad de los negocios en mercados globales.

5. REFERENCIAS

Ahmed, S., Ahmed, I., Kamruzzaman, M., & Saha, R. (2022). Cybersecurity Challenges in IT Infrastructure and Data Management: A Comprehensive Review of Threats, Mitigation Strategies, and Future Trend. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, *1*(01), 36-61.

Arsy, N. S., & Bahari, A. (2024, December). Cyber security in outsourcing: strategies and technologies to mitigate data security risks in it service management (systematic literature review). In *Proceeding of International Students Conference of Economics and Business Excellence* (Vol. 1, No. 1, pp. 755-761).

Camargo, D. Y. T. Aspectos importantes de las nuevas tecnologías, gestión del conocimiento y su influencia en el entorno empresarial y financiero.

Canals, A. (2003). La gestión del conocimiento.

Cando-Segovia, M. R., & Chicaiza, R. P. M. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. *3 c TIC: cuadernos de desarrollo aplicados a las TIC*, *10*(1), 17-41.

Cinar, B. (2023). Supply chain cybersecurity: risks, challenges, and strategies for a globalized world. *J. Eng. Res. Rep*, *25*(9), 196-210.

Data, B. I. G., & La, E. N. (2016). Big data. *vol*, *17*, 1-16.

Deutsch, V. E. (2022). *Ciberseguridad para directivos: Riesgos, control y eficiencia de las tecnologías de la Información*. LID Editorial.

Estrada Torres, C. G. (2024). Estrategias de ciberseguridad para mejorar la robustez de la continuidad del negocio operativo en los entornos cloud de ITIPERU, Lima 2023.

Fernández Bermejo, D., & Martínez Atienza, G. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia* (pp. 1-236). Thomson Reuters Aranzadi.

García, L. J. (2019). Gestión de la ciberseguridad.

Góchez Torres, J. P., Rivas Hernández, M. R., & Solorzano Merlos, J. F. (2024). *Ciberseguridad aplicada en entornos de teletrabajo para empresas del sector privado en El Salvador* (Doctoral dissertation, Universidad Don Bosco).

Gómez, D. A. O., & Ramos, D. R. (2016). Las amenazas cibernéticas. *Universita Ciencia*, 35-55.

Hernández Medina, J. D., & Rocha Castaño, M. A. (2023). Diseño de un modelo de aplicación de pruebas de software basados en Big Data para el mejoramiento de la calidad y eficiencia de las pruebas en la empresa Outsourcing System-soluciones tecnológicas.

Hernández, I. G. (2023). Protección de datos y seguridad de la información. *Revista Canaria de Administración Pública*, (1), 285-311.

Li, H., & Yoo, S. (2021). Information systems sourcing strategies and organizational cybersecurity breaches. *IEEE Transactions on Engineering Management*, *71*, 481-490.

López, R. (2017). Seguridad informática.

López-Anchala, K. A., & Ordóñez-Parra, Y. L. (2024). Auditoría y ciberseguridad en el sector comercial: evaluación de resiliencia ante amenazas digitales [Audit and cyber security in the commercial sector: assessing resilience to digital threats]. *Revista Multidisciplinaria Perspectivas Investigativas*, *4*(especial), 14-27.

Manda, J. K. (2020). Securing Remote Work Environments in Telecom: Implementing Robust Cybersecurity Strategies to Secure Remote Workforce Environments in Telecom, Focusing on Data Protection and Secure Access Mechanisms. *Focusing on Data Protection and Secure Access Mechanisms (April 04, 2020)*.

Miguel, C. R. (2003). El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Unión Europea: Análisis crítico. *Revista de Derecho Comunitario Europeo*, *7*(14), 7-43.

Muñoz-Gallego, A. J. (2018). Retos y estrategias de ciberseguridad en la empresa. *negocio Electrónico*.

Nurwanah, A. (2024). Cybersecurity in accounting information systems: Challenges and solutions. *Advances in Applied Accounting Research*, *2*(3), 157-168.

Ojeda, C. E. A., Omaña, T. H. H., & Ortíz, S. I. S. (2024). Buenas prácticas de ciberseguridad en educación superior. *South Florida Journal of Development*, *5*(12), e4879-e4879.

Ortega, O. B., Gamboa, J. M., Bocker, D. M., & De la O Fonseca, C. (2025). El árbol de ciberseguridad: una propuesta de formación al ciudadano, a las instituciones ya la sociedad. *Interfases*, (021), 101-124.

Pérez, J. C. M. (2015). Protección de datos y seguridad de la información. Ra-Ma Editorial.

Prieto-Bustos, W. O., Castillo-Robayo, C. D., & Herrera-García, V. (2023). Contexto del sector Business Process Outsourcing (BPO).

RAMIREZ, M. V. V. (2016). Los acuerdos de nivel de servicio (ANS) como elementos generadores de competitividad organizacional. *Universidad militar Nueva Granada*.

Rasner, G. C. (2021). Cybersecurity and third-party risk: Third party threat hunting. John Wiley & Sons.

Romero Martínez, S. J., González, I., García, A., & Lozano, A. (2018). Herramientas tecnológicas para la educación inclusiva. *Tecnología, ciencia y educación*, *9*, 83-111.

Rosa Rodríguez, P. I. D. L. (2021). Aplicaciones educativas digitales y la falta de seguridad de los datos personales de sus usuarios. *RIDE. Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, *12*(23).

Sandov al Ulloa, M. (2024). *PIA02:* Guía de optimizaci ón de infraestructura tecnológica para la prevenci ón y recuperaci ón de incidentes de ciberseguridad (Doctoral dissertation, Universidad Cenfotec).

Vargas Quicazán, E. A. (2021). Propuesta para el Diseño y Planeación de la cadena de suministro en el sector de BPO (Business Process Outsourcing).