TRABAJO DE GRADO
Opción Seminario-Diplomado.

Informe Técnico

Gestión de ciberseguridad en servicios tercerizados (outsourcing) en entornos organizacionales

Corporación Universitaria Remington.
Facultad de Ingeniería
Programa Académico: Ingeniería de Sistemas

Tutor:
Jorge Mauricio Sepúlveda Castaño

Estudiantes:
Luis Miguel Blanco Soto

Jeferson Castañeda Restrepo

David Esteban Sánchez Morales

2026.

Dedicatoria

Aprovechamos este espacio para mencionar a aquellas personas que estuvieron con nosotros desde el comienzo y fueron un soporte importante durante este proceso. En primer lugar, este trabajo está dedicado a nuestras familias, quienes desde el inicio de la carrera nos brindaron apoyo constante, comprensión y motivación en los momentos más difíciles.

Gracias a la confianza, la compañía y las palabras de aliento que nos ofrecieron, fue posible continuar adelante y superar los retos que se presentaron a lo largo de nuestra formación académica y profesional. Su respaldo ha sido fundamental para no rendirnos cuando las dificultades parecían mayores que nuestras propias fuerzas.

También cabe resaltar que este trabajo no habría sido posible sin nosotros mismos, quienes coincidimos en este seminario y conformamos un grupo de trabajo que, con aprendizaje y esfuerzo compartido, logró intercambiar ideas, construir conocimiento y desarrollar un proyecto que hoy finalizamos con satisfacción.

Dedicamos igualmente este informe al docente, quien con sus enseñanzas y orientación ha contribuido a nuestro crecimiento en conocimientos y al desarrollo de habilidades personales durante este proceso. Cada explicación, lección y consejo aportado en los espacios académicos ha sido importante para la construcción de nuestro camino profesional y ético.

De igual manera, reconocemos que este logro no solo representa un esfuerzo mutuo, sino también el resultado del trabajo en equipo y de la confianza de las personas que han estado presentes durante esta etapa de nuestras vidas. Cada palabra de ánimo, cada consejo y cada gesto de apoyo fueron piezas fundamentales para mantener la motivación y continuar avanzando hacia este objetivo.

Finalmente, este trabajo simboliza el esfuerzo, la constancia y la dedicación invertidos durante todo el proceso de formación. Representa también la esperanza de seguir creciendo tanto en el ámbito académico como en el profesional, llevando con nosotros los mejores aprendizajes y valores adquiridos a lo largo de este camino.

Agradecimientos

Agradecemos a nuestras familias por el apoyo y la motivación que nos brindaron durante la realización de este trabajo, ya que su respaldo fue fundamental para avanzar y cumplir con este requisito de grado. También agradecemos a nuestro tutor por la orientación y el acompañamiento ofrecidos en cada etapa de la estructura y el desarrollo del informe.

Asimismo, queremos mencionar a la universidad por brindarnos los recursos y las herramientas necesarias para comprender el proceso de elaboración del informe técnico. Gracias a estos espacios de aprendizaje fue posible entender mejor la importancia de la investigación, el análisis y la organización de la información dentro del proceso académico.

Este trabajo también representa los aprendizajes adquiridos a lo largo de la formación académica, ya que en él se aplicaron conocimientos, habilidades y criterios desarrollados durante la carrera. Cada etapa del proceso permitió comprender la importancia de la disciplina, la responsabilidad y la dedicación en la elaboración de un trabajo técnico.

Finalmente, la realización de este informe no solo cumple con un requisito académico, sino que también refleja el esfuerzo y la constancia invertidos durante la carrera. Asimismo, representa una oportunidad para continuar fortaleciendo y proyectando las competencias profesionales y éticas adquiridas tanto en el ámbito personal como en el laboral.

Tabla de Contenidos

Resumen

El presente informe técnico analiza la gestión de la ciberseguridad en servicios tercerizados (outsourcing) dentro de entornos organizacionales. Actualmente, muchas empresas delegan procesos tecnológicos a proveedores externos con el fin de optimizar la eficiencia operativa, reducir costos y acceder a conocimientos especializados; sin embargo, esta práctica también implica riesgos asociados a la seguridad de la información.

A lo largo del documento se presentan los fundamentos conceptuales que sustentan el trabajo, incluyendo definiciones y referencias relacionadas con la seguridad de la información, la gestión de riesgos cibernéticos, los acuerdos de nivel de servicio (ANS), los indicadores clave de desempeño (KPI) y la normativa colombiana relacionada con la protección de datos personales. Este marco teórico permite comprender los principios que respaldan la propuesta y contextualizarla dentro del campo tecnológico.

Asimismo, se describe el proceso de desarrollo e implementación de una propuesta orientada al fortalecimiento de la ciberseguridad en servicios tercerizados, detallando las etapas del trabajo, las herramientas tecnológicas consideradas y los procedimientos aplicados para su estructuración. También se expone la lógica general del sistema, los componentes involucrados y la forma en que interactúan para cumplir con los objetivos planteados.

Durante el desarrollo del trabajo se aplicaron principios de organización, planificación y análisis técnico con el propósito de garantizar que la propuesta respondiera adecuadamente a los requerimientos establecidos. Este proceso incluyó la identificación de necesidades, el diseño de

una alternativa funcional y su planteamiento mediante el uso de herramientas tecnológicas apropiadas, buscando optimizar la gestión de la información y fortalecer la seguridad de los sistemas.

El informe también incorpora recursos visuales, como tablas, diagramas e imágenes, que facilitan la representación y comprensión de la información relacionada con el sistema propuesto. Finalmente, se presentan conclusiones derivadas del análisis y de la experiencia obtenida durante el proyecto y el seminario que proporcionó las pautas necesarias para el desarrollo del presente informe, permitiendo ampliar los conocimientos y resaltar la importancia de implementar políticas de seguridad, gestionar adecuadamente los riesgos y establecer controles técnicos y administrativos que minimicen vulnerabilidades en servicios tercerizados y protejan los activos digitales de las organizaciones.

En general, el trabajo evidencia la importancia de integrar conocimientos teóricos y habilidades prácticas para abordar problemas reales mediante soluciones tecnológicas, demostrando cómo el uso adecuado de herramientas y metodologías contribuye al desarrollo de proyectos eficientes y seguros en el ámbito académico y profesional.

3.1. Palabras clave

Ciberseguridad, outsourcing, seguridad de la información, gestión de riesgos y protección de datos.

3.2. Objetivos

Objetivo general

Analizar la gestión de la ciberseguridad en servicios tercerizados (outsourcing) dentro de entornos organizacionales, identificando los principales riesgos, controles y buenas prácticas que permitan proteger los activos digitales y garantizar la seguridad de la información.

Objetivos específicos

• Identificar los principales riesgos cibernéticos asociados a la tercerización de servicios tecnológicos en las organizaciones.

• Describir las herramientas tecnológicas, marcos normativos y buenas prácticas utilizadas para la protección de la información en entornos de outsourcing.

• Proponer controles técnicos y administrativos que fortalezcan la gestión de la ciberseguridad en servicios tercerizados, alineados con la normativa colombiana vigente de protección de datos personales.

4. Marco conceptual y contextual

4.1. Ciberseguridad en las organizaciones

En la actualidad, la ciberseguridad se ha convertido en un elemento fundamental para el funcionamiento de las organizaciones debido al creciente uso de tecnologías digitales y a la dependencia de los sistemas informáticos para el desarrollo de las actividades empresariales. Las empresas manejan grandes volúmenes de información a través de plataformas tecnológicas, redes de comunicación y sistemas de almacenamiento digital, lo que incrementa la necesidad de proteger

dichos recursos frente a posibles amenazas cibernéticas (Microsoft, s. f.; Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-a).

La ciberseguridad puede definirse como el conjunto de estrategias, herramientas, políticas y prácticas destinadas a proteger los sistemas informáticos, las redes y la información digital frente a accesos no autorizados, ataques informáticos o daños que puedan afectar la confidencialidad, integridad y disponibilidad de los datos (Microsoft, s. f.; Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-a).

El aumento de ataques cibernéticos en los últimos años ha llevado a las organizaciones a fortalecer sus medidas de seguridad informática. Entre las amenazas más comunes se encuentran el malware, el phishing, los ataques de ransomware y las intrusiones en redes corporativas. Estas amenazas pueden generar pérdidas económicas, daño reputacional y filtración de información sensible si no se implementan mecanismos adecuados de protección (Microsoft, s. f.; Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-b).

Por lo tanto, las empresas deben implementar políticas de seguridad, sistemas de monitoreo y controles tecnológicos que permitan prevenir incidentes y responder de manera oportuna ante posibles vulnerabilidades dentro de sus infraestructuras tecnológicas (Microsoft, s. f.; Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-a).

4.2. Outsourcing en servicios tecnológicos

El outsourcing, también conocido como tercerización de servicios, es una estrategia organizacional mediante la cual una entidad delega determinadas funciones o procesos a proveedores externos especializados. En el ámbito tecnológico, esta práctica es frecuente debido a la complejidad de los sistemas informáticos y a la necesidad de contar con personal capacitado para su gestión (Microsoft, 2024; National Institute of Standards and Technology, 2023).

La tercerización de servicios tecnológicos puede facilitar el acceso a capacidades especializadas, así como a servicios gestionados por terceros para el soporte técnico, la administración de infraestructura y la seguridad de la información. Además, puede contribuir a la eficiencia operativa cuando existen controles y responsabilidades claramente definidos (Microsoft, 2024; National Institute of Standards and Technology, 2023).

Sin embargo, la implementación de modelos de outsourcing también implica riesgos relacionados con la seguridad de la información. Cuando una organización comparte datos con proveedores externos, aumenta su exposición a vulnerabilidades en el manejo de la información, accesos no autorizados o fallas en los controles de seguridad (Microsoft, 2024; National Institute of Standards and Technology, 2023).

Por esta razón, es fundamental que las organizaciones establezcan acuerdos claros con los proveedores externos, definan políticas de seguridad adecuadas y supervisen constantemente el

cumplimiento de los estándares de protección de la información (Microsoft, 2024; National Institute of Standards and Technology, 2023).

4.3. Seguridad de la red y la nube

La seguridad de la red y la nube en el outsourcing se refiere al conjunto de políticas, prácticas y tecnologías que implementan tanto la empresa contratante como el proveedor externo para proteger la infraestructura de red y los servicios en la nube frente a accesos no autorizados, ataques y pérdida de datos. En este contexto, se establecen acuerdos de seguridad, control de accesos, cifrado de la información, monitoreo constante, uso de firewalls y mecanismos de autenticación, con el fin de garantizar la confidencialidad, integridad y disponibilidad de los datos, incluso cuando estos son gestionados o almacenados por terceros (Microsoft, 2024; Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-a).

4.4. Arquitectura en seguridad informática

La arquitectura en seguridad informática, enfocada en empresas y entornos de outsourcing, es el diseño estructurado de políticas, controles, tecnologías y procesos que protegen los sistemas de información, tanto internos como aquellos gestionados por proveedores externos. Esta arquitectura define cómo se organizan y relacionan elementos como redes, aplicaciones, datos y accesos, incorporando mecanismos como autenticación, cifrado, segmentación de red y monitoreo continuo. En el contexto del outsourcing, también establece responsabilidades compartidas, estándares de seguridad y controles que garantizan la confidencialidad, integridad y disponibilidad

de la información, incluso cuando los servicios son operados por terceros (Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-a; OWASP Foundation, s. f.).

4.5. Seguridad de la información

La seguridad de la información es un componente esencial dentro de la gestión de la ciberseguridad en las organizaciones. Su objetivo principal es proteger los datos y sistemas informáticos frente a posibles amenazas que puedan comprometer su funcionamiento o afectar la confidencialidad de la información (Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-a; OWASP Foundation, s. f.).

La seguridad de la información se basa en la implementación de políticas, procedimientos y controles tecnológicos diseñados para garantizar la protección de los activos digitales de una organización. Estos controles pueden incluir mecanismos de autenticación, cifrado de datos, monitoreo de redes, sistemas de respaldo de información y políticas de acceso a los sistemas informáticos (Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-b).

La protección de la información debe ser considerada una responsabilidad estratégica dentro de las organizaciones, ya que la pérdida o alteración de datos puede generar consecuencias significativas en términos operativos, financieros y reputacionales (Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-b; OWASP Foundation, s. f.).

Por esta razón, las empresas deben adoptar una cultura organizacional orientada a la seguridad de la información, en la cual tanto los empleados como los proveedores externos comprendan la importancia de proteger los datos y aplicar buenas prácticas en el manejo de la

información digital (Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-b; OWASP Foundation, s. f.).

4.6. Tríada CIA en la seguridad de la información

Uno de los modelos conceptuales más utilizados en el campo de la seguridad informática es la tríada CIA, la cual establece tres principios fundamentales para la protección de la información: confidencialidad, integridad y disponibilidad (OWASP Foundation, s. f.; Wallarm, 2025).

Tabla 1

Tríada CIA

Principio	Descripción	Ejemplo
Confidencialidad	Garantiza que la información solo sea accesible por personas autorizadas.	Uso de contraseñas y cifrado.
Integridad	Asegura que los datos no sean modificados sin autorización.	Control de versiones.
Disponibilidad	Garantiza que la información esté accesible cuando se necesite.	Copias de seguridad y servidores estables.

Nota. Elaboración propia a partir de OWASP Foundation (s. f.) y Wallarm (2025).

La confidencialidad se refiere a la protección de la información frente a accesos no autorizados. Este principio busca garantizar que los datos solo puedan ser consultados o utilizados por personas que cuenten con los permisos correspondientes. Para lograrlo, se utilizan mecanismos como contraseñas seguras, cifrado de información y sistemas de autenticación (OWASP Foundation, s. f.; Wallarm, 2025).

La integridad se relaciona con la exactitud y consistencia de los datos. Este principio asegura que la información no sea modificada de manera indebida o sin autorización. Para proteger

la integridad de los datos se implementan controles como registros de auditoría, sistemas de control de versiones y validaciones de información (OWASP Foundation, s. f.; Wallarm, 2025).

Por último, la disponibilidad garantiza que los sistemas informáticos y la información se encuentren accesibles cuando los usuarios autorizados los necesiten. Para ello se implementan medidas como copias de seguridad, redundancia de sistemas y mantenimiento de la infraestructura tecnológica (OWASP Foundation, s. f.; Wallarm, 2025).

La aplicación adecuada de estos tres principios permite establecer una base sólida para la protección de la información dentro de las organizaciones (OWASP Foundation, s. f.; Wallarm, 2025).

Figura 1

Modelo de la tríada CIA en seguridad de la información

Nota. Adaptado de Wallarm (2025).

4.7. Gestión de riesgos cibernéticos

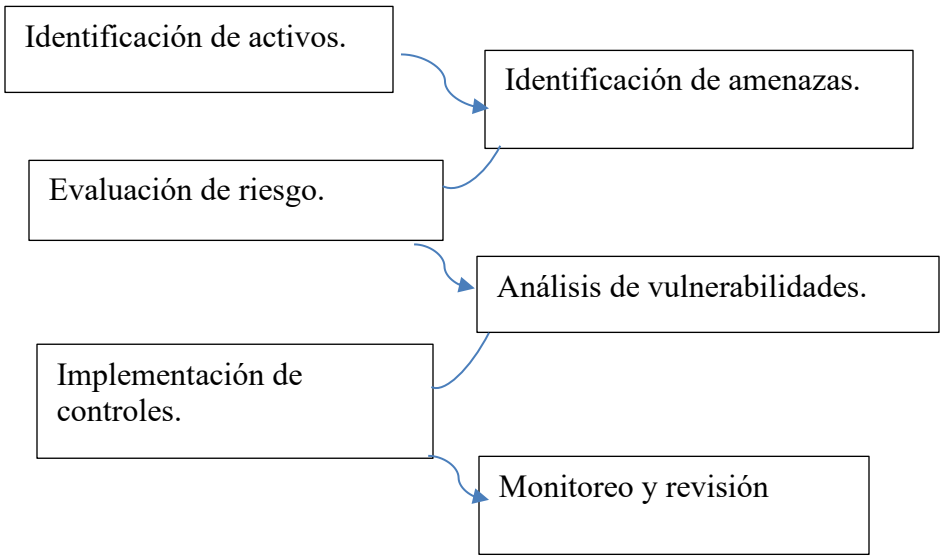

Figura 2
Diagrama de gestión de riesgos cibernéticos
Nota. Elaboración propia.

La gestión de riesgos cibernéticos es un proceso fundamental dentro de la ciberseguridad organizacional. Este proceso consiste en identificar, analizar y mitigar los posibles riesgos que puedan afectar los sistemas informáticos y la información digital de una organización (IBM, s. f.; Instituto Nacional de Ciberseguridad, s. f.).

La gestión de riesgos permite a las empresas anticiparse a posibles amenazas y establecer medidas preventivas para reducir el impacto de los incidentes de seguridad. Este proceso incluye etapas como la identificación de vulnerabilidades, el análisis del impacto potencial de los ataques

informáticos y la implementación de controles de seguridad adecuados (IBM, 2024; Instituto Nacional de Ciberseguridad, s. f.).

Entre las estrategias utilizadas para gestionar los riesgos cibernéticos se encuentran la implementación de políticas de seguridad, el monitoreo continuo de las redes, la capacitación del personal y la aplicación de herramientas tecnológicas de protección (IBM, s. f.; Instituto Nacional de Ciberseguridad, s. f.).

Una adecuada gestión de riesgos permite fortalecer la resiliencia organizacional frente a los ataques cibernéticos y mejorar la capacidad de respuesta ante incidentes de seguridad (IBM, 2024; IBM, s. f.; Instituto Nacional de Ciberseguridad, s. f.).

4.8. Normativa de protección de datos en Colombia

En el contexto colombiano, la protección de los datos personales se encuentra regulada por diferentes normas jurídicas que buscan garantizar el manejo adecuado de la información de los ciudadanos. Una de las principales disposiciones en este ámbito es la Ley 1581 de 2012, la cual establece reglas generales para la protección de datos personales (Congreso de la República de Colombia, 2012).

Esta normativa define los principios y obligaciones que deben cumplir las organizaciones públicas y privadas al momento de recolectar, almacenar o procesar información personal. Entre estos principios se destacan la legalidad, la finalidad, la seguridad y la confidencialidad en el

tratamiento de los datos (Congreso de la República de Colombia, 2012; Departamento Administrativo de la Función Pública, 2013).

El cumplimiento de estas regulaciones es especialmente importante en entornos de outsourcing, ya que las organizaciones pueden compartir información con proveedores externos. En estos casos, es necesario garantizar que los terceros también cumplan con las normas de protección de datos y adopten medidas adecuadas de seguridad para evitar la filtración o el uso indebido de la información (Congreso de la República de Colombia, 2012).

De manera complementaria, el marco normativo colombiano exige que las organizaciones asuman responsabilidades claras frente al tratamiento de la información personal y a la supervisión de los terceros que intervienen en dicho tratamiento, especialmente cuando existen servicios tecnológicos tercerizados (Departamento Administrativo de la Función Pública, 2013; Superintendencia de Industria y Comercio, 2020).

En consecuencia, la correcta gestión de la ciberseguridad en servicios tercerizados requiere la implementación de estrategias de seguridad, acuerdos de nivel de servicio claros y herramientas tecnológicas que permitan proteger la información y garantizar la continuidad de los servicios (Congreso de la República de Colombia, 2012; Superintendencia de Industria y Comercio, 2020).

5. Desarrollo e implementación

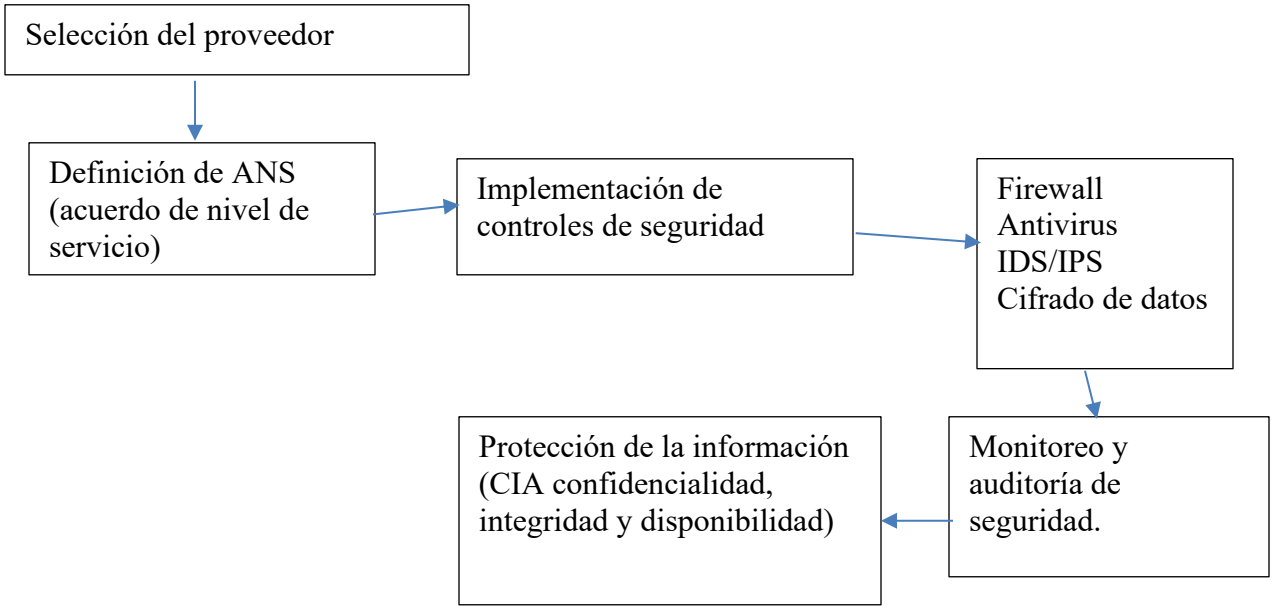

Figura 3

Demostración del flujo del sistema

Nota. Elaboración propia.

5.1. Implementación de la ciberseguridad en servicios tercerizados

La implementación de estrategias de ciberseguridad en servicios tercerizados se ha convertido en un aspecto fundamental para las organizaciones que delegan procesos tecnológicos a proveedores externos. En un entorno digital cada vez más interconectado, las empresas dependen de infraestructuras tecnológicas que requieren altos niveles de protección para evitar incidentes de seguridad que puedan comprometer la información y los sistemas informáticos (Microsoft, s. f.; National Institute of Standards and Technology, 2023).

Cuando una organización decide utilizar servicios de outsourcing, es necesario establecer mecanismos de control que permitan garantizar la seguridad de los datos compartidos con terceros. Estos mecanismos incluyen políticas de seguridad, protocolos de acceso a la información, sistemas de autenticación y medidas de monitoreo continuo de la infraestructura tecnológica (Microsoft, 2024; National Institute of Standards and Technology, 2023).

La implementación de controles adecuados permite reducir las vulnerabilidades asociadas a la tercerización de servicios tecnológicos y fortalece la protección de los activos digitales de las organizaciones. Asimismo, la adopción de políticas de seguridad claras facilita la definición de responsabilidades entre la organización y los proveedores externos (Microsoft, 2024; National Institute of Standards and Technology, 2023).

Por esta razón, la ciberseguridad debe ser considerada un componente estratégico dentro de la gestión organizacional, especialmente en aquellos entornos donde los servicios tecnológicos son administrados por terceros (Microsoft, s. f.; Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-a).

5.2. Gestión de riesgos en entornos de outsourcing

Tabla 2

Clasificación de riesgos

Riesgo	Impacto	Probabilidad	Medida de control
Acceso no autorizado	Alto	Medio	Autenticación multifactorial

Riesgo	Impacto	Probabilidad	Medida de control
Fuga de datos	Alto	Bajo	Cifrado de información
Ataque de malware	Medio	Alto	Antivirus y firewall
Error humano	Medio	Medio	Capacitación del personal

Nota. Elaboración propia con base en IBM (s. f.) e Instituto Nacional de Ciberseguridad (s. f.).

La gestión de riesgos cibernéticos es un proceso esencial dentro de la administración de servicios tecnológicos tercerizados. Este proceso permite identificar las amenazas potenciales que pueden afectar la seguridad de la información cuando las organizaciones comparten datos con proveedores externos (IBM, s. f.; National Institute of Standards and Technology, 2023).

El proceso de gestión de riesgos generalmente comienza con la identificación de posibles vulnerabilidades dentro de la infraestructura tecnológica. Estas vulnerabilidades pueden estar relacionadas con fallas en los sistemas informáticos, debilidades en los controles de acceso o errores humanos que faciliten la explotación de los sistemas por parte de atacantes (IBM, 2024; Instituto Nacional de Ciberseguridad, s. f.).

Posteriormente se realiza un análisis de riesgos que permite evaluar la probabilidad de que ocurra un incidente de seguridad y el impacto que este podría generar en la organización. Este análisis permite priorizar los riesgos más críticos y establecer estrategias de mitigación adecuadas para reducir su impacto (IBM, 2024; Instituto Nacional de Ciberseguridad, s. f.).

La implementación de procesos de evaluación continua permite mejorar la capacidad de las organizaciones para anticiparse a las amenazas y responder de manera oportuna ante posibles incidentes de seguridad (IBM, 2024; IBM, s. f.; Instituto Nacional de Ciberseguridad, s. f.).

En el contexto de los servicios tercerizados, la gestión de riesgos también implica evaluar el nivel de seguridad de los proveedores externos, verificar sus controles de protección de datos y garantizar que cumplan con los estándares establecidos por la organización (Microsoft, 2024; National Institute of Standards and Technology, 2023).

5.3. Herramientas tecnológicas para la protección de sistemas

Las organizaciones utilizan diversas herramientas tecnológicas para proteger sus sistemas informáticos frente a posibles amenazas cibernéticas. Estas herramientas permiten monitorear la infraestructura tecnológica, detectar ataques informáticos y prevenir accesos no autorizados a los sistemas (Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-b).

Entre las herramientas más utilizadas se encuentran los antivirus, los cuales permiten detectar y eliminar software malicioso que pueda comprometer el funcionamiento de los equipos informáticos. Asimismo, los firewalls cumplen un papel fundamental en la protección de las redes, ya que permiten controlar el tráfico de información y bloquear conexiones no autorizadas (Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-b).

Otra herramienta importante dentro de la seguridad informática son los sistemas de detección de intrusos (IDS), los cuales permiten identificar actividades sospechosas dentro de la

red. Estos sistemas analizan el tráfico de datos y generan alertas cuando detectan comportamientos que pueden indicar la presencia de un ataque informático (Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-b).

De manera complementaria, los sistemas de prevención de intrusos (IPS) permiten bloquear automáticamente ciertos tipos de ataques antes de que puedan afectar la infraestructura tecnológica de la organización. Estas herramientas trabajan de forma conjunta para fortalecer la seguridad de los sistemas y reducir las vulnerabilidades dentro de los entornos digitales (Fortinet, s. f.; Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-b).

5.4. Acuerdos de nivel de servicio (ANS) y KPI

Los acuerdos de nivel de servicio, conocidos como ANS, son documentos que establecen las condiciones y responsabilidades entre una organización y un proveedor externo que presta servicios tecnológicos. Estos acuerdos son fundamentales en entornos de outsourcing, ya que permiten definir con claridad los estándares de calidad, disponibilidad y seguridad que deben cumplir los proveedores (Amazon Web Services, s. f.).

Los ANS suelen incluir aspectos relacionados con la disponibilidad de los sistemas, los tiempos de respuesta ante incidentes, las políticas de seguridad de la información y los mecanismos de soporte técnico. De esta manera, las organizaciones pueden garantizar que los proveedores cumplan con los requisitos establecidos para la prestación de los servicios tecnológicos (Amazon Web Services, s. f.).

Por otra parte, los indicadores clave de desempeño (KPI) permiten medir el rendimiento y la eficiencia de los servicios tercerizados. Estos indicadores facilitan la evaluación del desempeño de los proveedores mediante el análisis de métricas relacionadas con la disponibilidad de los sistemas, la resolución de incidentes y el cumplimiento de los estándares de seguridad (Amazon Web Services, s. f.).

La implementación de ANS y KPI permite fortalecer la gestión de los servicios tercerizados y garantizar que los proveedores externos cumplan con las expectativas y requisitos de seguridad establecidos por las organizaciones (Amazon Web Services, s. f.; National Institute of Standards and Technology, 2023).

5.5. Monitoreo y auditoría de seguridad

El monitoreo continuo de los sistemas informáticos es una práctica fundamental para garantizar la seguridad de la infraestructura tecnológica en entornos de outsourcing. A través del monitoreo, las organizaciones pueden supervisar el funcionamiento de los sistemas, detectar actividades sospechosas y responder rápidamente ante posibles incidentes de seguridad (Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-a; Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-b).

Las herramientas de monitoreo permiten analizar el tráfico de red, registrar eventos de seguridad y generar alertas cuando se detectan comportamientos sospechosos dentro de los

sistemas informáticos. Estas herramientas son especialmente importantes en entornos donde muchos usuarios y proveedores externos tienen acceso a los sistemas de la organización (Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-b).

Además del monitoreo, las organizaciones deben realizar auditorías de seguridad periódicas con el fin de evaluar el cumplimiento de las políticas de seguridad y verificar que los proveedores externos estén aplicando las medidas de protección establecidas. Las auditorías permiten identificar posibles debilidades en la infraestructura tecnológica y proponer mejoras en los controles de seguridad (Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-a; Superintendencia de Industria y Comercio, 2020).

En términos generales, el monitoreo constante y la realización de auditorías periódicas contribuyen a fortalecer la capacidad de las organizaciones para prevenir incidentes de seguridad y garantizar la protección de la información digital (Ministerio de Tecnologías de la Información y las Comunicaciones, s. f.-a; Superintendencia de Industria y Comercio, 2020).

5.6. Buenas prácticas en la gestión de ciberseguridad

Para garantizar una adecuada gestión de la ciberseguridad en servicios tercerizados, las organizaciones deben adoptar una serie de buenas prácticas orientadas a la protección de la información y a la prevención de incidentes de seguridad antes y durante la implementación de servicios de outsourcing tecnológico (Instituto Nacional de Ciberseguridad, s. f.; OWASP Foundation, s. f.).

Entre estas prácticas se encuentran la implementación de políticas claras de seguridad de la información, la capacitación constante del personal en temas de ciberseguridad y la aplicación de controles de acceso adecuados a los sistemas informáticos, ya que el fortalecimiento de estos aspectos disminuye la vulnerabilidad. Además, es importante establecer mecanismos de monitoreo continuo y planes de respuesta ante incidentes que permitan actuar rápidamente en caso de detectar una amenaza (Instituto Nacional de Ciberseguridad, s. f.; OWASP Foundation, s. f.).

Otra buena práctica consiste en evaluar periódicamente el desempeño de los proveedores externos y verificar que cumplan con los estándares de seguridad establecidos por la organización. Esto incluye la revisión de los acuerdos de nivel de servicio, la realización de auditorías de seguridad y la evaluación de los controles de protección de datos implementados por los proveedores (Instituto Nacional de Ciberseguridad, s. f.; National Institute of Standards and Technology, 2023).

La aplicación de estas buenas prácticas permite fortalecer la postura de seguridad de las organizaciones y reducir los riesgos asociados a la tercerización de servicios tecnológicos (Instituto Nacional de Ciberseguridad, s. f.; OWASP Foundation, s. f.).

6. Conclusiones

El desarrollo del presente informe permitió analizar la gestión de la ciberseguridad en servicios tercerizados desde una perspectiva organizacional, técnica y normativa. A partir del marco conceptual y del desarrollo propuesto, se evidenció que la tercerización de servicios tecnológicos

puede aportar eficiencia operativa y acceso a capacidades especializadas, pero también incrementa la exposición a riesgos como accesos no autorizados, fuga de datos, malware y errores humanos.

Uno de los hallazgos más relevantes del trabajo fue confirmar que la protección de la información en entornos de outsourcing no depende de una única herramienta, sino de la integración de principios, controles y responsabilidades compartidas. En este sentido, la seguridad de la información, la tríada CIA, la gestión de riesgos cibernéticos y el cumplimiento de la normativa sobre datos personales constituyen una base esencial para orientar decisiones de seguridad y fortalecer la confianza en la operación de servicios tercerizados.

Asimismo, el análisis realizado permitió identificar que una gestión efectiva de la ciberseguridad requiere evaluar de forma continua a los proveedores externos, establecer acuerdos de nivel de servicio claros, definir indicadores de desempeño, aplicar controles de acceso, cifrado, monitoreo y auditoría, y promover la capacitación del personal. La combinación de estos elementos reduce vulnerabilidades y mejora la capacidad de prevención, detección y respuesta frente a incidentes de seguridad.

Desde el punto de vista académico y práctico, el informe también permitió consolidar habilidades de análisis, organización de la información y formulación de propuestas técnicas. El uso de tablas, diagramas y esquemas facilitó la representación del sistema planteado y contribuyó a explicar de manera más clara la relación entre riesgos, controles y buenas prácticas de ciberseguridad en entornos organizacionales.

En conclusión, la adecuada gestión de la ciberseguridad en servicios tercerizados debe asumirse como un componente estratégico de la gestión organizacional. Su fortalecimiento exige

una visión integral que combine políticas, herramientas tecnológicas, supervisión de terceros y cumplimiento normativo, con el fin de proteger los activos digitales, garantizar la continuidad de los servicios y disminuir la probabilidad de incidentes que afecten la información de las organizaciones.

7. Referencias

Amazon Web Services. (s. f.). *¿Qué es un acuerdo de nivel de servicio (SLA)?* https://aws.amazon.com/es/what-is/service-level-agreement/

Congreso de la República de Colombia. (2012). Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Departamento Administrativo de la Función Pública. (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=53646

Fortinet. (s. f.). *¿Qué es un sistema de prevención de intrusiones (IPS)?* https://www.fortinet.com/lat/resources/cyberglossary/intrusion-prevention-system

IBM. (2024, 9 de agosto). *¿Qué es una evaluación de riesgos de ciberseguridad?* https://www.ibm.com/es-es/think/topics/cybersecurity-risk-assessment

IBM. (s. f.). *¿Qué es la gestión de ciberriesgos?* https://www.ibm.com/es-es/think/topics/cyber-risk-management

Instituto Nacional de Ciberseguridad. (s. f.). *Gestión de riesgos: una guía de aproximación para el empresario.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

Microsoft. (2024). *Risk assessment guide for Microsoft Cloud.* https://learn.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide

Microsoft. (s. f.). *¿Qué es la ciberseguridad?* https://www.microsoft.com/es-es/security/business/security-101/what-is-cybersecurity

Ministerio de Tecnologías de la Información y las Comunicaciones. (s. f.-a). *Documento maestro de los lineamientos del Modelo de Seguridad y Privacidad de la Información.* https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401770_recurso_1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (s. f.-b). *Guía para la implementación de seguridad de la información en una Mipyme.* https://gobiernodigital.mintic.gov.co/692/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

National Institute of Standards and Technology. (2023). *Cybersecurity supply chain risk management practices for systems and organizations (NIST SP 800-161 Rev. 1, Update 1).* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf

OWASP Foundation. (s. f.). *Fundamentos de seguridad.* https://devguide.owasp.org/es/02-foundations/01-security-fundamentals/

Superintendencia de Industria y Comercio. (2020). *Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales.* https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf?trk=public_post_comment-text

Wallarm. (2025, 7 de abril). *Tríada de la CIA: definición y ejemplos*. https://lab.wallarm.com/what/definicion-de-la-triada-de-la-cia-ejemplos-de-confidencialidad-integridad-y-disponibilidad/?lang=es